UNIVERSITY OF GLOUCESTERSHIRE
at Cheltenham and Gloucester

Cyber-Risk Mitigation Strategies for German Manufacturing Medium-Sized Enterprises

A thesis submitted to the

University of Gloucestershire

in accordance with the requirements of the degree of

Doctor of Philosophy

in the School of Business, Computing and Social Sciences.

presented by candidate

Herbert Sedlmair

Submitted in March 2025

Supervisor: Dr. Dougie Yourston, Postgraduate Research Degrees Lead (PhD and DBA), and PhD Course Leader, Senior Lecturer

Abstract

The purpose of this study was to provide a new academic insight into cyber-risk mitigation (CRMi) strategies adopted in German-based manufacturing medium-sized enterprises. The main study adopted a constructivist approach, employing a descriptive qualitative method to conduct nine semi-structured interviews with executive managers in nine medium-sized enterprises. The main study was informed by an extensive systematic literature review that identified several research gaps, which were linked to the main theme of the project and the interview questions.

The study's first key finding highlighted the significant variation in cyber-risk preparedness amongst these German manufacturing medium-sized enterprises, including their CRMi and cyber-risk insurance (CRI) strategies. Their perception of the extent to which they were prepared for a cyberattack was influenced by resource constraints, external pressures, and challenges in integrating cybersecurity into their business activities; therefore, these operations tended to rely on reactive strategies. Although basic cybersecurity awareness was present, proactive and integrated CRMi strategies remained limited.

The second finding identified the increasing external pressure within their supply chain to become more CRMi and CRI compliant, with the need to gain certification and adopt more stringent cybersecurity measures. While some managers from medium-sized enterprises acknowledged the financial and operational benefits of CRI, others were deterred by associated high costs, unclear policies, and difficulties balancing transparency with data security.

The third finding emphasised these medium-sized enterprises' reliance on reactive measures despite increased dependence on technology, which introduces new vulnerabilities. These included human intervention, such as employee susceptibility to phishing attacks, which underscored the need for continuous training and integration of CRMi into business frameworks for resilience and growth in a digitised environment.

Finally, the relationship between CRMi and business success remained underexplored. These managers from medium-sized enterprises viewed CRMi as a cost rather than a strategic enabler, overlooking its potential to retain customer trust, prevent reputational damage, and foster innovation along with improving the business's competitive advantage.

This study made four key contributions. Firstly, the study highlighted the lack of academic research as to cybersecurity and risk mitigation, which can have a significant economic benefit for German manufacturing medium-sized enterprises, and has added to the current debate. Secondly, the study demonstrated how resource limitations and cost-benefit analysis can actively shape medium-sized enterprises cybersecurity investment decisions, emphasising intangible challenges like reputation loss and expanding the current academic focus beyond financial and operational risks. The third contribution of the study found current CRI strategies need to be devised to reflect the requirements of medium-sized enterprises, including being affordable, relevant, and aligned with their specific needs. Finally, this study created a dedicated CRMi framework to help medium-sized enterprises identify potential cyber-risks, implement proactive mitigation strategies, and sustain business success despite the challenges of ensuring budgetary and resource constraints are met while providing a positive return on security investment (ROSI).

Acknowledgement

In spirit, I deeply thank my parents for the virtues they instilled in me, the will to persevere, and ultimately, the strength to complete this work. I also extend my gratitude to my critics and doubters, whose challenges motivated me to keep fighting. A heartfelt thank you to my loved ones, whose unwavering support and belief in my abilities have been a constant source of strength. Their encouragement during my weak moments propelled me forward and made this achievement possible.

I am immensely grateful to my interview partners, without whom the significance of this work would not have been achievable. Through our virtual conversations, they provided sensitive, entrepreneurial insights into cyber-risk assessment and management, enriching my research and giving me confidence in my academic pursuits. Their diverse perspectives and willingness to share their expertise have been invaluable, shaping the depth and breadth of this study. It has been an honour to learn from such remarkable individuals.

On the academic side, I extend my sincere thanks to the University of Gloucestershire for giving me the opportunity to pursue this PhD. I am especially grateful to Dr. Dougie Yourston, whose guidance and experience as my supervisor kept my work moving forward and provided invaluable support. I also wish to thank Professor Kamal Bechkoum, the former academic director of the School of Business and Technology, for initially approving my research project. Working with and learning from you has been a privilege, and your professional expertise and encouragement have elevated my research to new heights. The knowledge and skills I have gained through this journey will undoubtedly benefit me in my future endeavours. Thank you for your support throughout this process.

DECLARATION

I herewith declare that the content of this thesis is my own work – except where noted and credited. I further declare that this PhD thesis was created in accordance with the guidelines and regulations of the University of Gloucestershire. I affirm that this thesis has not been submitted to any other educational institution in the United Kingdom or abroad or as part of any other academic award.

All views and opinions tendered in this PhD thesis are solely mine and not, in any way, those of the University of Gloucestershire.

Signed: Date: 30 March 2025

DOI: 10.46289/PLOZ9900

In the virtual realm, our identities are not just constructed; they are curated, shaped by the digital landscapes we inhabit. (The author)

Table of Contents

List of Figures ..... **XIII**

List of Tables ..... **XIV**

1 Chapter One Introduction **1**

1.1 Introduction 1

1.1.1 Problem statement 3

1.1.2 Aim of this study 3

1.1.3 Research objectives 3

1.1.4 Research motivation and background of the study 4

1.2 Definitions, trends and challenges 5

1.2.1 Definition of cyber-risks 5

1.2.2 Cyber-risk trends 5

1.2.3 Cyber-risks and challenges 6

1.2.4 Cybersecurity awareness 7

1.2.5 Cyber-risk mitigation 7

1.2.6 Cyber-risk insurance 9

1.3 Structure of the thesis 13

2 Chapter Two Literature Review **16**

2.1 Introduction 16

2.2 Systematic literature review 17

2.3 The systematic literature review protocol 17

2.4 Justification for conducting a systematic literature review 22

2.5 Definition of review scope and formulation of search string 25

2.6 Technical description of systematic literature search 26

2.7 Results, summaries, and sub-categorisation of the systematic literature review 29

2.8 Summary and overview of the publications 68

2.9 Analysis of publications within subcategories 71
2.9.1 Studies associated with subcategory “assessment tools” 72
2.9.2 Studies associated with subcategory: “challenges” 74
2.9.3 Studies associated with subcategory “cloud-based solutions” 77
2.9.4 Studies associated with subcategory “collective approach” 78
2.9.5 Studies associated with subcategory “training program” 79
2.9.6 Studies associated with subcategory “recommendations” 80
2.9.7 Studies associated with subcategory “risk assessment” 83
2.9.8 Studies associated with subcategory “cyber-risk insurance challenges” 84
2.9.9 Studies associated with subcategory “coverage” 85
2.9.10 Studies associated with subcategory “ransomware” 86
2.9.11 Studies associated with subcategory “innovation” 87
2.9.12 Linking subcategory summaries to research gaps and interview format 88
2.10 Summary of the literature review and the identified research gaps and informed research questions 88
3 Chapter Three Methodology 91
3.1 Introduction 91
3.2 Research philosophy 92
3.3 Research strategy 92
3.4 Ontology 93
3.5 Epistemology 93
3.6 Research design 94
3.7 Research participants 95
3.8 Research methods 100
3.9 Research approach 100
3.9.1 Deductive approach 100
3.9.2 Inductive approach 101
3.9.3 Quantitative approach 101

3.9.4 Qualitative approach 102
3.10 Data collection technique and development of the interview protocol 103
3.10.1 Outcome of the first interview 105
3.10.2 Outcome of the Pilot study 106
3.11 The fieldwork 108
3.12 The interview format 109
3.13 Content analysis 112
3.13.1 Qualitative content analysis according to Mayring 113
3.13.2 Description of approach intended in this study 114
3.13.3 The evolution of the research questions 114
3.13.4 Selecting material 115
3.13.5 Deciding on the nature of the content analysis 115
3.13.6 Determining the unit of analysis and coding 116
3.13.7 Contextualizing the information 116
3.13.8 Determining reliability of results 117
3.14 Analysis and coding of the data 117
3.14.1 Development of codes 117
3.14.2 The interview data coding strategy 123
3.15 The role of the researcher 124
3.16 Ethical issues 124
3.17 The validity of the study 126
3.17.1 Credibility 126
3.17.2 Transferability 126
3.17.3 Dependability 127
3.17.4 Confirmability 127
3.18 Methodological limitations 128
3.19 Summary of the Methodology Chapter 129
4 Chapter Four Findings 130

4.1 Introduction 130
4.2 The level of preparedness against cyber-risks within German medium-sized enterprises 130
4.3 The German medium-sized enterprises' cyber-risk mitigation strategies 134
4.4 The role of cyber-risk insurance within German manufacturing medium-sized enterprises and the risks covered by existing CRI-policies 142
4.5 Risk mitigation strategies adopted by medium-sized enterprises against cyber-risks 149
4.6 The relationship between specific risks and mitigation strategies within these German medium-sized enterprises 153
4.7 The medium-sized enterprise managers perception towards cyber-risk insurance 156
4.8 German medium-sized enterprises' preparedness against cybercrime risk and the attitudes towards balancing cyber-risk mitigation measures and business success 160
4.9 Summary of the Findings Chapter and key results addressing research gaps 163
4.9.1 Results relevant to research gap 1 - Limited research exists on the actual level of preparedness against cyber-risks, especially in the German manufacturing context. 164
4.9.2 Results relevant to research gap 2 - There is insufficient insight into the cyber-risk mitigation strategies currently adopted by German medium-sized enterprises. 165
4.9.3 Results relevant to research gap 3 - Limited understanding exists regarding the role of cyber-risk insurance within German medium-sized enterprises and what risks are effectively covered by existing insurance policies. 167
4.9.4 Results relevant to the topic cyber-risk mitigation and business success 168
5 Chapter Five Discussion 170
5.1 Introduction 170
5.2 The level of preparedness against cyber-risks 170
5.2.1 Adoption of cybersecurity strategies 170

5.2.2 The cyber-risk perception and preparedness 172
5.2.3 Resource constraints and outsourcing 174
5.2.4 Perception of cyber threats and risk vulnerability 177
5.2.5 Supply chain risk management 179
5.2.6 Summary on the level of preparedness against cyber-risks 181
5.3 Cyber-risk mitigation and cyber-risk insurance 182
5.3.1 Employee training and awareness as a risk mitigation strategy 182
5.3.2 Backup strategies and data recovery 185
5.3.3 Zero trust policies and authorisation control 187
5.3.4 Cloud-based solutions for cyber-risk mitigation 188
5.3.5 Dependence on external expertise 190
5.3.6 Cyber security compliance and certification 192
5.3.7 Adoption of cyber-risk insurance and emergency preparedness 194
5.3.8 Summary of the approaches and perspectives associated with cyber-risk mitigation and cyber-risk insurance 195
5.4 The relationship between specific risks and cyber-risk mitigation strategies 196
5.4.1 Proactive vs. reactive cyber-risk mitigation strategies 196
5.4.2 Identified potential cyber-risks and perceived vulnerabilities 198
5.4.3 Qualitative versus quantitative risk assessment 201
5.4.4 The cost-benefit analysis of cybersecurity investments 203
5.4.5 Summary as to relationships between specific risks and cyber-risk mitigation strategies 205
5.5 Medium-sized enterprise managers' perception of cyber-risk insurance and its role as a potential solution within cyber-risk mitigation strategies 206
5.5.1 Challenges in understanding cyber-risk insurance coverage 206
5.5.2 Cyber-risk insurance as part of a broader cybersecurity strategy 209
5.5.3 Summary of medium-sized enterprise managers' perceptions of cyber-risk insurance and its role in cyber-risk mitigation strategies 210

5.6 Medium-sized enterprises' preparedness against cybercrime risk and the managers' attitudes to cyber-risk mitigation measures and business success .. 211
5.6.1 Dependence on IT infrastructure and production automation 211
5.6.2 External pressures driving cyber-risk mitigation strategies 213
5.6.3 The role of cyber-risk mitigation in business success: direct and indirect contributions 215
5.6.4 Summary of medium-sized enterprises' preparedness against cybercrime risk and the managers' attitudes to cyber-risk mitigation measures and business success 217
5.7 Summary of the Discussion Chapter 217
6 Chapter Six Conclusions 221
6.1 Introduction 221
6.2 Aim of the research 221
6.3 Overview of the study 222
6.3.1 Theoretical foundation 222
6.3.2 Research gaps and empirical approach 224
6.4 Findings and conclusions 225
6.4.1 Conclusion related to research gap 1: Limited research exists on the actual level of preparedness against cyber-risks, especially in the German manufacturing context 225
6.4.2 Conclusion on results related to research gap 2: There is insufficient insight into the cyber-risk mitigation strategies currently adopted by German medium-sized enterprises 226
6.4.3 Conclusion on results relevant to research gap 3: Limited understanding exists regarding the role of cyber-risk insurance within German medium-sized enterprises and what risks are effectively covered by existing insurance policies 228
6.4.4 Conclusion to cyber-risk mitigation and business success 228
6.5 Conclusions in relation to the initial research questions 229

6.5.1 Conclusions related to research question 1: What are the risk mitigation strategies adopted in German manufacturing medium-sized enterprises to mitigate against a cyberattack? 229
6.5.2 Conclusions related to research question 2: What is the relationship between specific risk factors and risk mitigation strategies within medium-sized enterprises? 230
6.5.3 Conclusions related to research question 3: How do medium-sized enterprise managers consider cyber-risk insurance as a vital option within their risk mitigation strategies? 231
6.5.4 Emerging contribution as to German medium-sized enterprises preparedness against cybercrime risk and the managers' attitudes to cyber-risk mitigation strategies to attain intangible business success 231
6.5.5 Revisiting the research objectives 232
6.6 Contribution to knowledge 234
6.6.1 Contribution to academic knowledge 235
6.6.2 Contribution to professional knowledge 240
6.7 Cyber-risk mitigation framework for German manufacturing medium-sized enterprises 241
6.8 Overview of the proposal framework 242
6.9 Approach, concept and objectives of the CRMi framework 242
6.10 Technical specification 244
6.11 Base risk management pillar (Step 1- 3) 245
6.11.1 Medium-sized enterprise organisational context (Step 1) 245
6.11.2 Asset identification and evaluation (Step 2) 248
6.11.3 Threat Indicator of compromise (Step 3) 249
6.12 Cyber-risk mitigation pillar (Steps 4 to 6) 250
6.12.1 Cyber security awareness (Step 4) 250
6.12.2 Cyber-risk mitigation (Step 5) 251
6.12.3 Cyber-risk insurance (Step 6) 257

6.13 Operations success pillar (Steps 7 to 9) 258
6.13.1 Potential residual primary/secondary losses (Step 7) 259
6.13.2 Critical success factors and key performance indicators (Step 8) 260
6.13.3 Business success (Step 9) 262
6.14 Summary on the proposed cyber-risk mitigation framework 262
6.15 Limitations of this study 265
6.16 Areas of future research 266
6.17 Summary of the Conclusion Chapter 267
6.18 Personal reflection 272
References 274
Annex 1: Cover letter sent to selected medium-sized enterprises 299
Annex 2: Interview consent form 303
Annex 3: Interview guide 305
Annex 4: Transcripted interview (Example No. 5) 311
Annex 5: Ethical Considerations 349

List of Figures

Figure 2-1: Method applied for conducting the SLR (Brocke et al., 2009) 22
Figure 2-2 The development of publications analysed in detail 68
Figure 2-3: The development for main categories 69
Figure 2-4: Development of publications within subcategories 70
Figure 2-5: The distribution of subcategories 70
Figure 3-1: The format of the study (own presentation) 109
Figure 3-2: Qualitative content analysis 113
Figure 6-1: Outline of CRMi framework 243
Figure 6-2: Cyber Physical System 245

Figure 6-3: Generic Risk Management Process 246

List of Tables

Table 2-1: Criteria used to eliminate publications from the initial search results 27

Table 2-2: List of categories and assigned papers 28

Table 2-3: Search results category 2: Cyber-risk mitigation – costs and benefits 31

Table 2-4: Search results Category 3: cyber-risk awareness SME 35

Table 2-5: Search results category 4: Cyber-risks - specific problems for SMEs 43

Table 2-6: Search results category 5: Cyber-risk mitigation measures in SMEs 56

Table 2-7: Search results category 6: Cyber-risk insurance 64

Table 2-8: Distribution of subcategories across main categories 71

Table 3-1: SME classification (according to ABl. of the EU L 124/36 of 20.05.2003) 95

Table 3-2: Profile of the Participants 99

Table 3-3: The outcomes of testing the research protocol 107

Table 3-4: Analysis and coding of the data 122

Table 6-1: Organisational Context (Step 1) 248

Table 6-2: Asset identification and evaluation (Step 2) 249

Table 6-3: Threat Indicator of compromise (Step 3) 250

Table 6-4: Cyber Security Awareness (Step 4) 251

Table 6-5: Preventive cyber-risk mitigation techniques (Technical, Step 5) 253

Table 6-6: Preventive cyber-risk mitigation techniques (Directional, Step 5) 254

Table 6-7: Detective cyber-risk mitigation techniques (Step 5) 255

Table 6-8: Corrective cyber-risk mitigation techniques (Step 5) 257

Table 6-9: Cyber-risk mitigation through cyber-risk insurance (Step 6) 258

Table 6-10: CSF and KPI (Step 8) 261

Table 6-11: CRMi positively influencing KPIs (Step 8) 262

List of Acronyms and Abbreviations

Abbreviation	Definition	Abbreviation	Definition
AI	Artificial Intelligence	IEC	International Electrotechnical Commission
BCM	Business Continuity Management	IIoT	Industrial Internet of Things
BI	Business Interruption	IoT	Internet of Things
BMWi	Bundesministerium für Wirtschaft und Energie	IP	Internet Protocol
BSI	Bundesamt für Sicherheit in der Informationstechnik	IS	Internet Security
BYOD	Bring Your Own Device	ISA	Information Security Awareness
CIO	Chief Information Officer	ISF	Internet Security Forum
C-level	Chief Executives	ISO	International Organisation for Standardisation
COVID	Coronavirus Disease	IT	Information Technology
CPS	Cyber-Physical System	KPI	Key Performance Indicator
CRI	Cyber-Risk Insurance	KRI	Key Risk indicators
CRM	Cyber-Risk Management	KSF	Key Success Factor
CRMi	Cyber-Risk Mitigation	LMS	Literature Management Software
CS	Cyber security	MS	MicroSoft
CSA	Cyber Security Awareness	NIST	National Institute of Standards and Technology
CSF	Critical Success Factor	OP	Operating System
CSM	Cybersecurity Management	RM	Risk Management
CSR	Corporate Social Responsibility	ROI	Return on Investment
DDoS	Distributed Denial of Service	ROSI	Return on Security Investment
EDI	Electronic Data Interchange	RQ	Research Question
ERM	Enterprise Risk Management	SLR	Systematic Literature Review
ERP	Enterprise Resource Planning	SMB	Small and Medium Business

Abbreviation	Definition	Abbreviation	Definition
EU	European Union	SME	Small and Medium-sized Enterprise
GDPR	General Data Protection Regulation	TISAX	Trusted Information Security Assessment Exchange
IACS	Industrial Automation and Control Systems	UK	United Kingdom
ICS	Industrial Control System	US	United States
ICT	Information and Communications Technology	USA	United States of America
IEC	International Electrotechnical Commission	WIKI	Webbrowser software for a content management system

1 Chapter One

Introduction

1.1 Introduction

German small and medium enterprises (SMEs) are a major contributor to the German economy, with more than 99% of all businesses in this European country being SMEs, generating about 35% of the country's GDP and contributing almost 55% to the nation's net added value (BVMV, 2022). At the same time, these types of businesses have encountered a revolution with the emergence of technology, which led to what is known as the "new economy", spanning the period between 1996 to 2001, which marked the first significant digitisation of businesses in Germany. This first wave of digitalisation resulted in the introduction of websites, e-commerce, and electronic communication, which culminated in a series of innovation opportunities that could be realised at a relatively low cost and perceived limited risk. Since the advent of the new economy various iterations have emerged, such as "Industry 4.0". This new trend in digitalisation has prompted academic studies to explore the potential risks of these technological advancements, particularly for smaller or medium-sized operations (Astor et al., 2016).

While Chapter One and Chapter Two discuss SMEs generically, the empirical investigation presented in this thesis focuses specifically on medium-sized enterprises, as defined in Table 3-1 (derived from ABl. of the EU L 124/36). This definition reflects the composition of the interview sample, which, as explained in Chapter Three, section 3.11, comprised exclusively managers from medium-sized manufacturing enterprises; therefore, the aim and objectives of the research, as presented in sections 1.1.2 and 1.1.3, are also focused on medium-sized enterprises.

This emergence of questioning the potential risks associated with Industry 4.0 has led to governmental interest in technological developments, including from the German Federal Ministry of Economics and Energy (Bundesministerium für Wirtschaft und Energie, BMWi). The Ministry of Economics and Energy highlighted the need for further usage of technology to increase competitiveness, innovation, and digitisation in business, including SMEs, while ensuring that businesses do not become targets of cybercrime. A Bitkom survey conducted in

2022 further confirmed this BMWi initiative, finding that only 30% of participating SMEs with a staff size between 100 and 499 considered themselves leaders in digitisation (bitkom.org, 2022, p. 7). This stands in stark contrast to the 54% of larger organisations with more than 500 employees who expressed their perception of being digital leaders. However, the drive towards Industry 4.0 requires agility, together with international competitiveness, to be able to meet the challenges of a further fast-growing implementation of ICT (Bartsch et al., 2018).

Reflecting this need to become more competitive through adopting new technological solutions, SMEs have increased their dependence on digitalisation, making them more dependent on new technologies, infrastructures, or service providers (OECD, 2021). Consequently, these businesses, including SMEs, have become increasingly reliant on technology, making them more vulnerable to cyberattacks.

Adoption of cyber-risk security frameworks and standards is becoming increasingly necessary to address this issue. When digitally transforming the business, the primary areas to focus on are data security and privacy. The theft of sensitive digital data or espionage has affected 46 percent of German respondents, who stated that their company had been the victim of digital theft within the last year (Statista, 2024). This includes sensitive physical documents, samples, components, or even machines stolen from more than a fifth, or 22%, of industrial enterprises (Statista, 2024). A survey by Lee (2020) confirmed this, indicating a rise in reported security risks due to digitisation and increased technological interconnectivity. However, the paradox lies in the fact that companies heavily reliant on digitalisation, typically large businesses, tend to assert that their technological infrastructure is sufficiently robust in terms of security protocols and standards, while small businesses, often serving as suppliers to large corporations, tend to be less aware of potential cyberattacks (Bartsch et al., 2018).

For many SME businesses, cyber-risk security has now become a key area for organisational security management to deal with to ensure that the availability, integrity, and confidentiality of data is maintained (Ključnikov et al., 2019). Businesses are increasingly adopting various international standards, such as ISO/IEC 27001, to safeguard their information from potential cyberattacks. However, to meet the required standards there is a need for significant investment, but it can be cost-inhibiting for an SME to implement all the protocols. If this

standard is not followed, the business is potentially vulnerable to a cyberattack, which could lead to loss of production, business, and reputation.

1.1.1 Problem statement

The aforementioned evidence, along with the previous research by Bartsch et al. (2018), suggests that German SME businesses may not have implemented adequate cybersecurity protection. Part of the reason can be attributed to investment costs, lack of management awareness, expertise, or by the willingness to take a calculated risk. However, SMEs are increasingly being targeted, making them both the victims of directed attacks or being used as a vehicle to attack another larger business or governmental concern. At the same time, Bartsch et al. (2018) suggested that SMEs do not see themselves as a viable target, and many believe that mitigation strategies would be both overly technical and too costly to implement.

1.1.2 Aim of this study

Reflecting the above, this study intends to meet the following aim:

- To investigate the attitudes and strategies adopted by German medium-sized manufacturing managers in response to the growing cyber-risks due to advantaged attack methods driven by the increased usage of digitalisation.

Based on this aim, the study intends to research the perceptions and experiences of these medium-sized managers toward cyber-risk mitigation (CRMi) by exploring which frameworks, measures, and strategies have been effectively adopted.

1.1.3 Research objectives

The objectives of this study are:

- To critically identify from the current academic debate as to what CRMi strategies are adopted to manage potential cyber threats.
- To critically analyse from the findings generated from the German manufacturing medium-sized managers as to the strategies adopted to manage and mitigate against potential cyberattacks.

- To critically evaluate from the findings as to how German manufacturing medium-sized managers mitigate against potential cyberattacks.
- To provide a new critical academic insight into how German-based manufacturing medium-sized enterprises mitigate against potential cyberattacks.

1.1.4 Research motivation and background of the study

National and international competition, along with the increased digitalisation of society and the economy, has resulted in a proliferation of internet-based applications. This has led to businesses, including SMEs, needing to adopt digital technological solutions (Garzoni et al., 2020). At the same time, there has been a rise in high and low levels of severity of reported cybercrime incidents. As companies become more dependent on their digital infrastructure, they also become more vulnerable to cybercrime attacks. This dependency has led to ransom demands from cybercriminals, losing data and functionality of the digital infrastructure, but also losing reputation with clients, suppliers, and peers (Conteh & Royer, 2021). To address this, the European General Data Protection Regulation (GDPR) came into force in 2018. The directive required companies to be held fully responsible for implementing technical and organisational measures to protect third parties' data from being accessed by unauthorised individuals. While the GDPR sets out the standards for the appropriate handling of data, the Council of Europe's Budapest Convention focuses on cybercrime standards for storage of data, which could be used as evidence in cybercrime prosecutions. These two frameworks have provided the measures that need to be taken to prevent potential cybercrime activities occurring, which is a requirement for all companies, irrespective of their size, to implement (Wicki-Birchler, 2020). However, despite the importance of meeting these statutory requirements, the published research on CRMi, including cyber-risk insurance (CRI), is limited, particularly in terms of SME managers' strategies and experiences (Alahmari & Duncan, 2020; Zwilling, 2022). This is particularly relevant for the manufacturing sector, where supply chains are the primary focus of investigations into CRMi strategies (e.g., Manuj and Menzer, 2008).

1.2 Definitions, trends and challenges

Before presenting a critical review into the topic of cyber-risk, attacks and cyber security awareness in the next chapter, the literature review, this section will provide an overview and summary of these three themes.

1.2.1 Definition of cyber-risks

Cyber-risks can be defined as "operational risks to information and technology assets that have consequences affecting the confidentiality, availability, and/or integrity of information or information systems" (Cebula & Young, 2010, p. 1). Prominent cyber-risk events can include data breaches and cyberattacks, which have been increasingly more prevalent due to the reliance on technology in business (Allianz, 2021; Raina, 2023). Cyberattacks have become ranked in the World Economic Forum's Global Risk Report (2024) as one of the biggest potential challenges faced by businesses, including German SMEs. These cyberattacks can include ransomware, malware, and DDoS attacks. However, Cremer et al. (2022) identified the lack of reliable and up-to-date research into cyber-risks, concluding that this was the main hindrance for the development of effective risk management measures and strategies, including around the area of cyber-risk insurance. Reflecting this, Cremer et al. (2022) recommended further research into cyber-risks, particularly around the themes of risk awareness and business behaviour.

With a cyberattack the outcome can be a data breach, which can cause a detrimental loss to a business. Khan et al. (2021, p. 315) defined a data breach as being a "security incident in which sensitive, protected, or confidential data are copied, transmitted, viewed, stolen, or used by an unauthorised individual". Data breaches often involve a large amount of sensitive data, such as personal employee or customer information, being accessed by an unauthorized external party with often malicious motives (Goode et al., 2017).

1.2.2 Cyber-risk trends

With businesses increasingly becoming more reliant on digital solutions and following the Coronavirus (COVID-19) pandemic, the proliferation of remote working from home has seen this practice becoming normalized. This has led to the trend of employees now using their

personal devices at remote and workplace locations. This trend of personal unauthorised devices has led to business activities becoming potentially more vulnerable to cyberattacks, which has led to the business environment needing to be managed more carefully. This has resulted in the emergence of several major trends:

- Cybercrime-as-a-service: cyberattacks and breaches are increasingly being conducted with the evolution of cybercrime-as-a-service, where cyber mercenaries are hired to carry out sophisticated attacks and breaches (Paquet-Clouston & García, 2023).
- Cloud applications and third-party service providers: businesses are in the process of moving out their critical information and infrastructure to third parties mostly driven by cost and administrative reasons, they is also a significant increase in cyberattacks and breaches from third parties (Ouda et al., 2022).
- AI and predictive analytics are playing a major role in the future as the production of data can be processed more effectively with this technology; however, they require different environments to be used.

1.2.3 Cyber-risks and challenges

A report by Allianz Risk Barometer in 2023 indicated that cyber and business interruption is the biggest threat to the economy (Allianz, 2023). For Germany, 45% of those risks ranked were associated with a cyberattack, including the potential for causing an interruption to business activities. Interestingly, SMEs represented about half of Allianz's respondents, confirming the recognized importance of this threat for this size of business. However, post-COVID-19, many SMEs had to quickly digitalise their businesses, but the development of IT security and respective investments has not always kept pace (Allianz, 2023). Instead, SMEs have become increasingly vulnerable to cyberattacks, particularly in the following areas:

- the operational domain,
- technical domain and
- management domain (Hahn, 2016).

In explaining this, Hahn (2016) saw the operational domain as ensuring functional capability, while at the same time maintaining a high level of availability of the production facilities. The technical side was related to the risks and challenges based on the use of embedded systems and insecure network protocols. From a management perspective, the low level of user and

operator awareness, inadequate regulation of IT security in production, and long equipment lifecycles pose additional risks (Hahn, 2016).

1.2.4 Cybersecurity awareness

In Germany, there has been a rapid increase in cyberattacks regardless of the business size or sector (Adamos et al., 2023; Oxford Analytica, 2023). Cyberattacks have emerged to be a major threat to businesses, including SMEs, who may not have adequate IT skills and financial support to prevent a cyberthreat. The World Economic Forum (WEF) published a global risks perception survey amongst SMEs and concluded that “data fraud and theft” was ranked as global risk number four, followed by “cyberattacks” (Raina, 2023). In this report, the WEF contended that "cyber-risk awareness and preparation will help organisations [SMEs] balance the value of new technologies against the cyber-risk that comes with them" (Raina, 2023, n.p.). To address this form of risk, cybersecurity is a solution that provides an overarching barrier against this activity through the protection of technologies, processes, and controls. This also involves safeguarding current networks, programs, and devices from unauthorised access (IT Governance, 2023). One of the primary roles of cybersecurity awareness (CSA) is to safeguard the confidentiality and availability of information, as well as to maintain the integrity of data (Von Solms & Von Solms, 2018). This necessitates a business's awareness and the implementation of robust security measures and protocols (Kim, 2022). One such measure could be the implementation of a dedicated team that is regularly examined to ensure satisfactory results in cybersecurity awareness (Bada & Nurse, 2019). However, as mentioned previously, this can be problematic as SMEs, which are the focus of this study, tend to have limited financial resources and expertise.

1.2.5 Cyber-risk mitigation

In the contemporary digital landscape, cyber-risk mitigation (CRMi) has become a central pillar of organisational resilience. As part of a broader risk management framework, CRMi constitutes an integral aspect of organisational resilience by enhancing an organisation’s ability to anticipate, absorb, and recover from cyber-related disruptions (Carías et al., 2020). As the frequency and sophistication of cyber threats escalate, enterprises, including small and me-

dium-sized enterprises (SMEs), must prioritize structured and proactive approaches to address vulnerabilities, minimize damages, and ensure operational continuity (Lutkevitch, 2021).

Among these approaches, CRMi stands out as a systematic framework for reducing both the likelihood and impact of adverse cyber events. By employing well-coordinated strategies, CRMi enables organisations to build a more robust defence against evolving threats and reinforces their ability to maintain stability in the face of cyber incidents. These strategies integrate risk identification, assessment, and management practices aimed at achieving a robust security posture. Unlike measures that solely react to incidents, mitigation emphasizes anticipation and preparedness, enabling organisations to maintain functionality even under cyber duress (Dash et al., 2022; Kumar et al., 2021).

An essential aspect of CRMi is risk reduction, which involves implementing measures to decrease the potential loss associated with cyber events. This approach may also extend to actions that reduce the likelihood of risks occurring. For instance, employing multi-factor authentication or deploying advanced threat detection systems can significantly lower both the impact and probability of cyber threats (Kejwang, 2022). Complementing this, risk transfer strategies, such as cyber-risk insurance (CRI), provide organisations with mechanisms to allocate the financial burden of cyber-risks to external parties. By transferring potential losses, enterprises can mitigate financial exposure while focusing resources on prevention and response (Hubbard & Seiersen, 2023).

Key to CRMi is a structured methodology that begins with identifying and cataloguing potential threats. Assessing the likelihood and impact of these threats provides a foundation for prioritising resources and actions. Mitigation measures, such as implementing advanced cybersecurity technologies, rigorous policies, and response protocols, are then deployed to address these risks effectively (Zwilling, 2022). This process also requires continual monitoring and refinement to adapt to the dynamic nature of cyber threats.

As in the domain of cyberspace, the “positive” manifestation of risk is widely welcome, the focus is naturally on any devastating negative effects. This implies the implementation of a CRMi framework which undertakes to capture that negative uncertainty by de-risking, reducing, or mitigating the risk landscape. Consequently, once such actions are executed, a higher level of confidence to achieve envisaged goals should be established (Lee, 2021).

Cyber Physical Systems (CPS), particularly in manufacturing, underscore the importance of tailored mitigation strategies. These systems integrate hardware, software, and connectivity, which collectively expand the attack surface. For SMEs, effective mitigation in such contexts demands robust security architectures, real-time monitoring, and zero-trust principles to reduce vulnerabilities and maintain operational integrity (Jbair et al., 2022; Wang et al., 2024). This need is particularly pronounced for German manufacturing SMEs, which face unique challenges due to constrained resources and expertise. As a result, cost-effective CRMi strategies become vital for these organisations to address their specific constraints while maintaining resilience.

Focusing on high-priority assets, leveraging automated and scalable solutions, and aligning security investments with business objectives may allow SMEs to bolster resilience without disproportionate expenditures (Dutta et al., 2022; Pfister & Lehmann, 2023). Such measures could ensure that critical operations are protected while maintaining financial viability.

Further on, successful CRMi approaches can integrate seamlessly into the broader risk management framework of an organisation. While it requires clear accountability structures, adherence to regulatory standards, and continuous improvement mechanisms (Nunes, 2018), it equally could foster a culture of cybersecurity awareness and readiness, which equips employees at all levels to recognize and respond to threats effectively.

In summary, CRMi represents more than a defensive posture; it is a proactive strategy for ensuring long-term security and organisational resilience. Through the adoption of advanced technologies, predictive analytics, and strategic planning, enterprises can reduce vulnerabilities and enhance their capacity to navigate the evolving cyber landscape. These efforts not only protect assets but also fortify stakeholder trust, contributing to sustainable growth and operational excellence (Lutkevitch, 2021). As cyber threats evolve, the integration of emerging technologies, such as artificial intelligence and machine learning, will further strengthen predictive capabilities and reinforce defences.

1.2.6 Cyber-risk insurance

German manufacturing SMEs face escalating threats from cyberattacks, which pose significant risks to their operations, data integrity, and reputations. Unlike traditional risks, cyber-

risks are inherently unpredictable, interconnected, and capable of causing widespread disruption. In this vulnerable environment, cyber-risk insurance (CRI) has emerged as a potential solution, offering financial protection against these threats while incentivising best practices. However, uncertainties surrounding the availability and adequacy of CRI, along with significant limitations in coverage and accessibility, highlight the need for a cautious and nuanced approach.

Insurance has traditionally addressed three primary risk categories: damage to assets, business interruption, and third-party liability (Rejda & McNamara, 2017). In the context of cyber-risks, these principles have been extended to include incidents such as data breaches, ransomware attacks, and network failures. CRI policies designed specifically for cyber-risks offer tailored solutions that address both first-party and third-party liabilities. Such policies enable SMEs to recover from financial and operational setbacks, safeguarding their continuity and growth (Wrede et al., 2020). For manufacturing SMEs, this coverage is particularly vital, as cyberattacks can disrupt production lines, compromise procurement systems, and result in the theft of proprietary data. Third-party coverage provides liability protection for claims arising from breaches or failures that affect external stakeholders, such as customers and suppliers (EIOPA, 2019).

The increasing sophistication and frequency of cyberattacks have exposed the limitations of traditional cybersecurity measures, compelling organisations to consider CRI as part of a broader cyber-risk mitigation (CRMi) strategy. Ransomware, for example, has evolved to include double extortion tactics, where attackers demand payment not only to decrypt files but also to prevent the public release of sensitive data (Farao et al., 2020). The rise of Ransomware-as-a-Service (RaaS) has further exacerbated these risks by enabling attackers with minimal technical expertise to deploy sophisticated tools available on the Dark Web (Farao et al., 2020). Such attacks frequently target managed service providers, causing cascading effects that disrupt multiple dependent organisations. While CRI has the potential to alleviate the financial burden of ransom payments, legal costs, and operational disruptions, questions persist about the comprehensiveness of coverage, particularly in cases involving negligence or ambiguous policy exclusions.

Business email compromise (BEC) is another growing threat, particularly during the transition to hybrid work models. Attackers exploit unauthorised access to employee email accounts to impersonate users, facilitating fraudulent financial transactions and causing substantial data breaches (Marotta et al., 2017). While CRI policies often include provisions for fraud-related losses and forensic investigations, the extent of coverage varies widely across insurers, with limitations such as coverage caps and exclusions creating vulnerabilities for policyholders. Similarly, the prevalence of supply chain attacks highlights the interconnected nature of modern business operations, where attackers exploit dependencies among third-party vendors to compromise multiple organisations through a single point of failure. Despite the critical need for coverage in such scenarios, insurers face challenges in assessing and pricing these systemic risks, often resulting in narrowly defined or limited policy provisions.

As outlined above, the evolving nature of cyber threats presents significant difficulties for the insurance industry in providing comprehensive coverage. The lack of robust historical data, combined with the dynamic and unpredictable nature of cyber-risks, complicates underwriting processes. Many insurers have introduced stricter criteria, including the exclusion of nation-state attacks and requirements for policyholders to implement stringent cybersecurity standards. These developments raise concerns about the accessibility and affordability of CRI, particularly for smaller organisations that may lack the resources to fulfil these requirements. Additionally, the issue of non-affirmative or "silent" cyber coverage, where traditional insurance policies neither explicitly include nor exclude cyber-risks, creates further ambiguity and potential exposure. This emphasizes the need for insurers to expand affirmative policies that explicitly address cyber-related liabilities (Vieira et al., 2020).

Despite its potential advantages, the adoption of CRI faces several challenges. The complexity of underwriting, driven by the lack of standardised tools for risk modelling and accumulation control, hinders the development of reliable pricing models. Insurers struggle to evaluate correlated risks, where a single incident can trigger claims across multiple policies (Jain, 2022). This interconnected nature of cyber-risks, combined with the scarcity of actuarial data, often results in high premiums and limited policy options, deterring many SMEs from investing in CRI (Scheuermann, 2016). Furthermore, the integration of IoT technologies in manufacturing has introduced new dimensions of risk, as IoT devices are often designed with

functionality prioritised over security. Vulnerabilities in IoT architectures, combined with a lack of standardisation, increase the risk of breaches (Radanliev et al., 2018). CRI can mitigate these risks by covering losses linked to IoT vulnerabilities, though insurers must refine actuarial models and deepen their understanding of IoT ecosystems to offer comprehensive solutions (Aldasoro et al., 2022).

Beyond financial protection, insurers play a proactive role in strengthening the cyber resilience of SMEs. By offering their expertise in risk assessment, security benchmarking, and incident response planning, insurers contribute to improving cybersecurity practices within organisations. Linking policy conditions to recognised standards, such as ISO 27001 or NIST, incentivises SMEs to adopt best practices and align with insurer expectations (Allianz Risk Barometer, 2023). Pre- and post-incident services, including employee training, forensic investigations, and public relations support, position insurers as active partners in risk management (Jimenez-Sanchez, 2017).

In summary, CRI has the potential to emerge as an indispensable tool for organisations, particularly German manufacturing SMEs, in navigating the complexities of an increasingly digitalised world. By providing financial protection against cyber threats and incentivising best practices, CRI could contribute to safeguarding operations, data, and reputations. However, its limitations necessitate a cautious approach. Collaboration between organisations, insurers, and policymakers is regarded as essential to address challenges such as data availability, standardised risk assessment processes, and comprehensive coverage options. Rather than serving as a standalone solution, CRI is ought to be integrated into a broader CRMi strategy that includes technical defences, employee training, and incident response planning. As the threat landscape continues to evolve, the role of CRI could grow, but its effectiveness will depend on continued innovation within the insurance sector and proactive adoption of multi-layered cybersecurity strategies by organisations. However, in its current state, CRI could serve as a supplementary measure rather than a comprehensive solution, but it remains a critical component in enhancing organisational resilience and ensuring long-term success (Cremer et al., 2022).

1.3 Structure of the thesis

This introductory chapter, Chapter One, outlines the research background of the study, providing an overview of the cyber-risk landscape and its challenges in today's digital and AI-driven world. It also includes themes related to cyber security awareness, cyber-risk mitigation (CRMi), and cyber-risk insurance (CRI). Based on these themes, the chapter has presented the aim and the objectives of the study, which will be addressed throughout the research project.

Chapter Two will present the current academic debate in the form of a systematic literature review (SLR) that is specifically related to SMEs and the challenges, perceptions, and experiences as to CRMi and CRI. The chapter is focused on providing a comprehensive overview of the theoretical discussions surrounding these topics. This overview will present the current debate and identify any research gaps, which will inform the formulation of the research questions for this study. The SLR will highlight the importance of using cyber-risk assessment tools and the critical issue of implementing appropriate cyber-risk mitigation plans suitable for SMEs, particularly since this size of business has limited resources, personnel, expertise, financial backing, and cyber-secure systems.

Chapter Three will set out the methodology and approach adopted in the research project by using a qualitative interpretative strategy. The chapter will introduce the study's participants: managers from German manufacturing medium-sized enterprises who were willing to participate. The participants came from seven sectors of manufacturing: semiconductors, print technology, electronics, plant engineering, woodworking, metal processing, and confectionery. The chapter will set out the research strategy approach adopted, including the pilot study, which was then incorporated into the main study, the coding strategy of using a thematic analysis approach, along with setting out and acknowledging the limitations of adopting an interpretivist study and the ethical protocols followed.

Chapter Four presents the findings of this interpretivist study, generated from semi-structured interviews. The study included an initial pilot interview, which provided invaluable lessons to refine subsequent interviews. The main study comprised interviews with nine managers from German manufacturing medium-sized enterprises, all based in Germany. The sample was drawn from seven key sectors within manufacturing, as outlined in Chapter Three. The participants held positions as either executive directors or chief information officers. The findings were organised around themes identified during data analysis, revealing

seven key areas: medium-sized enterprises' CRMi strategies, the role and coverage of CRI policies, CRMi strategies for mitigating cyber-risks, the relationship between specific risks and CRMi strategies, medium-sized enterprise managers' perceptions of CRI, their preparedness against cybercrime, and their attitudes towards balancing CRMi with business success. This chapter concludes by addressing the research gaps and providing results relevant to the interplay between cyber-risk management and organisational success.

Chapter Five will set forth the discussion of the findings (Chapter Four) in the context of current academic knowledge, as presented in Chapter Two. This chapter will cover the themes and debates surrounding CRMi strategies and the role of CRI in German manufacturing medium-sized enterprises, with a focus on highlighting key insights, theoretical contributions, and practical implications. The discussion begins by examining the level of preparedness, CRMi strategies, and CRI and then further explores the relationship between specific risks and CRMi strategies. The chapter also delves into the manager's perception of CRI and its potential role as a solution. Finally, it concludes by examining the medium-sized enterprises' preparedness against cybercrime risk, as well as the managers' attitudes towards CRMi measures and business success. Therefore, this chapter attempts not only to synthesize the findings but also offers a reflective and critical lens for comprehending the implications of this research.

Chapter Six, as the final chapter, will revisit the research aim and questions before presenting the conclusions drawn from the findings and reflections on the research gaps and initial questions. The chapter highlights the study's contributions to academic theory and practical applications. In particular, the study shows that cybersecurity and risk reduction are not given enough attention in the economically important sector of German manufacturing medium-sized enterprises, especially from the point of view of senior management and leadership. The outcome demonstrates how resource constraints and cost-benefit analyses influence cybersecurity investment decisions while emphasising the intangible influences of cyber-risks, such as reputation loss, thus broadening the focus beyond financial and operational concerns. The study critiques current cyber-risk insurance models, advocating for SME-specific policies that are affordable, relevant, and tailored to their needs. The chapter further proposes a dedicated CRMi framework designed to help medium-sized enterprises identify risks, implement effective mitigation strategies, and sustain business success despite

cyber threats, ensuring alignment with budgetary constraints and maximising return on security investment (ROSI).

The chapter sets out the study's limitations, including the need for broader participation from interview partners to achieve more generalisable findings. Finally, the chapter offers suggestions for future research and concludes with a personal note on the study's relevance and value.

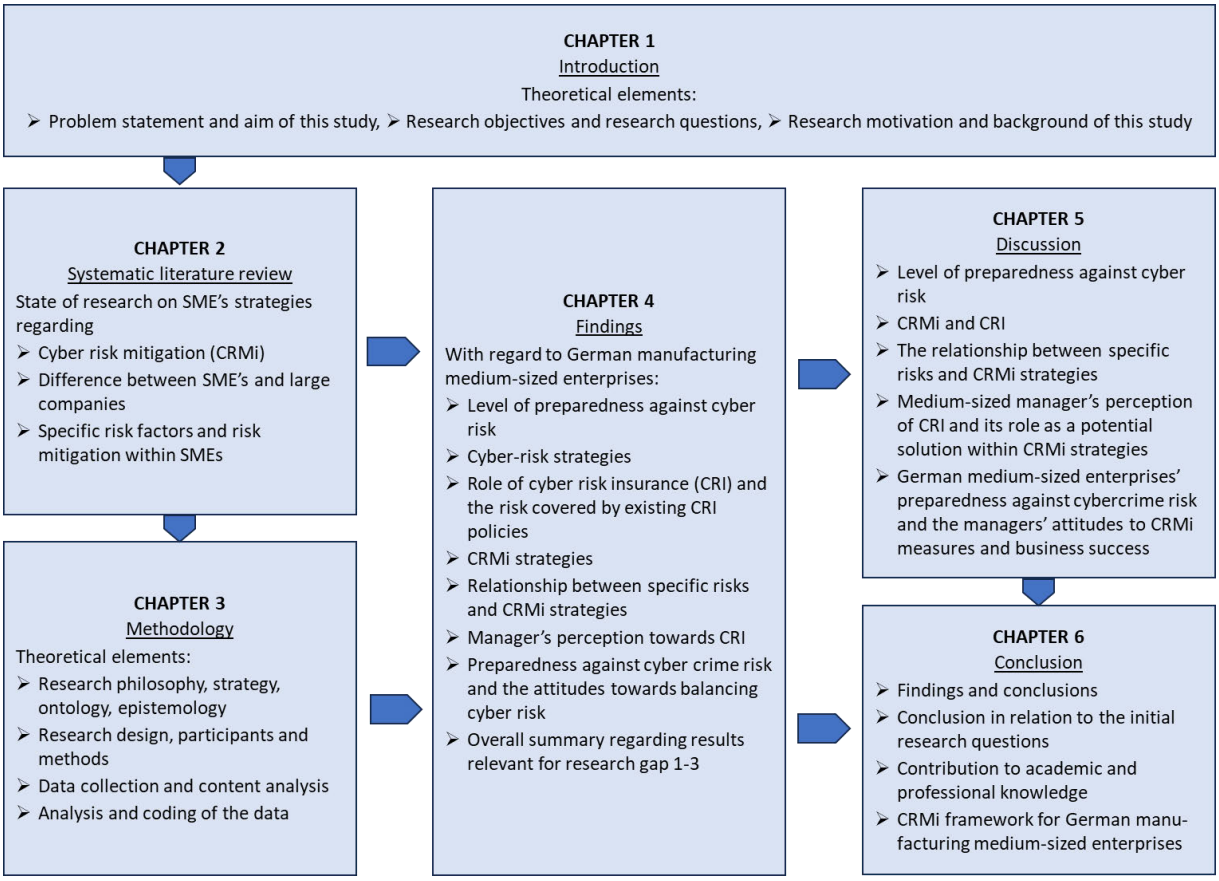


Figure 1-1: Structure of the thesis

2 Chapter Two

Literature Review

2.1 Introduction

Given the importance of cyber-risk protection, the available relevant literature and academic research on cyber-risk mitigation (CRMi) related to SMEs is interestingly limited (Falkner & Hiebl, 2015; Tøndel et al., 2015). For Tøndel et al. (2015), although there has been extensive research from a large multinational business perspective, this is a lack of literature related to SMEs. This omission is problematic as the sector is a major German GDP generator, and a cyberattack could potentially damage a business, the supply chain, and ultimately the country's economy. To address this, this chapter intends to present a critical review of the current academic debate about CRMi strategies and associated business measures from a holistic perspective before focusing on existing knowledge related to German SMEs in the manufacturing sector. This will include presenting the current debate associated with cyber-risk strategies and the relevance of this research project.

To achieve this, this chapter will present the existing literature from a broad perspective and provide in-depth insight and context (Boote & Beile, 2005). The chapter will set out and justify the decisions taken by the researcher as to the demarcation of the study, including the boundaries of the themes and topics being researched. This approach was informed by Webster and Watson's (2002, p. xiii) argument that "an effective review creates a firm foundation for advancing knowledge". The chapter will also identify those themes already explored along with those unexplored topics, including knowledge gaps, while facilitating theory development. This approach is aligned with Levy and Ellis (2006), who contend that the key characteristics of a literature review are:

- To analyse the existing knowledge methodically and then synthesize the quality of the literature.
- Provide a firm foundation for the research.
- Provide a robust justification for the selection for the intended research methodology.
- To demonstrate how the research will contribute a new insight into the overall body of knowledge or advance the existing knowledgebase.

To achieve this, a thorough literature review will be conducted on the debate surrounding the opportunities and challenges of managing cyber-risk mitigation. This review will assess the potential influence on business and the strategies adopted, with a particular focus on German manufacturing SME perspectives. Finally, the outcome of the existing literature will be discussed as to the existing gaps of knowledge and the research questions that need to be asked in the qualitative semi-structured interviews. The main objective of the qualitative part of the study is to address the identified gaps in academic knowledge by providing new and critical academic insights. To present the current academic debate, this study adopted a systematic approach, which will be justified in the next section.

2.2 Systematic literature review

To understand the underlying research problem, a critical literature review needs to be conducted. By conducting this review, the outcome can be used to form a theoretical and conceptual framework, which in the case of this study is to determine how German manufacturing SMEs have implemented cyber-risk insurance into their risk mitigation strategies, then determine the level of effectiveness and success. The researcher also wanted to understand the current debate associated with the conditions and finances needed to protect against a cyberattack. Given the limited literature available and the novelty of this topic, the researcher conducted a documentary analysis of relevant literature and policies.

To validate the theories and ideas generated from the existing literature and documentary analysis, a qualitative data collection technique was employed (Kosub, 2015). This approach provided deeper insights into critical themes, such as the necessity of cyber-risk insurance, potential obstacles to its adoption, and the processes required for implementation. By analysing these aspects qualitatively, the study enabled a more comprehensive understanding of the underlying issues and themes (Tøndel et al., 2015).

2.3 The systematic literature review protocol

Lack of information or understanding about a specific knowledge gap typically prompts the conduct of a literature review, which then concentrates on enhancing this theme (Saunders et al., 2020). To achieve this, rather than broadening the research questions, writers including Randolph (2019) suggest outlining what questions the literature review should answer or

inform. Therefore, the purpose is to ultimately identify and then formulate a problem from the literature review that is most suitable to study. The rationale for this is based on the premise that firstly, the approach would help to avoid losing focus on the research and ultimately the research questions. Secondly, the strategy would guide the selection of sources for the review. After careful consideration of these aspects, particularly the significance of the literature as the study's foundation, the criteria below guided the selection of literature sources, leading to the adoption of an in-depth review approach that ultimately helped to achieve the research objectives:

- To critically identify from the current academic debate as to what cyber-risk strategies are adopted to manage potential cyber threats.
- To critically analyse from the findings generated from the German manufacturing SME managers as to the strategies adopted to manage and mitigate against potential cyberattacks.
- To critically evaluate from the findings as to how German manufacturing SME managers mitigate against potential cyberattacks.
- To provide a new critical academic insight into how German-based manufacturing SMEs mitigate against potential cyberattacks.

This study decided to conduct a systematic and not a narrative review of the current literature. This strategy therefore suggested that the problem formulation in this study was informed and influenced by the main areas of interest: cyber-risks in SMEs, from which emerging themes in the existing literature can be identified.

There are many approaches to obtaining knowledge, whether it is new or existing. Such approaches could include personal experience or professional reflection. Alternatively, it can be socially derived, for instance through the exchange of experience with peers and experts, attending conferences, or being informed by professional training. Irrespective of how the researcher reaches the focus of the study, this process could be seen as being subjective and therefore unreliable without being academically and rigorously justified. This is the same when the research is based on or grounded in a single source of information, where the study is too narrow to be seen as creditable or reliable. Therefore, when undertaking research to tackle theoretical and practical issues, it might be necessary for a researcher to choose a more robust means to gain knowledge. One such possibility to close a knowledge

gap is conducting a comprehensive literature review. To achieve this, there are two main approaches: narrative and systematic. The following section will provide a brief overview of the characteristics of the two approaches.

To select the appropriate method for conducting a literature review, there are a few approaches that could have been adopted. The first is the narrative approach. Boell and Cecez-Kecmanovic (2015) focused on the narrative approach on summarising existing knowledge and drawing conclusions for the researcher's own work. Narrative reviews are the traditional approach to literature reviews, particularly when conducting a scientific or business research project. Even though this approach was ultimately rejected, the review methodology is widely used by researchers and, when conducted correctly, can provide a critical analysis of recent publications and up-to-date knowledge about a defined topic (Cipriany & Geddes, 2003). Although the narrative approach covers a wide range of issues due to its comprehensive methodology, it conceals the decision-making process regarding the relevance and validity of the included sources in the literature review presentation (Collins & Fauser, 2005). Narrative reviews tend to be intuitive aggregates of individual research findings (Johnson, 1989) and have some advantages and a distinct characteristic that provides the possibility to cover much broader questions compared to systematic reviews. This strategy therefore allows for the specific selection of key texts and a deep focus on selected aspects in a certain field of enquiry, which gives the researcher more space and flexibility to critically examine the sources and statements and possibly question the assumptions and ideas behind them in more depth.

A narrative review tends to describe arguments, current states, and latest developments in focused areas of inquiry. Therefore, the approach can then construct theoretical insights and present new perspectives by identifying weaknesses or omissions of selected key texts (Rumrill & Fitzgerald, 2001). Finally, a narrative review can be less time-consuming compared to systematic reviews, which makes this approach a good choice for practitioners aiming to conduct a literature review.

However, there are limitations. A key limitation with a narrative review is that different reviewers might have different opinions on what the key texts and the most influential authors in a topic area are. This could lead to the argument that the narrative review is less objective and reproducible compared to a more systematic approach. Furthermore, narrative reviews

may lack thoroughness and possibly emphasise whatever points the researcher desires. This is encapsulated in the perspective of Bent, Shojania, and Saint (2004, p. 249): "[I]n narrative reviews, authors pick … the studies they discuss and the depth at which they discuss them. Consciously or not, their biases and interests [;] affect how they present the findings [;]". Therefore, conclusions made by the researcher could be drawn from a biassed or subjective perspective, despite the facts in the evidence (Dijkers, 2009). This then brings into question the level of subjectivity, which may result in severe inconsistencies of research findings based on reviews of identical issues (Ladhani & Williams, 1998; Suri, 1998). This viewpoint is particularly important for inexperienced researchers who may be approaching the topic for the first time and find the process difficult to conduct. The outcome could be the generation of a low-quality review that lacks any depth and limited focus (Cook et al., 1997).

As a response to this critique of the narrative review, there has been the emergence of a more systematic approach (Tanenbaum, 2005). This systematic methodology was designed around providing quality of the review process through improving the designing and conducting the research in a more systematic, transparent, and reproducible manner (Tranfield et al., 2003). Collins and Fauser (2005) stated that a systematic review is more appropriate for research that has a focused, clearly defined topic and specific research questions. As noted above, there are possible drawbacks to using a narrative review strategy, leading to the consequences of incorrect reviews, particularly amongst inexperienced reviewers. In contrast to a narrative review, a systematic approach provides an overview and synthesis of sources that contains a statement of objectives, materials used, and methods applied, acting as an audit trail. Through using a systematic approach, the strategy can synthesise the literature to make more explicit the debate (Greenhalgh, 1997; Saunders et al., 2020; Tranfield et al., 2003). Systematic reviews can develop methods and strategies for locating relevant publications on defined topics, including explicit criteria addressing content and methodological quality. By using specified criteria, the systematic review attempts to reduce reviewer subjectivity. The process involves clearly stated, explicit, and transparent methods for reviewing the literature that are comprehensible, reproducible, and objective (Collins & Fauser, 2005). Systematic literature reviews are therefore widely seen as providing good quality evidence, which now includes business-associated research (Tranfield et al., 2003).

Fundamental to research is the need for reliable information and transparency, which is seen as being essential for practitioners and researchers. Writers including Tranfield et al. (2003) have argued that a focused approach based only on one kind of evidence could lead to inappropriate decisions being made, therefore possible alternatives or contradictions being neglected (Dixon-Woods et al., 2005). To address this limitation, Tranfield et al. (2003, p. 207) advocated and emphasised that systematic reviews should be applied to the management field to "produce a reliable knowledge stock and enhanced practice by developing context-sensitive research," thereby ensuring that the knowledge is not limited, neglected, or intentionally overlooked. Therefore, addressing the possible drawbacks of narrative reviews and the strong tendency towards evidence-based decision-making has resulted in a trend to cover a wider scope of knowledge when conducting a literature review in a management research project, which was adopted in this study.

Based on the aforementioned information, Kitchenham and Charters (2007) recommend that the initial step in conducting a literature review should involve defining the research objective, followed by the development and definition of a search strategy and review protocol. Following this, the data or literature should be selected, and the strategy criteria should be established and then maintained. Following these steps allows the actual analysis of the existing literature to commence. A similar approach was proposed by Brocke et al. (2009), who suggested first defining the review scope, for example, by developing research questions. This can then inform the conceptualisation of the topic, which includes the criteria for the literature.

A literature review tends to be carried out to establish the current academic debate, which then informs the research topic using empirical methods. Therefore, the purpose of a systematic literature review was used to identify the current debate based on the potential research gaps. Based on this, questions for the empirical, qualitative questions were then developed. Out of the three approaches outlined above, the method applied in this study fol-

lowed the strategy proposed by Brocke et al. (2009), due to the logic of reviewing the current literature and debate then formulating the research questions, therefore informing the overall study. The methods followed in this review are presented below:

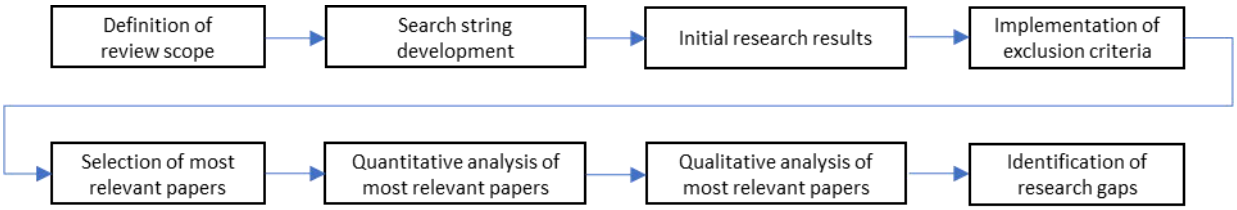


Figure 2-1: Method applied for conducting the SLR (Brocke et al., 2009)

2.4 Justification for conducting a systematic literature review

Fink (2019, p. 254) stressed that a systematic literature review (SLR) is a "systematic, explicit and reproducible method for identifying, evaluating, and synthesizing the existing body of completed and recorded work". Therefore, this review is focused on identifying, appraising, selecting, and synthesising the existing literature in the relevant field of interest (Fink, 2019). For Tranfield et al. (2003), this strategy plays a crucial role in developing an evidence-based understanding that contextualizes the relevant research. A SLR represents a significant methodology and approach for researchers and is widely used in different research areas, e.g., the health sector (Mulrow, 1994) and other disciplines, including business (Higgins & Green, 2008; Tranfield et al., 2003).

There are a series of phases or stages to follow when conducting a SLR. The first phase was the screening of existing academic literature, which included research into cyberattacks, mitigating strategies, supplier relationship management (SRM), and original equipment manufacturer (OEM) usage by suppliers (Colicchia & Strozzi, 2012). One issue to emerge from the first phase was the difficulty associated with finding best practice as to cyber-risk mitigation strategy in the literature, which could be transferred into management implications related to cyber-risk and insurance strategies for SMEs. To address this potential issue, Tranfield et al. (2003) identified that evidence-based research is a strategy that can be used through drawing on professional experience and related articles. Therefore, the researcher considered a combined approach that involved conducting a SLR based on academic sources, while also drawing from professional experience and associated literature. This proved to be insightful, as themes such as supply chain resilience in global and heterogeneous supply networks were a relatively new and still largely unexplored field of interest but could be better

understood by drawing on professional experience and literature outside the parameters of purely academic research (Cohen & Lee, 2020).

However, it should be noted that the review conducted in this chapter did follow a robust systematic approach that involved gathering literature from extensive usage of academic databases and was focused on cyber-risk mitigation and SMEs. A detailed and planned process was followed to identify and understand the current debate, which then informed the study's research questions. Ultimately, only relevant articles were selected for this review, which will be presented later in this chapter.

As the literature review was being conducted, it emerged that the research into the management of cyberattacks and mitigation was mainly based on narrative reviews. Many of those studies, which were narrative, lacked thoroughness and completeness, only providing a descriptive account of cyber-risks and mitigation strategies. The process also reflected the conclusions of Fink (2019) and Hart (1998), who noted that the choice of topic and search for materials for a study are frequently biassed or influenced by the researcher. To avoid any form of material redundancy, it was essential to consider all research related to the field of interest. This was achieved by ensuring that practitioners and academic sources were included in the initial stage of the systematic approach (Tranfield et al., 2003). The approach followed Mulrow and Cook's (1998) advice on how to improve the overall research process, including the possibility of detecting discrepancies and enabling the researcher to integrate valid information more efficiently, therefore providing a robust and extensive insight into the current debate by adopting this strategy.

Mulrow (1994) earlier contended that adopting a SLR can significantly improve the transparency, reproducibility, and synthesis quality of the activity. SLRs are, by definition, retrospective, since the studies included can only be identified after they have been published. During this process, the review should maintain a practical perspective (Higgins & Green, 2008), although limiting any form of personal bias. Explicit and systematic methods therefore can lead to more reliable results, which in turn act as a basis for drawing conclusions and making decisions (Antman et al., 1992; Higgins & Green, 2008; Oxman & Guyatt, 1993). This is particularly important in this study as to the cyber-risks that are faced by German manufacturing SMEs. In the context of cyber-risk mitigation, it was crucial that the respective research studies aligned with the current debate, which included perspectives from large multinationals.

By carrying out a systematic review, the researcher was able to develop a set of "field-tested and grounded technological rules" (Aken, 2004 p. 220) and therefore achieve a robust and critical insight into the current debate. Higgins and Green (2008) further advocated and outlined the following six steps for preparing and maintaining a systematic review: the review should start by formulating the problem, followed by locating and selecting suitable studies. Next, the quality assessment of studies should be carried out. The next step deals with the data collection before analysing and presenting the results. The results are then interpreted, improving and updating the reviews, which is the final step. Tranfield et al. (2003) and Fink (2019) also recommend applying a similar approach and sequence to management research needs and listed the following nine points consisting of the two major stages of planning the review (Stage I) and conducting the review (Stage II), as shown in the following list (Tranfield et al., 2003, p. 214):

Stage I−Planning the review:

- Phase 0 - Identification for the need for a review.
- Phase 1 - Preparation of a proposal for a review.
- Phase 2 - Development of a review protocol.

Stage II−Conducting a review:

- Phase 3 - Identification of the research question.
- Phase 4 - Selection of studies.
- Phase 5 - Study quality assessment.
- Phase 6 - Data extraction and monitoring progress.
- Phase 7 - Data synthesis.

Stage III−Reporting and dissemination:

- Phase 8 - The report and recommendations.
- Phase 9 - Getting evidence into practice.

While the focus of this SLR was to identify best practices in SMEs cyber-risk strategies and to understand the perspectives associated with seeking insurance against cyberattacks in the German manufacturing sector, some weaknesses were identified. In the medical field, it has been noted that systematic reviews are not always fully reliable (Moher et al., 2007). To address this, writers including Higgins and Green (2008) advocate the usage of guidelines and standards to improve the standard of reporting while ensuring high quality and reliability.

There are however certain limitations arising from conducting of the literature review which should be acknowledged. The literature search was conducted primarily via Google Scholar,

supported by the University of Gloucestershire's Discovery service, which, while providing a broad in coverage, may not index all domain-specific or proprietary academic sources. Furthermore, only English-language publications were included, which may appear to limit the study's which was focused on German manufacturing medium-sized enterprises. However, it is worth noting that academic research in this field is overwhelmingly published in English, and earlier test searches indicated a negligible presence of relevant German-language academic articles. As noted, the time frame for the searching was from 2015 to 2023 during the preliminary searches, which showed limited relevant literature prior to 2015. While these decisions were methodologically justified, the results indicated an omission for certain niche or non-English-language contributions to the topic.

2.5 Definition of review scope and formulation of search string

Following the guidance of Brocke et al. (2009), this study employed a two-phase literature review process. A preliminary narrative literature review, presented in Chapter One, was first conducted to develop an overall understanding of key themes related to cyber-risk mitigation (CRMi) in German manufacturing SMEs. Specifically, the review explored: (1) the CRMi strategies adopted by SMEs, (2) the relationship between specific risk factors and corresponding mitigation strategies, and (3) the role of cyber-risk insurance as a potential component within these strategies. This narrative review also served to contextualize the research within the broader discourse of organisational resilience and cybersecurity. This approach helped define the scope of inquiry and establish the thematic boundaries necessary for a more focused and rigorous systematic literature review (SLR).

The insights derived from the narrative review were then used to formulate the search strategy, inclusion/exclusion criteria, and initial search strings for the SLR, in line with the framework proposed by Brocke et al. (2009). While preliminary research questions were used to guide the SLR, the ultimate identification of research gaps was derived inductively from the SLR results. These research gaps, in turn, led to the refinement and finalisation of the central research questions addressed in this study.

To summarise, the main interest of the SLR is related to the SMEs' cyber-risk mitigation strategies. Reflecting this, the search string was formulated as follows:

"SME" AND "cyber-risk" AND "mitigation"

2.6 Technical description of systematic literature search

The systematic literature review was carried out using mainly the University of Gloucestershire's Discovery database and Google Scholar. However, with Google Scholar, the search engine did not allow for bulk download of search results; therefore, a software package called Publish or Perish was used. After entering a search string and specifying the range of year or years of publication and the literature database to be used along with the maximum number of search results, the software searches enabled the researcher to access the literature. The use of the Publish or Perish software allowed for the export of the search results in different formats, including a spreadsheet.

This process commenced on November 6, 2023 and the last search was carried out on November 24, 2023, using the search string "'SME" AND "cyber-risk" AND "mitigation". The search was limited to publication years 2015 to 2023, as earlier searches had already shown that, up to 2014, there had only been a handful of publications relevant to the search string used. To enhance the searching process within Publish or Perish, there was an option to exclude citation records or patents. The decision was made to exclude citation records since trial searches had shown that with this option activated, only citations of a publication were shown in the search results, which then required additional analysis to identify the full publication. Patents were excluded since the search was focused on identifying academic literature only.

Using the above-mentioned parameters, 525 search results were identified. These results were exported into a literature management software (LMS) for organisation and subsequently processed within the LMS for further analysis. The following steps were then carried out to filter the publications and refine the analysis, as outlined in Table 2-1:

Table 2-1: Criteria used to eliminate publications from initial search results

Criteria	Rationale	Number of results remaining following application of criterion
Original results		525
Publication year not available.	These were mostly sources considered non-citable for a PhD-thesis (e.g., Masters' theses).	493
Eliminate all publications with any field in LMS containing:	A large body of cybersecurity literature is dedicated to the role of	

Table 2-1: Criteria used to eliminate publications from initial search results		
Criteria	Rationale	Number of results remaining following application of criterion
"infrastructure" OR "military" OR "banking" OR "infrastructure" OR "homeland" OR "catastrophe" OR "healthcare" OR "water" OR "financial services".	cybersecurity for the safe functioning of critical infrastructure or in the banking system or national security (military) sector. These are not considered of relevance to this study.	441
Reduce search results to any field in LMS containing: "SME" OR "small business".	The initial search results from the "Publish or Perish" were not sufficiently focussed.	267
Reduce results in the LMS to fields not containing "success".	Success is another aspect of interest to this study, yet there were no results NOT including the term success.	267
Reduce search results to publication type "Journal Article".	Books included non-citable sources (e.g., Bachelor and Master theses) or were not accessible (only individual chapters of Google-Books).	188
Add books with any field in LMS containing "small business".	Books dedicated to "small business" were to be included in results.	194
Eliminate publications where SME is an acronym for something other than small and medium enterprise	SME is sometimes used for "subject matter expert".	191

Table 2-1: Criteria used to eliminate publications from the initial search results

For the remaining 191 publications, the titles, abstract, and where available, keywords were analysed to enable the categorisation of the publications. The process also included reviewing the publications which did not align or could be categorised. At this stage, these articles and publications were eliminated from the search results. The remaining categorised articles were then analysed as to the content. The outcome of this process is presented in Table 2-2:

Table 2-2: List of categories and assigned papers			
No.	Categories	Rationale	Number of papers assigned
1	Cyber-risk mitigation – generic.	Papers dealing generically with cyber-risk mitigation measures, in which SMEs were only mentioned but not specifically the subject of investigation.	36

Table 2-2: List of categories and assigned papers			
No.	Categories	Rationale	Number of papers assigned
2	Cyber-risk mitigation – cost and benefits.	Papers in which cost- and benefit calculations in the context of cyber-risk mitigation measures were investigated explicitly.	7
3	Cyber-risk awareness in SMEs.	Papers presenting studies on cyber-risk awareness in SMEs.	6
4	Cyber-risk – specific problems for SMEs.	Papers in which specific problems of SMEs in the context of cyber-risk mitigation were focused.	22
5	Cyber-risk mitigation – measures in SMEs.	Papers focussing on cyber-risk mitigation measured, tailored for the requirements of SMEs and/or experience with such measures.	29
6	Cyber-risk insurance.	Papers presenting insurance as a potential element of cyber-risk mitigation.	15
7	National strategies for cyber-risk management.	Papers presenting or reporting on national strategies. SMEs are mentioned in these as potential beneficiaries of such strategies.	13
8	Papers eliminated from results as they fulfil any of the elimination criteria presented in Table 2-1.	Upon closer inspection, these papers were categorized to fall under elimination criteria established earlier (e.g., SMEs mentioned as beneficiaries of finance sector's cybersecurity measure).	63

Table 2-2: List of categories and assigned papers

It should be noted that some articles were assigned to more than one category; for example, a paper could be relevant for both categories 4 and 5. However, those papers categorised in categories 7 and 8 were sometimes aligned with 1, and were eliminated from further analysis since this study was focused on SMEs. Categories 2 was retained as the cost-benefit aspect was relevant, particularly in the context of researching the theme of business success following a cyberattack.

The categorisation of the selected publications, as presented in Table 2-2, was developed through a deductive analysis approach, guided by the overarching themes of the study. Titles, abstracts, and where available, keywords were reviewed to group papers into meaningful categories aligned with the research focus on cyber-risk mitigation (CRMi) in SMEs. This

categorisation was based on the researcher's interpretation and judgement, informed by the theoretical context and the relevance of each publication to the research.

In a subsequent phase, and based on a more detailed analysis of the full texts, subcategories were also developed to allow for a more nuanced classification of the content and methodological approaches of the papers. This process involved identifying dominant themes and assigning them as subcategories where appropriate. As can be seen in Tables 2-3 to 2-7, subcategories were sometimes assigned across different main categories, reflecting overlapping or cross-cutting themes. These overlaps are further summarised in Table 2.8. These subcategories were not predefined but emerged through iterative analysis and interpretive reading, enabling a more nuanced and robust synthesis of the literature base.

2.7 Results, summaries, and sub-categorisation of the systematic literature review

Table 2-3 below shows only the results for those publications that are aligned with the search criteria. This table provides a summary of the results, a summary of the papers, the category, and the focus. While analysing the journal content from the 79 papers selected for closer analysis based on the content of the articles, another two publications needed to be eliminated as these studies met the exclusion criteria, because they were either not relevant or non-citable. Following this process, subcategories were also identified to allow for a more robust strategy to identify the content of the article. Tables 2-3 through 2-7 below show that papers within different categories were sometimes assigned the same subcategories, indicating a crossover or synergy of themes. Overall, Hoppe et al. (2021) confirm in their industry survey that the major obstacles to the implementation of cyber risk mitigation (CRMi) in SMEs across countries are deficiencies in risk culture, specifically in perception, knowledge, and attitude towards cyber security, as well as a strained market for IT experts. Their findings also suggest that the relationship between cyber security culture and cyber-risk management is critical for a successful CRMi.

Table 2-3: Search results category 2: Cyber- risk mitigation – costs and benefits				
Author(s)	Year	Title	Results	Subcategory
Anderson, R., and Moore, T.	2006	The economics of information security.	The authors found that incentives are becoming as important as technical design in achieving dependability. Security topics like security like bugs, spam, phishing, and law enforcement strategies, have enabled information security to offer invaluable insights into more general areas like peer-to-peer system design. Programmers and testers have now balanced their efforts, to prevent the erosion of privacy, and the politics of digital rights management.	Challenges
Ishikawa, T.	2017	A Study on Evaluation Methodology of Cybersecurity Investment.	Development of a method to assess the financial value of cybersecurity breach risk. Analysis of data included the leakage cases in Japan and provides a comparison between compensation in Japan and the USA with characteristics of personal data. This included the searchability, cancellability, retrievability; The development of corporate valuation based on the Twitter reputation index (event study method) to evaluate the effectiveness of cyber-risk insurance from both qualitative and quantitative perspectives. The study used the Monte-Carlo simulation to consider various possibilities, concluding that cyber-risk insurance is an effective solution for security management and risk management.	CRI Challenges
Nelson, N., and Madnick, S.	2017b	Trade-offs between digital innovation and cybersecurity.	The research introduced a framework for CIOs to evaluate cybersecurity risk/reward trade-offs. A set of practical recommendations was provided to assist companies in assessing their positioning on the innovation/cybersecurity matrix, understanding the underlying factors influencing that position, and improving their management of these trade-offs. The research highlighted the growing importance of cybersecurity as a strategic priority, with some companies viewing it as a competitive advantage. However, only 13% of companies believed they had successfully balanced cybersecurity with innovation, experiencing minimal negative impacts. The study also noted that while some companies took on excessive risk without fully realizing it, others missed out on technology-enabled innovation opportunities.	Innovation
Kazemargi, N., and Spagnoletti, P.	2020	IT investment decisions in industry 4.0: evidences from SMEs.	This study examined the strategic decisions of SMEs in Italy regarding IT investments in Industry 4.0. The study revealed that SMEs are more likely to invest in digital technologies and integrate advanced technologies across various sectors and regions. The research underscores the importance of aligning IT investments in emerging technologies with business strategies, as large enterprises have been extensively researching Industry 4.0. The findings highlighted the need for SMEs to adapt their IT strategies accordingly.	Recommendations

Table 2-3: Search results category 2: Cyber- risk mitigation – costs and benefits				
Author(s)	Year	Title	Results	Subcategory
McLilly, L.	2020	Exploring a Cost-Benefit Cloud-Based On-Demand Cybersecurity Service Solution for Small Businesses: A Quantitative Examination - A Dissertation Presented in Partial Fulfilment of the Requirements for the Degree of Doctor of Computer Science.	Small businesses struggle with cybersecurity due to limited resources, despite recognizing the growing threat. A survey showed 65% have faced cyberattacks, yet only 4% follow recommended practices. Security as a Service (SECaaS) could help but is difficult to scale for small businesses' diverse needs. This research proposes a cost-effective cloud-based cybersecurity service system (CODCSSSB) tailored for small businesses. To address design complexity and high development costs, the study used data analytics to quickly identify and fail requests that the system cannot handle. This approach reduces development time and improves design accuracy by identifying weaknesses efficiently.	Cloud-based solutions
Rawindaran, N., Jayal, A., Prakash, E., and Hewage, C.	2021	Cost Benefits of Using Machine Learning Features in NIDS for Cyber Security in UK Small Medium Enterprises (SME).	Cybersecurity increasingly challenged SMEs, especially with the rise of wired and wireless connections, leading to more malicious activities. Balancing technology advancement with costs was crucial, particularly in convincing finance directors to invest in IT infrastructure. This study, conducted during the COVID-19 pandemic, compared OpenSource tools (SNORT, pfSense) and Cisco devices for intrusion detection in both home and office environments. Findings showed that OpenSource tools required high expertise, while Cisco offered more reliable detection through its subscription model. The study emphasized the importance of balancing IT expertise and costs to effectively secure SME data, in line with GDPR requirements.	Recommendations
Pfister, P., and Lehmann, C.	2023	Returns on digitisation in SMEs—a systematic literature review.	The impact of digitisation on SMEs, as well as the value and return on digital solutions, was investigated. Fourteen added values were categorized as financial and strategic digital benefits, with the most cited returns being efficiency, cost reduction, productivity growth, customer satisfaction, and competitive advantage. Key digital solutions included social media, websites, cloud computing, and data analytics. The study also highlighted five primary benefits of digital value creation: increased revenue, improved customer and employee satisfaction, efficiency, and productivity. Eight case studies showed a positive return on investment from digital solutions aimed at revenue growth or cost reduction. For SME managers, guidelines to enhance business performance through digitisation, starting with standardized use cases and subscription-based solutions that offered immediate returns, were recommended.	Recommendations

Table 2-3: Search results category 2: Cyber-risk mitigation – costs and benefits

The perspectives offered by the various authors above in Table 2-3, indicated that there was a complex interplay between technological innovation, cybersecurity, and strategic investment, especially in the context of SMEs. The studies independently provided a unique angle on how businesses can navigate these challenges, highlighting both the opportunities and risks involved. In reviewing the question of whether incentives and economic considerations are as important compared to technical design in achieving cybersecurity and digital innovation, this was based on propositions given by Anderson and Moore (2006) and Ishikawa (2017). Anderson and Moore (2006) asserted that in distributed systems composed of computational resources owned by entities with divergent interests, aligning incentives is crucial for achieving system dependability. The authors argued that technical design alone is insufficient, as the motivations and economic interests of the stakeholders play a significant role in how effectively these systems function. Here, economic incentives, such as the cost of security breaches or the financial benefits of protecting privacy, can drive better outcomes than technical measures alone. Ishikawa (2017) supported this argument of Anderson and Moore (2006) by demonstrating the importance of evaluating cybersecurity investments through a financial lens. Ishikawa (2017) found that the economic valuation of cybersecurity breach risks in Japan was comparable to the USA, emphasising that understanding the financial implications of data breaches, including compensation and the impact on corporate reputation, is essential for informed decision-making. The use of tools like Monte Carlo simulations and the Twitter reputation index to quantify these risks illustrates how economic analysis can guide more effective cybersecurity strategies, supporting the view that incentives are critical.

However, critics including Nelson and Madnick (2017a) have argued that placing too much emphasis on incentives and economic factors could lead to a narrow focus that overlooks the technical complexities and nuances of cybersecurity. Nelson and Madnick (2017a) highlighted the difficulty of balancing cybersecurity with digital innovation, noting that only 13% of companies report success in this area. For Nelson and Madnick (2017a), while economic incentives are important, the technical challenges involved in securing innovative digital technologies require substantial expertise and resources. This suggests that without a strong technical foundation, even the best-aligned incentives may fall short in addressing the sophisticated threats that modern systems face. Moreover, Kazemargi and Spagnoletti (2020)

provided further evidence of the importance of aligning IT investments with business strategies, particularly in the context of Industry 4.0 for SMEs. While economic considerations are undoubtedly important, Kazemargi and Spagnoletti (2020) revealed that the strategic integration of digital technologies requires a deep understanding of both the technical and business environments. This outcome suggests that to achieve the desired outcomes, a strong technical strategy must complement the valuable incentives and economic analysis.

Proponents of the incentive-based approach might counter that focussing on economic and strategic considerations does not negate the need for technical expertise but rather enhances it. McLilly (2020) illustrated this by proposing a cloud-based cybersecurity service system (CODCSSSB) tailored for small businesses. McLilly's (2020) research showed that by using data analytics to streamline the design and implementation of cybersecurity solutions, businesses can achieve cost-effective and technically sound security measures. This approach demonstrates that economic incentives can drive the development of innovative, technically robust solutions that are accessible even to resource-constrained SMEs. Similarly, Rawindaran et al. (2021) highlighted the role of machine learning in enhancing network intrusion detection systems (NIDS) for SMEs. Meanwhile, Rawindaran et al. (2021) argued that while technical expertise is required, the cost-benefit analysis of different tools (e.g., OpenSource vs. Cisco devices) is crucial for making informed decisions that balance security needs with financial constraints. This reinforces the idea that economic and technical considerations are not mutually exclusive but are interdependent in the pursuit of effective cybersecurity.

The debate underscores the complex interplay between economic incentives, technical design, and strategic decision-making in cybersecurity and digital innovation. While critics emphasise the need for robust technical solutions, the evidence presented by Anderson and Moore (2006), and Ishikawa (2017), suggested that the alignment of incentives and considering economic impacts are equally crucial for achieving dependable and secure systems. Therefore, the most effective approach likely lies in integrating both perspectives, ensuring that economic incentives drive the development of technically sound and strategically aligned cybersecurity measures.

Table 2-4: Search results Category 3: cyber-risk awareness SMEs				
Author(s)	Year	Title	Results	Subcategory
Quesada, I.	2016	Seccord - Deliverable 5.5 Catalogue Year 3.	SECCORD's Deliverable 5.5 Catalogue Year 3 highlighted the advancements in cloud monitoring, enabling new applications and business models. The focus in cybersecurity has shifted from detective and reactive technologies to proactive and predictive technologies, with big data technologies incorporating predictive aspects and integrating previously separated tools. The deliverable addresses SME-specific issues such as access to finance, innovation processes, and cross-border markets, providing incentives for wider adoption, such as cyber-risk insurance, and enabling further improvements through collaboration and cooperation. The study also stated that SME employees do not have formal CS training; the main driver is compliance (e.g., data protection legislation).	Challenges
Muhirwe, J., and White, N.	2016	Cybersecurity awareness and practice of next generation corporate technology users.	Cybersecurity awareness has a significant impact on one's cybersecurity practice and behaviour, leading to the proposal for regular cybersecurity awareness activities. A combination of awareness events and training is recommended. While the study did not effectively predict awareness of cybersecurity, the article did show that training had a significant relationship with cybersecurity awareness.	Training program
Ashby, S., Bryce, C., and Ring, P.	2018	Risk and the strategic role of leadership.	The ACCA research project examined how SME boards address risk management, focusing on their integration of strategy and risk discussions and the development of their skills (RI-SKeet: risk intelligence, skills, knowledge, experience, education, and training). The study identified challenges in these areas, particularly the evolving roles of directors and the differences within unitary boards. The study highlighted the critical role of near-miss incidents and actual losses in prompting strategic risk discussions, with cyber-risk being a key concern. Boards often seek external expertise to enhance their RI-SKeet, as shown by a manufacturing company's proactive response to a cyberattack during an audit, which prevented a potential disaster.	Challenges

Table 2-4: Search results Category 3: cyber-risk awareness SMEs				
Author(s)	Year	Title	Results	Subcategory
Binkhorst, V.	2020	Improving Cyber-Risk Communication: Mental Models of VPN in a professional services firm in the Netherlands.	This study employed a mental model approach, semi-structured interviews, and a three-part scenario-based drawing task to investigate the risk perception of eleven laypeople and eight experts. The data was analysed using the grounded theory method, and a substantive theory was formed on the similarities and differences between the mental models of experts and laypeople of VPN in a professional services firm in the Netherlands. The study recommended designing more effective and efficient risk communication in the cybersecurity field to raise people's risk awareness and resilience.	Recommendations
Eilts, D.	2020	An empirical assessment of cybersecurity readiness and resilience in small businesses – Dissertation.	Small businesses must balance cybersecurity readiness and resilience to manage risks and maintain operations during cyberattacks. Unprepared businesses face costly consequences from breaches, making it vital to enhance their cybersecurity posture. Key challenges included identifying what to protect and understanding common threats. The NIST Cybersecurity Framework offers valuable guidance for small businesses to integrate cyber threat prevention and response into their processes. U.S. government and non-profit initiatives, such as CISA's Cyber Essentials and NIST's Small Business Cybersecurity Corner, provided resources and training to help small businesses improve their cybersecurity strategies. These efforts support building a culture of cyber readiness and response to mitigate risks effectively.	Challenges
Armenia, S., Angelini, M., Nonino, F., Palombi, G., and Schlitzer, M. F.	2021	A dynamic simulation approach to support the evaluation of cyber-risks and security in-vestments in SMEs.	Development of a system dynamics methodology and tool (SMECRA—SME cyber-risk assessment) to support cybersecurity investment decisions for SMEs by evaluating cyber-risk and past investments. The tool can evaluate a SME's cybersecurity status and the impact of investments on an organisation's risk profile, thereby enhancing cybersecurity awareness.	Recommendations

Table 2-4: Search results Category 3: cyber-risk awareness SME

The perspectives from these studies presented a comprehensive view of the challenges and strategies for enhancing cybersecurity in SMEs. Quesada (2016) focused on compliance as a primary driver, but this approach may lead to a minimalistic and reactive cybersecurity posture that does not fully address the complexities of cyber threats. Muhirwe and White (2016) offered a complementary perspective by emphasizing the critical role of cybersecurity awareness in shaping behaviour and practices. Muhirwe and White (2016) argued that regular cybersecurity awareness activities, combined with formal training, are essential for enhancing cybersecurity within organisations. While the study of Muhirwe and White (2016) did not conclusively predict an organisation's cybersecurity awareness, it did establish a significant relationship between training and awareness, advocating for a balanced approach of both training and awareness initiatives, which can transform cybersecurity from a mere compliance issue into an ingrained organisational practice.

In contrast, Ashby et al. (2018) highlighted the critical role of leadership, suggesting that the direct involvement of board members, driven by regulatory requirements and experiences with cyber-risks, can elevate the importance of cybersecurity within the organisation. This perspective aligns with Eilts (2020), who advocated for integrating cybersecurity into routine business activities.

The work of Armenia et al. (2021) contributed a systems-thinking approach to the debate by developing the SME cyber-risk assessment (SMECRA) tool. This dynamic simulation model could help SMEs evaluate cybersecurity investments and assess their impact on the organisation's risk profile. Armenia et al. (2021) argued that by using system dynamics, SMEs can better understand the interplay between various factors influencing their cybersecurity posture, which can lead to more informed decisions about where and how to invest in cybersecurity measures. This approach not only supports decision-making but also can enhance awareness by showing the tangible impact of investments on an organisation's risk profile.

Adding to this, Binkhorst (2020) offered valuable insights into cyber-risk communication using a mental model approach. His findings on the similarities and differences between experts' and laypeople's perceptions of VPN usage underscored the importance of understanding these mental models to design more effective risk communication strategies in cybersecurity. By improving risk awareness and resilience within SMEs, such strategies could bridge

the gap between technical expertise and layperson understanding, ultimately strengthening organisations' overall cybersecurity posture.

In summary, compliance is a necessary starting point, but as suggested by Quesada (2016), there is a need to supplement these practices with regular awareness activities and training, as advocated by Muhirwe and White (2016). The involvement of leadership in risk management, as emphasised by Ashby et al. (2018), is crucial for elevating cybersecurity to a strategic priority. Both Eilts (2020) and Armenia et al. (2021) added practical tools and methodologies for integrating cybersecurity into daily business operations and making informed investment decisions. Furthermore, Binkhorst (2020) highlighted the significance of tailored risk communication strategies that align with the mental models of various stakeholders to improve awareness and resilience. By combining these elements, SMEs can develop a robust, proactive, and sustainable cybersecurity strategy that goes beyond mere compliance and effectively mitigates risks. However, what remains unclear is the extent of this for manufacturing SMEs.

Table 2-5: Search results category 4: Cyber-risks - specific problems for SMEs				
Author(s)	Year	Title	Results	Subcategory
Stahl, B. C., Lichtenstein, Y., and Mangan, A.	2003	The limits of risk management: A social construction approach.	The traditional risk management approach was based on a flawed assumption about risk objectivity. This provides the managers with a false sense of security and can prevent them from addressing risks that could be unique to an organisation or a situation. It is therefore suggested that risks should be viewed as social constructions, as they are more suitable for dealing with both the positive and negative aspects of risk.	Challenges
Manuj, I., and Mentzer, J. T.	2008	Global supply chain risk management strategies.	The study explored risk management strategies in global supply chains (SCs), highlighting their higher risk compared to local SCs. The study proposes a five-step framework to assist managers in choosing risk management strategies. The framework categorised risk decisions into horizontal, vertical, and diagonal effects. Horizontal effects involve choosing multiple suppliers for critical components; vertical effects involve postponing supplier expectations; and diagonal effects involve opting out of a product line. The framework offers three main benefits: an integrated framework for managing global SC decisions, the use of multiple risk assessment tools for qualitative and quantitative analysis, and recognition of dynamic SC environments.	Challenges
Musa, S. N.	2012	Supply chain risk management: identification, evaluation and mitigation techniques	The study identified mitigating risks that are crucial for effectively managing supply chain risk (SCRM) and maintaining supply chain performance during disruptions. To understand the impact of risks on supply chains (based on make, source, and deliver operations), the performance measures for monitoring supply chains about material, financial, and information flows are identified, and three risk mitigation strategies were determined for improving system performances: (1) A dynamic pricing policy to balance supply and demand under supply yield risk. (2) A system dynamics model to assess disruption impacts and the effectiveness of dual-sourcing, information sharing, and order splitting in improving supply chain performance. (3) A study on capacity expansion using the Bass diffusion model, emphasising the importance of timing, sales planning, and initial inventories for managing risks in new product launches.	Challenges

Table 2-5: Search results category 4: Cyber-risks - specific problems for SMEs				
Author(s)	Year	Title	Results	Subcategory
Thompson, P. B.	2012	Ethics and risk communication.	Risk communication and "social interactions" may either amplify the level of clarity or vagueness in the way such mitigation strategies in turn are processed or interpreted. One source of ethical failure in risk communication lies in the inadequate theoretical understanding of ethically significant assumptions embedded in risk discourses.	Challenges
Renaud, K.	2016	How smaller businesses struggle with security advice.	The study found that SMEs express a need for advice and information but still suffer from a high level of uncertainty about security. Cybercriminals discount the risk of cyberattacks, which can have financial repercussions and impact long-term business. Official bodies attempt to help SMEs by transmitting threat messages and providing information about threat control mechanisms. SMEs should take four types of security measures: deterrent measures, preventive measures, corrective measures, and detection measures. The results showed that SMEs are uncertain about how to mitigate cybersecurity threats, and the uncertainty is caused by various institutions offering advice based on their own experiences. Larger companies may exclude SMEs that have experienced cyberattacks as suppliers.	Challenges
Renaud, K. and Weir, G.R.S.	2016	Cybersecurity and the Unbeatability of Uncertainty.	SMEs are aware of risks, but only a few take even basic measures. Cybercriminals are increasingly targeting SMEs due to their perceived weak defences, as it is believed that SMEs do not implement all necessary security measures to resist such attacks but only implement a small subset of available precautions. The study suggested that conflicting online advice from industry and official bodies causes uncertainty, hindering SMEs from taking necessary actions to improve their resilience. The conclusion was to recommend actions to better inform SMEs and help them secure their systems more effectively. Ultimately, the study suggested that SMEs should take the threat seriously and implement necessary security measures to protect their systems.	Challenges
Dayalan, M.	2017	Cyber-Risks, the Growing Threat.	Cyberattacks are not only limited to small organisations but also pose a threat to large corporations. Digital attackers frequently deceive SMEs into believing they are not under threat, but they are now focusing on them because they are easy to target, more vulnerable due to budgetary constraints, and have the potential to penetrate larger corporations. SMEs struggle with CRM because they are more susceptible to highly visible breaches. The main reasons for increased threats include a lack of cyber security policies, employee training, and recovery plans. SMEs must understand how to avoid attacks that continue to increase.	Challenges

Table 2-5: Search results category 4: Cyber-risks - specific problems for SMEs				
Author(s)	Year	Title	Results	Subcategory
Grocke, D.	2017	Emerging cybersecurity threats in large and small firms.	Nearly all organisations believe they have a suitable cybersecurity strategy in place, but less than 50% believe they have a cybersecurity strategy or controls that align with their business's needs. SMEs require dedicated CS plans to validate that the right tools are in place and are in alignment with critical business requirements. Therefore, SMEs are missing out on well-defined, documented, and measured readiness, response, and recovery systems and processes, as well as effective responses to complex cyber threats and vulnerabilities. Implementing software and tools that are not isolated or incorrectly positioned to enable rapid response and recovery through collaboration with service providers, partners, and customers can be very effective in addressing technical compliance and assisting in reporting against regulatory requirements.	Challenges
Kivimaa, K.	2017	How to increase SME's trust in Cloud Service Providers.	*MSc-Thesis – NOT further considered*	*None*
Osborn, E., and Simpson, A.	2017	On small-scale IT users' system architectures and cybersecurity: A UK case study.	Existing cybersecurity practices not well suited for needs of SMEs (small scale IT users [(SSITU]). SSITUs treated as consumers rather than partners in B2B interaction. Passwords are main key for SSITUs to influence cybersecurity, all other aspects managed by supply chain. Lack of OS updates for older handheld devices is a problem. Differences between micro (<10) and medium (10-249) employees. Medium companies have more control of their networks and devices. Organic development of IT infrastructure in mature companies was a problem (e.g., legacy devices).	Challenges
de Oliveira, L. S., Soares Echeveste, M. E., Cortimiglia, M. N., and Gularte, A. C.	2019	Open innovation in regional innovation systems: Assessment of critical success factors for implementation in SMEs.	The proposed framework aims to assist the enterprise in the Implementation Process of Open Innovation (IPOI), orienting them about the necessary resources, actions, and decision-making in the process. In addition, it provides managers with an understanding of the elements, critical success factors (CSF), and other determinants that impact the success of this strategy.	Innovation

Table 2-5: Search results category 4: Cyber-risks - specific problems for SMEs				
Author(s)	Year	Title	Results	Subcategory
Alahmari, A., and Duncan, B.	2020	Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence.	The questions of how to create cybersecurity behaviour on a company and employee level, how to build robust cybersecurity risk management (CRM), and how to avoid business disruptions after a successful cyberattack in SMEs was explored. Their review identified 5 major perspectives that play a key role in SMEs' CRM, which are threats, behaviours, practices, awareness, and decision-making, respectively. Their study confirmed other findings, such as SMEs' denial that cybercrimes pose actual threats to them in the modern era. SMEs are usually more vulnerable to the threat of cyberattacks because they adopt a low-cost approach using minimum cybersecurity, and in most cases, SMEs are suffering regarding CRM, specifically due to aspects of their managerial priorities and strategies.	Challenges
He, C. Z., Frost, T., and Pinsker, R. E.	2020	The impact of reported cybersecurity breaches on firm innovation.	The levels of innovation following a cybersecurity breach (CSB) as an important determinant of firm longer-term growth and profitability are investigated. The findings suggest a link between CSBs and future strategic decisions related to firm-level innovation and investment decisions.	Innovation
El Baz, J., and Ruel, S.	2021	Can supply chain risk management practices mitigate the disruption impacts on supply chains' resilience and robustness? Evidence from an empirical survey in a COVID-19 outbreak era.	The study examined the role of supply chain risk management (SCRM) in reducing disruption impacts on supply chain resilience during the COVID-19 pandemic. It uses structural equation modelling on survey data from 470 French companies. The resource-based view and organisational information processing theories, supported by the results, suggest that firms should develop interconnected SCRM practices to enhance their resilience. However, not all firms had the necessary resources, creating a decision dilemma for SC managers. The authors suggested that firms should build cooperation with other SC members to prepare for different disruption scenarios that a single firm cannot mitigate.	Challenges

Table 2-5: Search results category 4: Cyber-risks - specific problems for SMEs				
Author(s)	Year	Title	Results	Subcategory
Kalhoro, S., Rehman, M., and Ponnusamy, V.	2021	Extracting key factors of cyber hygiene behaviour among software engineers: A systematic literature review.	A SLR on cyber hygiene behaviour (CHB) was conducted to secure digital lives. They found that positive CHB factors include risk and threat awareness, self-efficacy, IoT devices, and awareness & training culture, while negative factors include theft, phishing, social and technical barriers, and low budget. The research suggested that organisations should adopt a practical approach to improve cyber hygiene practices, providing better protection, security, monitoring, and maintenance of software development organisations' networks. The study aimed to educate software engineers on the relationship between factors and cyber hygiene, enabling them to develop and maintain effective security systems. The study emphasizes raising knowledge and awareness of cyber hygiene among software engineers through employee training programs.	Challenges
Mlakar, I., Jeran, P., and Šafran, V.	2021	A Cost-Effective Security Framework to protect micro enterprises: PALANTIR e-commerce use case.	SMEs are targeted more frequently than large corporations. SMEs focus IT continuity rather than defending information resources. Use of own devices in SMEs/MEs reduces capital expenditures (CAPEX) but constitutes a risk. A cloud-based solution concept “security as a service” was suggested.	Cloud-based solutions
Pfeifer, M. R.	2021	IT security in SMEs—Threats and Chances for Supply Chains.	SMEs play a crucial role in value-creation in supply chains, but often struggle with resource constraints and IT security. Studies showed that SMEs often mistreat this field due to insufficient finances and human resource capabilities. Over 50% of companies were victims of IT attacks, and supply chains are attempting to mitigate these risks. As data exchange is essential for industry 4.0 and smart manufacturing, it is important for all supply chain members to protect this data. Blockchain technology, like Bitcoin, can enhance security in manufacturing, logistics, and supply chain data exchange, benefiting both SMEs and Large Entities.	Challenges
Strupczewski, G.	2021	Defining cyber-risk.	A comprehensive cyber-risk concept should encompass the source of cyber-risk, the object of cyber-risk, and the impact of cyber-risk. Therefore, the author proposed the following definition: "Cyber-risk is an operational risk associated with activities in cyberspace, threatening information assets, ICT resources, and technological assets, which may cause material damage to tangible and intangible assets of an organisation, business interruption, or reputational harm.”	Challenges

Table 2-5: Search results category 4: Cyber-risks - specific problems for SMEs				
Author(s)	Year	Title	Results	Subcategory
Hoppe, F., Gatzert, N., and Gruner, P.	2021	Cyber-risk management in SMEs: insights from industry surveys.	This study stated that SME's cyber-risk management (CRM) process needed to be constantly scrutinized. The results indicated that deficiencies in risk culture, as well as a strained market for IT experts, as there are major obstacles to the implementation of CRM in SMEs, and that these challenges are similar across countries. Also, the findings suggest that the relationship between cyber security culture (perception, knowledge, and attitude) and CRM is critical for a successful CRM.	Challenges
Mzileni, I and Ncubukezi, T.	2022	Impact of information security threats on small businesses during the COVID-19 pandemic.	This study examined the impact of information security threats on small businesses during the COVID-19 pandemic. A qualitative survey in South Africa showed a knowledge gap regarding information threats, despite most businesses being aware of their negative impact on operations. Some small businesses showed minimal awareness and understanding of information security threats, their impact, and proactive mitigation strategies. The study concluded with recommendations to protect against information security threats. The main measures taken by SMEs are passwords, firewalls, backup systems, and insufficient updates of antivirus or antispyware software. The study highlighted the need for more research on information security threats for small businesses.	Challenges
AL-Dosari, K., and Fetais, N.	2023	Risk-management framework and information-security systems for small and medium enterprises (SMES): A meta-analysis approach.	Established IT risk-management frameworks, such as NIST and ISO, were considered foundational but too focused on compliance rather than proactive security, making them less suitable for SMEs. The proposed risk-management tool assesses the dimensions of risk within the context of SME information systems. The research findings suggested that SMEs, despite their limited resources, can still implement a comprehensive risk management strategy by effectively managing the components of information democracy.	Challenges
Wang, J., Ho, C. Y. C., and Shan, Y. G.	2024	Does cybersecurity risk stifle corporate innovation activities?	The impact of cybersecurity risk on corporate innovation activities was investigated by reviewing risk-taking and precautionary savings. In summary, the study found that corporate innovation is negatively affected by cybersecurity risk, which can be explained by firms' precautionary savings and risk tolerance levels. Particularly affected are smaller and financially constrained firms in high-risk cybersecurity and technology-intensive industries.	Innovation

Table 2-5: Search results category 4: Cyber-risks - specific problems for SMEs

The above articles in Table 2-5 indicated a collective challenge to traditional risk management approaches, particularly in the context of supply chains, cybersecurity, and innovation. These studies highlighted the need for more dynamic, context-specific, and ethically aware strategies that account for the unique risks faced by different types of organisations, especially SMEs. The studies emphasised that risk management should be more than just a compliance exercise; it should integrate social, ethical, and strategic considerations to enhance resilience and innovation while effectively mitigating threats. In contextualising this, Stahl et al. (2003) critiqued the traditional risk management framework for its reliance on the assumption of risk objectivity, which they argue is fundamentally flawed. This approach, Stahl et al. (2003) suggested, can provide managers a false sense of security by treating risks as quantifiable and universally applicable entities, leading to a neglect of the unique risks that may arise in specific organisational contexts. Their proposition that risks should be viewed as social constructions offered a more nuanced understanding, emphasising that risk perception and management are influenced by social, cultural, and organisational factors. This perspective was crucial for addressing both the positive and negative aspects of risk, enabling organisations to adopt more tailored and context-sensitive risk management strategies.

Opponents of this view (e.g., Schlesinger, 2018, as noted in Table 2-7) argued that the social constructionist approach might add valuable insights, but it risks undermining the objectivity and rigour traditionally associated with risk management. Schlesinger (2018) therefore advocated for structured and objective risk management frameworks, such as those involving cyber-risk insurance governance. These frameworks focus on quantifiable measures of risk, which are crucial in manufacturing industries where precision and consistency are paramount, in contrast to the more subjective social constructionist perspectives.

In Identifying the challenges SMEs face in implementing effective cyber-risk mitigation, Strupczewski (2021) and Hoppe et al. (2021) both provided a definition of cyber-risk and emphasised the critical role of cyber security culture and the shortage of IT experts. Whereas Hoppe et al. (2021) defined CRM more from a cultural perspective, Strupczewski (2021) is more concrete, suggesting it should encompass operational risks associated with activities in cyberspace, threatening information assets, ICT resources, and technological assets, which may cause material damage to an organisation's tangible and intangible assets, business interruption, or reputational harm.

The perspective of fostering cybersecurity behaviour and culture at individual and organisational levels was emphasised by Alahmari and Duncan (2020) and Kalhoro et al. (2021) and aligns with existing arguments (e.g., Hoppe et al., 2021) about the importance of improving resilience. By identifying actionable factors like awareness, training, and risk perception, practical insights to enhance cybersecurity practices are added to the overall discussion.

Further, the topic of global supply chain risk management (SCRM) evolved. Earlier, Musa (2012) focused on SCRM, emphasizing the importance of identifying, evaluating, and mitigating risks to maintain performance during disruptions. The three key strategies identified were dynamic pricing, system dynamics modelling, and capacity expansion, which are aimed at balancing supply and demand, assessing disruption impacts, and managing risks during new product launches. Manuj and Mentzer (2008) contribute to the debate by proposing a structured framework for managing risks in global supply chains (SCs), which are inherently more complex and riskier than local SCs. The framework of Manuj and Mentzer (2008) categorises risk management strategies into horizontal, vertical, and diagonal effects, offering an integrated approach that combines qualitative and quantitative risk assessment tools. This structured approach is designed to help managers navigate the complexities of global supply chains by providing a clear methodology for decision-making. In recent years, criticism has come from El Baz and Ruel (2021), who contend that while Manuj and Mentzer's (2008) framework is comprehensive, it may be too rigid to adapt to the highly dynamic nature of global supply chains. The rapid pace of change in global markets, coupled with unpredictable external shocks like the COVID-19 pandemic, requires a more flexible and adaptive approach to risk management. El Baz and Ruel (2021), for instance, highlighted the importance of interconnected SCRM practices that can enhance resilience in the face of such disruptions. Furthermore, El Baz and Ruel (2021) argued that rigid frameworks may not fully capture the need for agility and cooperation among SC members to effectively mitigate risks in an ever-changing global environment.

The debate around cybersecurity, particularly for SMEs, and whether it is a persistent vulnerability reveals a significant gap in effective risk management practices. Renaud (2016) and Renaud and Weir (2016) highlight the challenges SMEs face due to conflicting advice from various sources, which creates uncertainty and hampers the implementation of robust cybersecurity measures. SMEs, often operating with limited resources and expertise (Mzileni

and Ncubukezi, 2022), are perceived as easy targets by cybercriminals, reinforcing the need for targeted strategies such as continuous training and regular updates to basic security measures to mitigate their vulnerability to cyberattacks.

This vulnerability is exacerbated by the lack of a comprehensive cybersecurity strategy that aligns with their specific needs and constraints. Dayalan (2017) and Grocke (2017) also discussed the growing threat of cyber-risks to both SMEs and larger corporations, noting that SMEs are particularly vulnerable due to budgetary constraints and lack of proper cybersecurity policies, making them easier targets for cyberattacks. Both Dayalan (2017) and Grocke (2017) stressed the need for SMEs to implement more robust security measures and align them with critical business requirements.

Bridging the gap between compliance and the adaptive, proactive measures required in SMEs, AL-Dosari and Fetais (2023) extended the discussion by criticising traditional compliance-focused frameworks (e.g., NIST, ISO) and instead offer tailored risk management tools for SMEs.

However, proponents of a more tailored approach, such as Mlakar et al. (2021), have suggested that cost-effective solutions like cloud-based "security as a service" models can help SMEs manage their IT continuity and cybersecurity needs without overwhelming their resources. However, some scholars, such as Hoppe et al. (2021), argue that these solutions, while useful, may not fully address the root causes of SMEs' vulnerability. Hoppe et al. (2021) identified the deficiencies in risk culture and the strained market for IT experts as major obstacles to effective CRM in small and medium-sized enterprises; to address this, they suggested that a fundamental shift in cybersecurity culture, coupled with better access to expertise, is necessary for SMEs to overcome these challenges.

The influence of cybersecurity risks on innovation and firm performance, particularly in SMEs, does add an additional layer of complexity to the debate. For de Oliveira et al. (2019), open innovation in SMEs is only possible when focussing on the critical success factors, which refer to the necessary resources and decision-making processes. Furthermore, Wang et al. (2024) argued that cybersecurity risks can stifle corporate innovation, particularly in smaller and financially constrained firms. The need for precautionary savings and the fear of potential breaches can lead to a more conservative approach to innovation, thereby hindering long-term growth and profitability. This view is supported by He et al. (2020), who found

that cybersecurity breaches can significantly impact a firm's strategic decisions related to innovation and investment. However, this perspective might be criticised for focussing too heavily on the negative aspects of cybersecurity risks. While such risks can constrain innovation, He et al. (2020) contended that this can also drive firms to innovate in ways that enhance their cybersecurity capabilities, potentially leading to the development of new products and services that strengthen their competitive position.

The academic debate on risk management outlines a clear tension between traditional, structured approaches and the need for more adaptive, context-sensitive strategies. While traditional risk management frameworks provided a valuable tool for standardising risk assessment and decision-making, these are increasingly being challenged by approaches that recognise the social construction of risk, the dynamic nature of global supply chains, and the unique challenges faced by SMEs in the cybersecurity domain.

To address these challenges, a more integrated approach to risk management is needed, one that combines the rigour of traditional methods with the flexibility and adaptability required in today's complex and rapidly changing environment. This approach should also incorporate a stronger emphasis on ethical considerations, as highlighted by Thompson (2012), who focused on building a robust cybersecurity culture, particularly in SMEs, as suggested by Hoppe et al. (2021). Also, as part of the cybersecurity culture, Osborn and Simpson (2017) highlight the problems associated with outdated devices and organically developed in-house IT infrastructures.

Further temporal and/or situational strategies to enhance cyber resilience for individual and organisational resilience were presented by Kalhoro et al. (2021) on cyber hygiene practices and Mzileni and Ncubukezi's (2022) focus on the COVID-19 pandemic's impact on SMEs. Both insights emphasised the importance of dynamic and adaptive measures during global disruptions.

In summary, the evolving perspectives on risk management underscore the importance of moving beyond one-size-fits-all solutions. By embracing a more holistic and adaptive approach, organisations can better navigate the risks they face, enhance their resilience, and continue to innovate in a rapidly changing world.

Table 2-6: Search results category 5: Cyber-risk mitigation measures in SMEs				
Author(s)	Year	Title	Results	Subcategory
Osborn, E., & Simpson, A.	2015	Small-scale cyber-security.	Cyberspace is constantly evolving, and threats are increasing. Cybersecurity experts focus usually on high-value assets. SMEs, also known as small-scale IT users (SSITU), often receive insufficient attention. SSITUs intersect with large enterprises (LE). The authors suggested that the research community should consider small-scale cyber security, a cross-disciplinary problem, as it could be a potential backdoor to larger companies.	Challenges
Such, J. M., Vidler, J., Seabrook, T., and Rashid, A.	2015	Cyber-security controls effectiveness: a qualitative assessment of cyber essentials.	Analysis of Cyber Essentials tools used in SME networks. The results showed that timely update of patches is essential. Periods of vulnerability between patch release and update installation. Aside from use of software tools employee training is essential. Some hardware and software must be considered inherently flawed. These constitute unmitigable risks and need to be removed. A list of such hardware and software should be used and updated within SME networks. SMEs should partake in collective cybersecurity activities, for example: Cyber-security information sharing network.	Collective approach
Mijnhardt, F., Baars, T., and Spruit, M.	2016	Organisational characteristics influencing SME information security maturity.	Standard norms such as the ISO 27000x series are considered overly complicated for SMEs, leaving these organisations with no easy-to-understand toolkit to address their security needs. A Characterizing Organisations' Information Security for SMEs (CHOISS) model to relate measurable organisational characteristics in four categories (General, In & Outsourcing, IT Dependency, and IT Complexity), 11 organisational characteristics, and measured through 47 parameters is proposed to help SMEs in cyber-risk assessment and implementing cyber-risk mitigation measures. The authors argued for simpler guidelines that support SMEs' cyber-risk assessment and mitigation measures, while not qualifying for ISO certification. This research builds upon the Information Security Focus Area Maturity (ISFAM) model for SME information security.	Assessment tools
Nykänen, R., and Kärkkäinen, T.	2016	Supporting cyber resilience with semantic wiki.	The proposed semantic wiki-based approach for SMEs to manage information security risk knowledge within organisations offers a technical platform for controlled cyber security risk management. This platform, based on the NIST SP 800-53 control catalogue, provided a low barrier for SMEs lacking extensive cyber security skills to exclude irrelevant risks and controls. The semantic search functions assist in identifying risks with significant cascading effects on availability. However, the current metamodel has limitations, such as the exclusion of assets and countermeasures that are linked through vulnerabilities and threats. A centralised repository for threats and vulnerabilities was be considered, and incident management elements should be linked to assets and risks. Essentially, this is another approach towards collective cybersecurity.	Collective approach

Table 2-6: Search results category 5: Cyber-risk mitigation measures in SMEs				
Author(s)	Year	Title	Results	Subcategory
Pawar, S.A.	2016	Business domain specific least cybersecurity controls implementation (BDSLCCI) framework for small and medium enterprises.	This research study identified gaps in SMEs' cybersecurity implementation and suggested implementing step-by-step strategies to prevent hacking. Main obstacles for SMEs are: (i) costs to implement cybersecurity controls, (ii) lack of resources for implementation and maintenance, (iii) not finding a roadmap to invest in cybersecurity control implementation, and (iv) available cybersecurity standards or frameworks need a big investment. The study also emphasised the importance of unique compliance requirements for the domain. Essentially another "collective" approach by making existing knowledge available to SMEs.	Collective approach
Saber, J.A.	2016	Determining small business cybersecurity strategies to prevent data breaches – Dissertation.	This qualitative case study explored cybersecurity strategies implemented by small business leaders to protect their systems from data breaches. The study identified three themes: policy, training, and technology. The policy concentrated on data protection and external threats; the training focused on employee awareness and training; and the technology focused on cyber warfare and cloud-based companies. The importance of a cybersecurity strategy that enforces the least privilege and encourages open data access is emphasized. SMEs should use cloud computing services to avoid the need for in-house servers and remove the burden of data protection, which becomes the responsibility of the cloud provider.	Cloud-based solutions
Bell, S.	2017	Cybersecurity is not just a 'big business' issue.	Recommendations for SMEs to develop CS strategies based on National Institute of Standards and Technology (NIST) cybersecurity framework (Proactive: Identify - Protect. Reactive: Detect, Respond & Recover) Flat hierarchies and short communication are advantages of SMEs. Resilience as main concept. Eight essential elements: Application whitelisting; Disabling of untrusted MS Office macros, application patching, User application hardening (disabling of Adobe Flash Player and untrusted Java), restrict administrative privileges, multi-factor authentication, patching of OS, daily back-ups.	Recommendations

Table 2-6: Search results category 5: Cyber-risk mitigation measures in SMEs				
Author(s)	Year	Title	Results	Subcategory
Kapoor, K., Renaud, K., and Archibald, J.	2018	Preparing for GDPR: helping EU SMEs to manage data breaches.	The study identified three main issues hindering SMEs' effective response to data breaches, despite their size and limited resources. The first issue is an overemphasis on technical security measures, which persists even in the face of increased human involvement in information security. The second issue was the lack of consistent response, causing stress for employees. The third issue is a lack of a mechanism for learning from previous data breach events and responses. The suggested framework proposes simple guidelines and develops a step-by-step approach for SME-specific GDPR compliance. Security breaches should always be expected. Specific measures before breach, during breach response, and after breach response. Documentation of all steps and communication with stakeholders is essential.	Recommendations
Osborn, E., and Simpson, A.	2018	Risk and the small-scale cyber-security decision making dialogue—a UK case study.	SMEs (SSITUs) seek easy to use solutions. Interviews showed low awareness about risks and available resources, lack of threat intelligence. SMEs face difficulties meeting cybersecurity (CS) expectations of larger enterprises in supply chain. CS problems are reputational risk. Protection of customer and supplier data, IP protection, potential customer loss use of social media as motives for engaging with CS. Other problems: mix of private and professional use of devices, change between private and office networks, BYOD policies. This paper suggested risk assessment-based approach to CS.	Challenges
Ajuzie, G.	2019	Cybercrime prevention among small businesses in the greater Houston area: A qualitative exploratory case study – Dissertation.	The study aimed to explore the experiences of small business owners in the Greater Houston area who had been victims of cybercrime. The focus was on preventing cybercrime, identifying cyberattacks, and coordinating effective strategies to combat cybercrime. The study indicated that small business owners should collaborate with law enforcement agencies to be more resilient in identifying cyberattacks, preventing security breaches, and coordinating to mitigate cybercrime from affecting the overall business. One of the findings of the journal was the collaboration with other organisations is essential for a successful cyber security policy, as it slows down cybercrime activities and makes perpetration more expensive. The cooperation with public institutions and collective approaches to cybercrime prevention were identified as potential solutions.	Collective approach

Table 2-6: Search results category 5: Cyber-risk mitigation measures in SMEs				
Author(s)	Year	Title	Results	Subcategory
Consoli, A., and Kovatcheva, E.	2019	Cybersecurity Training for SME: Filling the Gap or Corporate Strategy?	The exponential connection of devices to the Internet and new online services exacerbates security issues, with cyberattacks posing a significant threat to economies. SMEs require support and awareness about potential risk exposure and problems caused by unsecured networks. A curriculum design for cybersecurity training for learners ranging from teenagers to seniors using a design thinking approach is proposed. The learning process includes empathy, problem definition, ideation, prototype development, and testing. The Erasmus+ project REDucing the CYBERsecurity Management Skills Gap in SMEs focusses on cybersecurity risk management, with six modules designed and developed for distance learning. The modules will follow common frameworks and be enriched by scenarios selected by consortium partners to cope with the challenges relating to cybersecurity, particularly for SMEs.	Training program
Dimitrov, W., and Rasheva-Yordanova, K.	2019	Toward Overcoming The Disproportion Between The Demand For Professionals And The Provision Of Training In Cybersecurity.	The study was focused on identifying the existing disproportion in the supply and demand of cybersecurity professionals in SMEs, focusing on the need to regulate security measures in the digital world. It analyses cybersecurity competence frameworks, considering regulatory requirements of Europe and some national ones. The goal is to reduce deficits in training cybersecurity experts in educational structures and fill the gap of SME cyber security expertise. This is a step towards implementing the EU's common competences for cybersecurity skills in the SME sector, promoting technical and organisational expertise and corporate culture to comply with emerging regulations, directives, and laws related to cybersecurity and privacy and confidentiality. Identification of qualification profiles for different roles at different levels in CS and distinction between CS qualification courses and CS master's programmes.	Training program
Rae, A., and Patel, A.	2019	Defining a new composite cybersecurity rating scheme for SMEs in the UK.	Due to the experienced increase in cyberattacks, a cybersecurity risk rating system for UK SMEs was developed. Despite the government's publication of cyber threats, most SMEs did not undergo certification. This paper examined the disconnect between cyber threats and SMEs' current security postures and perceptions, identifying factors for improving security behaviours and engagement with best practices. The authors proposed a new foundational composite cybersecurity rating scheme for SMEs in the UK, which measures security behaviours, perceptions, and risk propensity. The scheme, based on behavioural and technical audits, provides higher insight, engagement, and accuracy into an SME's individual security posture.	Assessment tools

Table 2-6: Search results category 5: Cyber-risk mitigation measures in SMEs				
Author(s)	Year	Title	Results	Subcategory
Benz, M., and Chatterjee, D.	2020	Calculated risk? A cybersecurity evaluation tool for SMEs.	A methodology for SMEs to assess SMEs cybersecurity risk and resilience using the National Institute of Standards and Technology's Cybersecurity Framework (CSF) was presented. The tool, which consists of a 35-question online survey, aims to help IT-leaders self-rate their maturity within the five categories of the NIST framework: identify, protect, detect, respond, and recover. The self-evaluation tool (cybersecurity evaluation tool, CET) is also for SME-managers to rate the company's caber maturity in NIST framework categories.	Assessment tools
Consoli, A., Kovatcheva, E., Nesurini, A. M., and Siarova, S.	2020	Cyber-security awareness for SME managers.	SMEs must address risks in information security to ensure business continuity and avoid financial, reputational, and other losses when using new technologies in businesses. To achieve this, vocational education training was developed. The project phases include identifying skill gaps in cybersecurity management, identifying competencies to close these gaps, creating a competence framework, and designing and developing training modules. The project phases also involve identifying the market, ensuring compliance with cybersecurity laws and legislation, identifying cybersecurity risks, analysing these risks in SMEs, prioritising these risks, responding to these risks, and monitoring these risks. The developed training provides awareness of cybersecurity among SMEs and tries to increase the awareness level with organisational measures.	Training program
Idahosa, M. D.	2020	Strategies for Implementing Successful IT Security Systems in Small Businesses – Doctoral Dissertation.	This study explored strategies used by small business owners in Florida to protect confidential company data from cyberattacks. The research involved semi structured interviews and a review of relevant company documents. Thematic analysis revealed four themes for protecting business data against cyberattacks: security information management strategy, organisational strategy, consistent security policy, and cybersecurity risk management strategy. The findings suggested that small business owners could develop an organisational strategy by incorporating procedures for protecting and responding to cyberattacks. This could lead to increased customer confidence, economic growth, and employment gains for residents within the community.	Assessment tools

Table 2-6: Search results category 5: Cyber-risk mitigation measures in SMEs				
Author(s)	Year	Title	Results	Subcategory
McLilly, L.	2020	Exploring a Cost-Benefit Cloud-Based On-Demand Cybersecurity Service Solution for Small Businesses: A Quantitative Examination.	The small business sector is facing challenges in cybersecurity due to the rise of cybercrimes and limited funding. Only 4% of small business owners have implemented all US Small Business Administration's cybersecurity best practices. Security as a service (SECaaS) providers struggle to scale down to meet the diverse and dynamic cyber security needs of millions of small businesses. A cloud-based on-demand cybersecurity service system (CODCSSSB) as a cost-effective solution was proposed. The research used data analysis to evaluate all relevant use cases and identify failures in CODCSSSB, allowing the system to quickly fail requests without wasting resources and time. This quantitative examination approach validated security service requests and identifies design weaknesses with low development time and accuracy.	Cloud-based solutions
Ncubukezi, T.	2020	A proposed integration of the Monte Carlo model and the Bayes network to propose cyber-security risk assessment tool for small and medium enterprises in South Africa.	Cyber-risks pose a significant threat to SMEs in South Africa, as they can harm information assets and potentially quantify cybersecurity crimes. While cybersecurity is a legal requirement for large corporations, it remains unclear whether SMEs have a clear framework in place to combat these risks. The study recommended that SMEs use a cyber-risk assessment tool that integrates a Monte Carlo simulation tool with artificial intelligence to proactively respond to cybersecurity risks. The proposed tool is aiming to predict risk cause, impact, likelihood, and systematic trends. Also, identification of common cyber-crimes and their impact on SME's, examination of dependent and independent cyber-risks, and developing a cyber-framework using the Bayesian model are part of the proactive cybersecurity risk response plan for SMEs in South Africa.	Cloud-based solutions
Schmitz, C., and Pape, S.	2020	LiSRA: Lightweight Security Risk Assessment for decision support in information security.	A cybersecurity (CS) risk assessment tool was developed, tailored to the needs of SMEs. Framework is based on four phases: Domain expert input develops domain-specific attack trees. Users input the maturity of company-specific CS control measures. Based on these, company-specific risk is computed. Eventually recommendations for security measures are provided.	Cloud-based solutions

Table 2-6: Search results category 5: Cyber-risk mitigation measures in SMEs				
Author(s)	Year	Title	Results	Subcategory
Armenia, S., Angelini, M., Nonino, F., Palombi, G., and Schlitzer, M. F.	2021	A dynamic simulation approach to support the evaluation of cyber-risks and security investments in SMEs.	The authors criticised the static view of an organisation's cyber posture by utilising self-assessment frameworks, particularly for SMEs, who often lack the necessary skills or resources to effectively manage and invest into their cybersecurity. Therefore, a system dynamics methodology and tool (SMECRA—SME Cyber-Risk Assessment) to support cybersecurity investment decisions for SMEs by evaluating cyber-risk and past investments was developed. The tool has the capacity to evaluate a SME's cybersecurity status and the impact of investments on an organisation's risk profile, thereby enhancing cybersecurity awareness. The tool is useful for SMEs that wish to manage their own cybersecurity risk, as well as for insurance companies in their economic evaluation of residual risks that SMEs wish to externalise.	Assessment tools
Aurelien, J.	2021	Exploring Effective Defensive Cybersecurity Strategies for Small Businesses.	The research interviewed 10 IT leaders to examine the defensive security strategies small businesses need to employ to safeguard their information assets. Implementing effective strategies is crucial against the rapid evolution of sophisticated cyberattacks. Small businesses often fall into cyber security nihilism, downplaying cyberattacks and becoming targets for cybercriminals. The study's findings revealed commonalities among small enterprises, which could inform future strategic decisions for a robust defensive security posture. The findings could help decision-makers improve the security landscape for small businesses, addressing the unique requirements of their businesses. The findings could assist in making strategic decisions to improve the security landscape for small businesses.	Recommendations
Boletsis, C., Halvorsrud, R., and Pickering, J. B.	2021	Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment.	This study aimed to improve cybersecurity awareness and communication among IT personnel, security experts, and non-technical personnel in SMEs. By using a user journey approach, the researchers model human behaviour and visually map SMEs' practices and threats, while visualising the socio-technical actor network. The study used two modelling languages: Customer Journey Modelling Language (CJML) and System Security Modeller (SSM), which are used to model and visualise work processes in terms of user journeys. The context-specific model visualisations optimize perceived job characteristics, enhancing autonomy and encouraging intrinsic motivation and psychological ownership of cybersecurity for all actors within the complex socio-technical systems described by the SMEs interviewed.	Assessment tools

Table 2-6: Search results category 5: Cyber-risk mitigation measures in SMEs				
Author(s)	Year	Title	Results	Subcategory
Carías, J. F., Arriza-balaga, S., and Labaka, L.	2021	Cyber resilience self-assessment tool (CR-SAT) for SMEs.	SMEs face significant cyber threats, which require robust cyber resilience capabilities to mitigate risks and minimise disruption. However, due to limited resources, SMEs often lack dedicated personnel for operationalising these capabilities. This article developed and tested a web-based tool to help SMEs follow a systematic process for operationalising or implementing cyber resilience. The tool includes a cyber resilience framework with essential policies, a progression model, and prioritisation of these policies. The framework, progression model, and prioritisation are transformed into a cyber resilience self-assessment tool (CR-SAT) and tested in three case studies to evaluate its usefulness, completeness, and improvement based on end-user feedback.	Assessment tools
Mlakar, I., Jeran, P., and Šafran, V.	2021	A Cost-Effective Security Framework to protect micro enterprises: PALANTIR e-commerce use case.	The PALANTIR framework was designed to help SMEs to secure their infrastructure. It provides a Risk Assessment platform for informed cybersecurity investment decisions. The platform used advanced AI models in SecaaS mode to protect infrastructure and resources, utilising threat sharing. The Remediation Engine offers a tailored solution for policy design, ensuring cost-efficiency in achieving and maintaining adequate protection levels. Overall, PALANTIR offers a cost-effective solution for SMEs.	Assessment tools
Pfeifer, M. R.	2021	IT security in SMEs—Threats and Chances for Supply Chains.	In the study, SMEs overestimate their preparedness. SMEs lack finances and human resources for state-of-the-art measures. CS is also a supply chain security issue. Block chain may provide a framework for better supply chain security. There is a need for better CS management in SMEs.	Challenges
Tam, T., Rao, A., and Hall, J.	2021	The good, the bad and the missing: a narrative review of cyber-security implications for Australian small businesses.	SMEs face resource constraints, process organisation legal structures and know-how issues in the context of CS. Their advantages are agility, large cohort-size and decentralised IT structure. Alliances between SMEs could assist intelligence support and threat information. Zero Trust Model as a potential solution (i.e., protection of each service rather than strong perimeter and weak internal protection).	Recommendations

Table 2-6: Search results category 5: Cyber-risk mitigation measures in SMEs				
Author(s)	Year	Title	Results	Subcategory
Brown, S., Fox, S., Hewage, C., and Khan, I.	2022	Threat modelling of cyber physical systems: A real case study based on window cleaning business.	Analysing the potential threats related to use of IoT-devices by an SME, the study was based on DREAD (damage, reproducibility, exploitability, affected users and discoverability) risk assessment model. This study demonstrated how a systematic approach can assist with identification of risks.	Recommendations
Mthiyane, Z. Z. F., Poll, H. M. v. d., and Tshehla, M. F.	2022	A Framework for Risk Management in Small Medium Enterprises in Developing Countries.	In development of an overall enterprise risk management framework for small enterprises, with cybersecurity (CS) as one element of this. SMEs lack resources for sophisticated CS management. Outsourcing was suggested as one potential approach.	Recommendations
Zeiringer, J. P., Durst, S., and Thalmann, S.	2022	Show Me What You Do and I Will Tell You Who You Are: A Cluster Typology of Supply Chain Risk Management in SMEs.	Analysis of SMEs' supply chain risk management strategies. Identification of five different types of SMEs' risk management strategies: Collective risk eliminators (risks seen as threat and eliminated if possible), collective playing it safe seekers (risks seen as difficult to manage, insurance preferred), collective risk-ignoring knights of fortune (little attention to risks, mostly micro-enterprises), collective neglecting imperturbable ones (unresponsive attitude towards risks, little risk assessment).	Challenges

Table 2-6: Search results category 5: Cyber-risk mitigation measures in SMEs

Osborn and Simpson (2015, 2018) and Rae and Patel (2019) initiated discussions on risk assessment approaches tailored to the specific needs of SMEs. Osborn and Simpson (2015, 2018) emphasised simple, user-friendly solutions designed for small-scale IT users (SSITUs), addressing SME's unique vulnerabilities as potential entry points into larger enterprise networks. Their work underscored the importance of integrating SMEs into broader cybersecurity frameworks to strengthen overall security. Rae and Patel (2019) criticised existing frameworks as too static and disconnected from real-world security behaviours and perceptions within SMEs. They proposed a composite cybersecurity rating scheme combining behavioural and technical audits, offering a dynamic and context-sensitive tool for assessing SME's security postures. This approach challenged traditional models, like those of Osborn and Simpson (2015, 2018), which emphasised theoretical frameworks over practical engagement.

Ncubukezi (2020) advanced the discussion by recommending a cyber-risk assessment tool that integrates Monte Carlo simulations with artificial intelligence, aiming to predict the cause, impact, likelihood, and trends of cybersecurity risks. In the same way, Armenia et al. (2021) solved problems with static self-assessment frameworks by creating SME Cyber-risk Assessment (SMECRA), a flexible tool that checks cybersecurity risks and the effects of investments. SMECRA employs a system dynamics methodology to assess an SME's cybersecurity status, support decision-making, and enhance awareness, benefiting both SMEs managing their risks and insurance companies evaluating residual risks.

Complementing these approaches, Schmitz and Pape (2020) introduced a Lightweight Security Risk Assessment (LiSRA) for decision support in information security, a framework tailored to SMEs. This tool uses a four-phase process involving domain-specific attack trees, company-specific control maturity assessments, and risk computations to provide actionable security recommendations. Schmitz and Pape's work aligns with the dynamic and technical methodologies of Rae and Patel (2019) and Ncubukezi (2020), reinforcing the need for practical, SME-focused tools. In this overall discussion, models and frameworks for dynamic, practical, and socio-technical approaches to SME cybersecurity are examined; also, Boletsis et al. (2021) emphasise context-sensitive, dynamic, and user-centric frameworks.

Mlakar et al. (2021) added to these discussions by introducing the PALANTIR framework, a cost-effective security solution designed to protect SMEs, particularly micro-enterprises. The

framework uses a risk assessment platform and advanced AI models in a SecaaS mode to secure infrastructure and resources, while its remediation engine ensures cost-efficiency and tailored policy design. This method goes along with McLilly's (2020) focus on cloud-based solutions and Armenia et al.'s (2021) focus on making risk-informed investment decisions. It shows how important it is for small businesses to have cybersecurity tools that are easy to access and can grow as needed.

Brown et al. (2022) contributed to the discussion by focusing on threat modelling in cyber-physical systems, specifically in the context of SMEs using IoT devices. Using the DREAD risk assessment model (damage, reproducibility, exploitability, affected users, and discoverability), the study analysed the risks in a real-world SME case involving a window cleaning business. Their results showed that a methodical approach can help small businesses find and understand IoT risks, which become more important as they adopt connected technologies. This paper adds to the focus on useful frameworks seen in Rae and Patel (2019) and Schmitz and Pape (2020), showing how important it is to use specific methods to evaluate new technological risks.

Mthiyane et al. (2022) expanded the discussion by addressing enterprise risk management (ERM) frameworks for SMEs in developing countries, incorporating cybersecurity as a critical element. Given SMEs' resource limitations, the study highlighted outsourcing as a viable strategy to manage sophisticated cybersecurity needs effectively. This aligns with earlier calls for practical solutions tailored to SMEs' constraints, such as those of Saber (2016) and McLilly (2020).

In examining the complexity of cybersecurity models, Mijnhardt et al. (2016) argued that existing standards, such as the ISO 27000x series, are overly complex and unsuited to SMEs. They proposed the CHOISS model, which simplifies risk assessment by focusing on measurable organisational characteristics and shifting away from overly technical standards toward accessible, actionable guidelines. Benz and Chatterjee (2020), however, developed an alternative approach by adapting the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF) into a self-evaluation tool. This tool enables SMEs to assess their cybersecurity maturity across the framework's five categories. Bell (2017) similarly emphasised the relevance of the NIST framework for SMEs by proposing strategies that balance

proactive measures (e.g., identifying and protecting assets) with reactive measures (e.g., detection, response, and recovery). Bell (2017) listed eight important resilience measures that can be tailored to the structures and abilities of small businesses, including application whitelisting, disabling untrusted macros, and multi-factor authentication.

Such et al. (2015) advocated for collective approaches to cybersecurity, emphasising timely patch updates, employee training, and the importance of information-sharing networks. Pawar (2016) complemented these ideas by proposing the BDSLCCI framework, which offers domain-specific strategies and a step-by-step roadmap to help SMEs implement cybersecurity controls effectively. Idahosa (2020) extended this discussion by exploring organisational and policy-driven strategies and identifying key themes, such as security information management, risk management, and consistent security policies. These approaches not only strengthen SME's defences but also contribute to broader socioeconomic outcomes. Aurelien (2021) built on this focus by addressing the risks of cybersecurity nihilism and advocating for defensive strategies to improve SMEs' cybersecurity readiness through strategic decisions and organisational efforts.

On the technological front, McLilly (2020) emphasised a cloud-based, on-demand cybersecurity solution for SMEs, addressing economic constraints and scaling issues. Saber (2016) similarly advocated for leveraging cloud services to offload data protection responsibilities from SMEs to specialised providers. Kapoor et al. (2018) expanded on this by focusing on GDPR compliance, proposing simple, step-by-step guidelines for managing data breaches. They identified three main obstacles for SMEs: an overemphasis on technical measures, inconsistent response strategies, and a lack of mechanisms for learning from past breaches. Kapoor et al.'s framework stresses the importance of preparation, documentation, and stakeholder communication before, during, and after breaches. Nykänen and Kärkkäinen (2016) gave a different technological view by suggesting a semantic wiki-based platform for handling cybersecurity risks. This platform would use a structured approach to avoid unnecessary risks and make handling cybersecurity easier for small businesses. This contrasts with Saber's (2016) cloud-based approach, which emphasises leveraging existing technologies to offload responsibilities rather than introducing new tools.

In the realm of training and awareness, Ajuzie (2019) highlighted the importance of collaboration with law enforcement and other organisations to mitigate cybercrime, particularly for

resource-constrained SMEs. Consoli et al. (2020) emphasised training as a cornerstone of cybersecurity readiness, focussing on filling skills gaps to prepare SME managers for emerging threats. Dimitrov and Rasheva-Yordanova (2019) addressed the shortage of cybersecurity professionals in SMEs, advocating for regulated competency frameworks to align training with demand. They proposed developing qualification profiles and distinguishing between basic and advanced training programmes to strengthen SME expertise and meet regulatory requirements. Finally, regarding supply chain security, Tam et al. (2021) discussed the advantages of decentralised IT structures and alliances among SMEs, suggesting that a Zero Trust Model could effectively protect individual services. Pfeifer (2021) and Zeiringer et al. (2022) emphasised the interconnectedness of SMEs in supply chains, warning that security vulnerabilities in one SME could cascade across the network. Pfeifer proposed blockchain frameworks for secure supply chains, while Zeiringer et al. classified collective approaches to managing supply chain risks.

In summary, the academic debate on SME cybersecurity reflects a spectrum of approaches, from practical, cost-effective solutions like McLilly (2020), Saber (2016), Mlakar et al. (2021), and Brown et al. (2022) to complex, model-driven frameworks such as Rae and Patel (2019) and Mijnhardt et al. (2016). The contrast between collective strategies, as advocated by Ajuzie (2019) and Such et al. (2015), and individualised or technological solutions, like those of Nykänen, Kärkkäinen (2016), and McLilly (2020), highlights the ongoing struggle to balance theoretical rigour with practical applicability. Ultimately, these discussions underscore the need for tailored, scalable solutions that address SMEs' diverse needs while ensuring robust cybersecurity practices that adapt to the evolving threat landscape.

Table 2-7: Search results category 6: Cyber-risk insurance				
Author(s)	Year	Title	Results	Subcategory
Freund, J., and Jones, J.	2014	Measuring and managing information risk: a FAIR approach.	The quantitative Factor Analysis of Information Risk (FAIR) methodology aids managers in making more informed business choices by comprehending their organisation's risk and potential losses, which can be distinguished in: • Primary loss flows, which are productivity and replacement costs and • Secondary losses are competitive advantage, fines and judgements, and reputation.	Recommendations
Malhotra, Y.	2015	Risk, Uncertainty, and Profit for the Cyber Era: Model Risk Management of Cyber Insurance Models Using Quantitative Finance and Advanced Analytics.	The study investigated the reliance on value-at-risk (VaR) as the primary model for cyber-risk insurance modelling and revealed that VaR has limitations in modelling tail and systemic risks. The study creates qualitative frameworks to compare the relative levels of tail and systemic risks that come with cyber-risk to financial risks that are usually modelled with VaR. The analysis revealed that cyber-risk entails exponentially higher tail risks and systemic risks, making VaR unfit for reliance as the primary risk model for cyber-risk insurance modelling. The study also presented an alternative coherent risk measures as superior alternatives to VaR and empirically demonstrates their application.	Risk assessment
Rejda, G. E., and McNamara, M. J.	2017	Principles of Risk Management and Insurance.	As to cyber liability insurance the study found two standard coverage approaches are discussed: (1) stand-alone cyber liability insurance forms and (2) a cyber liability endorsement that can be added to a business owner's policy or to a policy packaging management liability coverage. These coverages include protection against liability from data breaches, the cost of responding to such breaches, restoration costs, and business income.	Coverage
Nieuwesteeg, B., and Waard, B. d.	2018	The law and economics of cyber insurance contracts: a case study.	Analysis of insurance companies' strategies regarding cyber-risk insurance (CRI). Prices and coverages are difficult to compare. SMEs are reluctant to buy CRI due to high prices. Coverage is not standardised; little use of incentives for moral hazard measures; little claim data, few inferences as regards effectiveness of risk reduction measures.	CRI challenges

Table 2-7: Search results category 6: Cyber-risk insurance				
Author(s)	Year	Title	Results	Subcategory
Radanliev, P., De Roure, D., Cannady, S., Mantilla Montalvo, R., Nicolescu, R., and Huth, M.	2018	Analysing IoT cyber-risk for estimating IoT cyber insurance.	This paper explored the evolution of the Internet of Things (IoT) and its associated cyber-risks for the Industry 4.0 sector. The findings lead to the development of a new impact assessment model for IoT cyber-risk in Industry 4.0, but also identify challenges in understanding the types and nature of cyber-risks and their dependencies in this new space. The study introduces new risk metrics and identifies challenges in calculating the economic impact of IoT cyber-risk but admits that there is not enough data to come up with precise values yet.	Risk assessment
Schlesinger, M.	2018	Optimal Models for Cyber Insurance for the SME/SMB Markets.	To protect data, networks, and computers from cyberattacks, organisations must conduct reviews and implement solutions. A model for SMEs involves a Cyber Governance assessment to identify areas of deficiency and recommend the best course of action. Achieving cyber resilience can transform risk into an opportunity, giving an organisation an advantage over competitors. Good practices include reviewing or implementing a Risk Management System, creating a Business Continuity Plan, and having a Data Breach Notification Plan. Cyber-risk insurance should be a part of an organisation's board charter next to other types of insurance for assets or events.	CRI challenges
Franke, U., and Meland, P. H.	2019	Demand side expectations of cyber insurance.	Analysis of coverage expectations in cyber-risk insurance in different domains. In manufacturing, transport, IT and media, business interruption (BI) considered most important. In finance and retail loss of customer data and related lawsuits are most important issue. This differs from claims, in which incident response was most common (61%) and business interruption only constitute 4%. BI relevant in the context of ransomware attacks and cloud service outages. Latest risk is crypto-jacking or crypto-mining malware (i.e., processing capacity is “stolen”), which is considered large-scale/low-impact threat.	Coverage
Kavčič, T., and Delak, B.	2019	State of the cyber insurance products within Slovenian insurance companies.	Cyber-risk insurance is a crucial strategy for mitigating cyber threats and attacks. It protects companies and individuals from internet, Internet of things, and information technology infrastructure risks. The US accounts for 85% to 90% of the cyber-risk insurance market, while Europe accounts for 5% to 9%. However, smaller countries like Slovenia struggle to raise cyber-risk awareness and the survey revealed that only a few insurance companies offer cyber-risk insurance products. Insurers evaluate cyber-risk is estimated based on clients’ self-assessments (questionnaires); available offers cover data loss and liability for breaches of confidentiality (legal costs).	Coverage

Table 2-7: Search results category 6: Cyber-risk insurance				
Author(s)	Year	Title	Results	Subcategory
Cartagena, S., Gosrani, V., Grewal, J., and Pikinska, J.	2020	Silent cyber assessment framework.	The huge development of IT has created a digitally interconnected world, requiring more reliance on IT systems for process management. This has led to new insurance products and coverage, but also changes the risk landscape for non-life insurance classes. This risk is known as non-affirmative cyber-risk. Contract wordings often remain silent about potential losses resulting from IT-related events. The paper proposes a framework to help insurance companies address non-affirmative cyber-risk across their portfolios. The framework aims to help insurance analysts perform a structured analysis of the issue and is tailored to fit each insurer's structure and underwriting procedures, allowing for better risk understanding and mitigation actions.	CRI challenges
Labunets, K., Pieters, W., and Eeten, M. v.	2020	The Cyber Insurance Landscape.	The study explored organisational decision-making in cybersecurity and cyber-risk insurance (CRI) for companies, particularly Small and Medium Enterprises. It explored the CRI ecosystem and its various actors and their relationships. The research highlighted the need for more research on how companies make cybersecurity investment decisions. The study identified various internal and external factors influencing cybersecurity decisions and adoption of CRI. Many impediments to adoption arise from problems companies face when trying to buy CRI.	CRI challenges
Yousefi, A.	2020	AI-Enabled Cyber Insurance Platform for Small Businesses.	*MSc-Thesis – NOT further considered*	*None*
Vieira, A. C., Insua, D. R., Baylon, C., and Awondo, S.	2020	Risk Management Models for Cyber Insurance.	One difficulty SMEs must made as to cybersecurity decisions, includes involving the purchase of cyber-risk insurance, is that they often have an inadequate understanding of the cybersecurity risks. Budgetary constraints, with a lack of sufficient investment in cybersecurity, are another key issue. To address these problems, a new model to assist organisations with their Cybersecurity Risk Management model was developed. This model helps organisations determine their optimal cybersecurity resource allocation, or the best way for them to allocate their budget between investing in security controls to defend against cybersecurity threats and in cyber-risk insurance products to provide compensation in the event of an attack.	CRI challenges

Table 2-7: Search results category 6: Cyber-risk insurance				
Author(s)	Year	Title	Results	Subcategory
Oxford Analytica	2021	The cyber insurance market will grow rapidly.	As ransomware attacks lately increased this led to a rise in ransomware payments and cyber-risk insurance (CRI) premiums. The risks had outpaced the CRI market, leading to more firms purchasing CRI and insurers raising premiums and enhancing policies. While calls for governments to ban ransomware payments are growing, a full ban is unlikely. Public-private partnerships may be crucial in supporting cyber insurers and private firms, while large firms may consider creating their own insurance divisions to protect against price fluctuations.	Ransomware
Kenneally, E.	2021	Ransomware: a Darwinian opportunity for cyber insurance.	Ransomware sector is highly organised and *available as a service.* Due to high potential damage, there is high interest in insurance. Insurance companies are increasingly also active in risk assessment, health checks, third party digital forensics. As there is no legal compliance framework, insurance companies must identify best practices.	Ransomware
Zeller, G., and Scherer, M.	2023	Risk mitigation services in cyber insurance: optimal contract design and price structure.	This study looked at how to price pre-incident and post-incident services in cyber policies from the insurer's point of view. Specifically, it tried to figure out when a profit-maximising, risk-neutral, or risk-averse insurer should share the costs of risk mitigation services. The study demonstrated that the insurer would always charge the insured the full cost of self-protection services when pricing a single contract. However, this did not always happen when pricing self-insurance services or looking at a portfolio.	Risk assessment

Table 2-7: Search results category 6: Cyber-risk insurance

The field of cyber-risk insurance is multifaceted, involving critical discussions on the methodologies used for risk assessment, the design and adoption of insurance policies, and the challenges posed by emerging risks. This debate reflects the evolving nature of cyber threats and the need for robust frameworks to manage these risks effectively.

In the area of risk measurement, Freund and Jones (2014) proposed the Factor Analysis of Information Risk (FAIR) methodology, which provides a comprehensive, quantitative approach to managing information risk. By categorising losses into primary aspects, such as productivity and replacement costs, and secondary ones, like reputation and competitive advantage, FAIR offers a structured framework that helps organisations better understand and quantify their risk exposure. This granular analysis can assist in more informed decision-making, particularly in understanding the financial implications of potential cyber incidents. However, Malhotra (2015) criticises the reliance on Value-at-Risk (VaR), a traditional risk measurement tool, for cyber-risk insurance (CRI). Despite its widespread use in financial risk management, Malhotra (2015) argued that VaR fails to effectively model tail and systemic risks, such as key characteristics of cyber threats, therefore being inadequate for cyber-risks. Malhotra (2015) advocated for alternative coherent risk measures that better capture the extreme and systemic nature of cyber-risks, suggesting that VaR could lead to significant underestimations of potential losses in the cyber domain. This Malhotra (2015) debate was based on the suitability of different risk measurement methodologies for the unique characteristics of cyber-risk. Proponents of FAIR argue that its detailed breakdown of loss types allows for a more nuanced understanding of risk, which makes it particularly useful for organisational decision-making. Further, Malhotra (2015) emphasised that traditional financial models may not adequately account for the unpredictability and scale of cyber incidents. This debate highlights a broader discussion in risk management about the need to adapt existing tools or develop new ones tailored to the specific challenges of the digital age.

Regarding the expectations of SMEs for CRI coverage across different industries, Franke and Meland (2019) found that business interruption is a major concern in sectors like manufacturing, while in finance and retail, data loss is more significant. Given the different needs of companies taking out CRI, Nieuwesteeg and Waard (2018) argued that the lack of standardised CRI policies creates an additional barrier, especially for SMEs. Kavčič and Delak (2019) add that for small countries like Slovenia, only a few companies offer CRI products, and the

available products focus on data loss and liability for confidentiality breaches. Nieuwesteeg and Waard (2018) concluded that the non-standardised nature of CRI coverage, coupled with high costs, deters many SMEs from purchasing such policies, despite the increasing necessity for protection against growing cyber threats. This lack of standardisation and affordability limits the appeal of CRI, while insurers provide limited incentives for risk mitigation, exacerbating concerns of moral hazard. In contrast, Rejda and McNamara (2017) advocated offering more flexible, customised insurance products, such as stand-alone policies or endorsements that can be added to existing coverage. Such tailored solutions could potentially address the diverse needs of SMEs and encourage broader adoption of CRI by making it more accessible and adaptable to specific business risks. This approach allows businesses to tailor their insurance to their specific needs, potentially providing more targeted protection against cyber-risks. However, this flexibility comes at the cost of complexity, making it difficult for businesses to compare policies and understand what is covered. The debate over standardisation versus customisation reflects a fundamental tension in the CRI market. Standardised policies could simplify the purchasing process and make cyber-risk insurance more accessible to a broader range of businesses, particularly SMEs. However, stand-alone policies or endorsements offer customisation, enabling a more precise match between an organisation's specific risks and its insurance coverage. The optimal approach may involve finding a balance between these two extremes: sufficient standardisation ensures clarity and accessibility, while customisation allows for tailored risk management strategies.

To this conversation, Schlesinger (2018) added his idea that SMEs should include CRI in their overall risk and governance plans. One way they could do this is by using cyber governance assessments. By identifying deficiencies and implementing risk management systems, business continuity plans, and data breach notification strategies, SMEs could transform cyber resilience into a competitive advantage. This integration into governance underscores the growing recognition of CRI as a key business necessity, akin to traditional asset insurance.

IoT and Industry 4.0 are emerging risks that challenge the evolution of CRI. Radanliev et al. (2018) explored the complexities in this field. The interconnected nature of these technologies introduces dependencies and risks that traditional insurance models may not fully capture. The study by Radanliev et al. (2018) emphasised the need for new risk metrics and models but also acknowledged the difficulty in estimating the economic impact of these risks

due to a lack of sufficient data. Cartagena et al. (2020) revealed the concept of silent cyber-risk, referring to IT-related risks that non-life insurance contracts do not explicitly address. The authors proposed a Silent Cyber Assessment Framework to help insurers address this challenge by providing a structured method for analysing and mitigating such risks across their portfolios. This framework offers insurers a practical tool to better understand and adapt to the risks posed by the digital environment.

Labunets et al. (2020) explored the broader CRI landscape, examining how SMEs navigate cybersecurity and insurance decisions. They identified barriers to adoption, such as unclear policy language, affordability, and decision-making complexities, highlighting the need for further research to understand how SMEs decide to invest in CRI. In addition, Vieira et al. (2020) addressed the challenge SMEs face in allocating limited resources between cybersecurity measures and insurance. The authors developed a model to assist SMEs in determining their optimal cybersecurity resource allocation by balancing investments in defence mechanisms and insurance products.

Ransomware attacks have also significantly impacted the CRI market. According to Oxford Analytica (2021), these attacks have led to increased premiums and improved policies as insurers respond to the heightened risk environment. Kenneally (2021) discussed how the organised nature of ransomware operations has forced insurers to take a more proactive role in risk assessment, often involving digital forensics and third-party evaluations. The emergence of new risks, particularly those associated with IoT and ransomware, has sparked a debate about the adaptability of the CRI market. As new technologies and threat vectors evolve, traditional insurance models may struggle to keep pace. This has led to calls for the development of new risk assessment tools and metrics that can better capture the complexities of modern cyber-risks (e.g. Ncubukezi, 2020; Schmitz and Pape, 2020). Therefore, the environment has become a topic of debate. Kenneally (2021) also sees the role of insurers not just as passive risk transfer agents but as active participants in risk management, helping organisations to assess and mitigate risks before they result in significant losses. Zeller and Scherer (2023) added to this debate by examining the pricing of risk mitigation services in CRI policies. Their study analysed when insurers should share the costs of self-protection or self-insurance services, demonstrating that, while insurers often pass the full cost of self-

protection onto insured parties, they may take a different approach when pricing self-insurance services or portfolios. Their findings highlight the importance of aligning pricing strategies with the unique characteristics of cyber-risks.

As outlined above, the academic debate on CRI shows that the field is changing quickly because of how rapidly cyber threats are changing. This means that risk assessment tools, policy designs, and market responses need to be more advanced. As cyber-risks continue to grow in scale and complexity, it's important to talk about new risks like ransomware and IoT-related threats, as well as methods like FAIR vs. VaR and how to balance standardisation and customisation in policy design. For small businesses, these arguments show how important it is to include CRI in their overall risk management plans, even though it can be hard to figure out how much it costs, what it covers, and how to make decisions in this constantly changing field.

2.8 Summary and overview of the publications

To summarise the outcome of the literature review and provide further context, Figure 2-2, shows how the theme of cyber-risk has been studied over the past 10 years. The chart indicates an increased academic interest in 2020 and 2021, which then reduced significantly in 2022.

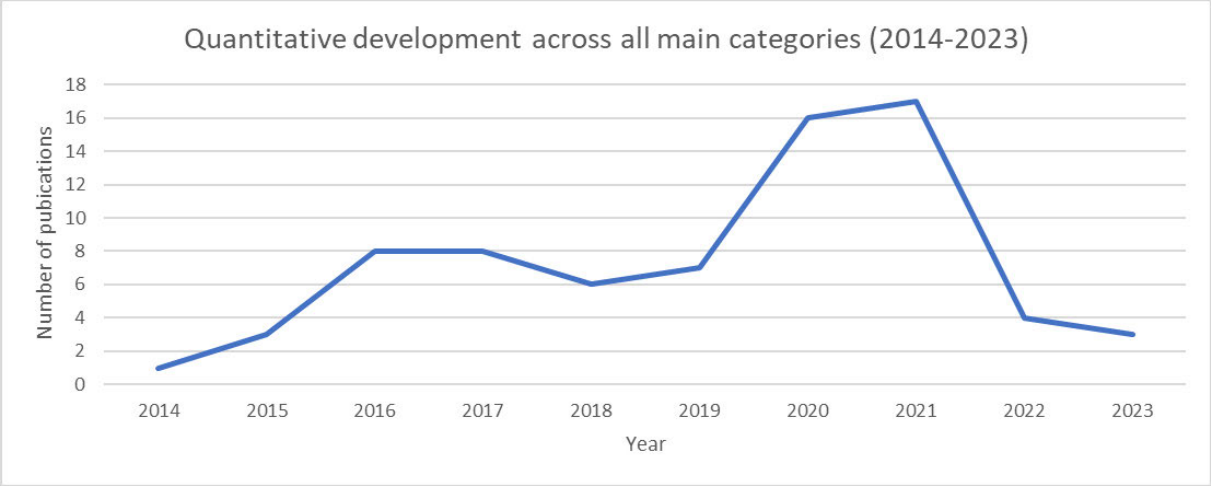


Figure 2-2 The development of publications analysed in detail (own presentation)

As can be seen from Figure 2-2, the annual number of publications increased from 2015 to 2021. The reduction in academic interest could be partly attributed to the fact that this literature review was conducted before the end of 2023. However, given that the last search was

carried out on November 24, 2023, one might have expected publications at least to be at the level of around 80% of those in 2021. However, there were only 22 publications for 2022, and amongst these, several were eliminated from the final search result as to their lack of relevance.

In Figure 2-3: Quantitative development within the identified main categories is shown below:

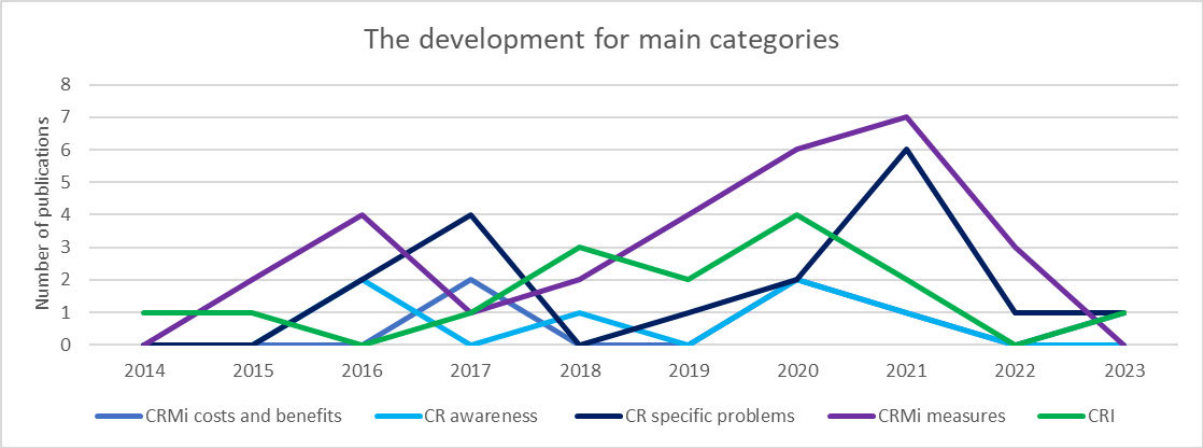


Figure 2-3: The development for main categories

From analysing Figure 2-3, it becomes evident that the overall trend was mainly due to the increased academic interest in the category of SMEs' "CRMi measures" (cyber-risk mitigation measures, and to a lesser extent in "CRI" (cyber-risk insurance). In the SME's "CR specific problems" (cyber-risk specific problems) category, publication activity peaked in 2017 and then declined. However, except for the "CRMi measures" and "CR specific problems" category, there were only a maximum of four publications annually in any of the other main categories identified for this study. An attempt was also made to analyse publication activities within the subcategories. This is shown in Figure 2-4 below.

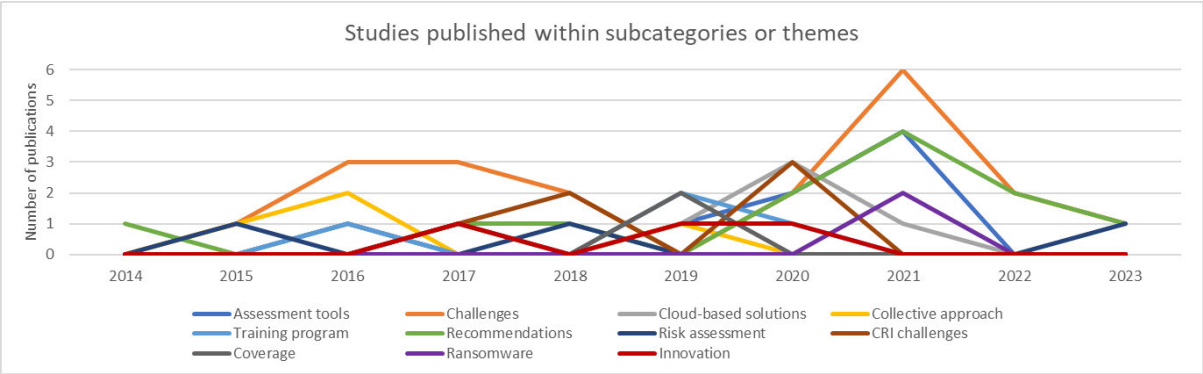


Figure 2-4: Development of publications within subcategories

Figure 2-4 indicates what publications related to the challenges associated with cyber-risk in relation to SMEs were published between 2015 to 2022. These studies included the assessment tools used by SMEs, which commenced in 2019. Also, in 2016 research into the use of cloud-based solutions in cyber-risk management for SMEs began to emerge.

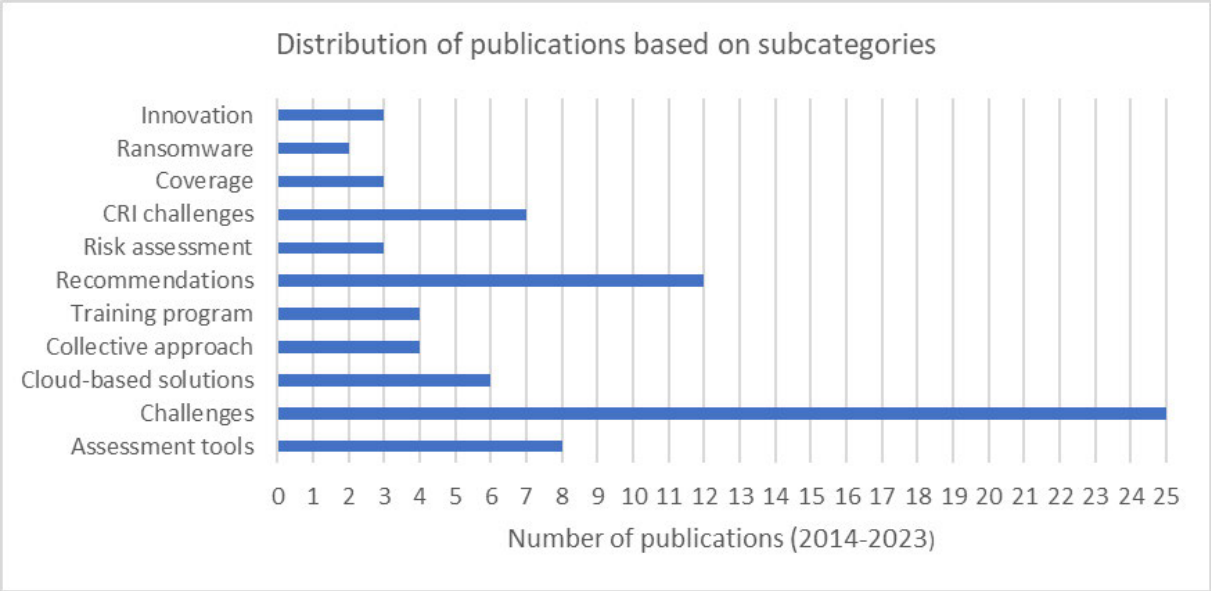


Figure 2-5: The distribution of subcategories

Figure 2-5 shows that the largest subcategory pf research found in this literature review was assigned to the subcategory “Challenges”. The two second largest subcategories were “Assessment tools” and “Recommendations”. The studies categorised under “Assessment tools” were mostly presented as checklists or questionnaires for SMEs to assess their cyber-risk readiness or risk level, as opposed to presenting their experiences and perceptions. The

studies categorised under "Recommendations" provided information on how SMEs could reduce their cyber-risk exposure. The four subcategories "Ransomware", "Coverage", "CRI Challenges" and "Risk assessment" shown in Figure 2-4 and Figure 2-5 fall under the main category of "Insurance".

To further enhance transparency regarding the categorisation process, Table 2-8 summarises the distribution of subcategories across the five main categories identified in the literature review. This cross-tabulation illustrates how certain subcategories appear across multiple main categories, reflecting thematic overlaps within the literature. This outcome supports the observation noted earlier that some subcategories emerged during full-text analysis and were not confined to one main thematic grouping.

Table 2-8: Distribution of subcategories across main categories

Subcategory	Category				
	CRMi costs and benefits	CR awareness	CR specific problems	CRMi measures	CRI
Assessment tools	-	-	-	8	-
Challenges	1	3	17	4	-
Cloud-based solutions	1	-	1	4	-
Collective approach	-	-	-	4	-
Training program	-	1	-	3	-
Recommendations	3	2	-	6	1
Risk assessment	-	-	-	-	3
CRI challenges	1	-	-	-	5
Coverage	-	-	-	-	3
Ransomware	-	-	-	-	2
Innovation	1	-	3	-	-

Table 2-8: Distribution of subcategories across main categories

The next section below will show how the final group of articles were categorised under the different subcategories, and set out how they were analysed.

2.9 Analysis of publications within subcategories

In this section and in the following subsections, the results are firstly individually presented, and then the key gaps in existing knowledge are set out, with indication of how they informed the study's research questions.

2.9.1 Studies associated with subcategory “assessment tools”

Those studies in the category of “assessment tools” tended to be focussed on method or methods used to assess an SME’s cyber-risk exposure.

Focussing on the organisational characteristics of SMEs, Mijnhardt et al. (2016) developed a model to measure the company’s information security maturity. In the study, Mijnhardt et al. (2016) advocated for a shift from excessively technical and complex standards, such as the ISO 27000x series, to more accessible and actionable guidelines that focus on measurable organisational characteristics. Their developed model would therefore better suit SMEs in cyber-risk assessment and implementing cyber-risk mitigation measures. Further to this technical model, Rae and Patel (2019) developed a composite cyber-risk rating system for SMEs, extending the technical component by introducing behavioural aspects. The technical aspects in Rae and Patel (2019) included network protection, system configuration, access control, protection against malware, and the threat caused or reduced due to a system update. The behavioural aspects were based on four criteria: perceptions and understanding, external personal attributes, external information, and regulations and requirements. The category of perceptions and understanding was focused on the decisions related to the relevance of the potential attack, the threat, perceived risk, and whether the information available was seen as being trustworthy. External personal aspects were associated with how decisions were informed, which included social, work, or professional networks and past experience. External information and service was related to the influence from business operation contacts, for example, from suppliers, customers, or even the competition. Finally, regulations and requirements were influenced based on the need to comply with regulatory requirements or compliance with voluntary standards. For Rae and Patel (2019), these aspects were important, but the study did not fully investigate or evaluate the categories presented. While these omissions are important, the methodology proposed could be potentially used for self-assessment and external evaluation, such as for determining risk levels when assessing the need to seek insurance. Later, Boletsis et al. (2021) advocated a system based on a more graphic visualisation of potential risks in business processes to provide a technical cyber-risk evaluation tool that can be used by a business. The method was intended to be used for undertaking a self-assessment and the results to inform the business of its potential cyber-risks. On closer examination of the proposed tool, for the assessment to be accurate,

an organisation needs to possess a high level of technical knowledge, indicating the methodology may be more relevant to consultants as opposed to the SME workforce, when determining and identifying potential risks. The method did, however, highlight areas for action to deal with specific threats but was more focussed on exemplary case studies rather than enterprise-wide risk evaluation from a SME perspective. Armenia et al. (2021) also devised and recommended a tool for cyber-risk assessment, focused on assisting companies, and in particular large organisations, to identify risks and classify them based on the severity of the potential damage. This information could then be used by the company to prioritise cyber-risk investments or for insurance companies to use to evaluate residual risks, when calculating insurance premiums. A similar approach had already been published earlier by Armenia et al. (2019); however, this publication lacked any SME focus and instead elaborated on cyber-risk assessment for larger enterprises only.

In the area of a cyber resilience framework dedicated to SMEs, Carías et al. (2021) presented a checklist of actions to take, ranging from the development of a cyber resilience strategy to the development of checking mechanisms or staff training programmes. The framework was structured into different areas, namely: governance, risk management, asset management, threat and vulnerability management, incident analysis, awareness and training, information security, detection processes and continuous monitoring, business continuity management, and information sharing and communication. To determine which areas were relevant, Carías et al. (2021) advocated the implementation of an electronic questionnaire to generate the results through a spider-graphic to represent an oversight of the individual areas before providing an overarching assessment. While the approach allowed the identification of specific areas of potential interest with higher and lower risk readiness, which could enable the prioritisation of risk management measures, there was a lack of any real academic insight, particularly related to SMEs.

In contrast to Carías et al. (2021), Mlakar et al. (2021) presented the concept for a methodology which combined risk assessment and risk management/risk mitigation using a cloud-based service. The concept was focused on a micro-enterprise business which provided services through the usage of decentralised devices. The proposal of Mlakar et al. (2021) was designed to manage risks related to malware attacks, attacks through smart devices, broken cryptography, improper session handling while using cloud services, ransomware, internal

attacks via compromised user accounts, and inadequate cybersecurity protection, for example not addressing potential security gaps. While informative, Mlakar et al. (2021), much like other studies related to this theme, did not focus on SMEs but rather provided a more generalised outcome, therefore may not be applicable for small businesses in the manufacturing sector.

Based on the above, two key themes emerged from the existing studies related to assessment tools. The first theme was associated with the need for risk assessment and risk evaluation, then the ability to prioritise these potential risks. The current academic debate has centred on the techniques needed to analyse potential cyber-risks and the information needed to provide guidance for the business. This information could include the potential economic impact following the incident and how to evaluate residual risk. The other category to emerge from the literature was how risk assessment and risk mitigation could be analysed, with the results from the risk assessment potentially being used to directly inform any mitigation measures or strategies.

2.9.2 Studies associated with subcategory: "challenges"

The next category was associated with the theme of challenges. A major challenge to emerge from the literature was related to a lack of knowledge and skills, which is often associated with SMEs, and which can result in a lack of awareness of cyber-risk management and mitigation strategies. Quesada (2016) pointed out that employees, which arguably include owners of a SME, often lack formal cyber-risk training. The main driver for SMEs, Quesada (2016) contended, is the need for the engagement of management in identifying and resolving cyber-risks, along with meeting legal requirements or compliance with associated standards. This lack of awareness included businesses not meeting minimum standards required, including the potential importance associated with insurance coverage. Alahmari and Duncan (2020) emphasised the importance of cybersecurity behaviour at both the company and employee levels. This knowledge is crucial for establishing a strong cyber-risk management process to prevent potential financial losses within an SME due to a business disruption following a cyberattack. Therefore, cybersecurity behaviour is regarded as important to identifying and understanding the potential of a cyberattack through proactive house practices and awareness. Hoppe et al. (2021) in their industry survey confirmed that deficiencies in

risk culture, which included the perception of, knowledge of, and attitude towards cyber security, along with suitable IT experts, are the major obstacles to the implementation of cyber-risk management strategies in SMEs.

In an earlier but related study, Renaud (2016) concluded that the lack of adequate cyber-risk measures was a challenge for SMEs. This lack of awareness and preparedness has manifested itself in the size of business becoming a potential target for cybercriminals; for example, Quesada (2016) points out that while SMEs might not be the primary target of an attack, they could serve as a gateway for cybercriminals to target larger enterprises. However, for those SMEs who have experienced a cybersecurity attack and therefore have been compromised, there is the risk of a cyberattack that could impact the supply chain to larger enterprises, potentially endangering their business model. For Renaud and Weir (2016), there was a confusion associated with the interpretation and usage of existing information and often a resulting lack of critical cyber-risk data for SMEs to use, which is another challenge for this size of business. For Renaud and Weir (2016), this lack of information could lead to some SMEs being only able to take basic measures rather than offering a robust response. In concluding, Renaud and Weir (2016) contended that more precise and concise information was needed, as without this detail, the SME is unable to adequately prepare or be able to respond to a cyberattack (Renaud & Weir, 2016). This finding of Renaud and Weir (2016) was supported later by Dayalan (2017) and Grocke (2017), who also came to the same conclusion that existing information on measures to minimise or mitigate against potential cyber-risks remains a challenge for SMEs to understand and act accordingly.

Another challenge associated with cybersecurity and the potential risk from the systematic literature review was related to how cybersecurity was perceived. Osborn and Simpson (2015) argued that dependent on the size of the SME, this influenced and informed the approach to cybersecurity. For Osborn and Simpson (2015), in medium-sized companies who employed between 10 and 249 employees, the business tended to adopt a professional and informed approach towards potential cyber-risks, which included the management of the company's network and devices. However, in contrast, micro-companies, those who have less than 10 employees, due to their size and number of workers, were less informed or familiar with cyber-risk security. For those more mature SME companies, there was the issue as to the use of legacy devices and a lack of awareness of updating operating systems and

software. Osborn and Simpson (2015) also found that software houses or suppliers tended to treat SMEs due to their size as consumers rather than B2B partners, while focussing primarily on services and products for large businesses. Again, part of the reason can be attributed to cybersecurity experts in software houses and suppliers focussing on high-value assets, such as banking, payment services, and insurance, while SMEs are neglected. Osborn and Simpson (2018) further extended this argument, highlighting a lack of risk awareness and information on cyber-risk management resources amongst SMEs. In reaching this conclusion, Osborn and Simpson (2018) also pointed out that this constitutes a reputational risk for SMEs, as a lack of cyber-risk and security management and particularly as to potential and actual breaches, can result in severe supply chain issues, including in larger enterprises. Alahmari and Duncan (2020) contended that SMEs are typically more susceptible to cyberattacks due to their adoption of a low-cost approach with minimal cybersecurity measures. As a result, SMEs often face challenges with their cyber-risk management process, particularly due to aspects of their managerial priorities and strategies.

A specific risk related to micro-companies and smaller medium enterprises was related to the trend of "bring your own device" (BYOD) policies and their potential cybersecurity risk: where there is a mixture of business and private devices being used; this can increase the risk of cybersecurity being compromised. Extending this further is also the risk associated with the protection of customer and supplier data, IP protection, potential loss of customers, along with issues related to the use of social media, which were further identified as important motivators for SMEs to engage with cyber-risk security; however, there is limited research related to how SMEs have addressed these challenges. Pfeifer (2021) attempted to explore this theme, identifying gaps between SMEs' self-assessment and cybersecurity policies, which included the associated risks, along with how these challenges are identified and strategies adopted. Based on this research, Pfeifer (2021) contended that the size of SMEs, combined with the lack of both financial and human resources or expertise, presents a unique challenge.

More recently and building on the work of Pfeifer (2021) as well as Mzileni and Ncubukezi (2022), recent studies have identified that a lack of resources in SMEs was the primary challenge and a key reason for their exposure to potential cybersecurity risks. Mzileni and Ncubukezi (2022) noted that this exposure to potential risks included a lack of understanding

and awareness of the need to update antivirus software, how to mitigate against anti-spyware, the need to address unsecure passwords, the lack of firewalls, and adequate backup systems, all of which are considered essential in addressing cyber-risks in a SME. In reaching this conclusion, Mzileni and Ncubukezi (2022) identified that there were clear knowledge gaps amongst SME owners and employees related to cyber-risk management. Mthiyane et al. (2022) also analysed overall enterprise risk management strategies in SMEs and contended that the management of cyber-risk is amongst the most challenging risks to address, particularly in a SME. In contextualising this, the lack of resources was considered to be the most important challenge for a SME. Mthiyane et al. (2022) identified the solution of outsourcing as one of the most common approaches adopted by SMEs to address this challenge of managing cyber-risks with limited resources.

To summarise the subcategory of "challenges", the following main themes emerged from the review of the literature, including that SMEs tended to lack information on cybersecurity management and mitigation strategies due to limited personnel and financial resources. In these studies, SMEs tended to overestimate their competences and underestimate their risk exposure. Part of the issue was associated with use of older hardware, not updating operating systems and software, and accepting the current practice of dual private and business use of hardware (BYOD). Interestingly, cybersecurity companies, including software houses, did not pay sufficient attention to SMEs and their specific business needs and requirements. Finally, SMEs being potentially exposed to cyber-risks could be seen as being a weak link in the supply chain of larger enterprises, which could lead to SMEs being cut out of these supply chains.

2.9.3 Studies associated with subcategory "cloud-based solutions"

The topic of cloud-based solutions emerged as the next theme. Those studies related to this category of cloud-based solutions included those focused-on SMEs and cyber-risk management strategies. Saber (2016) conducted a study on cyber-risk management activities within SMEs and recommended the introduction of new cyber management policies, ensuring that staff are adequately trained, and the usage of appropriate technology. As to the usage of appropriate technology, this included the use of cloud-based solutions for software and data storage to be part of any cyber-risk mitigation strategy, which may include outsourcing the solution to a cloud service provider (Saber, 2016). A similar solution was provided by McLilly

(2020), who concluded that since SMEs have limited resources, outsourcing cyber-risk responsibilities could be a viable option. However, this form of solution and service tended to be designed for large enterprises who are frequently cyberattacked and have sufficient financial resources. Since these services are difficult to scale down to SME requirements, McLilly (2020) advocated the development of a cloud-based solution based on a demand cybersecurity concept dedicated for SMEs. This solution would be based on data analytics technology and then provided on an individualised basis. Ncubukezi (2020) also suggested that cyber-risk solutions should be based on a cloud approach and AI technologies should be tailored for the needs of SMEs. The question which emerges is whether SMEs want this type of solution.

Schmitz and Pape (2020) suggested a need for the development of risk assessment tools specifically adapted to SMEs. In achieving this, Schmitz and Pape (2020) contended that the strategy should be designed and implemented in four distinct phases. While informative, the study only described the concept of the system and did not explore the current usage and perspective of cyber-risk challenges faced by SMEs.

To summarise the above, the existing literature indicates that cloud-based solutions could potentially be used for software access and data storage, which means that cyber-risk solutions are outsourced. To achieve this, existing research indicates that cloud-based cyber-risk solutions could be a potential solution for meeting SME cyber-risk mitigation needs, but the question is whether this solution is actively wanted or used by this sector.

2.9.4 Studies associated with subcategory "collective approach"

The next theme to emerge from the systematic literature review was related to cyber-risk, which was associated with adopting a collective approach. In addressing the theme of collective approach, Such et al. (2015) identified a lack of patching or updating of OS and software, which emerged as a potential cybersecurity threat. This included the time-lag between the release of security patches, which are released to address an imminent attack, and their installation on an SME's device. For Such et al. (2015), this challenge for SMEs could be addressed by having these new upgrades or patches applied in a timely manner; however, the focus of the software houses tended to be large company-centric. To address this, Such et al. (2015) advocated that SMEs should work cooperatively with other entities to ensure that

hardware and software information on security upgrades and patches are shared. Nykänen and Kärkkäinen (2016) suggested that the development of a cybersecurity WIKI could be used as a collective approach for SMEs; however, what could not be determined from the study was whether SMEs were prepared to advocate for this approach or share their data. This was also highlighted by Pawar (2016), who identified costs, lack of resources, and priorities amongst SMEs as being a major challenge when meeting a potential cyberattack. To address this, Pawar (2016) called for and identified the need for a shared collective strategy. Later, Ajuzie (2019) carried out case study research amongst SMEs, which focused on the lack of knowledge and resources in this type of business. To overcome this lack of resources, Ajuzie (2019) advocated the collective usage of cloud software as a possible solution to expand services while also providing additional cyber-risk security.

2.9.5 Studies associated with subcategory "training program"

The literature review identified the significance and importance associated with training programs for SMEs' owners and employees. Since the next generation of employees are now the new corporate technology users, Muhirwe and White (2016) suggested the need to focus and concentrate on a combination of awareness events and training specifically as to cybersecurity awareness, practice and behaviour**.** Consoli and Kovatcheva (2019) proposed a new cybersecurity training programme embedded into SMEs, which was elaborated on by Consoli et al. (2020). For the development of this form of training programme to be effective, the first stage advocated by these writers is the identification of potential skills gaps, including identifying competences and gaps in knowledge. These identified gaps in skills, knowledge and competences would then inform the training programme content. The content can include compliance with cybersecurity laws and legislation, how to identify potential cybersecurity risks, the prioritisation of these risks, and how to respond to and monitor potential threats. Developing on this theme, Dimitrov and Rasheva-Yordanova (2019) identified the skills required for cyber management at different levels of seniority throughout the organisation, which ranged from security and data analyst to cybersecurity risk managers, but questioned whether this was relevant in an SME. Based on this, Dimitrov and Rasheva-Yordanova (2019) then suggested that the required skills are then matched to different competency and potential cyber-threats. However, what these studies did not investigate was the actual format and content of these cyber-risk training programmes, along with the focus

of this provision used currently in SMEs. While the studies presented above have advocated cybersecurity training, Muhirwe and White (2016) raised the question of whether training can adequately equip employees with an awareness of cybersecurity. However, despite this question of Muhirwe and White (2016), as noted previously training can bring about cybersecurity and risk awareness, but its effectiveness is dependent on the training's content and focus.

2.9.6 Studies associated with subcategory "recommendations"

The subcategory of "recommendations" emerged from the systematic literature review as a means to potentially address the challenges of a cyberattack. Bell (2017) provided a step-by-step guide for SMEs to address a potential cyberattack, recognising that SMEs have limited resources, but also that these types of businesses tended to have flatter hierarchies and good internal communications, which can be an advantage in creating new and responsive policies compared to larger enterprises. Bell (2017), in presenting this, set out proactive measurements of the identification of potential risks and then which measurements and strategies are needed to protect against this threat. These recommendations included application whitelisting, disabling of untrusted MS Office macros, application patching, user application hardening such as disabling of Adobe Flash player and untrusted Java codes, restriction of administrative privileges, usage of multi-factor authentication, patching of the OS, and daily backups. Freund and Jones (2014) highlighted the importance of measuring and managing information risk by identifying primary and secondary loss scenarios. For Freund and Jones (2014), the authors suggested that management should focus on potential losses, such as productivity and replacement costs, and assess outcomes based on outcome, competitive disadvantage, fines, and reputation damage. To achieve this, Freund and Jones (2014) proposed the FAIR methodology, a quantitative approach to risk measurement. This approach can help organisations understand their risk exposure and make informed decisions, particularly regarding the financial implications of potential cyber incidents. Brown et al. (2022) elaborated on cybersecurity in the context of Internet of Things (IoT) devices, and focused on the fact that cybersecurity was only relevant to high-risk service tasks such as payment services but was also relevant to comparatively mundane activities. To address this,

Brown et al. (2022) recommended that businesses should rank risks and then provide support for these outcomes through focusing the resources more strategically. While informative, what these studies did not do was investigate the actual experiences of SMEs.

When reviewing technical solutions, Pfister and Lehmann (2023) found that digital technologies can yield significant positive returns on investment, such as increased revenue or reduced costs in manufacturing. Based on these findings, key digital solutions, such as cloud computing and data analytics, have the potential to generate substantial returns. They recommended that SME managers establish guidelines to enhance business performance through digitisation.

In a similar study, Armenia et al. (2021) support SME's decision-making on investments in cybersecurity by developing a system dynamics methodology and tool for cyber-risk assessment. The proposed tool of Armenia et al. (2021) assesses the cybersecurity status of SMEs and the impact of investments on their risk profile, thereby enhancing cybersecurity awareness. It also proves beneficial when considering cyber-risk insurance and its residual risks. However, for Rawindaran et al. (2021), when analysing different cyber-risk solutions in relation to available software tools, there is a potential trade-off between ease of use and affordability. In contextualising this, Rawindaran et al. (2021) contended that open-source solutions were a potential solution for SMEs who have limited financial resources but also required a high level of subject knowledge by the user. Again, while informative, Rawindaran et al. (2021) and Bell (2017) provide insightful recommendations; however, as noted by Kapoor et al. (2018), the focus of much research has investigated the likely approaches of SME decision makers as regards to their cyber-risk security solutions and the measures taken before, during, and after a cybersecurity breach, but not based on their experiences. In this context, Aurelien (2021) presented a framework for cyber-risk recommendations designed for management in a SME, which was based on six main areas. These areas included the development of a plan, an assessment of technology used in the business, the requirements of internal and external stakeholders', how to assess the impact of potential cyber breaches, how to assemble defensive tools, and the implementation of measures. Again, while informative, the study did not really provide any insight and depth as to the experiences encountered by the SMEs. However, partly addressing this, Tam et al. (2021) attempted to cap-

ture how these recommendations and strategies were followed. The study found that businesses tended to have dedicated virtual private networks, instigating strong password policies (sometimes using third-party identification solutions), while restricting access to internal devices such as computer workstations in offices. There were various policies implemented, including the prevention of malicious software being uploaded. While these strategies were considered adequate for larger enterprises, Tam et al. (2021) concluded that they may be inappropriate or not feasible for SMEs. To address this, Tam et al. (2021) concluded that SMEs should base their cyber-risk security strategies on a zero-trust model, in which every cyber interaction is considered a potential risk but should be resource centric. The study also advocated cooperation between SMEs should be used to exchange information on cyber-risks, a theme covered previously. What Tam et al. (2021) did not study was whether SMEs are prepared to share, outsource, or exchange their services or data. El Baz and Ruel (2021), in partly addressing this, referred to building cooperation with other companies to prepare for different disruptions and impact scenarios that a single firm cannot mitigate, due to a lack necessary resources and financial capabilities.

In summary, there are a series of recommended solutions to address potential cybersecurity risks, which range from securing devices through to restricting access to networks used in the office environment. The following themes emerge from this section: Firstly, the acknowledgment that SMEs often have limited resources and knowledge dedicated to managing cybersecurity risks (e.g., Rawindaran et al., 2021; Tam et al., 2021). SMEs face unique challenges, including trade-offs between affordability and usability, reliance on open-source tools, and the suitability of solutions like zero-trust models. These factors highlight the need for resource-centric strategies tailored to SMEs, with cooperation and information-sharing among SMEs playing a vital role in overcoming these challenges. Secondly, the need for structured, forward-looking cybersecurity strategies (e.g., Bell, 2017; Freund and Jones, 2014), focusing on identifying risks, implementing preventative measures, and managing risks through frameworks like FAIR. Third, the integration of digital technologies, such as cloud computing, data analytics, and cybersecurity investment tools, to enhance business performance and effectively manage risks (Pfister & Lehmann, 2023; Armenia et al., 2021).

While these studies have provided structured guidelines and recommendations for cyber-risk mitigation, there has been limited research into the actual experiences of cyber security

and cyberattacks amongst SME managers. This includes whether SMEs understand and rank potential threats, as proposed by Brown et al. (2022), when prioritising resources. Finally, the question is also whether SMEs are prepared to be cooperative with external entities, including other SMEs, as to the identification of potential risks and even using outsourcing facilities as a potential solution.

2.9.7 Studies associated with subcategory "risk assessment"

The next theme identified through the literature review was related to risk assessment. Studies within this subcategory and those analysed in subsequent sections were classified within the main category under "insurance". While these studies did not necessarily focus on SMEs, their inclusion was due to their relevance to protecting against or mitigating the outcome of a cybersecurity risk. Malhotra (2015) analysed common risk assessment methods and concluded that the main challenge posed by a cyberattack is uncertainty as to the potential outcome. A cyber-risk can be defined as an event that can lead to potential damage and has multiple outcomes. This aligns with the fact that risks are often strongly interconnected, as is frequently the case in cyber-risk scenarios, where a single incident can result in multiple losses. To protect against this, insurance is a potential business option to mitigate against this activity. For Malhotra (2015), insurance is a viable option for a business, but it requires an extensive analysis of the potential cyberattack; therefore, there is a need to conduct an extensive risk assessment. To be effective, Malhotra (2015) recommended that all incidents are considered based on using a conventional statistical analysis, which is informed and derived from the data generated from the risk assessment. Radanliev et al. (2018) arrived at a similar conclusion by identifying the difficulty of conducting and analysing data from a quantitative risk assessment for the purpose of cyber-risk insurance due to the low level of reliable data. However, while cyber-risk is increasingly common, definitive and reliable data on damage levels as well as the probability of specific types of incidents occurring are often not available, which is even more problematic for SMEs, as this type of business often does not have the resources needed to capture all possibilities. These studies by Radanliev et al. (2018) and Malhotra (2015) indicate that a quantitative risk assessment can only be effective if there is sufficient data available to calculate potential risks using conventional statistical methods, which is also a challenge for SMEs. Moreover, when there is insuf-

ficient available data, conventional statistical methods for risk calculation tend to be inaccurate, which brings into question the relevance of using this methodology to determine cyber-risk insurance (CRI).

In response to the persistent lack of reliable statistical risk and loss data, Zeller and Scherer (2023) provided an alternative that revolves around the optimal pricing of CRI services. Zeller and Scherer (2023) indicated that insurers should share the costs of risk mitigation services. Obviously, the insured SME expects the insurer to fully recognise the cost of self-protection when pricing the contract, but it is understood that the insurer may need to adjust pricing for other services based on the SME's risk profile and market conditions. From the above, it is possible to conclude that academic knowledge of cyber-risk assessment and valuation remains limited and continues to evolve. Therefore, the supply uncertainty of insurance providers drives the growing dissatisfaction of SMEs in their role as potential buyers of CRI and as seekers of risk mitigation.

2.9.8 Studies associated with subcategory "cyber-risk insurance challenges"

Focussing on the challenges linked to cyber-risk insurance (CRI), writers including Nieuwesteeg and Waard (2018) analysed different CRI models to capture SMEs' usage of CRI. For Nieuwesteeg and Waard (2018), SMEs tended to be reluctant to buy CRI due to the perceived high prices and premiums. In reaching this conclusion, Nieuwesteeg and Waard (2018) noted that the insurance companies often found it difficult to assess risks in this type and size of business and therefore tended to charge higher premiums due to the uncertainty of potential risks. This had led to CRI contracts having multiple clauses included to cover potential unknown and uncertain risks. Consequently, as noted by Nieuwesteeg and Waard (2018), the insurance coverage offered was not extensive. Schlesinger (2018) also analysed the relevance of CRI. Like Nieuwesteeg and Waard (2018), Schlesinger (2018) also found that comparing potential CRI was problematic, and then concluded that one of the main challenges was how insurance providers could accurately quantify risks.

Cartagena et al. (2020) highlighted another key challenge associated with CRI, but from an insurance provider perspective. While insurers tended to exclude specific risks or to limit financial coverage for some types of cyber-outcomes, the lack of knowledge about potential

risks and/or their financial consequences meant that insurers found it difficult to develop explicit lists of risks that could be excluded from the insurance policy. To address this, Cartagena et al. (2020) advocated that an initial risk assessment was essential, within a systematic framework focused on assessing potential cyber-risks at an individual business level.

In analysing the existing market for CRI related to a SME, Labunets et al. (2020) identified that this type and size of business were often reluctant to publish their cyber-risk strategies and activities, which was seen as an important restriction in determining insurance coverage, as sharing information could also benefit other companies. In reaching this conclusion, Labunets et al. (2020) tested different policy options, including the coverage duration, requirements for risk reducing measures, and higher premiums needed to insure against higher risks, but found that the coverage on certain individualised options tended to increase the premium significantly, making insurance coverage challenging. Like Schlesinger (2018) and Cartagena et al. (2020), Labunets et al. (2020) also found that the main challenge for CRI was associated with having insufficient information related to potential cyber-risks and called for further research.

More recently, Vieira et al. (2020) focused on how CRI contracts were formulated. Amongst the facets associated with CRI, the study investigated the usage of dynamic pricing-based solutions, which can be used to assess the company's IT infrastructure along with their suppliers, to provide a holistic assessment of a potential cyberattack. However, determining these risks from the individual and related business perspectives will be particularly challenging, as risk quantification requires all parties to be open and transparent (Vieira et al., 2020).

To summarise the above, premiums can be high because insurance companies are often unable to determine accurately potential cyber-risks and therefore cannot quantify the premiums needed to cover the consequences of a cyberattack. There is also the challenge associated with gaining an open insight into the IT infrastructures and cybersecurity strategies needed to ensure that the insurance coverage is appropriate. Due to this lack of knowledge about potential risks, insurance providers tend to exclude certain risks from individual policies, which either increases SMEs' potential exposure to risk or their premiums.

2.9.9 Studies associated with subcategory "coverage"

The next theme was associated with cyber-risk insurance was coverage.

Rejda and McNamara (2017), and later Franke and Meland (2019), analysed the types of risk coverage. Rejda and McNamara (2017) noted that the insurance industry offers two standard forms of cyber liability coverage: firstly, as a standalone; secondly, as an add-on to a business owner's existing policy. Many commercial insurance carriers offer the addition of a cyber liability or data breach endorsement to a professional liability or general liability policy, although this may come with numerous exclusions and limitations. However, as technology improves, SMEs have realised that the small cost version of an endorsement is insufficient and that they need a tailored, stand-alone cyber-risk policy, which offers coverage for both expenses and liabilities related to a covered cyber incident. Despite the inclusion of liability protection from data breaches, response costs, restoration expenses, and business income in all these coverages, it remains unclear which form offers more benefits to the insurance buyer. Franke and Meland (2019) analysed these types of risk coverage used by SMEs and compared the requirements and claims following a cyberattack. What emerged from Franke and Meland's (2019) study was that business interruption was seen as one of the most frequently required insurance coverages in the manufacturing and IT sectors, whereas in the finance and retail industries, the focus was on the loss of customer data. However, in analysing the claim data further, the study indicated that the incident response was the most frequent insurance claim, whereas business interruption, which included ransomware attacks, was rarely claimed. The focus on this type of coverage including ransomware was due to the increased reporting of the potentially detrimental consequences of such attacks, like the loss of business, reputation, or recovery time, which will be explored in the next section.

2.9.10 Studies associated with subcategory "ransomware"

Leading from above, the emergence of ransomware is seen as a significant potential cyberthreat, which led Oxford Analytica (2021) to highlight that ransomware attacks were increasing, and this had led to company awareness but also the importance of seeking cybersecurity insurance premiums. This business-based study by Oxford Analytica (2021) highlighted that this form of cyberattack tended to be focused on governmental and large businesses, due to attackers seeking a significant payment. Oxford Analytica (2021) noted that small business entities, like SMEs, were not seen as a potential target but in the future may become attractive targets for attackers. Like Oxford Analytica (2021), Kenneally (2021) also pointed out that ransomware may be the key component and aspect for CRI. In reaching this conclusion,

Kenneally (2021) noted that this new threat has become a key cyberthreat, which means that insurance companies are paying closer attention, requiring businesses to have minimum standards to reduce the insurer's exposure. To assist in this, Kenneally (2021) indicated the need for more transparency as to cyber-risk strategies to mitigate ransomware attacks. However, while informative, these studies have focused specifically on large organisations and businesses; the question is whether this is applicable and relevant for SMEs.

Based on the above, ransomware is increasingly becoming a significant cyber-risk, which means that due to the potential high financial damage created by a single incident, the need for suitable insurance coverage will lead to higher premiums. What remains unclear is whether ransomware is a potential cyberthreat for SMEs or whether, in the future, they will become a target for attackers, and what are the perspectives or experiences of this size of business when faced with this cyberattack.

2.9.11 Studies associated with subcategory "innovation"

The analysis of the literature revealed a debate about the connections between cybersecurity and business performance, included Nelson and Madnick (2017b), who provided a set of practical recommendations to assist a company in assessing its own positioning on the innovation/cybersecurity matrix. From Nelson and Madnick's (2017b) perspective, there is a link between higher levels of cyber-risk mitigation (CRMi) and innovation, which needs to be established. Later, de Oliveira et al. (2019) established a primary connection between success and innovation, identifying CRMi-measures as being innovative skills and technology, which indicated that a business's capacity to adopt new technological advancements was a key indication for success, but it needed to include an awareness of potential cyber-risks. Reflecting this, de Oliveira et al. (2019) investigated the managers' perceptions of how CRMi strategies and cyber security investments can enable business success while mitigating a cyberattack. In a similar study, He et al. (2020) found that companies that had experienced a cyberattack tended to react with a reduction in innovation activities; however, innovative activities should increase CRMi-measures and strategies following this form of attack. Wang et al. (2024) also reached a similar conclusion and suggested that although cybersecurity risks pose a significant threat to highly innovative companies, this should serve as an incentive to enhance cybersecurity measures instead of paradoxically reducing innovation activities.

2.9.12 Linking subcategory summaries to research gaps and interview format

The preceding subcategory summaries in sections 2.9.1 to 2.9.11 highlight the recurring challenges, proposed solutions, and limitations identified in the current literature on cyber-risk mitigation in SMEs. A key insight from this review is the limited empirical insight into SMEs' cybersecurity practices, especially within the German manufacturing context. Much of the academic discourse in this area has focused on theoretical frameworks, desktop analysis, or technical modelling, with relatively few studies capturing the actual experiences, decision-making processes, or perceptions of SME managers.

The absence of such practical, experience-based evidence enabled the identification of the formulation of the research gaps outlined in section 2.10, which directly informed the study's research questions. These gaps also shaped the empirical research design, with the key themes from the literature, such as risk assessment, challenges, cloud-based solutions, insurance, and training, mapped into the structure of the semi-structured interview guide. This approach ensured alignment between the academic discourse and the real-world context of SMEs. Although the literature review has presented the debate associated with SMEs, the research gaps and associated questions identified in this section have been deliberately narrowed to focus on the empirical scope of the experiences of medium-sized enterprises. This focus and refinement both align the study's methodological design with the purpose of the project: to explore the cyber-risk mitigation strategies in greater depth, specifically from the perspective of the German manufacturing sector. The resulting themes were not only used to formulate the research questions but also informed the semi-structured interview guide, as detailed in section 3.12.

This approach ensured that the theoretical insights from the literature were grounded in and tested against the practical realities faced by German manufacturing medium-sized enterprises. The resulting themes were not only used to formulate the research questions but also informed the semi-structured interview guide, as detailed in section 3.12.

2.10 Summary of the literature review and the identified research gaps and informed research questions

In this section, an extensive summary of the above literature review will be presented alongside the identified research gaps that informed the formulation of the research questions. The chapter has presented the relevance of using cyber-risk assessment tools, which can be

either based on a systematic analysis of the cyber-risk exposure or alternatively informed potential risks. What emerged from the literature review was the topic of cyber-risk mitigation (CRMi) as being a critical issue for SMEs. The chapter has indicated that SMEs often do not have adequate cyber-risk strategies and insurance implemented within their organisation. The primary reasons can be attributed to a lack of resources, personnel, expertise, financial, and cybersecure systems, but also to the fact that SMEs tend to overestimate their level of preparedness against cyber-risks. This has led to the first research gap:

- **Resulting research gap 1: Limited research exists on the actual level of preparedness against cyber-risks, especially in the German manufacturing context.**

A cyberattack can have significant consequences, such as operational or financial losses and potentially reputational damages, which could lead to exclusion from supply chain activities. This may be due to the fear and perception that the SME may compromise other entities in the supply chain and possibly a higher level of risk exposure.

The literature review also identified the trend towards outsourcing various activities, including cloud-based services, which can enhance cybersecurity. This strategy also addresses the identified lack of knowledge and resources in a SME, which could be addressed by a collective or shared approach. The literature review suggests how companies could work collectively to exchange information, resources, and patches to enhance cybersecurity.

There were a small number of publications focused on training programmes, which included how to assess cyber-risks and how to manage or respond to a potential attack.

- **Resulting research gap 2: There is insufficient insight into the cyber-risk mitigation strategies currently adopted by German medium-sized enterprises.**

Since cyber-risk insurance is considered to form one important element of a company's CRMi strategy, the technique of risk transfer to a third party, coverage elements, and the complex interplay between the medium-sized enterprise's CRMi and the insurer's requirement are outlined in a separate chapter on "cyber-risk insurance" (see section 5.3).

As regards potential insurance coverage (see section 5.5), a discrepancy between medium-sized enterprises' wishes for cover and actual claims was found. While enterprise managers desire protection against business interruption or loss of customer data, most claims are related to incident response.

Ransomware emerged and constituted an increasing risk, which can potentially lead to higher financial damages related to this type of attack; however, both insurers as well as their clients are increasingly aware of this problem.

- **Resulting research gap 3: Limited understanding exists regarding the role of cyber-risk insurance within German medium-sized enterprises and what risks are effectively covered by existing insurance policies.**

The research gaps identified from the systematic literature review provide the basis for the formulation of the study's central research questions. These questions are derived directly from the gaps outlined above and are presented as follows:

- **RQ1: What are the risk mitigation strategies adopted in German manufacturing medium-sized enterprises to mitigate against a cyberattack?**
- **RQ2: What is the relationship between specific risk factors and risk mitigation strategies within medium-sized enterprises?**
- **RQ3: How do medium-sized enterprise managers consider cyber-risk insurance as a vital option within their risk mitigation strategies?**

3 Chapter Three Methodology

3.1 Introduction

This chapter will present, discuss and justify the methodology adopted in this research project to study the perceptions and experiences of mitigating against cyber-risks and attacks in German manufacturing medium-sized enterprises. However, one of the fundamental questions that needs to be asked, considered, and addressed in any research social science project is what the nature of reality is and how knowledge can be gained. To achieve this, there is a need to understand the ontological and epistemological issues associated with this research project. A study's methodology tends to consist of collecting, analysing, and using data to address one or more research questions or problems to achieve the research objective(s) (Saunders et al., 2020). Therefore, the methodology involves the researcher attempting to establish the reality or knowledge needed to address the focus of the study. Gill and Johnson (2002) stated that the choice of a research method needs to clearly set out and the researcher should justify the assumptions associated with the nature of knowledge and the method or methods used to gain a critical insight into the phenomena being examined.

Reflecting on this, this chapter intends to outline the strategy adopted from a philosophical perspective and the research approaches used when conducting the main study. This will include the rationale behind the choices made before presenting the study's potential limitations. As both Silverman (2021) and Blaikie (2007) noted, most researchers inevitably tend to face the dilemma of needing to decide the most appropriate research methodology. In facing this challenge, it is necessary to recognise that there is often a tension between the nature of what is being investigated and the researcher's own worldview. Blaikie (2007) captured this by stating that the world is made up of representations that are creations of individual minds' (Blaikie, 2007, p. 16) and not simply based on the existence of independent truths. Therefore, it is necessary to obtain knowledge about reality based on the worldview of the researcher. Reflecting this, this study adopted what Blaikie (2007, p. 8) called an inductive approach, which is seen as being a "bottom-up" strategy to understand the concept and theories related to social life and actors. By adopting this approach, it is then possible to generate an accurate and authentic account that enables the research results to accurately

reflect the experiences and perceptions associated with the strategies adopted to mitigate against cyberattacks in German manufacturing medium-sized enterprises.

3.2 Research philosophy

Research philosophies are academic assumptions which describe an individual researcher's understanding of social reality, which is accepted in a particular academic field (Bryman & Bell, 2015). The philosophy of research can be defined as a broad concept that indicates the way knowledge and its nature relate to the research. Saunders et al. (2020) contended that research philosophy is a broad term which refers to a system of beliefs and assumptions about the development and the nature of knowledge that informs the research project.

Through undertaking the research, the researcher can enhance their understanding of the knowledge by applying existing research theories, materials, and studies to the intended project design (Easterby-Smith et al., 2002). Therefore, the researcher needs to determine the research design and strategy for the study, which is often referred to as the research paradigm. Guba and Lincoln (1994) argued that a research paradigm consists of three basic features, which can be used to characterise the ways of studying a social phenomenon, such as the cyber-risk mitigation in a medium-sized enterprise (Saunders et al., 2020). The research paradigm is determined by the way a researcher approaches the basic research questions in terms of their ontological, epistemological, and methodological positionality (Guba, 1990). In the next sections, the methodological perspectives of a research paradigm are justified.

3.3 Research strategy

The research strategy is the choice that finally leads to the adoption of a specific set of ontological and epistemological assumptions that the researcher will follow (Blaikie, 2007). Easterby-Smith et al. (2021), and earlier Alvesson and Deetz (1999), noted the distinction between quantitative and qualitative approaches or paradigms. One of the important considerations that all researchers need to understand and follow is having a clearly defined research strategy. This decision in determining the research approach is important; however, considering and understanding the ontological, epistemological, and axiological implications is critical. If these research fundamentals are not considered, the outcome of the study can lead to

unintended research results. The strategy adopted in this study was a qualitative interpretative approach, as the key method of inquiry reflected the researcher's philosophical position. In light of this, the next section will specifically set out the philosophical position of this study, commencing with the ontological position.

3.4 Ontology

Ontology is a branch of philosophy that is concerned with the nature of what exists (Crotty, 1998). Therefore, ontology is centred on how the researcher chooses to define what is reality and what is real. Ontology comprises the nature of reality and its existence (Easterby-Smith et al., 2021), in the sense of defining an understanding of reality. Therefore, the ontological questions every researcher must ask are: what is the nature of reality, and what is the knowledge associated with this reality? The knowledge of reality for this study is to interpret the experiences, perspectives, and perceptions of the participants as to mitigating against cyber-risks and attacks in a German manufacturing medium-sized enterprise.

The ontological stance of the researcher consists of how the nature of social reality can be captured. Ontology is often classed into two opposing groupings or paradigms: positivist and social constructivist, which are also referred to as objectivist and subjectivist. While positivists contend that knowledge can be obtained through objective measurement and classification of an independent external reality, this research study takes the opposite position, as it was seeking a subjective lens of reality. Being subjective, this study's ontological positionality takes the view that "something exists only when you experience it and give it meaning" (Hatch & Cunliffe, 2006, p. 12), which is relevant when studying the experiences of German manufacturing medium-sized enterprises when mitigating against a cyberattack. Therefore, the ontological positionality of this constructionist research study assumes that these German-based medium-sized enterprises do not extensively mitigate against potential cyberattacks, however, have various strategies in place, which are informed by their perceived risks.

3.5 Epistemology

Unlike the ontology, but closely aligned to this concept, epistemology is based on how the researcher forms knowledge and how the data to do so will be gained (Hatch & Cunliffe,

2006). Epistemology is therefore focused on the theory of knowledge, which assists the researcher to find the best means to understand and explore the nature of the world (Easterby-Smith et al., 2021). Epistemology is therefore concerned with how the researcher understands and knows reality. The epistemological question is, therefore: what is the nature of the relationship between knowledge seekers and knowledge?

Given the subjective nature of this study, the research's epistemology position must align with the philosophical approach that determines and establishes the type of knowledge that exists. Reflecting this, Crotty (1998, pp. 8–9) stated that epistemology "is the theory of knowledge embedded in the theoretical perspective and thereby in the knowledge." Therefore, for this study, its worldview is focused on interpreting the perceptions and experiences of mitigating against a cyberattack. Therefore, the constructivist's epistemology is a subjective view of social issues based on the reality of addressing cyber-risks. The social constructivist view is that reality is not a single truth but multifaceted. Here, the reality is not external or objective but must be socially constructed, and meaning can only be understood through people's interactions with others (Easterby-Smith et al., 2021).

The social constructivist approach of this study was focused on the experiences and perceptions of those in German-based manufacturing medium-sized enterprises as to their mitigating cyberattack strategies, but also drawing on the researcher's experiences in this field of interest (see Personal Reflection, section 6.18). The next section outlines the research design that was used to collect the data.

3.6 Research design

A research strategy is essential to ensure that the findings are dependable and trustworthy, which are vital for a constructivist study. Reflecting this, and to achieve the intended outcome, the research design needs to ensure that the selection of a method and then deciding a framework are essential when conducting the research. The research design can therefore be defined as the "research plan", which includes and incorporates the research aims, the purpose of the study, the intentions, and ideas. The research design was focused on German-based manufacturing medium-sized enterprises as a sector but was not considered a case study. Instead, the research design for determining the participants was based on the following criteria, informed by the current definition provided by the European Commission:

- The staff headcount.
- The annual turnover or the equity in the balance sheet, based on the latest approved. accounting period.

This is illustrated in Table 3-1, as the SME classification:

Table 3-1: SME classification (according to ABl. of the EU L 124/36)				
Company category	Staff headcount	Annual turnover	OR	Annual balance sheet total
Medium-sized	< 250	≤ EUR 50 million		≤ EUR 43 million
Small	< 50	≤ EUR 10 million		≤ EUR 10 million
Micro	< 10	≤ EUR 2 million		≤ EUR 2 million

Table 3-1: SME classification (according to ABl. of the EU L 124/36 of 20.05.2003)

The selection of SMEs for this study eventually led to a focus on the category of "medium-sized" companies, with two of the companies with slightly higher staff headcount and annual turnover. The next section presents the study participants' profile.

3.7 Research participants

The rationale for selecting a certain participant for this study was primarily informed by ensuring those selected had the correct experience around cyber-risk mitigation strategies. However, this approach to the research design was also focused on avoiding a one-sided view of the research problems and themes, which meant that the initial selection drew on the industry database of the IHK-Bayern "Industrie- und Handelskammer" to provide a wide scan of the sector. The following selection criteria were applied:

- All states in Germany
    - Industries: Automotive, industry and production, manufacture of high-tech series products, production of models, samples, or prototypes, development of products, measurement, testing, and analytics.
- Economic sectors
    - Production of paper, cardboard, and associated goods, production of printed matter, reproduction v. recorded sound, and image, production of chemical

products, pharmaceutical products, rubber and plastic goods, glass and glassware, ceramics, stones, earth, and metal products.
    - Production of data processing devices, electronic and optical products, electrical equipment, mechanical engineering, motor vehicles and motor vehicle parts, and production of furniture.
- Company size classes
    - 100 - 199 employees
    - 200 - 499 employees
- Company type and legal form
    - Headquarters or branch office permanently established

The database query generated 956 potential companies, of which 50 were randomly selected by the researcher. The address registered on the database was used to contact the companies, either via the company website or by contacting the C-level manager based on their published personal contact details. A cover letter was sent (see Annex 1), which contained a brief description of the research project and an outline of the interview. After two to three weeks, individuals were contacted by telephone and asked about their willingness to participate in the study.

Of the total of 50 medium-sized enterprises and individuals contacted, five experts from five different companies tentatively agreed to participate. However, none of those initially considered were ultimately prepared to be interviewed due to the sensitivity of the topic. The feedback and reason for not committing to the study included:

- We generally do not provide any sensitive information to third parties.
- We are currently very busy with various projects and internal commitments. Unfortunately, we therefore have to reject your request. Nevertheless, thank you for your interest and for your understanding.
- We have discussed this internally and would not like to provide any information about it. Nevertheless, we wish you much success in your research work.
- After consultation, there is no interest in an interview.
- We do not disclose any information about our IT security.

Following this outcome, the study selection process sought to engage with three prominent industry associations:

- Branchenverband der deutschen Informations- und Telekommunikationsbranche (Bitkom, Industry Association of the German Information and Telecommunications Sector),
- Bundesamt für Sicherheit in der Informationstechnik (BSI, Federal Office for Information Security), and
- Verband Deutscher Maschinen- und Anlagenbau e. V. (VDMA, German Mechanical Engineering Industry Association).

These associations were active in providing press releases on SME IT security issues, including statistics on different characteristics related to cyber issues. The public relations manager at Bitkom was contacted, and after internal consultation with their security expert, the following email message was received, declining the offer to assist:

> *"After consulting with our security experts, I unfortunately do not see any direct possibility of supporting you. It is also difficult for us to reach the SMEs from the manufacturing industry that you are addressing; we carry out our studies as representative telephone surveys with the help of an external service provider, not as membership surveys. Perhaps the BSI and the people responsible for the Alliance for Cyber Security there could help you further."*

Based on the advice from Bitkom, the researcher then contacted BSI, firstly via an email and subsequently a follow-up telephone call. BSI also declined to assist:

> *"…we do not support academic work, and we are also not willing to disclose any contact details of member companies due to GDPR reasons, and we also do not contact member SMEs to promote academic work."*

Finally, an email contact was made to the VDMA but resulted in no reply.

The researcher then reached out to various third parties who had close contacts with German manufacturing medium-sized enterprises. These individuals were either known privately or through previous business relationships and were requested to act as a gatekeeper or intermediary to recruit suitable medium-sized enterprises.

The researcher was uncertain about the number of medium-sized enterprises which could be accessed to participate in this research project, as the initial feedback revealed that the managerial leaders of these medium-sized enterprises harboured concerns and a reluctance to disclose sensitive information about their company's cyber strategy. However, through

the establishment of reliable private and/or business relationships, nine interview partners finally agreed to participate.

The reason the participants ultimately agreed to discuss a highly sensitive and strategically guarded topic such as cyber-risk mitigation can be largely attributed to the researcher's existing professional position and personal network. After formal outreach to randomly selected firms and established industry associations proved unsuccessful, largely due to confidentiality concerns and reluctance to disclose information on IT security, access was achieved exclusively through trusted intermediaries who acted as gatekeepers. These contacts, drawn from the researcher's private and professional circles, facilitated introductions to the managers of medium-sized enterprises who were otherwise unlikely to participate. All nine interviewees who took part in this study were recruited via this informal, trust-based approach.

Importantly, the researcher had no influence over which companies were contacted by these intermediaries, meaning the final selection was shaped by availability and opportunity rather than strategic targeting. While this introduced an element of randomness in sector and geographic distribution, it reflects the pragmatic reality of gaining access for research in this field.

From a constructivist perspective, this access strategy is fully aligned with the study's epistemological stance, since the knower and the known are inseparable (Lincoln & Guba, 1985), and knowledge is generated through relational trust and co-constructed meaning (Charmaz, 2014; Kraus, 2013). Knowledge was generated through relational trust and co-constructed meaning, rather than objective detachment. Moreover, the research design employed a triangulation strategy that included theoretical triangulation through insights from the systematic literature review, empirical triangulation by comparing perspectives across nine medium-sized enterprises managers from diverse industrial sectors, and experiential triangulation, where the researcher's own professional background informed both access and the nuanced interpretation of participant responses. This layering enhanced the credibility and interpretive depth of the study, while acknowledging that the findings are contextually grounded rather than universally generalisable.

The profile of the participants is shown below in Table 3-2:

Table 3-2: Profiles of participants and medium-sized enterprises						
Inter-view partner	Position	MSE	Industry sector	Staff headcount	Annual Turnover in €M	SME classifica-tion
1	MP	One	Semiconductor	70	50	midsized
2	MP	Two	Print technology	250	54	midsized
3	MP	Three	Electronics	115	15	midsized
4	MP	Four	Plant engineers	270	60	midsized
5	MP	Five	Metal processing	195	45	midsized
6	MP	Six	Confectionery	250	50	midsized
7	EVP IT	Seven	Metal processing	100	38	midsized
8	MP	Eight	Woodworking	72	10	midsized
9	CIO	Nine	Metal processing	290	65	midsized
Legend: MP: Managing Partner, EVP: Executive Vice President, CIO: Chief Investment Officer						
All participating medium-sized enterprises (MSE) were based in Germany and represent medium-sized firms. For reasons of confidentiality, individual company locations are not disclosed in the table; however, participants were drawn from the following federal states: Baden-Wuerttemberg (4), Bavaria (2), Hesse (1), Lower Saxony (1), and North Rhine-Westphalia (1).						

Table 3-2: Profile of the Participants

While the original aim was to focus on medium-sized enterprise managers entrusted with or responsible for cyber-risk mitigation in order to capture a variety of organisational perspectives, the final interview sample reflects a strong managerial focus, with participants typically holding the position of owner and/or executive director. This outcome was shaped both by the strategic design of the study and by practical constraints in accessing participants. In many German mid-sized manufacturing firms, IT and legal functions are either outsourced or not organised as separate departments. Cybersecurity responsibilities are often centralised at the executive level, particularly in firms with lean administrative structures. Due to the sensitive nature of the topic, most companies preferred that only top-level managers speak on their behalf. While the study does not focus on technical implementation or legal frameworks, the inclusion of two IT executives the CIO and EVP IT helped ensure that operational aspects were

still reflected in the managerial narratives. A more technical investigation would have shifted the study's focus away from strategic decision-making and into system-level or compliance-based discussions, which were not central to this research.

3.8 Research methods

In choosing the research method, consideration was given to how to generate rich data through exploring the individual perceptions and insights of the sensitive issue of mitigating against cyber security risks and attacks. The study opted for a semi-structured interview strategy, as the approach offers a flexible option that enables the discovery of unexplored areas but also enables the researcher to expand on new and emerging themes (Mitchell & Jolley, 2010). For Mitchell and Jolley (2010), semi-structured interviews also allow the researcher to ask the participants to clarify the areas of specific interest and importance as they emerge from the interviews. The use of semi-structured interviews therefore enabled the investigation of those participants' perceptions, which was conducted on a one-to-one basis as the subject area was sensitive. This usage of semi-structured interviews also enabled a high content of validity to be achieved using pre-defined concepts generated and informed by the current academic debate by means of open questions (Mitchell & Jolley, 2010). The next section focusses on the different research approaches available but also justifies the strategy adopted.

3.9 Research approach

While conducting any research project, it is possible to apply a variety of different approaches, methods, and techniques for the data collection strategy. Bryman (2016) noted that there are two forms of research approaches: deductive and inductive, which are related to the two key research methods, quantitative and qualitative. The deductive and inductive approaches together with the two research methods are presented in the following sections, beginning with the deductive approach, even though an inductive strategy was selected.

3.9.1 Deductive approach

As an approach, deductive reasoning is a means of testing a theoretical proposition through a research strategy that either proves or disproves a hypothesis or an assumption (Saunders

et al., 2020). Bryman and Bell (2017) and Woiceshyn and Daellenbach (2018) contend that a deductive approach can be characterised as the relationship between research and theory, while Rubin and Babbie (2020) argued it can be defined as a research process that is grounded in deductive logic in which the researcher begins with a assumption before deducing hypotheses and, finally, gathering data to test or validate the original assumption. The deductive research approach tends to move from the general to the particular in the sense of beginning from a theory and deducing hypotheses from it by testing them and reconsidering the theory (Locke, 2007; Nola & Sankey, 2007; Trochim, 2006). The deductive approach consists of quantitative features in which numerical data is presented in a statistical format to understand the relationship between theory and research; therefore, it is closely aligned to positivism.

3.9.2 Inductive approach

Locke (2007) and Woiceshyn and Daellenbach (2018) stated that an inductive approach is the opposite of deductive reasoning. This means moving from the specific to the general, where empirical evidence of a phenomenon or area of new interest is understood before the development of concepts and theories. Crowther and Lancaster (2012) argued that inductive research is an approach that generates new outcomes and theories, as opposed to proving or falsifying a hypothesis, as the existing knowledge does not fully exist or remains unknown. Based on the two approaches, inductive reasoning was the most suitable because it enabled the development of new theories as the existing knowledge of cyber security risks and mitigation strategies remains unknown from a German medium-sized enterprise perspective.

3.9.3 Quantitative approach

Closely related to the debate associated with deductive and inductive approaches is qualitative and quantitative research. Bryman (2017) distinguished between two types of research methods: qualitative and quantitative. The quantitative method focusses on generating topics for a critical demonstration of a determined research problem, which is based on existing or known knowledge. To generate the data, a questionnaire or survey is often used for a quantitative research project because it provides a quantitative instrument to measure facts or opinions of a population (Creswell & Creswell, 2017). For Becker et al. (2012), quantitative

researchers tend to seek explanations and predictions that can be generalised to the population being sampled. Quantitative research therefore includes comparatively large and representative data sets; otherwise, a generalised inference cannot be made. This need for a large data set is problematic, as in this study, the number of participants is limited due to the sensitivity of the subject area.

Quantitative methods have advantages as well as disadvantages. One of the advantages of a quantitative method is that it is considered an objective method for illustrating facts that are largely constant, but this information or knowledge needs to exist (Silverman, 2024). However, one major disadvantage of using questionnaires or surveys is the researcher's limited ability to ensure that responses are valid and reliable. For instance, there is often no way to confirm that the intended participant completed the survey, which can compromise data quality. Additionally, while surveys allow respondents to answer sensitive questions more honestly due to anonymity (Silverman, 2024), they rely on well-established theoretical frameworks to be effective. If the underlying knowledge is unclear or incomplete, designing a meaningful questionnaire becomes challenging, potentially leading to misleading or unusable data.

3.9.4 Qualitative approach

While a quantitative approach is usually closely related to positivism, a qualitative strategy is closely related to interpretivism. As a philosophy, positivism holds that only known or factual knowledge can be obtained through measuring (Moses & Knutsen, 2019), an interpretive paradigm contends that knowledge is gained by understanding the viewpoints and perceptions of those being studied (Easterby-Smith et al., 2021).

Gray and Grove (2020) argued that qualitative research is an interpretive methodological approach that provides more subjective data than quantitative research. A qualitative study is the means to provide a comprehensive approach to study and understand a social phenomenon, and therefore requires in-depth criticality and probing, while engaging with multiple perspectives (Marshall et al., 2021). Bryman (2016) described qualitative research methods as having a flexible structure that allows the research focus to change as the research progresses. In comparison to quantitative methods, where the researcher is isolated from what is being studied, qualitative methods enable the researcher to become part of the research

process, which provides a deeper understanding of the context of the study. Furthermore, the data collected tends to be in the form of words, text, and images, and when this data is analysed, a theory or new insight can emerge.

In the search for deeper understanding, a qualitative approach typically studies fewer participants, so it does not attempt to determine generalised patterns. Through adopting an inductive qualitative approach, it was possible to determine the various strategies adopted in these German-based manufacturing medium-sized enterprises to mitigate against potential cyberattacks.

3.10 Data collection technique and development of the interview protocol

Once the methodology was established, a pilot interview was considered before proceeding and conducting the main study. At the outset of the literature review, several significant themes emerged which informed the interview questions; however, due to the limited number of potential participants a dedicated pilot study was not feasible. Nevertheless, the researcher recognised the importance of undertaking a pilot study, therefore the first interview was seen as being a pilot but also part of the main study, by including a reflection on lessons learnt from this interview that were then used to inform the subsequent interviews. As the purpose of the pilot study is to determine whether the themes emerging from the literature review are valid, and to ensure that the interview addressed the central aim of the study, this first interview was important (Oppenheim, 2000).

The first interview revealed that the pilot exercise was essential. Firstly, the pilot interview involved testing the wording of the questions, establishing the length of the questionnaire, avoiding ambiguous questions, and making suggestions for analysing the data, along with testing the technique selected for collecting the data. Secondly, the data from the first interview confirmed that the six main categories in the interview guideline were well-chosen to align with the research objectives and purpose of this study, effectively matching the intended framework.

However, after considering some of the responses about cyber-risk management and mitigation strategies, and their potential influence on more sustainable and enhanced business success, an important refinement emerged from the pilot interview. Initially, the questions

focused heavily on the risk manager's technical expertise in cyber-risk mitigation. Upon reviewing responses, it became clear that a broader management viewpoint was required, one that captured the leadership's strategic approach to risk rather than purely technical considerations. This shift was particularly significant for medium-sized enterprises, where decision-making regarding cyber-risks is not solely the domain of risk managers but is often influenced by leadership and management perspectives on business sustainability.

For instance, the pilot interview revealed a sense of self-assuredness among medium-sized enterprise leadership regarding risk assessment, along with an acceptance of potential threats and a pragmatic view of the likelihood of advanced AI-driven attacks and ransomware incidents. This managerial confidence in assessing risks shaped their approach to mitigation, emphasising risk acceptance rather than outright elimination, as well as the role of compliance with industry norms and certifications in managing cyber-risks. These insights underscored the need to refine the interview questions to better capture how medium-sized enterprise leadership perceives and integrates cyber-risk management within broader business strategies, particularly in the context of supply chain requirements and cyber-risk insurance.

To enhance the robustness of the first interview and ensure a structured approach, an action research loop was adopted (Kemmis et al., 2014). This iterative approach involved obtaining critical feedback from the participant both before and after the interview to evaluate how well the protocol was followed. However, it should be noted that the action research loop was applied only for the first interview and not for the subsequent ones, although ongoing improvements were made throughout the study.

One of the key reasons for using an action research spiral model, as advocated by Kemmis et al. (2014), was to allow the researcher to gain a deeper understanding of the interview protocol in practice. Additionally, it facilitated a structured pre-planning process, providing firsthand insights into how interviewees—particularly medium-sized enterprise managers—responded to the research questions. This approach also helped evaluate how medium-sized enterprises leadership perceived and articulated their role in cyber-risk management, offering valuable insights into their strategic decision-making processes in contrast to a purely technical risk assessment perspective.

3.10.1 Outcome of the first interview

The emerging themes were generated from the literature review to create the main study interview protocol. These central themes included cyber-risk management practices, German medium-sized enterprises' cyber-risk strategies and their components, cyber-risk in the context of Industry 4.0 and IoT, the relationship between cyber-risk management and business success, and the role of cyber-risk insurance within German medium-sized enterprises, including the risks covered by existing insurance policies. The interview protocol encompassed these central themes and provided a basis for subsequent follow-up interview questions. The interview protocol provided a detailed summary as to the necessary steps to be followed in conducting the interviews. This ultimately formed the basis of the researcher's guidance for the interviews and for notetaking during the protocol, which included noting any thoughts, reflections, and particular observations about the participant, and was ultimately used throughout all the interviews. This process provided an informative reference and an aide-mémoire, acting as a memory aid during the coding process. The protocol proceeded by following this sequence of steps:

1. The participant's general experience: As mentioned above the participant was asked in advance by email, and then through MS Teams, to complete the consent letter that included an overview of the themes to be addressed in the interview. The participant was asked to schedule a date for an interview at their convenience. The reason for this approach is that the participant could freely arrange the interview time according to their availability. Reflecting the University's ethical guidelines, the accompanying information also stated that the data would be kept confidential, and that the participant's identity would remain anonymous.
2. Interview warm-up. Critically aware that most research interviews are generally conducted between strangers, the protocol can be constrained by time and can include a great deal of personal and possibly sensitive information, which may not be adequately discussed. To address this the first part of the interview covered the research aim, reassuring the participant of confidentiality, anonymity, and requesting permission to record the interview, and the assurance that they would be provided with a summary of the overall research outcomes at an appropriate future date if they wanted.

The data collection for the first interview/ pilot project and subsequent interviews was undertaken in five stages:

- Stage 1 - Involved initially approaching the identified contacts independently requesting whether they were prepared to participate.
- Stage 2 - An email was sent to those who agreed to participate to confirm their participation.
- Stage 3 - Once the participant agreed to participate and the background information had been received, arrangements were made to meet via Microsoft Teams, and the participant was informed what to expect in the interview.
- Stage 4 - Conducting the interview via Microsoft Teams due to COVID-19 restrictions and precautions.
- Stage 5 - At the end of each interview, the participants were asked for feedback about the interview process.
- Stage 6 - During the first interview phase, then with the main study, consideration was given to the participants' non-responsiveness. Where a question was unanswered, the researcher determined whether the question needed to be reworded due to misunderstanding. If the non-responsiveness was associated with the theme, the interviewee was reminded of their right to end the interview or to continue the process, but to focus on another theme.

3.10.2 Outcome of the Pilot study

The findings of the first interview / pilot study were analysed from two perspectives. Firstly, as to the extent that the research strategy and interview protocol were effective and suitable, and that the outcome achieved the study's aim. The results from the pilot study were designed to ensure that the main fieldwork research protocol was effective and suitable. Another consideration was given to the power relationship between the participants and the researcher, in the language used, and finally to determine whether the pilot study generated sufficient in-depth and rich data.

Table 3-3: The outcomes of testing the research protocol	
The outcome of testing the research protocol	Outcome
Test whether the selected tool (Microsoft Teams) was suitable for the intended process.	The tool selected for the interview was found to be suitable.
Determine the appropriateness of the process to generate information and rich descriptions and avoid repetition.	Data from Interview 1 indicated that six categories were effective in achieving the research objectives. However, the interview questions were adjusted to incorporate management perspectives (see Annex 3). Adherence to norms and certification procedures, particularly for medium-sized enterprises involved in supply chains and for preparing for cyber-risk insurance, was identified as crucial for effective cyber-risk mitigation.

Table 3-3: The outcomes of testing the research protocol

As can be seen above from Table 3-3, the outcome of testing the research protocol informed the main interview protocol. The pilot interview revealed that Medium-Sized Enterprise One's experience demonstrated a reactive approach to cybersecurity, focussing on internal security measures like backups and firewalls after phishing attacks. The company prioritised meeting legal requirements but avoided exceeding them due to cost concerns. While the interviewee, as the manager, acknowledged the importance of contingency planning and redundancy, he remained hesitant to invest in cyber-risk insurance (CRI), viewing it as unnecessary given their existing internal safeguards. The interviewee's reliance on business interruption insurance for non-cyber-risks like a fire over CRI reflected a broader perception that cyberattacks are less of a threat to smaller businesses, despite growing evidence of their vulnerability.

Furthermore, the pilot study generated several topic areas, which informed the final interview questions:

- Firstly, the fine-tuning of the questions to assist in comprehending the reasons or obstacles that prevent the development of a formal cybersecurity risk mitigation (CRMi) strategy or policy, along with those characteristics associated that determine the investment or prioritisation of cybersecurity measures.

- Secondly, since Medium-Sized Enterprise One relied heavily on internal capabilities, further questions were added regarding medium-sized enterprise's overall confidence in their current cybersecurity measures to protect against future attacks, especially in an environment where cyber threats evolve.
- Thirdly, to what extent does the rise of IoT in Industry 4.0 and the medium-sized enterprise's integration into larger supply chains present significant cybersecurity challenges and increase the cyber vulnerability, and to what extent does undergoing external certifications or insurance processes help mitigate such additional risk?

3.11 The fieldwork

For the first / pilot interview and then the main study, the process involved conducting the research using three distinct activities that needed to be undertaken before beginning the main study. The first activity involved documenting the emerging themes from the literature review, which provided the conceptual framework for the study. The second activity was based on the outcomes of the first or pilot interview, to ensure that the framework and the questions had sufficient depth to enable the research aim to be achieved. Finally, the third activity was to determine whether there were any additional themes emerging. The primary research was conducted over two months: it began in December 2023. The interviews on average lasted approximately 1 hour. The procedure followed is presented below in Figure 3-1:

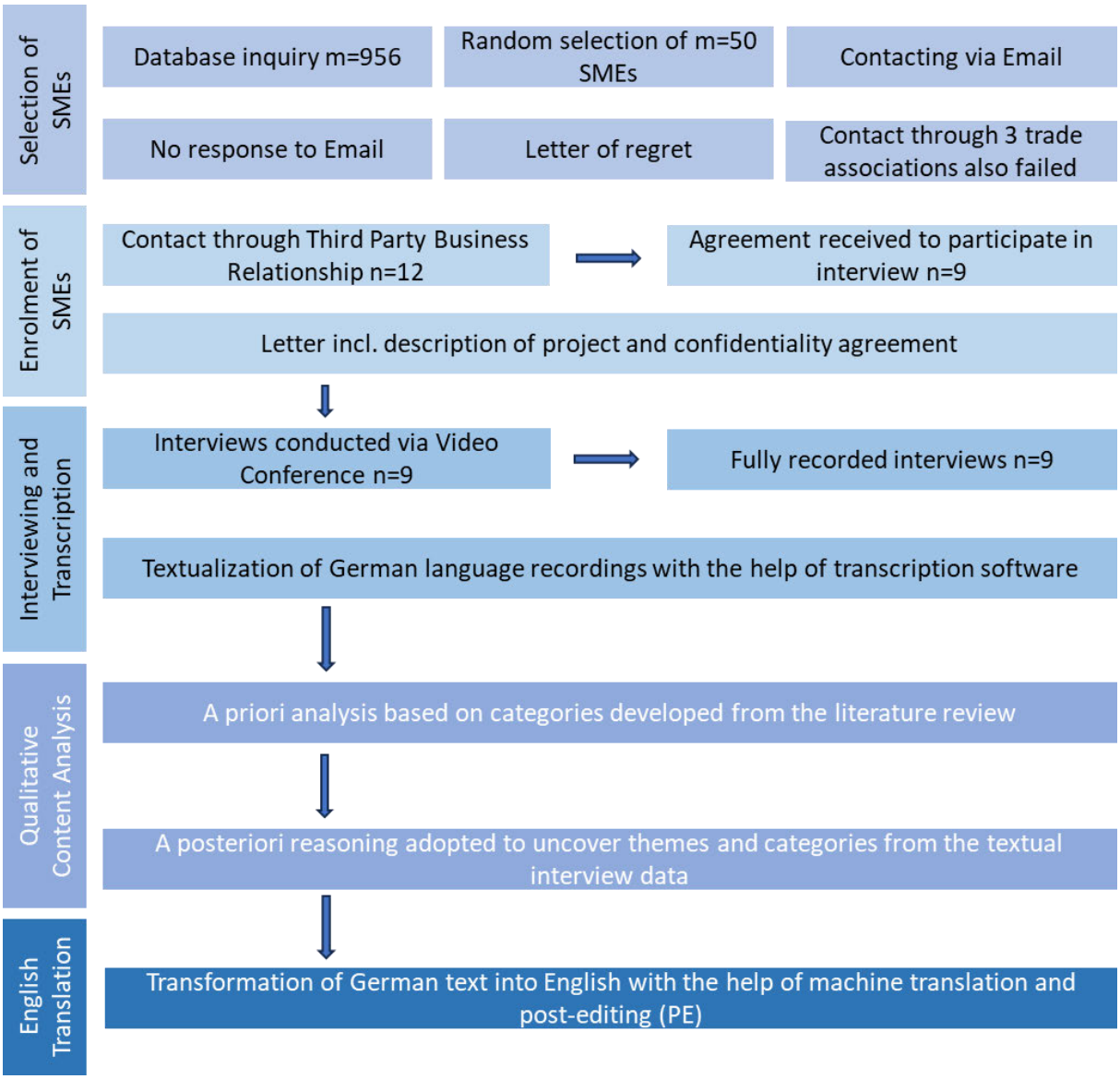


Figure 3-1: The format of the study (own presentation)

3.12 The interview format

The final interview format and questions were divided into six distinct phases. The first set of questions was the introductory section, which included a short introduction by the interviewer and an overview of the project. The interviewer then inquired about the company profile, which included a brief description of the sector, products produced, the number of employees, and the number of B2B and B2C clients, including the size of the B2B clients. The interview then moved to the professional background and experience of the interviewee, in-

cluding their technical or business education and experience within the sector and the company. The next step involved discussing the participant's role in the company, including whether they were the owner or an employee, as well as their managerial level.

The main section was focused on the information related to the company's cyber management strategies. The questions were linked to the research gaps identified in the literature review, as presented in Chapter Two.

- Theme One: Cyber-risk management practices.
    - What is the level of preparedness against cyber-risks within German medium-sized enterprises?
    - Has the interviewee's company already been a victim of a cyberattack?
    - How well does the interview partner consider the company to be prepared against cyber-risks?
    - Which cyber-risks does the interviewee consider to be a threat for their company?
- Theme Two: German medium-sized enterprise's cyber- risk strategies and what is involved.
    - Does the company have a cyber-risk strategy?
        - If answered YES to above, provide information about the cyber-risks?
        - If answered NO, explain the reasons why?
    - Provide information on which measures the company takes to manage or mitigate cyber-risk
    - From the measure adopted above, which are the most important ones?
    - When dealing with other companies like suppliers or clients, how does the company assess their cyber-risk exposure, and what mitigation measures and strategies are adopted?
    - What are the main problems for the company in context of cyber-risks?
    - What is the potential financial damage the company is exposed to in the context of cyber-risks?
    - What are the costs of the company's cyber-risk management and mitigation measures?

- Theme Three: Cyber-risk and Industry 4.0/IoT.
    - What is the interview partners assessment as to cyber-risk and Industry 4.0, modern networked production facilities?
    - Is the company affected by this issue?
        - If YES, explain how and what policies/measures exist in this context?
    - What is the interview partner's assessment regarding cyber-risk and Internet of Things (IoT)-devices?
    - Please explain how and what policies/measures exist in this context?
- Theme Four: Cyber-risk management and business success.
    - How does the interviewee consider cyber-risk management to contribute to business success?
    - Where does cyber-risk management stand in context with other business success factors?
- Theme Five: What is the role of cyber-risk insurance (CRI) within German medium-sized enterprises and what risks are covered by existing insurance policies.
    - Has the company ever purchased CRI, has insurance in place, or is considering taking out cyber-risk insurance? Please explain the reasons why or why not.
    - What types of risks are or intended to be covered in existing or planned cyber-risk insurance?
    - Where does the interview partner see CRI as an element of cyber-risk management strategy?
    - How does the interview partner assess the relationship between insurance costs and damage costs covered by CRI?
    - How does the interview partner assess an acceptable relationship between costs for cyber-risk management and mitigation and CRI?
    - What risks does the interview partner considered to be manageable by a company's cyber-risk management strategy and measures and what residual risks should be covered by CRI?

In a final concluding section, the interview partners were given the opportunity to provide additional information relevant to cyber-risk and cyber-risk mitigation in the context of their company's business operations. This included other topics related to cyber-risk that were important to the medium-sized enterprises.

3.13 Content analysis

Holsti (1969, p. 14) contended that content analysis can be defined as “any technique for making inferences by objectively and systematically identifying specified characteristics of messages”. Weare and Lin (2000, p. 272) observe the “outline of content analysis as a systematic and quantitative scientific method for measuring the content of messages have existed for centuries”.

Given these premises, it is not surprising that content analysis is among the principal methods of inquiry recommended and preferred by constructivist scholars in various disciplines. As Weber (1990, p. 13) noted “there is no simple right way to do content analysis”. The methods must be defined according to the aims and problems of research. Content analysis can be used for many purposes, e.g., to identify the intention of those who communicate a message, to reflect the cultural patterns of groups and companies, and to reveal the focus of certain actors (Weber, 1990).

To start with, a useful differentiation of the unit of analysis is among the sampling, the recording, and the context units. For the recorded message, the focus is on the whole message received from the interviewee, which can be further subdivided in its various, separable components such as paragraphs, sentences, or single words. However, by doing so, it is imperative to remember the connection of separable components in relation to the whole context in which the specific message is located (Krippendorff, 2018; Weare & Lin, 2000).

In a next step, categories need to be developed, such as length, frequency counts, emphasis, and qualifications of certain parts (Krippendorff, 2018). The categories are pivotal for the assessment of validity and reliability of the analysis (Carmines & Zeller, 1979), and it is crucial to reach the right trade-off between “reliability” and “validity” of the categories (Weber, 1990). Finally, the level of internal consistency and accuracy depends on the ambiguity in the words’ meaning as well as by the choices made by the researcher in defining the categories and the coding rules.

The first level, the frequency of categories, analyses how many times in each transcript of an interview the categories of the vocabulary that have been created according to the main frames appear. Frames are general codes through which actors interpret complex issues. These interpretive schemes simplify external reality via a selective process through which

the actors emphasise certain aspects rather than others. Different frames represent alternative ways to address a "theme", which in this project could be almost anything, from "cyber awareness" to the "cyber-risk mitigation", "cyberattack", "cyber insurance", or "medium-sized enterprise success factors". Any construction of the cyber-risk mitigation process can thus be viewed as an effort across all these different frames.

The second level of analysis, which is called keywords in context (KWIC), illustrates the extracted piece of text where the term is inserted for a length of three lines, allowing a better understanding of its meaning. In fact, a word isolated from its context may cause some mistakes. For instance, identical words may have a different meaning, or some terms could be simply negations. Thus, interpretation and selection are essential tasks for guarantying effectiveness of content analysis tools.

The third level of analysis is the wordlist: the frequency of words, included in the preliminary vocabulary, used in the text. In recent years, social scientists have substantially increased the sophistication of content analysis tools, especially thanks to the advent of personal computers and the relevant, specialised software (Weare & Lin, 2000).

3.13.1 Qualitative content analysis according to Mayring

The qualitative content analysis followed the method by Mayring (2015, 2022) and Mayring & Fenzl (2014), using the eight steps shown in Figure 3-2:

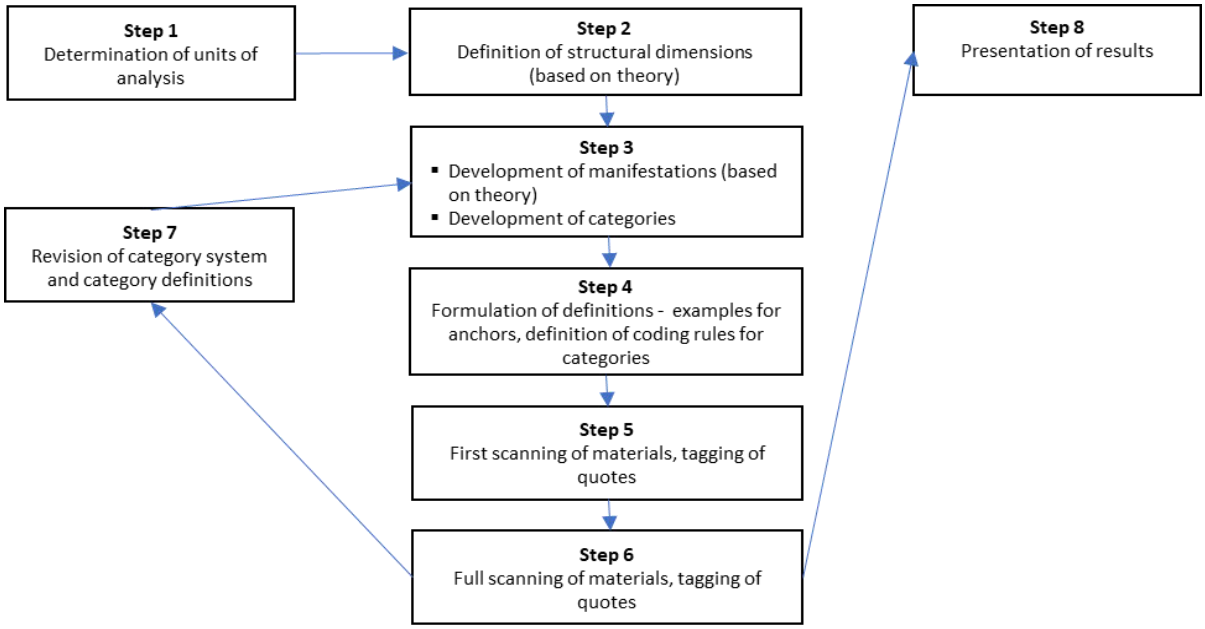


Figure 3-2: Qualitative content analysis

Source: Mayring (2015, 2022)

Using this approach, the first units analysed were the interviews. By following this approach, a series of structural dimensions were defined which were then aligned to the existing theory. The next step was associated with the manifestation of the theory which had emerged from the literature review. Then in Step 4, the definitions of the individual categories were set out and coding rules defined, based on the wording or type of statement, which is allocated to a specific category. Step 5 involved the first scan of a subset of interview data, and the quotes were grouped to the appropriate categories. This is then followed by a full scan of the entire interview data. In Step 7, a revision of coding was performed, which potentially resulted in a revision of the categories. If necessary, Steps 3 to 6 were then repeated. Once the coding process had finished, the results were then analysed and presented. An in-depth description and account of the analysis in this study will be presented later in Chapter Four.

3.13.2 Description of approach intended in this study

A content analysis based on the transcription of interview data can help learn more about essentially unavailable public issues. Content analysis involves developing "a set of procedures to make inferences from text" (Weber, 1990). For the application of this methodology, Klotz and Prakash (2008) propose considering a series of eight steps (which are quite similar to those proposed by Mayring, 2022), as outlined in section 3.13.1, before beginning the analysis.

3.13.3 The evolution of the research questions

Within the framework of this research project, the purpose of interviewing senior management leaders from German-based manufacturing medium-sized enterprises was to reveal how these individuals exerted control over cyber-risk within their organisation. The interviews were also designed to determine how mitigation techniques could be adopted effectively in a competitive business environment. To achieve this, a content analysis strategy was used to understand medium-sized enterprise managers' expectations, strategies, advisory systems, and the actions needed to ensure that cyber standards and norms were maintained and met. Therefore, the research questions asked were focused on seeking meaning from the interviews with these medium-sized enterprise leaders (Klotz & Prakash, 2008).

3.13.4 Selecting material

The rich insights gathered from the interviews was suitable for the content analysis, as the strategy enabled the examination of verbal and nonverbal behaviour (Hermann, 1986). As the study was focused on how senior management leaders, and in particular, Chief Executive Officer (CEO), Chief Information Officer (CIO), and Chief Risk Officer (CRO) in these medium-sized enterprises interpret the challenges associated with cyber-risk challenges, the use of a content analysis approach enabled the researcher to gain this insight from the interviewees. This included how leaders behaved and how the interviewees represented themselves through their responses. Ultimately, the interviews enabled the researcher to learn and understand the personal perspective of the interviewee as to mitigating against cyber-risk, and their style of decision-making.

After collecting and categorising the spontaneous interview responses generated from these medium-sized enterprise leaders, their managerial perspective provided a means to determine how these individuals saw and perceived cyber-risks. The data also helped the analysis to recognise sensitive interview context.

As the interview partners were leaders of German manufacturing medium-sized enterprises, and the research project being finally presented in English, the content of the interviews needed to be translated from German. This therefore created a challenge as to the accuracy of the translation process, as often words can mean different things in other languages. To overcome this, the interviews content was therefore analysed in their German original version.

3.13.5 Deciding on the nature of the content analysis

Since this project followed the research paradigm of interpreting and understanding cyber-risk mitigation strategies by interviewing medium-sized enterprise leaders, the focus of attention was not on the frequent use of certain words and phrases generated in the interview but what is likely to exist or be “present” or “absent” from the themes and meaning. This means that an interview response needed to be carefully examined for *“*what it conveys given its context and circumstances*”* (Holsti, 1969, p. 32). This type of analysis often involves working with several themes that may become significant, which can lead to the creation of independent nodes, or alternatively the outcomes emerge together.

While pursuing an interpretivist approach, although purely qualitative, it is worthwhile considering measuring the frequency of certain words or phrases, known as contingency analysis. Consideration was given to seek the frequency of these medium-sized enterprise leaders' usage of certain themes. The usage of contingency analysis enabled the exploring of words, phrases, or themes which emerged, which could be mapped out to evaluate a potential relationship between two categories (Hermann, 1986). In the context of this study, particular interest may be centred on the relationship between the emergence of a new cyberattack and how medium-sized enterprises plan to mitigate the risk. For example, please refer to the interview transcription in the Annex 4, which illustrates the cyberattack at 00:32:40 and the medium-sized enterprise's reaction to this incident at 00:35:42 in the recording.

3.13.6 Determining the unit of analysis and coding

By determining the number of questions asked, the researcher indirectly controlled the length of the material. From this, a system of enumeration or unit of aggregation was chosen. Once decisions were made regarding the units of analysis and enumeration, the researcher designed the rules and procedures to guide the process of drawing inferences from the material (Mayring, 2015).

As part of this process, the study specifically applied Step 5 of Mayring's (2015) approach when analysing the material generated from the interviews. This step involved focusing on verbs or action words to explore how medium-sized enterprise leaders took responsibility for cyber-risk management or initiated mitigation actions. Particular attention was given to how these actions were proposed or implemented by the medium-sized enterprise individuals, providing insights into their approaches to managing cyber-risks.

3.13.7 Contextualizing the information

Having decided on the unit of analysis and developed a set of coding rules and procedures, the next phase followed Step 6 (Mayring, 2015), which was used to contextualise the interview data to seek the nuances and complexities as to how cyber-risk could be mitigated. When the interview data was coded and the reoccurrences determined, any extreme or different beliefs expressed could be identified.

3.13.8 Determining reliability of results

In Step 7, this phase required the generation of results to be reliable or trustworthy, which is important when replicated by other researchers. In practice, this means that similar results are produced when similar coding rules are employed, rather than the duplication of the same perspectives from other German-based medium-sized enterprise leaders. This was achieved through using an intercoder strategy. Hermann (1986) described the intercoder strategy as enabling reliability of the data to be achieved to the extent to which there is an agreement as to how to code the same content, where the goal is to achieve consistency and validity.

3.14 Analysis and coding of the data

This section will present the two coding strategies, commencing with the literature review, before presenting the interview data.

3.14.1 Development of codes

Initially, a first list of codes was developed based on results from the systematic literature review, as presented in Chapter Two. As a result of this, an initial codebook is presented in Table 3-4 below:

Table 3-4: Analysis and coding of the data

Category	Code	Definition	Explanation
Assessment tool	Assessment	Tools and methods to assess and mitigate cyber-risk.	Focussing on tools and methods to assess and mitigate medium-sized enterprise's cyber-risk exposure including any visualisation of potential risks in business processes.
Assessment tool	Rating	Cyber-risk rating system.	Based on technical as well as behavioural aspects.
Assessment tool	Technology	Technical aspects to reduce or mitigate cyber-risk.	Includes network protection, system configuration, access control, protection against malware and system update.
Assessment tool	Behaviour	Behavioural aspects to reduce or mitigate cyber-risk.	Includes four groups of factors. Perception and understanding considers decision influences based on perceptions and views of relevance, threat, risk, and trust of information available.

Table 3-4: Analysis and coding of the data			
Category	Code	Definition	Explanation
Assessment tool	External	External personal and/or service aspects.	Relates to the influence of external know-how.
Assessment tool	Regulations	Cyber regulations and requirements.	Influences based on the regulatory environment or compliance with voluntary standards.
Assessment tool	Evaluation	External evaluation.	Internal evaluation of cyber-risk but also external risk level assessment for insurance purposes.
Assessment tool	Identification	Identify and classify cyber-risk.	Identify risks and classify them based on the severity of potential damage.
Assessment tool	Resilience	A checklist of cyber resilience actions.	The checklist can include strategic actions (e.g., governance, CRM, threat and vulnerability management, incident analysis, IS, BCM) as well as staff training programmes.
Assessment tool	Cloud	Cloud-based service.	Cloud-based service offers combine risk assessment and CRM/CRMi in relation to a variety of attacks (e.g., through malware, smart devices, broken cryptography, ransomware).
Assessment tool	Risk mitigation	Cyber-risk mitigation measures.	Approaches which combine risk assessment and risk mitigation, in which results from risk assessment directly inform mitigation measures.
Challenges	Skills	Medium-sized enterprise managers and employees.	Insufficient knowledge and skills lead to a deficiency in understanding cyber-risk management and mitigation strategies.
Challenges	Stakeholder	Internal stakeholder such as employees, managers, and owners.	Internal stakeholders may lack formal CRMi training.
Challenges	Norm	Norms help inform people about acceptable security behaviour.	Legal norms or company standards are considered as drivers for an engagement in CRMi.
Challenges	Target	Medium-sized enterprise as a target for a cyberattack.	Medium-sized enterprises believe they are not a main cyber target, even though cyber criminals are interested in using them as a back door to attack larger enterprises.
Challenges	Supply chain	A supply chain includes all suppliers of raw materials and parts and consumers of manufactured goods.	Medium-sized enterprises with improper cybersecurity are running a risk of getting cut off from the supply chain of larger enterprises, therefore potentially endangering their business model.

Table 3-4: Analysis and coding of the data			
Category	Code	Definition	Explanation
Challenges	Information	Lack of information.	Existing information on measures against cybersecurity is too confusing, which could constitute a reputational risk.
Challenges	Devices	Use of legacy devices.	Use of legacy devices as well as lack of update of operating systems and software are challenges in establishing cyber security.
Challenges	Resources	Lack of resources.	A lack of resources could result in outdated antivirus, antispyware, firewall, and backup systems, as well as weak passwords; all of which are essential for cybersecurity and CRMi tools.
Challenges	Knowledge	Knowledge gaps amongst medium-sized enterprise owners and employees.	Knowledge gaps which are associated with Cyber Security Assessment (CSA) and the technological threats and types of avoidance behaviour.
Challenges	Behaviour	Behavioural attitudes towards CRM and CRMi.	An overestimation of own competences and an underestimation of risk exposure could lead to a collective risk elimination, play it safe or risk-ignoring attitude.
Challenges	BYOD	Bring your own device.	Specifically problematic practices are also dual private and business use of hardware (BYOD).
Cloud-based solutions	Outsourcing	Outsourcing to cloud service providers.	Cloud based solutions for software and data storage is recommended, as representing a considerable part of CRMi.
Cloud-based solutions	SaaS	Software as a Service (SaaS).	Development of cloud-based CRMi solutions with the help of SaaS to enhance cyber security.
Collective approach	Co-operation	Co-operation within medium-sized enterprise networks.	Analyse specific issues and then suggest co-operation within medium-sized enterprise networks as solution.
Collective approach	Sharing	Sharing of cybersecurity information.	Networks of medium-sized enterprises should co-operate by keeping lists of risky hardware and software as well as information on security patches.
Collective approach	Platform	Common information platform.	Collective approach for medium-sized enterprises to jointly improve their CRMi.
Collective approach	Authorities	Information exchange also with law enforcement authorities.	Information exchange not just amongst medium-sized enterprise but also with law enforcement authorities as another collective

Table 3-4: Analysis and coding of the data			
Category	Code	Definition	Explanation
			solution with the aim of establishing institutionalised information exchange forums in this context.
Collective approach	Co-operation	When medium-sized enterprises exchange information.	Working together as a team, co-analysis with other medium-sized enterprises on CRMi.
Training programme	Training	Training programme to improve CRMi.	For medium-sized enterprises' owners and employees.
Training programme	Skills	Identification of skills required for CRM and CRMi.	This should take place at different levels of seniority and roles involved in cybersecurity, ranging from data analyst to cybersecurity risk manager.
Recommendations	Resources	Limited resources in establishing proactive cybersecurity measures.	Resources can take proactive measures of the identification of potential risks and taking measures to protect against them and is complemented with reactive elements of incident detection, incident response and recovery.
Recommendations	Software	Technical solution such as CR management software tools.	For open source or commercial software solutions there is a trade-off between ease of use and affordability.
Recommendations	Security	Guidelines for CRM to take measures before, during and after a cybersecurity breach.	Three main problems are identified in the context of medium-sized enterprises' CRMi activities, overemphasis of technical security measures, the second a lack of consistency when responding to CS breaches, the third a lack of learning from such instances.
Recommendations	Planning	The development of a CRMi plan.	A CRMi is suggested to include scenario, emergency, incident response, resource, and budget planning.
Recommendations	Technology	Assessment of technology used by the medium-sized enterprise.	The process involves assessing the technology used in the business, understanding the requirements of both internal and external stakeholders, assessing the impact of potential cyber breaches, assembling defensive tools, and implementing necessary measures.
Recommendations	Motivation	A focus on internal and external stakeholders' motivation.	Motivation on existing cyber-risk strategies a transparency in the business as to the potential of a cyberattack and the need to ensure that the business met existing legal requirements, but interestingly not to exceed these standards, as this would be seen as being costly to implement.

Table 3-4: Analysis and coding of the data			
Category	Code	Definition	Explanation
Recommendations	Impact	Assessment of the impact of potential breaches.	Consequences of potential breaches regarding tangible and intangible property and its effect on innovation, long-term growth, and profitability.
Recommendations	Defence	The assembly of defensive tools.	Policy to promote dedicated virtual private networks, restrictive access rules internally and for third-party identification, malicious software being uploaded etc.
Recommendations	Measures	The implementation of cyber security measures.	Upgrading of technical and non-technical cyber security measures as programs and systems including firewalls, security software and intrusion monitoring as well as employee training.
Recommendations	Zero Trust model	Once the network's defence from external is surpassed, it is possible to access more vulnerable elements of the network.	CRMi strategies as being based on a model, which consists of a hard outer shell with a soft inner structure while the latter is the risk factor.
Recommendations	Threat	Ranking of threats.	Ranking of threats is suggested to provide recommendations for prioritising which measures to take first.
Recommendations	Behaviour	Implementation of internal decision-making structures.	Nimble internal decision-making structures are advantages of medium-sized enterprises to initiate CR management strategies.
Recommendations	Co-operation	Co-operation between medium-sized enterprises.	Co-operation for the identification of risks is suggested.
Recommendations	Outsourcing	Outsourcing of technology.	Outsourcing is a potential solution as regards the technological aspects of CR management.
Risk assessment	Uncertainty	The lack of certainty and a state of limited knowledge.	The main challenge posed in relation to cybercrime is uncertainty.
Risk assessment	Data	Insufficient data to calibrate main parameter of formulas.	There are insufficient data available to calculate risks using conventional actuarial methods.
CRI challenges	Insurance premium	Charge of the insurer for the insurer to provide cyber-risk insurance.	Medium-sized enterprises are reluctant to buy cyber-risk insurance due to high prices charged by insurance companies.
CRI challenges	Data	Publication of claim data after an incident.	This would allow to compare providers on price as potential insurance solutions.

Table 3-4: Analysis and coding of the data			
Category	Code	Definition	Explanation
CRI challenges	Risk mitigation	Decreased likelihood of errors, security breaches etc. through cybersecurity measures.	Guidance on whether the financial investment in a CRI is justified by the potential benefits.
CRI challenges	Risk quantification	Assessing and calculating the potential financial impact of medium-sized enterprise's cyber threats.	Insurance companies find it difficult to quantify cyber exposure due to the complexity of risks and lack of historical data.
CRI challenges	Data	Any facts, data or knowledge about IT security.	Medium-sized enterprises are reluctant to publish their CRMi activities in the process of seeking insurance cover.
CRI coverage	Business interruption	Insurance indemnification for a financial loss.	Business interruption is the most frequently asked coverage in manufacturing and IT, whereas loss of customer data is in finance and retail.
CRI coverage	Incident response	A set of instructions to help IT staff detect, respond to, and recover from network cyber security incidents.	Incident response is the most frequently claimed type of coverage.
CRI coverage	Questionnaire	Cyber security readiness.	Questionnaires from insurer could provide potential guidelines for medium-sized enterprises.
CRI coverage	Coverage	Insurance coverage is the amount of risk, liability, or potential loss that is protected by insurance.	There is a discrepancy between coverage desired by medium-sized enterprises and actual claims.
Ransomware	Attack	A cyberattack is an attempt by hackers to damage or destroy a computer network or system.	Ransomware is an increasing risk and may become problematic for insurers due to high financial damage created by single incidents.
Ransomware	Transparency	Clarity on any cyberattacks and resulting losses.	There is a need for more transparency as regards ransomware attacks as well as failure of control measures since this will assist insurers to better quantify potential risks as well as to identify required CRM minimum standards.

Table 3-4: Analysis and coding of the data

The coding process revealed, however, that some codes were not relevant to the interviews, while others were seen as important.

3.14.2 The interview data coding strategy

Each of the interviews was recorded, transcribed and analysed, and then coded in German. The strategy followed the guidance of Jackson and Bazeley (2019), who advocated a template approach for coding the interview data, so that identifying emerging themes can be conducted in a systematic manner. A key consideration for the researcher was that in conducting semi-structured interviews there was the need to accurately analyse large quantities of rich data. To overcome this, the textual data was analysed using a template analysis framework. Both Braun and Clarke (2023) and King (2004) emphasise that template analysis is not grounded in any one specific methodology but allows the researcher greater flexibility when analysing and interpreting the findings. King (2004, p. 439) argued that a template analysis provides flexibility in the coding structure. This flexibility includes the usage of a priori or predetermined themes to be used together with a more grounded theory approach to organise the findings.

Reflecting this, a qualitative content analysis approach was used to code and then categorise the data, which was organised in a hierarchical order, thereby assisting the analytical process. As the data collection process proceeded, the approach was subjected to constant revisions where new and existing nodes were removed or added. In this study, the revision process included analysing the interview transcripts and drawing on the observational notes from the fieldnotes, which resulted in changes to the theme's position and level in the template hierarchy. As the process progressed, consideration was given to the possibility of introducing new codes or altering or changing the level of existing codes in the framework.

Although a qualitative content analysis has several benefits, there are also associated weaknesses. A key limitation is that if the nodes are predefined from the existing literature, some of the interview data may be overlooked. To address this, the researcher ensured that the coding process was frequently revisited until the key themes and relationships had been established. Furthermore, the semi-structured interviews, being conducted, interpreted, and analysed in German, ensured that all themes were correctly understood and interpreted.

The initial structure was based on the five themes, then sub-categories based on these themes were identified by analysing the interview transcripts, highlighting substantial themes, and then going through all the themes, line-by-line again, before a grouping of themes. During the coding process, firstly, all the groups were under six categories, plus a

category labelled “other–free codes.” Each category has then repeatedly reviewed to identify any new sub-theme or themes that related to others, but others were recoded into other categories and clusters as being “other free codes”.

3.15 The role of the researcher

Unluer (2012) indicated that the role of the researcher in a qualitative study is essential to enhancing the credibility, dependability, and trustworthiness of the research. To achieve this, the role of the researcher in this study was to gather data from a sensitive business perspective through conducting semi-structured interviews, then analyse and interpret the data (Creswell & Poth, 2016; Frels & Onwuegbuzie, 2013; Saunders et al., 2020). Creswell and Creswell (2017) argued that the role of the researcher in a study is important to conducting the study ethically throughout all stages of the qualitative research process. Yin (2018) recommended that researchers use appropriate data collection methods to maintain the creditability and robustness of the data. The researcher of this study is a professional in the field of cybersecurity but had no direct prior contact with the participants of this study. The questions were informed by the current debate and the professional experience of the researcher, but throughout the interviews, the participants viewpoints were not judged or influenced. To assist the process, the interviews were conducted in German, the native language of the interviewees and interviewer.

Critical to qualitative research is objectivity. A lack of objectivity on the part of a researcher could lead to the creation of false perceptions and assumptions about the research process. To address this objectivity, the focus of the knowledge gained for this study, along with the environment in which the study was conducted, adhered to the ethical standards and guidelines of the University of Gloucestershire, thereby permitting the participants to present their perspectives without judgement.

3.16 Ethical issues

Undertaking research with human actors, and in the case of this study, those directly responsible for cybersecurity in German-based manufacturing medium-sized enterprises presents the researcher with several challenges, dilemmas, and decisions. Reflecting these, this section sets out the ethical issues associated with this study. The research was conducted

within the Principles and Procedures framework of the University of Gloucestershire, which was informed by the British Educational Research Association (BERA, 2018) and the British Sociological Association (BSA, 2017).

It was recognised that it is the researcher's responsibility to ensure that the "physical, social, and psychological well-being of research participants must not be detrimentally affected by the research" (University of Gloucestershire Research Ethics Handbook, 2024), so that the participant provides free and informed consent. To achieve this, the researcher from the outset sought to inform the participants of the nature and purpose of the study. This included the reasons for undertaking the research and how the findings and outcomes would be presented and then used. The participants' anonymity was guaranteed while they were also assured of the confidentiality of the data. This was achieved by changing the names to pseudo-names and their medium-sized enterprise's identity anonymised. The data was stored securely and accessible to the researcher only.

The power relationship between the participants and the researcher was also taken into consideration. The power relationship is centred on the shift of balance that occurs during the interview process. To address this, the researcher provided an outline of the themes of the interviews in advance and then facilitated open communications with the participant before and then during the interview (Bravo-Moreno, 2003). The participants were also reminded of their right and the opportunity to object to answering questions at any time during the interview process (Brinkmann & Kvale, 2005).

Informed consent was obtained from all participants, ensuring that the individual participant fully understood the nature and purpose of the study. This was achieved by providing them with a written summary of the research aim and structure, then checking that they understood and agreed before the interview commenced.

Assurances concerning anonymity and confidentiality were given in writing and repeated verbally prior to the commencement of each interview. Anonymity was achieved through changing the identity of the participants and the inclusion of minimal personal information related to the individual, thereby protecting their identity. Permission to record and transcribe the interviews was sought on an individual basis. Finally, the recordings were handled with care and stored securely on a password-protected computer.

3.17 The validity of the study

Careful consideration was given to the robustness of the research design. To achieve this, the study followed Guba and Lincoln's (1994) four criteria, namely, creditability, transferability, dependability (or bias), and confirmability. The study also adopted and followed trustworthiness as the fifth criterion.

3.17.1 Credibility

Credibility refers to how believable or trustworthy the findings are. For research to have credibility, the researcher must represent the experience of those being interviewed so that they are understandable to the academic reader. This can be achieved by following several strategies. This included constant observations, refocusing on those areas that are specifically important to the study, and returning to the interview data so that the researcher can check and verify the outcome. To assist with creditability, Guba and Lincoln (1994) and Lincoln et al. (2011) advise researchers to ensure that the data is authentic or real. In this study, all participants interviewed were directly related to cybersecurity working in a German-based manufacturing medium-sized enterprise.

Finally, Guba and Lincoln (1994) advocate labelling to enhance creditability, which involves the researcher continually returning to specific themes. In this study, a template analysis was used to code the data, and an interview guide assisted the researcher to cover all the themes. The participants were also given the opportunity to check the transcripts once the data was transcribed, validating the narrative's authenticity.

3.17.2 Transferability

Transferability enables future researchers to access the findings and use the approach adopted for later studies. However, according to Baxter and Eyles (1997), transferability is less important to the qualitative researcher than creditability. However, the intention of this study was that the data findings might be transferable to other similar organisational sizes but in other sectors.

3.17.3 Dependability

Unlike transferability, dependability is essential for qualitative research. A qualitative study must ensure that trust exists in the research and within the integrity of the narrative. Dependability relates to whether the findings are likely to apply to similar situations and the outcomes are credible. Dependability ensures that in the future, the data can be accessed for further analysis. In this study, the interviews were recorded in German, so that at any stage during the analysis, rather than being solely dependent upon notes, the participant's actual words could be reviewed upon and listened to. While recording can be intrusive, the process in MS Teams needed to be handled sensitively with the participant's consent being sought, likewise with notetaking. This duality enhanced the "rich" content of the participant's account, and the researcher returned to the interviews several times during the analysis and coding stages, thereby enhancing the dependability of the study.

To achieve dependability of the interpretation of the data being free from bias and errors, Lincoln and Guba (1985) advise that the researcher's decisions must be made clear and transparent in the sense that the participants are allowed to speak without any influence from the researcher. It was also important for the researcher to continuously go back to the recorded data and listen repeatedly to what the participants have voiced during the interview sections. Through this, bias and errors regarding the findings, and interpretations of the research data can be minimised, and dependability of the study data can be achieved.

3.17.4 Confirmability

Confirmability refers to the extent to which research findings are determined by the participants' perspectives rather than influenced by the researcher's subjective biases. To enhance confirmability, qualitative researchers must provide a transparent account of how their personal interests and motivations may have impacted the research process, including data collection, analysis, and interpretation (see sections 2.3, 3.13, 3.15 and 3.16). Huberman (1995) emphasises that honesty, authenticity, and truthfulness are fundamental to conducting rigorous and credible qualitative research. While honesty and truthfulness are essential ethical considerations, authenticity - understood as faithfully representing the data - ensures that the narrative remains accurate, unbiased, and reflective of the participants lived experiences.

However, as discussed in the Limitations, in section 6.15, one recognised challenge of this study was that the researcher was solely responsible for conducting the interviews and analysing the data. This could have introduced potential biases or limitations in the findings. To mitigate this, the researcher maintained an immersive engagement with the data, continuously reviewing interview transcripts and audio recordings to refine interpretations. Additionally, the researcher actively sought external validation by engaging in discussions with participants, fellow doctoral candidates, and academic supervisors. These critical discussions served as a form of external review, challenging interpretations and ensuring that conclusions were rooted in the data rather than subjective perceptions.

3.18 Methodological limitations

Compared with a quantitative empirical approach, an interpretative methodology can create difficulties concerning the validity and reliability of the project and data. Reliability can be described as the requirement that the research findings be repeatable (Burr, 2015; Gill & Johnson, 2010; Willig, 2013). But this can only be achieved if the same outcomes can be repeated; however, owing to the different research participants and their perspectives on their own medium-sized enterprises, this would not be possible. As validity, the difficulty encountered could be "the extent to an account accurately represents the social phenomena to which it refers" (Hammersley, 1990, p. 57). Hammersley (1990) acknowledged that validity can be a difficult concept when applied to qualitative research, as the individuals' own conceptualisations and perceptions are unique.

The credibility and justification of the research depend heavily on identifying and highlighting clear gaps in perceptions between the participants and the researcher. To achieve creditability and justify how the data is interpreted, the method used needs to pay particular attention to the participants' use of language. This process includes a clear explanation of how the participants' assumptions and reality may differ from those of the researcher. Mindful of this necessity, a log of research developments was kept from the outset of the study, noting progress points, insights, and the details of the procedures undertaken at each stage. Where appropriate, the literature was revisited, and advice was sought.

One of the challenges in qualitative research, particularly when using a qualitative and inductive approach, is that the method produces an extensive amount of rich, interesting data to

analyse. Separating the data into themes can be considerably challenging and reflects an inherent tension highlighted by Easterby-Smith et al. (2012, p. 129) between "creating meanings and counting frequencies". In this study, this challenge was addressed by creating free coding nodes for interesting categories of material to be categorised. By adopting this approach, data that did not immediately relate to the core coding structure was able to be refined using these free nodes and then reviewed several times to ensure the focus was maintained while keeping the emergent theme relevant.

3.19 Summary of the Methodology Chapter

To generate an in-depth inside view of the topic of this study, a social constructivist approach was adopted to investigate the experiences and perceptions of those working in a German-based manufacturing medium-sized enterprise as to mitigating against a cyberattack.

The sampling for the study involved nine participants, due to the sensitivity of the theme. This led to the decision that the first interview was also the pilot study. The outcome of the first interview informed the remainder of the study.

The research question and the corresponding three sub-questions were informed by the first interview / pilot study, with all interviews conducted online via MS Teams because of COVID-19 precautions. All interviews were conducted in the German language and were recorded, transcribed, and translated into English. The data was analysed using a thematic approach following a thematic framework.

The coding concept was revisited frequently until the key issues and connections were identified. The 47 codes were clustered into categories, including one labelled "other–free" for codes that did not fit into any specific category. Each category was analysed repeatedly to identify sub-themes that emerged from individual statements or connections between themes.

A final revision of the overall structure and the connection of the codes and clusters were reviewed once again to ensure that all were clearly defined and allocated. The findings and discussions of the study are explained in the next chapter focuses on the analyses of participants' findings and discussions. The study followed the ethical guidelines of the University and ensured that the data was collected and secured safely.

4 Chapter Four
Findings

4.1 Introduction

As laid out in Chapter Three, it was decided to use qualitative content analysis for the empirical element of this study. To this end, the state of the art of research was identified using a Systematic Literature Review (SLR) in Chapter Two. The SLR as well as other literature analysed in this study (see, e.g., Ključnikov et al., 2019) have also shown that the involvement of senior-level management is critical for the success of cyber-risk mitigation strategies and measures. Therefore, it was decided to seek out senior-level managers within German medium-sized enterprises as interview partners.

4.2 The level of preparedness against cyber-risks within German medium-sized enterprises

The interviews initially focused on the medium-sized enterprise's preparedness as to how to address the ramifications of a potential cyberattack. From the interviews, three of the managers mentioned that their business had some form of dedicated cybersecurity strategy implemented within the business. This was illustrated by Interviewee 7, who highlighted and discussed the types of security policies adopted and the areas covered, which included the strategy to address the outcome of a cyberattack, but this focus on cyber-risks was only one facet of other potential threats to the business presented in the medium-sized enterprise's disaster recovery strategy:

> *All possible scenarios are discussed, this includes having the electricity cut off or running out of gas through to the response and strategy if the managing director is kidnapped, and of course, what happens if we have a cyberattack (Interviewee 7).*

This theme of scenario planning and cyberattacks being part of the medium-sized enterprises' overall security plan was also shared by Interviewee 5, who highlighted that cyberattacks were recognised as a potential threat, but were amalgamated into the overall business security and recovery plans:

> *We do scenario planning. We plan for almost all eventualities. This includes cyberattacks, like the loss of our payroll systems or loss of our servers. We see a cybersecurity attack as part of our potential threats which also includes terrorism. What we can't do is have a*

dedicated policy and plan for only potential cyberattacks, as it is potential, and we have other priorities, but we are aware and potentially prepared (Interviewee 5).

Companies that did have a dedicated cyber-risk management strategy within their organisation tended to focus on their preparedness through having a dedicated team being responsible for managing cybersecurity issues. Interviewee 9 noted that his medium-sized enterprise has appointed an information officer who had established a cyberattack flow process as to how the business would respond and manage the potential risk of a cyberattack:

We have appointed an information security officer, as we understand the importance of being prepared. This appointment has led to the development of control information flows process, so we can proactively now respond to the threat and the outcome of a cyberattack (Interviewee 9).

However, in contrast to Interviewee 9, for those medium-sized enterprises who did not have a dedicated cyber-risk management strategy or team, the business did have some form of CRM process. An example of this was in Medium-Sized Enterprise Two, where the responsibility for cyber security resided in the IT department, indicating the synergy and associated expertise that this team had in managing and responding to a cyberattack:

Our cybersecurity preparedness and information security is the responsibility of the IT organisation, but they do report directly to me. The IT department have the best expertise to enable us to be prepared and in the event of an attack, to be able to respond and recover our systems (Interviewee 2).

This lack of a dedicated cybersecurity team outside the remit of the IT department or an individual specifically nominated to manage this potential risk, highlighted a weakness in Medium-Sized Enterprises Two's preparedness. This issue was also observed in Medium-Sized Enterprises Three, Four, Five, and Eight, where cybersecurity responsibility for their preparedness primarily fell on the IT department, as reflected in the comments of Interviewee 3:

Of course, we do recognise the importance of a cybersecurity strategy, and the threat of an attack. But if we were to start implementing a robust cybersecurity policy across all departments like most larger companies do now, we wouldn't be able to afford this (Interviewee 3).

This perspective of Interviewee 3 confirms the common assumption amongst these German manufacturing medium-sized enterprises that one of the challenges to be prepared to manage potential cyber-risks was the lack of resources, which would allow them to establish a

dedicated CRM. However, even with the absence of a dedicated CRM strategy, the interviewees in this study did consider that this solution of a CRM strategy was important, particularly as to being kept informed about potential risks, indicating a degree of awareness and preparedness:

> *I used to subscribe to c't [magazine for computer technology], which is why I got stuck on "heise", and that meant that if something new comes along, I read about it together with whether there were any other topics that we needed to know about (Interviewee 1).*

The viewpoint of Interviewee 1 was shared by Interviewee 3, who also did not have a dedicated CRMi-strategy, but tried to have a degree of awareness and therefore preparedness through reading trade journals and magazines, but also held meetings focused on cybersecurity:

> *Since we are increasingly reliance on technology, therefore our IT hardware and software are important to us, and we have needed to acknowledge our dependence on our IT systems. We do therefore try and keep up to date with potential threats and ensure all our colleagues are aware of cybersecurity threats (Interviewee 3).*

This was shared by Interviewee 4, who elaborated on the perspective of Interviewee 3:

Although we do not have a formal CRM-strategy, we sit down, I would say two to three times a year, to look at cybersecurity threats and how we can manage these. It does show our awareness of the problem or the threat that cyber-issues have (Interviewee 4).

Despite the lack of a formal CRM-security policy, which could identify potential targets in their business for a cyber security attack, most medium-sized enterprises' representatives took the threat of cyber security breaches seriously, according to the interview data. There was an awareness of potential threats, but the lack of formal CRM-security policies and a dedicated team meant that the responsibility tended to be that of the IT department. However, in understanding this perspective more, and this theme reemerged throughout the interviews, was the perception of the medium-sized enterprise compared to other organisations in the supply chain. For many of the interviewees, their company was not a rewarding target for cyberattackers, as the information that could potentially be gained would be of little value to an attacker, as can be seen with Interviewee 3:

> *…as we do not hold or possess important information about configurations or details of the end customer, I would say that a cyberattack would only find limited information (Interviewee 3).*

Interviewee 3 then added:

> *…. what advantages would a third party like a hacker have if they attack us? He wouldn't have much information because even if he were to get our documents, he wouldn't be able to do much with them, and the overall value would be low (Interviewee 3).*

For Interviewee 4, he stressed that since the business' activities did not constitute a high level of intellectual property rights, the unique selling proposition of its business model being more practical orientated, would limit the interest of a cybercriminal:

> *We are currently experimenting in some areas where we think it can be done with cobots in the area of valve assembly, but the number of units are also different. We are also moving towards greater automation in the areas of soldering and welding, but we are still in the early stages, and the information on this is limited (Interviewee 4).*

These perspectives indicated a shared opinion that these businesses were not at risk from cyberattacks, and that related to the small size of the company. This included the type of information that could be gained through a cyberattack, and the small financial resources of the company meant that cyberattackers would not be interested in carrying out ransomware attacks.

To summarise the findings above, with the rapid changes in cyberattack technology, there has been an indication that this has led to constant monitoring of potential new risks, which has become a common practice in these German-based manufacturing medium-sized enterprises. Most of these medium-sized enterprises relied on studying professional literature and relevant websites, while the usage of formal cyber-risk mitigation (CRMi) networks was notably absent. The data from the interviewed medium-sized enterprise leaders can be grouped into three distinct categories as to their cyber-risk management strategies. The first group treats cyber-risk as a critical issue; therefore, they have adopted dedicated CRMi strategies, measurements, and allocated significant resources. The second group acknowledged the issue but addressed the primary threat as part of their broader IT strategy. The third group, which was represented by only a single interviewee, recognised the threat of a potential cyberattack but addressed this threat reactively on a day-to-day basis.

For these medium-sized enterprises, there was an awareness of the integrated nature of the supply chain, which required the establishment of robust cyberattack barriers within their

network, thereby becoming a part of their CRMi strategy. To support this, there was evidence of CRMi training being recognised as critical, which led to the provision embedded into the onboarding processes to reinforce the awareness of potential cyberattacks to other business activities, which included simulating phishing emails into their training programmes. Despite these strategies and initiatives, the technical CRM responsibilities often fell to a small IT team or even a nominated individual. Amongst the medium-sized enterprises studied, only one business (Medium-Sized Enterprise Nine) had a designated individual allocated to the role of CRMi.

4.3 The German medium-sized enterprises' cyber-risk mitigation strategies

The data presented above indicates that most of the medium-sized enterprises in this study did not have a dedicated cyber-risk mitigation (CRMi) strategy and that cyber-risks were amalgamated into other security responses to threats to the business. Based on this prevalent policy, the interviews then focused on the current cyber-risk strategies adopted in these German medium-sized enterprises. This included proactive strategies, such as using sensors, and applied even to medium-sized enterprises without a formal, dedicated CRMi security strategy:

> *With networking we use sensors, so we have a full overview of our network. This is of course very valuable, it has really given us many, many insights as to potential cyberattacks, and we have also been able to implement a series of proactive measures that have kept us safe from experiencing a serious cybersecurity attack (Interviewee 2).*

In expanding on this theme, Interviewee 2 then added that this usage of sensors identified potential weaknesses in the existing infrastructure:

> *…we have already – and I hope you don't misunderstand this, but when these sensors are correctly implemented through the network ports, we have discovered certain weaknesses indicating that we were vulnerable for a cyberattack, but then we closed these ports, and I hope that we have caught everything (Interviewee 2).*

From the perspective of Medium-Sized Enterprise Two, there was also plans for emergencies, which would allow for a quick reaction to an incident such as a cyberattack occurring:

… we attach great importance to the fact that our emergency planning is completed and that we have now guidelines in place. This is because our systems hold important information such as employees and suppliers addresses and telephone numbers which could make then a potential target for a cyberattack (Interviewee 2).

This monitoring of the technology infrastructure was also shared by Interviewee 5:

To do this, we rely on comprehensive security and vulnerability scanners and an event and incident management system on both the central and regional endpoints of our IT infrastructure. In addition to automated detection mechanisms, we have also a systematic response to any attempted attack which notifies us instantly (Interviewee 5).

Given the constant threat of a cyberattack, the medium-sized enterprise representatives were aware that this issue was always present, and was described as a competition between the attacker and the business, which was indicated by interviewee 8, who used the metaphor of a cat and mouse to illustrate the challenge:

Yes, unfortunately it is a game. It is like a cat and a mouse, and this will remain like this for the foreseeable future (Interviewee 8).

As noted in the previous section, most of the Medium-Sized Enterprises (One, Two, Three, Five, and Seven) had some form of previous experience of a cyberattack, and this had informed their current cyber-risk strategies, to varying degrees:

Our attack occurred when an invoice was opened in the quality area of the business. A good man in the quality department went and opened it. Since this experience we have changed our cybersecurity, we have a greater awareness of the potential threat of phishing activities, and how opening an attachment can stop our business (Interviewee 1).

The last part of the comment of Interviewee 1 was interesting, as it indicated an awareness following the cyberattack, but was only focused on future phishing attacks and no other potential cyber-risks. This perspective was shared by Interviewee 2, who recalled their cyberattack experience, and the impact to their testing infrastructure:

We had an encryption attack on our test system. Thank God it's just a test system. This happened a few years ago now, and we have not experienced another attack since. We have learnt an important lesson here, and how lucky we were, and we now train our staff as to being aware of possible phishing emails (Interviewee 2).

This was expanded on further by interviewees 2 and then by 7, as to their concerns about potential attacks through phishing and employees being unaware of the potential of this cyberattack:

> *But as we know, just a lack of attention amongst our employees is enough, and we are at the mercy of our team being vigilant. …So, I don't feel safe, definitely not, but I don't feel completely unprepared either, as we provide awareness training for all our teams (Interviewee 2).*

For Interviewee 7, it was the employees inadvertently opening an attachment and the attacker then able to destroy or corrupt the entire network:

> *Yes, so we say that the biggest risk is actually the threat of encryption, that we are then at a standstill with the network inaccessible just by opening an attachment, or that someone penetrates the network and doesn't even encrypt it, but simply destroys our infrastructure (Interviewee 7).*

These perspectives above included the recognised importance of cyber-risk training. The interviews revealed the importance associated with employee awareness, which all the interviewees highlighted and mentioned. For Interviewee 1, the training commenced when first onboarding a new employee into the business:

> *…when a new employee comes, our training commences, with training into data security, how we organise our IT services, email protocols and so on. I always do this myself (Interviewee 1).*

With Interviewee 5, the training programme was mandatory and included optional sessions to reinforce the employee's knowledge:

> *In addition, we provide our employees with the necessary tools through mandatory and optional training as well as attack simulations, e.g., phishing, as to how to identify significant attacks and implementing a rapid reporting and response following a cyber-risk (Interviewee 5).*

For Interviewee 5, the experience had led to more robust response to the cyberattack, which led to the adoption of the ISO 27001 standard in his medium-sized enterprise:

> *… after the hacker attack, we have relied on a risk-based approach that is based on the internationally recognized standard of ISO 27001. Adopting this ISO 27001 standard has seen us develop I think a comprehensive CMI strategy (Interviewee 5).*

For Medium-Sized Enterprise Five, as seen in the comment above, this was an example where a dedicated cyber strategy could be created based on a recognised standard, but had been implemented in response following a cyberattack. However, not all medium-sized enterprises, who had experienced a cyberattack reacted in such a logical and structured way, as shown by Medium-Sized Enterprise One. For Interviewee 1 who was a victim of a cyberattack, this business did not adopt a dedicated cybersecurity strategy:

> *The exact same thing happened, I think three years ago, and it wasn't My Pictures, it was just a Trojan that started encrypting. We were incredibly lucky that we noticed that straight away have stopped. The handful of files that caught this, we were able to play back from the backup and then we went to search and what was it, an email? An invoice was opened in the quality area. A good man in the quality department went and opened it (Interviewee 1).*

In explaining this further Interviewee 1 added:

> *And you have to say, we were really incredibly lucky that we noticed that straight away and fortunately nothing else has happened so far and that's the reason why we don't just have a backup for 10 days, but we can at least Recover 150 days. (Interviewee 1).*

Various cyber-risk strategies emerged from the interviews, which included a range of structured cybersecurity responses including some fundamental techniques and strategies. Examples included the management and storage of backup tapes, which were physically removed from the premises overnight, as shared by Interviewee 1 and then Interviewee 8:

> *In the past, before our cyberattack we always recorded on tape and took these tapes out of the house [off the premises] in case there was a fire. That was the extent of our security of our data. Now we have introduced further security measures including updating our virus software and taking more frequent backups of our systems (Interviewee 1).*
>
> *In the past we always recorded on tape and took the tape home in case there was a fire. Now we have regular backup procedures and restore activities to practice how we can recover from a cyberattack (Interviewee 8).*

For both companies, the backup tapes strategy was still followed, including getting the media physically out of the business in event of it being destroyed by fire. However, the potential risk of company data physically leaving the premises and being exposed to risks outside the company's control, for example, accidental loss or theft, was not considered or mentioned by these individuals, indicating the potential weakness in their current IT and cybersecurity policy.

The discussion then led to the strategy of using remote access, and the usage external platforms as a security tool. The usage of external platforms was a strategy which could be adopted to minimise the impact of a security breach, which included the usage of clearing houses for communication, order taking and invoicing. The use of these clearing houses indicates a perceived acknowledgement that this could minimise the risk of phishing attacks, as can be seen the comments of Interviewee 2 below:

> *We used clearing houses now as it has the potential to minimise any form of phishing or related cyberattacks occurring, but it does also come with its challenges. Within the company between the locations there is of course a lot of networking because we are reliant on remote automated processes now, and we work on the same ERP system, therefore we can send the data back and forth between companies on a client-specific basis, which includes the usage of clearing houses (Interviewee 2).*

In building on this theme of remote automative processes, Interviewee 4 stated that although clearing houses and remote access was beneficial there are also decisions to be made to ensure that remote access was secure, and whether the external entity was secure:

> *…we have had an Indian assembly unit in Mumbai since the beginning of last year. And of course, the question is always how do you network this unit? And we made a conscious decision not to include this unit in our ERP system or access to our remote clearing house. This decision has been purely based on potential cyber security risks (Interviewee 4).*

On the same theme of remote access, some of the medium-sized enterprises required access to their client networks, particularly when doing remote maintenance on equipment delivered to a client's production site. This also brought about unique challenges as to potential cybersecurity risks:

> *A lot of the services and maintenance we provide now takes place remotely, especially with troubleshooting. We are still relatively new as to the adoption and usage of production networking and the challenges of securing our and our customer's network against a cyberattack (Interviewee 4).*

This increased reliance on remote access highlights the challenges associated with cyber-risks, but also the need for strict cybersecurity policies and procedures. Interviewee 1 explicitly mentioned that his medium-sized enterprise had instigated a policy that prohibited employees from using personal devices for work. However, due to the increased use of remote home working during the COVID-19 crisis, the practice of staff logging in from their homes using their private internet access, typically WLAN, was seen as a potential risk which was

now accepted. This acceptance was also seen with the comments of Interviewee 7, who noted that the business was now connected with various external networks due to the automation of processing of incoming invoices, including sending data to authorities, and this also opened the medium-sized enterprise to potential cyberattacks:

> *…we have a few EDI connections to suppliers or to the external warehouse, for example. We also have connections with various authorities. Because many countries already have these e-invoicing regulations that require you to send your invoices and delivery notes electronically to the tax office. Therefore, we have needed to join our network to others and open ourselves to an increased possibility of a cyberattack (Interviewee 7).*

When the interviews then focused on the motivation behind the existing cyber-risk strategies adopted by these German-based manufacturing medium-sized enterprises, there were again a range of perspectives and opinions. For interviewee 1 there was a motivation associated with a transparency in the business as to the potential of a cyberattack and the need to ensure that the business met existing legal requirements, but interestingly not to exceed these standards, as this would be seen as being costly to implement:

> … our focus is that we follow and meet the legal standards and requirements as a retailer, but following other cybersecurity standards which are not needed like insurance, is something that we see as being inhibitive and too costly (Interviewee 6).

In contextualising this further, Interviewee 6 did indicate, as did Interviewee 7 that the current regulations for retailers around cybersecurity was weak, compared to large organisations and sectors:

> *… compared to who I supply, I would however add that the current regulatory requirements for cybersecurity are a little weak, and there really needed to be stronger as to addressing and preventing this form of activity impacting on us and our supply chain in the future (Interviewee 6).*

However, having more robust legal standards and requirements were seen as an additional challenge. Interviewee 7 saw that more resources would be needed to comply with the pending regulations:

> *We have now NIST 2, which is under the Cyber Resilience Act. This has led to us needing to comply with it, so we decided on using the ISO 27001 standard. A lot of the regulations comes down to us and how we implement our strategy. Then there is the AI Act and what*

> *the EU is thinking about as to what businesses should do in the future. It will soon be necessary to hire a few more in the IT department so we can meet these regulations (Interviewee 7).*

The NIST 2 requirement is a reference to the US National Institute of Standards and Technology's Cybersecurity Framework 2.0, which was released in 2023; however, it should be noted that at EU-level the Directive (EU) 2022/2555 titled NIS 2 Directive also deals with cybersecurity. It was published in December 2022 and requires all member States' national legislation to be passed and implemented by Autumn of 2024. Again, the level of regulatory requirements was seen as being a challenge which indicated the potential need for a higher level of engagement and revision to existing cyber-risk management strategies in these medium-sized enterprises:

> *Legal or certification compliance is sufficiently demanding without the introduction of new requirements. We are at the end of the day only one small part of the supply chain, and hackers tend to target the larger organisations leaving us alone (Interviewee 9).*

This last comment of Interviewee 9 is interesting, as to there was a shared perception amongst most of the interviewees that their medium-sized enterprise was too small to for a targeted attack of any significance, and that most of the cyber-risk was low level activities, therefore the existing protocols and strategies were adequate. This led to the question as to why the interviewees considered their existing strategies were adequate. What emerged was the theme associated with this perception of being a small player in the supply chain but also the associated costs of implementing an extensive cyber-risk strategy, a theme which was highlighted in the preparedness of the medium-sized enterprises. For Medium-Sized Enterprise Four and Five, the interviewees indicated that they had considered and estimated the potential damage associated with a cyberattack:

> *So, we, we tried to estimate the cost of recovery versus the cost of implementation. We have come up with somewhere between X and Y[1] million Euros in the worst-case scenario, but then we have to predict the likelihood of the event occurring and this has driven, informed and influenced our decision (Interviewee 4).*

[1] Actual figure mentioned in interview but deleted here for reason of confidentiality.

However, unlike Interviewee 4, for Medium-Sized Enterprise Five the impact of the hacker attack had led to the purchase of a cyber-risk insurance (CRI) policy as the event had impacted significantly on the medium-sized enterprise:

> *We had a hacker attack and that resulted in a real loss of revenue and profit. Now, after purchasing cyber-risk insurance, the net burden for the company in the future would be significantly lower than before, and also on the net profit. But I don't want to give you exact figures for reasons of confidentiality reasons, but we learnt an important lesson that insuring against this potential threat was important (Interviewee 5).*

For Interviewee 5, CRI was seen as an essential strategy for the business, as the original cyberattack had led to significant monetary losses, which had resulted in the medium-sized enterprise insuring against potential damages. This decision was however informed by the actual experience of a cyberattack, and not through proactive measures.

Based on the above, the responses from the German manufacturing medium-sized enterprise leaders as to how they approach CRM revealed a wide range of strategies and attitudes towards cybersecurity. Many of the medium-sized enterprise leaders lacked a dedicated CRMi strategy; instead, these businesses tended to integrate cyber-risks into broader security measures. Of the measurements adopted, some leaders indicated the use of sensors to monitor networks to identify vulnerabilities and implement emergency plans. However, responses to cyber incidents did vary, with some medium-sized enterprise leaders, like Medium-Sized Enterprise Five, having now adopted formal standards (ISO 27001) and even purchased CRI following an attack, while others, like Medium-Sized Enterprise One, still relied on more basic methodologies such as backups and had not developed a comprehensive CRMi strategy. To ensure resilience against potential cyber-risks, certification can motivate the medium-sized enterprises to become more proactive, particularly if potential clients demand detailed information on CRMi strategies. Throughout the interviews, these leaders did acknowledge their awareness of regulations, and about upcoming legal requirements in cyber-risk management but did express their views that these regulations were excessively demanding for the medium-sized enterprises to adhere to.

The interviews also highlighted the importance of employee training in preventing cyberattacks, particularly phishing, and how some medium-sized enterprises had developed extensive training programmes in response to previous incidents. A notable theme to emerge was the belief amongst some medium-sized enterprise leaders that they were too small to be

major targets, leading them to consider their existing measures to be adequate, despite potential vulnerabilities and the increasing complexity of potential cyber threats.

4.4 The role of cyber-risk insurance within German manufacturing medium-sized enterprises and the risks covered by existing CRI-policies

Building on the theme above, the interviews then focused on the role of cyber-risk insurance (CRI) within these medium-sized enterprises, and what risks were covered by their related cyber-risk strategies. For many of the interviewees there was a focus on the IT infrastructure and the recognition of their dependence on technology:

> *With our dependency on technology, if our servers were to fail completely, let's say through a cyberattack, we have a strategy in place which would still enable us to continue producing. The cost of recovery and outlay to restore our services back to normal would be expensive, but we have a strategy and documented processes in place (Interviewee 1).*

There was evidence from the interviews that for those medium-sized enterprises who had suffered a severe cyber-incident in the past had changed, and were more inclined to have radically modified their existing CRI policies:

> *For several years now, after our hacker-attack, we have relied on a risk-based approach that is based on the internationally recognized standard ISO 27001, a TISAX. We transformed our processes to follow an international recognised standard for dealing with potential cyberattacks (Interviewee 5).*

This experience and outcome were mirrored by Interviewee 9 who indicated that their perception towards CRI had changed, including their development of a robust cyber-risk strategy:

> *Except for one of our subsidiaries, which has already been certified for TISAX, we have ensured all our IT infrastructure is now compliant to international standards due to our previous experience (Interviewee 9).*

However, for those medium-sized enterprises who had no certification, the interviewees were not aware of how mitigating again cyber-risks could be informed by adopting or mirroring existing standards:

> *Ah, we've just taken that into account, but I have to be honest and tell you that I personally don't have any specific standards which we follow. We will need to look into this in the future as to which standards are best for our business (Interviewee 3).*

For medium-sized enterprises who had not yet been certified under one of the international standards, there was an interesting trend of clients and suppliers beginning to demand that these businesses gained some form of certification in the future:

> *If in the future we are asked to comply then yes, fine, if not then no. You always have to answer about 150 questions when you are dealing with new clients, because we don't have certification yet. The ISO standard is what we are aiming for in the future, but not yet (Interviewee 7).*

However, in the absence of these requirements, even with some of the medium-sized enterprises having well-structured processes and approach to their CRM, these interviewees still did not see the need for official CRM-certification:

> *Apart from our own self-certification, which is based on the ISO 9001, we don't yet have any formal certification, so we don't currently have TISAX or ISO, to be honest why should we, as our processes and procedures are robust (Interviewee 9).*

This perspective of Interviewee 9 indicated that although some medium-sized enterprises had adopted cyber-risk certification, others seemed to be more reluctant, and only motivated due to external demands from potential clients and suppliers.

When the interviews then moved onto focus on the role of CRMi in these medium-sized enterprises, the findings indicated a range of different technical solutions, with most of the participants identifying regular backups as a key and crucial CRMi strategy, as indicated above in the sections 3.14.1 and 4.3. For Interviewee 3, the main strategy was focused on backing-up of the data:

> *When it comes to backups, we have a three-stage concept. My IT manager updated me and said to me, he should know what I mean: disk-to-disk-to-tape (Interviewee 3).*

With Interviewee 5, the core security and recovery processes were based on the frequency of backup copies, and the location of the storage of this media:

> *As key IT security measures, we have increased the frequency of backup copies and determined the storage location to be outside of the company (Interviewee 5).*

In addition to the physical separation of backups, storage for longer periods was also noted by Interviewee 1:

… we don't just have a backup for 10 days, but we can at least recover the data from 150 days ago. Because you don't know how long the Trojan virus has been sleeping before it becomes active (Interviewee 1).

Unlike Interviewee 3 and 5, Interviewee 1 expanded on the theme of backups to include the use of secondary recovery or having a standby site:

The server is located in one locality, where a backup is also made. In the other building is where the backup is duplicated. This means that if one of the two buildings burns down, the data will be there. From a cybersecurity perspective, this means that if one server is infected, then the other system can take over and be used (Interviewee 1).

The use of firewalls was mentioned as an important CRMi measurement and strategy used by most of the participants. This included Interviewee 1, 3 and 4:

We use a free firewall. You may know the OPNsense Firewall? (Interviewee 1)

…of course, the firewall and other additional solutions and including the policy of changing passwords frequently, is essential. I think firewalls are a part but not the entire solution (Interviewee 3).

So of course, we have, or at least we have tried, to protect ourselves as best as possible with a firewall. We have a strict password policy and a dedicated server for suspicious emails to be checked and cleansed (Interviewee 4).

Interviewee 3 mentioned the additional measure of requiring frequent password changes. This measure was mentioned by Interviewee 4, where suspicious email would be sent to a separate server or network, which was not connected to the company's live infrastructure. This strategy can safeguard against potential harm and mitigates the possibility of overlooking a potentially crucial message.

Running redundant production infrastructure was another approach to protecting against potential cyber-risks. When a cyberattack happens and incapacitates one site, production can continue using a failover system:

We have four producing branches. Two of them work with wafers and chips, that is us here in Germany and in our branch in Slovenia, which can also produce the chips. Even with these four remote sites, we have one production IT environment and some form of hot-standby to fail over too (Interviewee 1).

An alternative was using or sharing a competitors' site, location or even services, which could act as a backup to allow for orders to continue to be processed:

One of the first things we would do would be to contact friendly competitors, let me say those with whom we otherwise have little to do with, but would certainly step in, and borrow or share their infrastructure (Interviewee 2).

Redundancy as a CRMi measure was another solution as it can also constitute using different suppliers if the current nominated suppliers are affected by a cyber-risk:

How about using alternative suppliers, as we do here, in the event of a cyberattack? It's about being agile and responsive. Once our agreed supplier recovers from the attack, business with them resumes, and lessons are learned (Interviewee 4).

Other solutions included the usage of an analogue approach, which requires keeping a higher level of products in storage, so if there is a cyberattack or loss of the IT system, then stock is still available to meet normal production and distribution requirements.

… we buy these lithium disks, the wafers, in their raw state, make a semiconductor out of them and then we stockpile the diodes and the silicon in quite large quantities. This means that during allocation times or when there are delivery difficulties, we are actually amongst the first to be able to provide the product (Interviewee 1).

An important CRMi-measure was the restriction of automated data exchange with external sites, and then require authorisation of any such exchange:

We have customers and suppliers remotely accessing our systems through our various portals, but they are closely managed and monitored for access activity (Interviewee 5).

But this was not the case for Interviewee 2, who did not have any automated data exchange services yet:

…customers can log in to our customer portal and of course that wouldn't work if we were somehow encrypted, but we don't have any automated data exchange with other companies at this point (Interviewee 2).

The interviews also explicitly mentioned how their medium-sized enterprise had set out policies prohibiting the use of employees' personal devices for work. However, due to the increased use of home offices during the COVID-19 crisis, the practice of staff logging in from their homes using their private internet access, typically WLAN, was seen as a potential risk as with Interviewee 4:

> *We have needed to manage more closely our employees as to accessing our network remotely. What we have done is to deny USB devices and plugging in personal and unauthorised technologies into our infrastructure (Interviewee 4).*

For many of the medium-sized enterprises in this study, they had chosen not to acquire CRI for the reasons outlined above. For these reasons, there were a few comments to emerge from the interviews, which included that the terms and conditions of the insurance needed to be more appealing and that the preventative security measures needed to be reasonable; otherwise, the existing methodologies were seen as being acceptable. One example to illustrate this was from Medium-Sized Enterprise One, who recognised the risk of data theft but, due to their own backup processes and technologies, had not considered insurance a necessity:

> *…what we don't have now, we don't have cyber-risk insurance, I hadn't considered that necessary until now. Let's put it this way, of course it's relatively difficult to defend yourself against data theft (Interviewee 1).*

However, for Medium-Sized Enterprise One, after experiencing a cyberattack, the potential loss of data was a warning and had resulted in the business considering taking out CRI, which covered future incidences. It was the potential financial losses from a business interruption that were seen as the important consideration for the insurance coverage. As the Medium-Sized Enterprise One manager noted, it was about the confidence of having higher security measures implemented because of the experience of a cyberattack rather than grouping the event with other disasters, such as a fire:

> *We once had a branch in Slovakia. What actually happened to them was that their data was deleted accidentally and the backup they had was no good and then they had to rework it for nine months, especially the financial accounting. And it didn't affect us directly, but it was also a warning example for us. That's why we don't take cyber-risk insurance lightly. But until now we were of the opinion that we didn't need it. We have protected ourselves well and now we don't see whether we need insurance. What is more essential for us is that we have business interruption insurance and we were glad that we had it when there was a fire. So, things like that are more essential, I think (Interviewee 1).*

For this medium-sized enterprise, the active acquisition of CRI was based on two main aspects: the need for business interruption coverage, and the renumeration of the costs associated with the recovery service following the event:

Yes, the decision to take out cyber-risk insurance there two things that were important to us. On the one hand, you can get help almost immediately if an attack happens. This is also a service that you buy so that you have access on the day or at the time when something happens. The fact that you get help immediately is an important point. And the other important point is that if there is a business outage over a longer period of time, you are adequately financially protected (Interviewee 8).

The aspect of recovery costs was also underlined by Medium-Sized Enterprise Two, who had implemented CRI as part of the business's CRMi strategy, by acknowledging that this form of insurance was not just bought because of protection reasons but also for the aftermath of the event and the service which the insurer provided. However, the scope of the policy coverage was not completely known to the manager, indicating that the total value and level of protection of the insurance remained unclear:

As of this year, we've had cyber-risk insurance for probably five or six years. Although I have to be honest, if you asked me, I wouldn't know exactly what is insured (Interviewee 2).

Some of the medium-sized enterprise interviewees considered CRI to be a fundamental method for covering the ramifications of a cyberattack, however, the decision as to what was adequate for their company was often left to the insurance broker to decide, and hence there was some doubt as to what was covered in the event of a serious cyberattack:

We were already aware many years ago that this risk absolutely had to be covered and how good it would be in the event of an emergency—you hear all sorts of different things. But we can only hope that we have bought sensible insurance from [insurance broker], who, in turn, have an overview of the market (Interviewee 2).

This perspective of Interviewee 2 was also shared with Interviewee 5; however, he speculated the types of risks which were and were not covered in the CRI policy:

Comprehensive insurance cover has been agreed in consultation with the insurance broker…Yes, well, I don't know in detail ad hoc. I think IT forensics and data recovery are covered after an attack, as well as the financial costs of business interruption and the costs of informing customers and contractual partners, i.e. crisis communication. I believe that a cover module for ransom demands is also part of the insurance up to a certain amount……but based on the experience we had with the ransomware attack, we should have looked more into such a policy beforehand and at least based our assessment of the material and intangible values on the coverage offered… All other risks that have a more substantial damage potential and whose extent would be financially dangerous for the company should be covered by cyber-risk insurance and relieved of the damage (Interviewee 5).

Medium-Sized Enterprise Six had not bought CRI as the business was uncertain about what form of coverage was available. Furthermore, the manager questioned whether their property insurance covered a cyberattack, together with business interruption and data loss:

> *I mean, if we were down for a day and could then start cooking again, it might not be so bad, but if they stole data that is relevant to us and we only get it through ransom blackmail, then that day is a waste. Because then it's of a larger dimension, or a different one. And that's why I think it's difficult to really grasp this. Yes, I think that we, I'm not even sure whether we have cyberattacks included in the business interruption insurance or whether they are excluded? You probably can't insure them at all, can you? (Interviewee 6).*

There were other medium-sized enterprise managers who seemed to have confidence in having some form of *silent* cyber coverage in their property insurance and liability coverage:

> *Yes, that's covered (Interviewee 3).*

One intriguing response to the question about CRI coverage was seen with Interviewee 7, who after acquiring CRI, now saw it as making the business a potentially lucrative target:

> *Well, it's actually something you don't talk about, because if you're insured, you're a prime target (Interviewee 7).*

In summary, almost all the interviewed medium-sized enterprise managers were aware of CRI. However, only a small number had either acquired or implemented CRI to safeguard their tangible and intangible assets from a potential cyberattack. However, even within this group, there was a tendency to leave the policy coverage to their insurance broker. As a result, there was no real in-depth knowledge about the coverage and potential limitations of the insurance policies. It could be deduced that although these medium-sized enterprises had some CRI, this group still predominantly relied on their own security protection and strategies.

Although CRI can be largely seen as complicated and perhaps not offering a real value for medium-sized enterprises, there was, however, an understanding that cyber-risk insurance did cover the outcome of a cyberattack within the supply chain and provided evidence of due diligence to external entities.

4.5 Risk mitigation strategies adopted by medium-sized enterprises against cyber-risks

With the focus on risk mitigation strategies, the interviews commenced with the current challenges and perceived weaknesses in the medium-sized enterprises. What emerged was the importance associated with the behaviour and expertise of the teams, as the team and the employees were seen as the frontline in preventing a cyber breach. Interviewee 1 stated teams need to be aware and pay attention to potential cyberattacks, particularly in emails:

> *… I often repeat the same mantra, that people must pay attention to their emails because, you know, the danger is between the keyboard and the chair, and I also personally talk to every new employee about data security and even conduct the training myself (Interviewee 1).*

For Interviewee 3, the risk mitigation strategies were clearly set out in the guidelines of the medium-sized enterprise:

> *There are clear guidelines, including when it comes to emails, for example, in principle, emails can only be opened if the email address is ultimately known. Otherwise, we'll stay away from it, put it into the spam folder and do not open it (Interviewee 3).*

This dependence on employee vigilance was also mentioned by Interviewee 8, who noted the prevalence of phishing emails, a theme covered above in section 4.2 and 4.3:

> *…I would say that the biggest weak point is, I also talked to my system partner about this, it is our people. …In our opinion, this happens through phishing emails, through malicious links, through activities which we as a team do not think about when accessing our emails (Interviewee 8).*

Then there was the associated self-overestimation and underestimation of the potential risk of a cyberattack, as can be seen with the comments of Interviewee 5:

> *Of course, given that employees are often positively self-assess themselves as to being able to recognise a potential threat, and that the company sees itself as often under the radar of hackers, we as a business are inclined to underestimate the potential threat of a cyberattack (Interviewee 5).*

This perspective of Interviewee 5 was informed following a severe hacker attack in the past, so that the statement also reflects a lesson learned from experience following the event. Although not aligned directly to employees, the interviews also revealed an interesting insight into the usage and reliance on external entities. The use of external know-how in the context

of cybersecurity was common amongst the medium-sized enterprises, but also both a reluctance and a willingness to share their experiences with other medium-sized enterprises. The external consultants were seen as providing independent advice that would not impact on their business due to the disclosure of their business practices:

> *Following our attack, we also got a consultant in who then created a list of potential cybersecurity risks and deviations with us, which we then worked through. This expertise did not exist here at the time and proved to be invaluable (Interviewee 2).*

For Interviewee 3, the external consultancy was part of the support needed for the IT infrastructure:

> *This is also the case with IT, that you need external information or support, and this is the same with assessing potential cyberattacks. We have always sought external advice (Interviewee 3).*

This perspective of Interviewee 3 was shared with Interviewee 5 and also Interviewee 8, who noted the importance of specialised skills:

> *For this purpose of cybersecurity, we involved an external service provider, why won't you? (Interviewee 5).*
>
> *But we also have additional support from a system house that provides us with appropriate support, advice and suggestions on cybersecurity. When it comes to the topic of firewalls or the whole security system, I would say that you need someone external because you don't have the inhouse expertise and independence (Interviewee 8).*

With interviewee 9, the usage of an external consultant was motivated and informed by the need to standardised the business to conform to new regulatory requirements:

> *… we are driving for standardisation via Palo Alto, then we are seeking SIAM via the data lake. The service provider, who has known us for two and a half, three years now, is prepared to offer us for 24 * 7 service and escalation and incident response services. This sort of expertise is definitely not in-house as we are too small (Interviewee 9).*

From the interview data above, external consultancy was seen as important for these medium-sized enterprises and had informed and influenced their CRMi-strategy. Part of the motivation could be related to the lack of resources in the business, due to their size. The theme of zero trust in cybersecurity emerged from the interviews, which included remote access from external sources, customers and the staff alike. This zero tolerance as to trust can be seen with the comments of Interviewee 5:

> *This policy of zero trust means that we have set out policies regarding access to users' devices on our corporate networks. With "Zero Trust", we can control and assess risks via user access permissions as needed, and is dependent on each person's job role and requirement (Interviewee 5).*

Another version of zero-trust policies was related to authorisation requirements. This is also relevant when conducting remote maintenance of the company's equipment, as noted by Interviewee 7:

> *If someone wants to connect to our network with their device, like our colleagues in maintenance, for example, it must be approved each time to ensure that the device is virus free (Interviewee 7).*

Protecting against security breaches by restricting unauthorised software installation on company devices was also followed by all the medium-sized enterprises:

> *… we ensure our mobile devices, and our outsourced computers have the correct software, virus scans and are regularly health-checked, and you can't install a program without authorisation, but remote computers and those in the home we have no idea or control, therefore leaving the medium-sized enterprise vulnerable, so we have restricted the usage of these devices (Interviewee 7).*

This theme of remote access then led to the discussion related to the usage of the Cloud, and cloud-based CRM services. During the interviews, it became evident that interviewees used the cloud for general usage, along with cloud-based software solutions such as MS Office and ERP software. However, as the interviews progressed some of the interviewees expressed their concerns about using cloud-based solutions, particularly because most were using remote solutions, such as Microsoft's Office 365, which could lead to the data being kept on servers in other countries, such as the United States, and present a potential security threat:

> *I'm not a fan of the cloud, although I know of course that the clouds that exist are very well secured, but then you do wonder about access and who actually can see the data (Interviewee 1).*

In addition, concerns that cloud solutions with many users might in themselves constitute an attractive target for potential hackers:

But the probability of a future attack or hack is simply much greater from my point of view. If there is a new target, then the cloud is an obvious one. How many 10,000s of people use the cloud, then think it must be becoming a primary target for hackers and then there is of course our data (Interviewee 3).

This perspective or concern of Interviewee 3, led to some medium-sized enterprises trying to avoid the over-usage of cloud -based services and solutions:

Cloud-based solutions no, definitely not. There is probably one or two utilities or services available on the cloud, which we access and use. If not for these services which are otherwise not available, we are very hesitant when it comes to the cloud. Of course, we are now being forced to do this to a certain extent by SAP policy (Interviewee 4).

It should be noted also that the use of cloud-based software was also seen as reducing cyber-risks, and that documents and data could be stored remotely and worked on collaboratively without being sent externally using e-mail, thereby avoiding the use of attachments or phishing emails:

It has become completely normal to only share links. Files are also sent, but we should be doing less email attachments, and reduce the opportunity for phishing attacks (Interviewee 2).

For Interviewee 2, there was also plans to transfer their ERP system to a cloud-based solution, indicating that the concept of remote storage was still seen as potentially a viable solution to counter cyber-risks:

…practically in the next 1-2 years, at the latest in 3 years' time, we are about to take the next steps into the cloud with our ERP system. We will be using Microsoft Dynamics. We are now in the preparation phase, but this is the future, remote access, handing over some of the responsibility to managing and securing our data to the cloud (Interviewee 2).

Some of the medium-sized enterprises also mentioned that they also used cloud-based services for their cyber-risk mitigation (CRMi) solutions:

We have now ProSoft Advanced XDR. This offers us now extended detection and responses, which is a new approach to address the threat of cyberattack, by detecting and providing real-time responses that enables a holistic protection against cyber-risks, for example unauthorised access, or misuse (Interviewee 4)

With our endpoints, we've have switched to Palo Alto. I'll say the Palo Alto client and the fact that we have the Palo Alto clients which are used on all our devices have enabled us

*to use the Palo Alto data lake. With this provider they have offered us 24 * 7 as to escalation and incident response services, which means we should have limited downtime in the event of a cyberattack (Interviewee 9).*

From above it is possible to surmise that cloud-based services are used by these medium-sized enterprises, but there is some scepticism about control over company data and the potential for the solution becoming a target for cyber criminals. However, some of the interviewees perceive the use of cloud-based services as a potential safeguard against cyber-risks, as the solution enabled the exchange of company data between various company sites, all without the data leaving the company's cloud. Then there were the potential advantages of using cloud-based services and solutions like cyber-risk management or even CRMi services.

4.6 The relationship between specific risks and mitigation strategies within these German medium-sized enterprises

The focus then changed to capture the relationship between identified specific risks and how the various mitigation strategies worked in these medium-sized enterprises. For Interviewees 2 and 5, they admitted that in their companies' cyber-risk strategies the assessment was from a qualitative perspective only:

No, we have not quantified the risks, we have only carried out a qualitative assessment, as to how big could the impact be, from being seen as high, medium or low. We have tried to get into the different categories and then went into the detail as to our thoughts, but we haven't really quantified them yet (Interviewee 2).

We do not have a quantitative approach to determine cyber-risks in relation to our tangible and intangible assets. We use more of a qualitative risk matrix that shows the potential impact of different attack vectors which are shown in different colours ranging from green to red (Interviewee 5).

Only one interviewee explicitly mentioned that in their medium-sized enterprise that there was some form of quantitative assessment used. But even this was the result of a specific question being asked by the interviewer:

Interviewer: Then do you use a mixture of qualitative and quantitative methods in risk assessment?

Interviewee: Exactly. Exactly. (Interviewee 9).

Interviewees 2, 7 and 8 expressed concerns about potential cyberattacks, and how concerned they were:

> *But as we know, just a lack of attention is enough, and we are a bit at the mercy of a cyberattack of some sort. Yes, exactly. So, I don't feel safe, definitely not, but I don't feel completely unprepared either (Interviewee 2).*
>
> *Yes, so we say that the biggest risk is actually the threat of encryption, and that we are at a bit of a standstill here as to what to do, as to preventing someone penetrating the network and simply destroys it (Interviewee 7).*

Then there was Interviewee 8 who noted the importance associated with cyberattack insurance:

> *Yes, the decision to take out cyber-risk insurance was based on two things or considerations, that were important to us. One was the help you get almost immediately if an attack happens, and the other is that self-assurance in the company that we have some form of external coverage (Interviewee 8).*

As to the impact of a cyberattack and the possible outcomes, Interviewee 3 noted that they had factored in potential loss of sales into their CRM strategies, but only for a few days:

> *We can actually react relatively quickly. As I said, in terms of value, I would then see a maximum of two days' sales being possibly lost, because we estimate that this is the time needed to respond, react and recover our systems (Interviewee 3).*

As to the impact of a cyberattack, the production value was seen as being measurable by determining the value of investing in cyber-defence measures, compared to the cost of the event occurring and the consequences afterwards:

> *I have never really discussed the budget for IT security measures. They, that is the team, all know that if the store is down for a day, it's much more expensive than any new firewall or any other type of cyberattack solution, so we are more proactive in this area (Interviewee 7).*

There was also the cost of cyber-risk insurance (CRI) as a cyber-risk mitigation (CRMi) measure, which was then compared with the potential loss to production and sales:

> *And the other important point is that if there is a business outage over a longer period of time, that you are adequately in a financially protected position. But this needs to be compared and balanced against the cost for a robust cybersecurity solution, which is never cheap (Interviewee 7).*

However, one of the interviewees voiced his concern that the potential of a cyber-risk occurring might be higher than estimated. This perspective was not related or represented the position of the company or its presence in the market, but informed by a more general view related to global politics:

> *Because of the overall global political situation, the risk has certainly become significantly greater, and I think the damage caused by cyberattacks has also become bigger, so I think strategies are being kept very tightly under wraps. I am personally convinced that there is a lot more going on than we read in the press or the media (Interviewee 4).*

From above, it is possible to summarise from the interviews that the medium-sized enterprise leaders followed a series of approaches, which included cyber-risk assessments and mitigation strategies. Most of the interviewees indicated that these medium-sized enterprises primarily used qualitative methods to assess cyber-risks, categorising them as being high, medium, or low, rather than employing quantitative assessment methodology. Only one medium-sized enterprise manager mentioned using a mix of both qualitative and quantitative cyber-risk assessment methods.

There were, however, concerns about potential cyberattacks, with some of the interviewees feeling vulnerable despite having some protection and recovery strategies in place. The interviewees highlighted the importance of CRI as to its immediate support during an attack and the immediate aftermath, providing some form of reassurance. One interviewee explained how their company incorporated potential sales losses into their CRMi strategies, estimating that the maximum impact of an attack would result in a loss of two days' sales while still being able to respond and recover quickly. The cost-effectiveness of investing in cyber-defence was also highlighted due to the interviewee's awareness but was seen as being determined by assessing the cost of the downtime compared to the initial financial outlay. Finally, one interviewee expressed his concern that the risk of cyberattacks might be underestimated due to the current global political situation, suggesting that the true extent of the threat might be more significant than what is being presented in the public domain.

4.7 The medium-sized enterprise managers perception towards cyber-risk insurance

As previously mentioned above, during the interviews the theme of cyber-risk insurance (CRI) was mentioned as being an important consideration or alternatively an unnecessary expense. The difficulty associated with quantifying the potential cyber-risk being covered and the premium needed to be paid also emerged from the interview data:

> *We have looked at cyber-risk insurance, but the insurance coverage is different compared to our other policies. I'll give you an example, we already had an offer at the time and then the hacker attack came. Today we have to say: the policy wouldn't have helped us much because it would have covered any damage up to a maximum of 50,000 Euros. With today's costs for recovery this would have not been enough (Interviewee 5).*

As indicated above, Interviewee 5 had suffered a major cyberattack, but the rejection of certain insurance policies was based on the experience, the extent of the damages, the premium payments, and the insurance coverage or pay-out which would have been too low. For Interviewee 7, the concern over insurance was related to whether the insurance company would be prepared to make the payment in the case of a cyberattack, or try and mitigate their losses:

> *I think the insurance company would do everything they can to avoid paying out the full amount and do everything they can to prove the attack was a result of our actions or inactions (Interviewee 7).*

Both interviewees shared a lack of trust amongst these medium-sized enterprises as to seeking insurance coverage. Another issue to emerge was that cyber-risk insurance was expensive, and this was being preventive, becoming the main reason why CRI had not been taken out:

> *Of course, when we thought about insurance against a cyberattack, our insurance company has provided us with examples and scenarios. But just look at everything that has happened to us recently and the outcome of our cyberattack, and then you need to balance of the cost of the premiums and the pay out and what it will cover (Interviewee 1).*

Despite the high costs, CRI could potentially ensure that the medium-sized enterprise had sufficient protection to cover the ramifications and outcome of the cyberattack, therefore making it potentially more of a viable solution:

Well, this question of costs comes up every year in the annual meeting with my insurance broker. I always get the same answer and I'm not interested. The premiums are too expensive for me. When I see all the conditions and the coverage, I will then weigh up the options and so far, I have decided not to take out the cyber-risk policy (Interviewee 3).

This perspective was not shared by all the interviewees. For Interviewee 5, even though there was a degree of scepticism after having experienced a major cyberattack he highlighted the benefits:

We have cyber-risk insurance and regularly undergo a cyber-risk security check by the insurer. We have also been supported by our cyber insurer, who regularly keeps us up to date with the latest security requirements and this is part of their service (Interviewee 5).

For Interviewee 8 he also reported positive experiences with using CRI:

… we have cyber-risk insurance here. We didn't have to do too much to adhere to the insurance requirements, but we have needed to meet all the requirements. As to the importance of cybersecurity, we perceive this type of insurance to be so important that we have to take the risk as seriously as a fire (Interviewee 8).

But again, this perspective of importance was challenged, particularly as to the associated costs of the premiums, as presented with Interviewee 5:

But I still think the insurance premium are set too high. This may well be due to the insurers' poor calculations and is probably also due to the high security surcharge, which makes it prohibitive for us (Interviewee 5).

The problem also arose when the requirements for insurance coverage needed additional costs to cover specific business requirements:

…the amount of damage is capped, or the policy premium is incredibly high. We have decided that it's better to invest the money in greater security technology, but we may look at it again in the future, but it is about value for money (Interviewee 7).

Even for those medium-sized enterprises who had taken out CRI, like Medium-Sized Enterprise Five, there were still some concerns about the value for money for insurance coverage:

If you estimate the risk, then I think you can now be happy if you are insured. At least that's what XXXX my insurance broker told me, but for us it is about value for money and ensuring that we are fully covered, but it is expensive (Interviewee 5).

This viewpoint of expense was shared by Interviewee 4:

> *We took out cyber-risk insurance with a German insurer XXXX[2] from 2015 or 2016 to 2021. What we have found is that the insurer's requirements to receive coverage have increased, I would say, exponentially year after year, therefore provided limited value and was too expensive. Then there were the increasing changes needed to comply with the insurance policies (Interviewee 4).*

The statement from Interviewee 4 reveals that the high resource requirements for obtaining coverage posed its own unique challenge. Therefore, satisfying these requirements could potentially reduce the motivation to seek CRI due to the expense. The perceived imbalance between premium costs and coverage also became evident, as seen with Interviewee 4 reflecting again on the costs:

> *…what it looked like to me at the time, and what struck me was that the company's insurance coverage was for 800,000 Euros, which in the cyber case is peanuts, I have to pay about half million Euros per year to have this insurance cover. … if I honestly quantify our risk at 10 to 12 million euros, then the eight hundred thousand through insurance won't help me either. Therefore, no value for money (Interviewee 4).*

One participant, Interviewee 9, noted the perceived imbalance between the insurance company and the medium-sized enterprise:

> *And then they, just between us, set the conditions. It's ok for me, but it could have been done a little differently. For an insurance person it was clear, it was, how do you say, a condition, and behind it there is an insurance calculation, then a business calculation and then certain conditions are put into the policy. You can't do that. I can understand it, but you don't do it. Now we have put the insurance up for tender, as we are seeking a policy which is favourable for both parties (Interviewee 9).*

As to the level of insurance coverage, the participant in this study, Interviewee 5 also noted the perceived information imbalance between the insurance company and the medium-sized enterprise:

> *I think all identified IT security risks that we classify as low after risk mitigation should be accepted by the insurance company. Then all other risks that have a more substantial damage potential and whose extent would be financially dangerous for the company*

[2] Actual company name deleted for anonymity reasons.

should be covered by cyber-risk insurance. If we have complied with all the requirements, then there is no need for the insurance (Interviewee 5).

While the rationale behind this statement is understandable, it also highlights the dilemma for insurance companies., as to the linkage between insurance coverage to certain conditions, which should cover quantifiable risks, but for potential financial damage in the worst-case scenario, the maximum level of coverage is difficult to assess and link to a premium.

To summarise the data presented above, CRI was firstly an issue due to uncertainty as to the value of the product, whether the policy covered the medium-sized enterprises' requirements and provided value for money. The interviewees from the medium-sized enterprises viewed the increasing levels of conditions required by insurers for insurance coverage as problematic, believing that such costly measures would make successful cyberattacks unlikely. A common theme in several interviews was a lack of trust in CRI companies in terms of their conditions and pay-outs. However, there were examples that indicated a trustful relationship between the medium-sized enterprise and insurers could exist, particularly if insurers also linked insurance cover to providing advice and support as to incident responses.

The findings presented above allow for a brief integrative reflection on the role and perception of CRI. While section 4.4 outlines the functional role of CRI as part of medium-sized enterprises' broader mitigation strategies, often embedded within backup, redundancy, and certification approaches, section 4.7 highlights how managerial perceptions shape whether and how CRI is actually implemented. These perceptions are frequently influenced by cost-benefit considerations, trust in insurers, and uncertainty around policy coverage. The managers' cautious or sceptical attitudes, therefore, do not contradict the role that CRI could play in cyber-risk mitigation but rather reflect a pragmatic response to perceived limitations and operational trade-offs. The two perspectives of strategic function and managerial perception are not contradictory but mutually illuminating, offering a fuller understanding of CRI adoption dynamics within the context of German manufacturing medium-sized enterprises.

Building on this reflection, the author proposes a practical solution to address the disconnect between medium-sized enterprise managers' perceptions and the realities of CRI. Based on the insights gathered, it appears unlikely that insurers themselves can effectively close this gap. From the perspective of medium-sized enterprise managers, insurers are not typically

regarded as trusted partners in risk mitigation, but rather as external risk takers with limited incentive to engage in transparent dialogue. This dynamic contributes to a structural information asymmetry, as medium-sized enterprises are understandably reluctant to disclose sensitive cybersecurity details to entities that may later assess their risk exposure or deny claims.

In the author's view, this challenge is compounded by the fact that cyber insurance remains a relatively young and evolving product category. With limited actuarial data and the added complexity of systemic and interconnected cyber risks, insurers adopt a cautious approach, often imposing stringent policy conditions. Rather than advocating for more regulation such as NIS2, which introduces compliance obligations but does not directly foster CRI adoption, the author suggests that a more effective solution may lie in leveraging industry associations as neutral intermediaries.

Organisations such as Bitkom or chambers of commerce could play a constructive role by offering anonymised benchmarking, trusted consultations, and clearer guidance on the actual value and limitations of CRI. These associations could also aggregate and share risk and incident data on an anonymous basis to help insurers better assess medium-sized enterprise specific risk profiles. Over time, broader acceptance of CRI may emerge if clients or supply chain partners begin to treat it, alongside certification, as a meaningful indicator of sound cyber risk management.

4.8 German medium-sized enterprises' preparedness against cybercrime risk and the attitudes towards balancing cyber-risk mitigation measures and business success

One factor that emerged from the interviews was the high dependency on a functioning IT network, and the need for production processes to be highly automated, which meant that there was a high reliance on a functioning and robust IT infrastructure. If a cyberattack occurred this could cause damage to the IT network, therefore production would have to stop, resulting in financial damages for at least for the duration of the disturbance. The interviewees all highlighted and acknowledged the high importance of a functioning IT system but also their willingness to take measures to ensure that a cyberattack could be prevented, as seen with Interviewees 2 and 8:

In the event of potential financial damage due to production stopping because of a cyberattack we have changed our thinking, we have invested in CRM software, we have staff training and awareness programs, and we are not aware of potential cyber-risks. If we cannot make any sales and we cannot make money, therefore we have no business. This means that the business literally stops (Interviewee 2).

Yes, the two aspects of major concern for us here, and I also say is the greatest danger is being underprepared and operating unethically. In other words, can someone with bad intentions do something in the background as we are not observant, and what measures and strategies are in place to recognise this threat? Then are we acting in a way that could compromise our customers or our suppliers to make then vulnerable to a cyberattack? (Interviewee 8).

To address this, many of the medium-sized enterprises had actively engaged with CRMi-measures, but also interestingly this had been demanded by their suppliers and clients. For suppliers, the requirement for CRM adoption was to minimise the impact to the potential loss of their own intellectual property and their supply chain activities:

The protection of our data was of course also an issue that we simply needed to address, and this was raised by our suppliers. We have had to change our order processes and agreements to ensure that they comply. This has included how we manage our supplier queries. The requirements were very detailed, as to how we set-up our systems, how the data centre was set-up, and what kind of security protocols are in place to prevent a cyberattack (Interviewee 2).

From the client perspective, the medium-sized enterprises needed to adopt certain cyber security measures, as recalled by Interviewee 7:

To conduct business, on average, we receive a questionnaire from a customer about our IT security every week. Often our customers are requiring us to make changes to our architecture when it comes to cybersecurity, especially from our medical customers (Interviewee 7).

However, there were also concerns related to the disclosure of certain details about cyber-risk management activities in the medium-sized enterprise, particularly as to external stakeholders. This included stakeholders who were seen as direct or indirect competition, raising the issue as to conflict of interest:

So, we are currently considering whether we will go along a recent client request, not because of the audit but in the way this audit will be carried out, which involves disclosure

of data locations and who is involved. XXXX[3] is our client, and they service or provide other services to other providers and competition (Interviewee 9).

The interviews then progressed on to the themes of cyber-risk mitigation (CRMi) as a tool to determine and achieve business success. There was a lack of consensus as to the benefits or usage as a success indicator, as shown below with Interviewee 7 and 9:

No, cyber-risk mitigation does not provide a bridge between risk and success. Success is more than cyber-risk security; it is about delivery and customer satisfaction (Interviewee 7).

It's just that the topic of KPIs such as monitoring, and availability of the product or service to the customer has nothing to do with security for me. For me, it's about productivity and hitting those key business targets and figures (Interviewee 9).

One could argue that these quotes represent the more traditional perspective as to business success and the associated indicators and measures. However, for Interviewee 3, there was a close synergy as to CRMi and key-performance indicators (KPIs):

Security is of course a very crucial aspect for our customers and therefore also an USP, or a selling point for us. Now, of course, we have to say that there is financial security, which means that we have to be financially viable or solvent. There is of course security and that is of course clear when it comes to the IT side of ensuring that our systems are working and operating (Interviewee 3).

The interesting point here is that interviewee 3 linked the issue of cybersecurity to the conventional success of meeting KPIs. A successful cyberattack would threaten production, which in turn would damage productivity. To summarise, the role of CRMi for business success must be interpreted not directly by means of conventional success indicators but in terms of association with the repercussions of a cyberattack on productivity, loss of revenue and sales along with company image and reputation.

From the responses above, the interviews highlighted the critical dependence of medium-sized enterprises on a robust IT network and automated production processes, making them highly vulnerable to potential cyberattacks. The interviewees recognised the severe financial

[3] Actual company name deleted for anonymity reasons.

consequences of such attacks, which could halt production and damage business operations. To mitigate these risks, these medium-sized enterprises had invested in CRMi software, staff training, and cybersecurity strategies. Interviewee 2 emphasised that business operations following a cyberattack would cease trading, underscoring the importance of preventing a cyberattack from occurring. Interviewee 8 raised concerns about being underprepared and the ethical implications of their actions, which were unable to protect their business for customers and suppliers. To achieve this, the medium-sized enterprise managers recognised the need to adopt a proactive CRMi strategy to protect suppliers and clients through adopting a robust cybersecurity strategy to protect intellectual property and ensure secure supply chain activities. However, some interviewees expressed concerns about disclosing cyber-risk management details to external stakeholders, fearing conflict of interest and confidentiality of data.

The discussion then shifted to the role of CRMi in business success. There was no consensus on whether CRM directly linked risk management to business success, with interviewees 7 and 9 viewing success more traditionally through delivery and customer satisfaction. However, Interviewee 3 saw a close connection between cybersecurity and KPIs, arguing that a successful cyberattack would harm productivity and, consequently, business success. Overall, the responses underscored the significance of CRMi in reducing cyber-risks and its indirect contribution to business success, which conventional success indicators cannot directly represent. However, the role of CRMi in business success becomes stronger when the protection of productivity, revenue, and reputation from the repercussions of a cyberattack is mitigated or reduced.

4.9 Summary of the Findings Chapter and key results addressing research gaps

Based on conducting a qualitative study, the interviewees revealed several important themes associated with how these German manufacturing medium-sized enterprises view and manage potential cyberattacks. Several themes emerged from the interviews, which addressed the study's research gaps and answered the research questions.

4.9.1 Results relevant to research gap 1 - Limited research exists on the actual level of preparedness against cyber-risks, especially in the German manufacturing context.

Based on the interview data presented in this study, German medium-sized enterprise managers are reasonably well prepared against potential cyber-risks. The medium-sized enterprise decision-makers tended to take cyber-risks seriously, however, often implementing basic measures like regular backups or installing firewalls.

The experience of a cyberattack was common among some of the German medium-sized enterprises, with most of these activities being through email, wherein employees were lured into clicking on an external link or opening an attachment that contained malware. Some of the cyberattacks also took the form of ransomware, where the company's IT systems are encrypted, and employees cannot access the network until the ransom is paid. However, these medium-sized enterprises were becoming more aware of this problem and had implemented internal training activities to make employees more aware of these cyber activities. These medium-sized enterprises had also incorporated cyber-awareness training into their onboarding procedures to educate new employees about risks and risk mitigation strategies when using their company's IT accounts.

Cyber-risk mitigation (CRMi) measures were seen as an important investment for several of the medium-sized enterprise's production infrastructures, as the interviewees recognised that a cyberattack could disrupt production capacity along with electronic communication channels and impede the ordering and payment systems. External actors were important considerations for these German medium-sized enterprises. These external connections included conducting business activities with larger companies, which often required some form of cyber-risk certification for all their suppliers. However, at the same time, some of the German medium-sized enterprises saw themselves as being relatively low-risk targets for a cyberattack, due to their size and lower financial power.

The level of cyber-risk preparedness amongst these German medium-sized enterprises varied. At the lowest level of CRMi, these businesses were aware of the problem and had taken some steps to deal with it, such as using firewalls, screening emails, and training employees to spot ransomware emails. They also kept their staff up to date on new developments, but there was no clear cyber-risk strategy or cyber-risk insurance coverage to go with it. Therefore, these businesses addressed cyber-risk mitigation on an ad-hoc basis. In contrast, some

of the medium-sized enterprises had adopted some form of CRMi strategies as part of the compgany's overall risk management strategy, but again there was no formal structured CRMi process being followed. There were, however, some medium-sized enterprises who had implemented a dedicated cyber-risk management strategy and had gained cyber-risk certification or were in the process of seeking this award. What clearly emerged across all cases is that the decision about how cyber risks were managed, whether through structured strategies, certification, or minimal reactive measures, resides almost entirely with the managers or executive decision makers themselves. This centralisation of responsibility means that the level of preparedness is closely tied to individual awareness, priorities, and willingness to invest. In mid-sized enterprises where the decision makers interviewed happened to be more proactive and well informed, preparedness tended to be higher. Conversely, when the topic was undervalued or seen as nonessential, cyber risk mitigation remained underdeveloped.

4.9.2 Results relevant to research gap 2 - There is insufficient insight into the cyber-risk mitigation strategies currently adopted by German medium-sized enterprises.

Those medium-sized enterprises with the lowest level of preparedness against cyberattacks (Medium-Sized Enterprise One, Four, and Six) had implemented only standard measures, such as firewalls, data backups, or the use of a VPN when logging into the company's network from outside. These medium-sized enterprises also imposed restrictions on staff who used their own devices for company work or restricted their ability to log into the company's network using private devices. The findings also indicated that these medium-sized enterprises informed the business through professional magazines or IT specialist internet sites as to recent developments.

At the next level of cyber-risk mitigation (Medium-Sized Enterprise Two and Three), there was constant monitoring for potential cyber threats, which included incident reporting systems being established. While cybersecurity costs were considered a major financial investment decision for protection against potential damages caused by a cyberattack, these businesses did have a structured approach to their cyber-risk mitigation (CRMi), which included the company's organisational structure, but lacked a dedicated individual or role for CRMi.

These medium-sized enterprises representatives did not consider their company to be a potential target for a cyberattack, either because of their small size or low levels of automation in their production processes.

At the highest level of cyber awareness, these companies had designed and implemented a dedicated cyber-risk strategy (Medium-Sized Enterprise Five, Seven, Eight, and Nine). The strategy adopted by these medium-sized enterprises included the implementation and further improvements as to the responsibility of either individuals or having a separate dedicated department. These medium-sized enterprises recognised the importance of external requirements, such as a certification scheme or cyber-risk insurance policy, to provide a formalised, structured approach to cybersecurity mitigation. Among the measures adopted included scenario training, in which potential threats were discussed and potential mitigation measures were tried and tested. These companies place significant emphasis on cyber-risk, and their decision-makers viewed cyber-risk mitigation measures as a critical investment. While the level of inside expertise in these medium-sized enterprises was high, these businesses still sought external specialism for cyber-risk mitigation as to the development of cyberattack mitigation strategies.

Importantly, the differences in strategy also reflect a broader spectrum of managerial attitudes, ranging from reactive compliance to proactive risk leadership. Medium-sized enterprises operating at the lower end of preparedness often adopted a more reactive posture, responding to incidents or external requirements only as needed. In contrast, those with structured and certified CRMi strategies tended to be led by managers with a proactive mindset who viewed cybersecurity as integral to operational resilience rather than a peripheral obligation. This contrast underscores the significant influence of leadership orientation in shaping the depth and sophistication of a medium-sized enterprise's CRMi efforts.

The certification and/or insurance was also seen as an important means to identify and indicate how the medium-sized enterprise had adopted best preventive practice against a cyberattack, and insurance was seen as an approach to mitigate against potential financial damage if a cyberattack occurred. However, even with this group of medium-sized enterprises, high insurance premium costs and the ratio between premium and pay-out in the event of a successful attack was seen as being not financially viable.

In addition to these findings, this study found that the medium-sized enterprises had separate office and production networks, therefore attempting to protect their networked machines from the consequences of a cyberattack. Therefore, these fragmented network architectures were another way to mitigate the consequences of a potentially successful cyberattack occurring throughout the entire business.

Communication was an important component in these cyber-risk mitigation strategies. The staff were informed about all fundamentals of cyber-risk mitigation, and where possible, in the event of a cyberattack two-way communication was established.

There was an increasing trend of clients and suppliers requiring external evidence of cyber-mitigation strategies, which had motivated these medium-sized enterprises to engage in cyber-risk mitigation. To assist in the meeting with these increased requirements, these medium-sized enterprises had begun to seek external advice on how the interviews showed that there was surprisingly little exchange with other medium-sized enterprises in the context of CRMi. Therefore, in terms of external communication, these businesses tend to rely on external networks, such as social media or professional support, as opposed to other medium-sized enterprises. Part of the reason could be attributed to not disclosing confidential information with their competitors.

4.9.3 Results relevant to research gap 3 - Limited understanding exists regarding the role of cyber-risk insurance within German medium-sized enterprises and what risks are effectively covered by existing insurance policies.

In this study, cyber-risk insurance (CRI) had only been adopted by those medium-sized enterprises who had proactively adopted a cyber-risk strategy, often due to the experiences of a cyberattack. However, even amongst these medium-sized enterprises, there were concerns about the high costs of premium payments and an uncertainty about whether their policies were good value. Interestingly, none of these medium-sized enterprises had made a claim on their policies; therefore, it was only their perceptions.

To emerge from the interviews was that one medium-sized enterprise had suffered substantial damage due to a cyberattack, who then compared their insurance coverage that had been offered at the time and concluded that the policy would not have been able to cover the actual financial loss. For another medium-sized enterprise, the ratio between premium

level and potential damage threshold was unattractive, as the annual premium was more than 60% of the potential cover. To remedy this, the medium-sized enterprise selected a self-insurance scheme by setting aside funds annually to build up reserves to cover potential damages from a cyberattack.

Overall, there was a general scepticism about the value of CRI. In addition, CRI policies also required the medium-sized enterprise to implement a comprehensive cyber-risk mitigation strategy, which would be costly. Therefore, these medium-sized enterprise managers were of the opinion that the company might be better off not taking out this form of insurance if the cyber-risk measures were not fully implemented. There were also concerns about the potential escalation of the requirements imposed by the insurers, which could lead to additional costs. The interviews revealed that when an insurance company offered practical advice and consultancy services, such as conducting security checks and providing practical support in the event of an incident, these medium-sized enterprises expressed a high level of satisfaction with this form of service. One potential explanation for this CRI scepticism lies in a strong tradition of perceived managerial autarchy within the selected mid-sized German manufacturing firms. While not used here in its strict economic sense, the term “autarchy” is employed to describe a mindset of operational self-sufficiency and minimal reliance on external institutions (Schenkenhofer, 2022). Many of these mid-sized enterprises have historically relied on internally managed approaches to risk, rather than quantitative risk assessments or externalised solutions. This mindset is often reinforced by the ownership structure of these businesses, where executive managers are also company owners and take pride in resolving issues in-house. Cyber risks, though acknowledged as real, were not commonly viewed as existential threats on the same level as financially devastating risks like fire or third-party liability, and were therefore managed with traditional technical safeguards such as backups, firewalls, and employee training. This autarchic approach is occasionally challenged when external requirements arise, for instance, through supply chain obligations or client expectations that demand certification, insurance coverage for cyber incidents, or other evidence of formal risk management and CRMi strategies.

4.9.4 Results relevant to the topic cyber-risk mitigation and business success

The interviews indicated a fundamental understanding and awareness towards the usage of success indicators and their usage to as measurement methodology. Productivity, orders and

sales, and various financial indicators, for example, income and sales, were mentioned along with the availability of raw material supplies and product storage. As to the instruments used to measure these indicators, there were the usage of conventional instruments such as regular reporting systems, quality checks, and comparison of actual figures with regular plan figures, which are also used by German manufacturing medium-sized enterprises, including quarterly reports, along with other techniques, including return on investment.

However, the interviews revealed that none of the above key-performance indicators (KPIs) were related directly to cyber-risk mitigation measurements or used to monitor and assess the avoidance of a cyberattack. When the medium-sized enterprise managers were asked directly whether they considered cyber-risk mitigation could be regarded as a success factor, two of the participants disagreed while only one interviewee agreed with the proposition. With the new legislation that came into force in Autumn of 2024 (EU NIS-2), this requirement means that companies need to review their cyber-risk mitigation strategies to ensure that they are complying. The interviews revealed an awareness of this development as it was coming in and considered this an additional reason why cyber-risk mitigation needed to be taken more seriously and KPIs and related measurements needed to be established.

5 Chapter Five
Discussion

5.1 Introduction

The purpose of this chapter is to critically analyse and interpret the findings presented in the previous chapter, the findings, in relation to existing literature as presented in Chapter Two. This discussion intends to present the results of the study in the context of existing knowledge within the field of cyber-risk mitigation (CRMi) strategies and cyber-risk insurance (CRI). Therefore, the chapter will present the key insights, theoretical contributions, and practical implications of the outcomes of the study. By drawing on relevant theories and empirical studies, this chapter seeks to situate the research findings within a broader academic context. The chapter opens with a critical review of the level of preparedness, CRMi strategies, and CRI before exploring the relationship between specific risks and the CRMi strategies that have been adopted. After that, it will present the managers' perceptions as to the usage of CRI and its potential as a solution for medium-sized enterprises to adopt to be better prepared to address the potential risks associated with cybercrimes, along with the CRMi measures and strategies recommended.

5.2 The level of preparedness against cyber-risks

Cybersecurity preparedness in German manufacturing medium-sized enterprises presents several unique challenges due to limited resources, varying levels of awareness, and differing approaches to managing and mitigating cyber-risks. Through interviewing the German medium-sized enterprise managers then drawing on the academic literature on cybersecurity, several themes emerge along with significant differences into how these organisations perceive cybersecurity risks and their approaches to handling them. These themes will be presented below, commencing with the cybersecurity strategies that have been adopted.

5.2.1 Adoption of cybersecurity strategies

Building directly on the interview themes presented in Chapter Four, section 4.2.1, where medium-sized enterprise managers described differing levels of formality in their cybersecurity approaches and a frequent reliance on general IT functions rather than dedicated CRMi

teams, this section examines how those findings align with, and diverge from, the academic literature.

The findings from interviews with German medium-sized enterprises support the existing academic literature, which indicates that most medium-sized enterprises lack any formal, dedicated cybersecurity CRMi strategy, and such cybersecurity strategies as exist are often incorporated into the broader security or IT functions. For the medium-sized enterprises in this study, the businesses tended to approach cybersecurity as part of an overarching disaster recovery strategy or within general IT responsibilities, which included adopting common practices including data backups and restrictions on personal device usage for work purposes. This approach of data security reflected a broader challenge identified by Mijnhardt et al. (2016), who highlighted that SMEs found existing cybersecurity standards to be complex and resource-intensive to implement. The medium-sized enterprises in this study could broadly be grouped into two categories: those with minimal, reactive cybersecurity measures; and those adopting more structured, proactive strategies. For many of these medium-sized enterprises, financial constraints significantly shaped their approach to CRMi. Several of the medium-sized enterprises found it financially unfeasible to implement a comprehensive CRMi strategy across departments, a significant barrier or challenge which academic literature extensively supports, including Pawar (2016), McLilly (2020), Pfeifer (2021), Armenia et al. (2021), and Carías et al. (2021).

However, it also emerged from the findings that a subset of medium-sized enterprises took more proactive cybersecurity measures, often catalysed by previous cyber incidents. Following cyberattacks, several medium-sized enterprises had begun to implement recognised standards like ISO 27001, through consulting with cybersecurity experts to identify vulnerabilities and acquiring CRI (see section 5.5) as a preventive safeguard. This post-incident shift in approach is supported by Rae and Patel's (2019) findings that many organisations tend to implement dynamic CRM measures only after a cyber incident reveals vulnerabilities in their existing systems. The increased CRMi readiness in these medium-sized enterprises, illustrated by the focus on hiring dedicated security officers or establishing a cyberattack response process, underscores an evolving approach to cybersecurity that responds adaptively to business needs and external threats.

There were also varied approaches to CRMi adoption, which can be shaped by the medium-sized enterprise's operational priorities, industry context, and available resources. These differences reflected the diverse ways managers balanced preventive investments with other business needs. Perceptions of CRI can include divergent views on its value, coverage, and analogies to traditional insurance, which is examined in further detail in section 5.5.

An increasing focus on regulatory compliance was evident among the medium-sized enterprises, with some companies emphasising the importance of aligning their cybersecurity measures with new regulatory standards, such as the NIST 2 requirements under the Cyber Resilience Act. This compliance-driven approach to CRMi suggests that medium-sized enterprises recognise the value of meeting regulatory standards, particularly in environments where non-compliance could have legal or financial repercussions. Consoli et al. (2020) supported the idea that regulatory requirements often drive organisational cybersecurity practices, pushing medium-sized enterprises toward more formalised approaches.

In summary, the study found that medium-sized enterprises demonstrated a spectrum of approaches to CRMi, which ranged from minimal, reactive measures to more structured, and proactive strategies following an incident. Some medium-sized enterprises had begun formalising CRMi and integrating insurance measures, often in response to previous cyber incidents, while others remained constrained by resource limitations and uncertainties regarding certain cybersecurity investments. This finding supports the work of Freund and Jones (2014), who advocated the adoption of frameworks like ISO 27001 or FAIR to enhance resilience, even for SMEs whose resources can be limited. The findings suggest that, despite the absence of formal CRMi strategies in many cases, these medium-sized enterprises generally valued cybersecurity risk management as essential for understanding potential risks and maintaining a baseline level of awareness and preparedness. The varied approaches reflect medium-sized enterprises' need to balance limited resources, regulatory compliance, and the growing demand for cybersecurity readiness, highlighting the importance of adaptable CRMi strategies that align with both business constraints and evolving threats.

5.2.2 The cyber-risk perception and preparedness

As presented in Chapter Four, section 4.2.2, the interviewees' comments showed a recurring belief among many medium-sized enterprises that their size and limited resources made

them unlikely targets for cyberattacks. Several participants described minimal investment in formal cyber-risk strategies unless externally required, while a smaller group reported proactive measures such as appointing dedicated cybersecurity staff. This section builds on those observations by comparing them with current academic perspectives on medium-sized enterprise vulnerability and preparedness, identifying where perceptions diverge from documented risks.

The study revealed a significant disparity between medium-sized enterprises perceived and actual vulnerability to cyberattacks. This difference indicated that both proactive and reactive cybersecurity measures were used, but also revealed an underlying reluctance to adopt formal security strategies unless they were mandated. Many of the medium-sized enterprises in this study believed that their small size and limited resources made them an unattractive target for cybercriminals, leading to a downplaying of potential cyber-risks. This perspective often resulted in a lower prioritisation of cybersecurity investments, with some medium-sized enterprises finding the costs of insurance and extensive protocols excessive compared to what they considered a minimal risk. This perception, however, contrasts with studies such as Brown et al. (2022), who argued that SMEs, especially those using IoT devices, are inherently vulnerable as they lack the type of security measures and defences that larger organisations have, making them easier targets. Radanliev et al. (2018) supported this perspective of Brown et al. (2022), emphasising that the rising use of IoT within Industry 4.0 increases vulnerability for medium-sized enterprises, as poorly secured devices create entry points for attackers. Conversely, the structured approaches adopted by some of the medium-sized enterprises, having appointed dedicated cybersecurity personnel to develop proactive response plans, demonstrated a higher level of preparedness and a more sophisticated awareness of potential cyber-risks.

In summary, the study highlighted a critical gap in cybersecurity preparedness among medium-sized enterprises, with interviews and academic literature indicating that there remains a misconception around SMEs' attractiveness as cyber targets. There was a common misconception that smaller organisations are "too small" to attract cybercriminals. However, this belief may be misguided, as it can make medium-sized enterprises more appealing to attackers due to their perceived lack of defences. However, the more proactive approaches taken by some medium-sized enterprises, alongside literature advocating for dedicated roles

and structured risk assessment models, underscore the importance of comprehensive cybersecurity strategies. Furthermore, proactive measures, such as identifying vulnerabilities and implementing early interventions, are critical in securing sensitive data and mitigating risks from threats like data breaches, malware, and ransomware.

As noted by Quesada (2016), there has been a shift in cybersecurity from reactive to predictive, proactive technologies, particularly through big data analytics, which allow for early threat detection and preventive action. This forward-looking approach enables medium-sized enterprises to minimise the impact of potential incidents and streamline recovery.

5.2.3 Resource constraints and outsourcing

As presented in Chapter Four, section 4.2.3, the interviewees frequently described how limited financial and technical resources shaped their cybersecurity decisions. Several managers openly acknowledged relying on in-house IT teams, even when those teams lacked the time or expertise for specialised cyber-risk mitigation. Other interviewees described outsourcing specific tasks to external providers, but often only when absolutely necessary. These perspectives provided the foundation for the following analysis, which compares such practical constraints to academic perspectives on outsourcing, cloud services, and collaborative cybersecurity strategies.

The finding generated from the interviews with these medium-sized enterprise managers, together with the academic literature, revealed a critical issue in the adoption of dedicated cyber-risk mitigation (CRMi) strategies among medium-sized enterprises, largely due to limited resources. Many medium-sized enterprises continued to rely on their internal IT departments to handle cybersecurity responsibilities, frequently citing financial and operational constraints as key reasons for not establishing dedicated CRM teams. This approach reflected a broader sentiment within the medium-sized enterprise sector, particularly in manufacturing, where there was a prevailing belief that resource limitations prevented a comprehensive CRMi strategy from being sustainable. As a result, cybersecurity remained more reactive than proactive for many medium-sized enterprises, leaving them vulnerable to potential threats.

The lack of specialised cybersecurity personnel within medium-sized enterprises contributed to inconsistent implementation of cybersecurity measures, with the absence of expertise

creating gaps in their defence systems. While some medium-sized enterprises actively monitored cyber threats and assessed strategies, the high costs associated with dedicated CRMi solutions deterred these businesses from formalising their approaches. This trend aligned with findings by Mthiyane et al. (2022), who suggested that financial and technical resource limitations prevent SMEs from investing in comprehensive CRMi frameworks, leaving them more susceptible to cyber threats.

To address these constraints, outsourcing emerged in the literature as a frequently recommended solution, offering SMEs access to specialised cybersecurity expertise without requiring a dedicated in-house team. A few medium-sized enterprises in this study recognised their internal resource limitations and relied on external consultants to address cybersecurity needs, especially for sustained incident resolution and proactive risk assessment. This trend aligned with the recommendations of Mzileni and Ncubukezi (2022), who advocated using specialised service providers to manage cybersecurity functions effectively. Franke and Meland's (2019) endorse outsourcing incident response as a viable option for SMEs with limited in-house capabilities. This strategy includes external consultants who bring industry-standard practices and expertise, helping SMEs identify vulnerabilities and respond more efficiently to incidents.

Despite academic literature such as Franke and Meland (2019), McLilly (2020), and Mthiyane et al. (2022) who advocate for outsourcing as a viable solution, many medium-sized enterprises remained hesitant to fully engage in outsourced CRM solutions, citing cost concerns and limited awareness of its benefits. For medium-sized enterprises already facing financial constraints, outsourcing cybersecurity appeared to be an additional expense, leading these businesses to perceive it as financially unviable. This reluctance was compounded by limited knowledge of how outsourcing could be structured to meet specific cybersecurity needs cost-effectively. Regulatory pressures added further strain, as compliance requirements, such as those under NIST 2 of the Cyber Resilience Act, placed additional demands on SMEs' internal resources. This regulatory context underscored the potential value of scalable solutions like outsourcing, which could help SMEs meet evolving standards without overburdening their existing teams. In summary, from the above debate sources including Franke and Meland (2019), McLilly (2020), Mthiyane et al. (2022) and Mzileni and Ncubukezi (2022)

have emphasised that outsourcing can offer flexibility and adaptability to SMEs' limited budgets, which is an essential CRMi measure even in resource-constrained environments.

Another solution that emerged from the cybersecurity literature (McLilly, 2020; Mlakar et al., 2021; Saber, 2016) to alleviate internal resource pressures while enhancing operational security was the use of cloud-based, on-demand cybersecurity services. This approach provides SMEs with scalable and cost-effective access to advanced tools and expertise. As discussed further in section 5.3.4, the often-reluctant position of SMEs, along with additional aspects of these models, including their potential to reduce significant upfront investments, will be specifically captured.

The academic literature from Pawar (2016) and Ajuzie (2019) also advocated for collective cybersecurity strategies, involving cost-sharing and shared resources, and the benefit for smaller SMEs that could not independently afford advanced cybersecurity measures. According to both scholars, implementing collective strategies, such as shared cloud-based platforms for cyber defence, could empower SMEs to pool resources and gain access to more robust cybersecurity measures.

However, many of the medium-sized enterprise managers preferred to rely on individualistic strategies, possibly due to concerns over data sharing, privacy, and the complexities of collaboration. The reluctance to adopt collective solutions indicated an opportunity to educate decision-makers, IT managers within medium-sized enterprises, and business stakeholders about the advantages of a shared cybersecurity approach. These benefits include greater affordability and enhanced security coverage. Awareness efforts could also target industry regulators, who play a role in shaping or enforcing cybersecurity strategies within medium-sized enterprises.

Based on the above, the findings revealed substantial challenges facing medium-sized enterprises in adopting comprehensive CRMi strategies, with financial, technical, and personnel limitations creating significant barriers to effective cybersecurity. Furthermore, solutions such as outsourcing, cloud-based services, and collective cybersecurity strategies could be seen as suitable solutions. However, these approaches remained underutilised by medium-sized enterprises, who frequently cited concerns about cost, data security, and limited understanding of alternative cybersecurity models.

5.2.4 Perception of cyber threats and risk vulnerability

As outlined in Chapter Four, section 4.2.4, many of the interviewees openly described how they believed that their organisation's size and modest data assets made them less likely to be targets for a cyberattack. Several of the interviewees recounted deprioritising investments in advanced security measures for this reason, while others admitted that minor incidents like phishing emails had nonetheless caused operational disruption. These firsthand accounts established the basis for the following analysis, which contradicts academic evidence (e.g., Pfeifer, 2021) that this size of business is less likely to be targeted. Instead, this study contends that these businesses are potentially attractive targets due to their weaker defences and close integration into larger supply chains.

Since many of the medium-sized enterprises in this study underestimated their vulnerability due to limited resources and believed themselves to be unlikely targets, there was a substantial gap between perceived and actual cybersecurity risks. Most of the interviewed medium-sized enterprise managers perceived that their small size and lower-value data made them less attractive to cybercriminals, often leading to a lack of prioritisation of cybersecurity investments. However, Dayalan (2017), Pfeifer (2021), and Renaud (2016) challenge the assumption that SMEs are less likely targets for cyberattacks, arguing that their weaker defences made them potential entry points for attackers to infiltrate larger networks or supply chains. These authors highlight that SMEs often underestimate the extent of their exposure, leaving critical vulnerabilities unaddressed. This reality compounds the significant operational risks SMEs already face, including cybersecurity breaches that disrupt workflows, compromise data, and result in financial losses. Poorly secured supply chains and IoT devices further increase exposure to attacks, while insufficient employee training can impair awareness of vulnerabilities to phishing and insider threats. Non-compliance with regulations risks legal penalties, and over-reliance on unsecured third parties amplifies these challenges. Such vulnerabilities can lead to downtime, reputational damage, and costly recovery efforts, ultimately threatening business continuity and customer trust. Without robust defences, SMEs remain exposed to data integrity issues, endpoint vulnerabilities, and IT system failures, jeopardising their operational stability in an increasingly interconnected digital environment.

While some medium-sized enterprise managers acknowledged phishing and other cyber threats, the interviewees often addressed the threat reactively rather than proactively.

Brown et al. (2022) highlighted that even minor incidents, such as a phishing email, could have significant operational repercussions for SMEs. These businesses further stressed that these seemingly minor events could trigger costly disruptions, particularly for underprepared SMEs. Although a few of the medium-sized enterprise managers reported heightened awareness and minor policy adjustments following incidents, academic research indicates that these reactive measures were insufficient for comprehensive cybersecurity preparedness.

Outsourcing emerged as a recommended solution for addressing internal resource gaps, providing medium-sized enterprises with specialised cybersecurity expertise and around-the-clock protection. Some medium-sized enterprises relied on external consultants to manage their cybersecurity needs, reflecting a trend supported by Franke and Meland (2019) and Mthiyane et al. (2022), who advocated for outsourcing among SMEs lacking internal capabilities. However, many medium-sized enterprises in this study remained reluctant to outsource fully, citing financial concerns and limited awareness of the benefits. Financial constraints continued to be a major barrier, as medium-sized enterprises often saw outsourcing as an added expense rather than a long-term investment in resilience.

Regulatory challenges further complicated cybersecurity efforts for the medium-sized enterprises surveyed. Some of the medium-sized enterprise managers reported that current regulations were less rigorous for small businesses than for larger enterprises, creating inconsistencies in cybersecurity practices and compliance. El Baz and Ruel (2021) argue that stronger regulations are necessary to improve SME resilience, particularly in global supply chains. Enhanced regulatory frameworks could provide SMEs with clearer guidance, encouraging them to prioritise CRMi investments. Without regulatory pressure, many SMEs might continue to underinvest in cybersecurity, leaving them vulnerable in an increasingly complex threat environment. This position is also supported by Grocke (2017), who stated that collaboration between SMEs as customers and IT service providers could be highly effective in addressing technical compliance and facilitating reporting against regulatory requirements.

In conclusion, the medium-sized enterprises' belief that their small size granted immunity from cyber threats was a misconception. Formalised CRMi strategies, either through standards like ISO 27001, outsourcing, or cloud-based services, are essential for effective CRMi.

Strengthened regulations, greater awareness of cybersecurity benefits, and proactive approaches are critical to enabling medium-sized enterprises to navigate cybersecurity challenges and bolster resilience across increasingly vulnerable supply chains.

5.2.5 Supply chain risk management

Chapter Four, section 4.2.5, captured the interviewees concerns about both the operational importance and the inherent risks of participating in interconnected supply chains. Several managers openly acknowledged vulnerabilities, particularly around EDI systems, electronic invoicing, and cross-organisation data flows; however, they also admitted that dedicated CRMi strategies were often absent. These opinions were then used to frame the study, which then compared these perceptions and practices with the academic literature on SME supply chain cybersecurity.

The interviews with medium-sized enterprise managers supported the studies of Pfeifer (2021) and Zeiringer et al. (2022) who underscored the considerable cybersecurity challenges inherent in integrating SMEs into larger interconnected supply chains. While many of the interviewed medium-sized enterprise managers acknowledged the risks associated with their roles within supply chains, there was an absence of a dedicated cyber-risk mitigation (CRMi) strategy. This limitation reflected a common theme amongst medium-sized enterprises: their limited resources led to insufficient investment in formalised cybersecurity, with these businesses focusing only on securing immediate network boundaries rather than adopting comprehensive CRM frameworks.

Existing literature highlighted the importance of formal CRMi strategies for SMEs, with Zeiringer et al. (2022) advocating that SME supply chain risk management should focus specifically on proactive risk elimination and avoidance. Due to the resource limitations identified, some of the medium-sized enterprises had opted for the risk avoidance strategy, which, while addressing immediate concerns, left potential critical gaps in their cybersecurity preparedness, increasing their vulnerability to threats. This mirrors Mthiyane et al.'s (2022) perspective that these approaches can enable SMEs to access specialised expertise and strengthen their risk management capabilities without incurring prohibitive costs.

In some medium-sized enterprises the businesses relied on external consultants, illustrating how outsourcing could support CRMi standardisation and meet compliance requirements

effectively. This outcome is aligned to Franke and Meland (2019) who advocated for outsourcing incident response to manage risks that internal teams might struggle to manage.

Regulatory requirements presented another major challenge for medium-sized enterprises, with many of these businesses perceiving that current cybersecurity regulations were less stringent for small entities than for larger organisations. Several of the managers cited specific vulnerabilities linked to Electronic Data Interchange (EDI) systems and compliance with electronic invoicing, which amplified their exposure to cyber-risks. This need for more robust regulatory support is aligned with El Baz and Ruel's (2021) recommendation for collaborative regulatory frameworks to strengthen SME resilience within supply chains.

Stronger regulations could help ensure that SMEs implemented consistent cybersecurity measures, making them less vulnerable entry points within interconnected networks. This is also supported by Oxford Analytica (2021) and Musa (2012) who emphasise that enhanced supply chain protections are essential, advocating for cybersecurity standards that integrate financial safeguards, like cyber-risk insurance (CRI), to cover potential losses.

This study has revealed that financial constraints pose a significant challenge for many medium-sized enterprises, often deterring these businesses from investing in CRMi and insurance.

This gap in expertise not only weakened the medium-sized enterprise cybersecurity defence, but also increased the vulnerability of the interconnected nature of a supply chain, as cyber threats could exploit these weaker links to disrupt broader networks. Some medium-sized enterprises also turned to cloud-based solutions, particularly for secure data sharing, remote access, and meeting international standards required for supply-chain participation. This outcome aligns with McLilly's (2020) and Ajuzie's (2019) findings that cloud adoption can help smaller firms meet partner expectations through scalable, cost-effective models. Operational benefits, risks, and governance considerations of cloud use are discussed further in section 5.3.4.

Recognising these challenges, some large companies have taken an active role in supporting their suppliers' CRMi efforts. This support has evolved from providing educational resources to directly facilitating the implementation of cybersecurity solutions. Other initiatives can include offering vetted solutions from selected partners and acting as enablers and collabora-

tors to streamline access to these resources for suppliers who may be facing similar challenges. These collaborative strategies highlight the importance of promoting awareness while assisting in addressing any potential resource gaps in smaller businesses through targeted information campaigns and support programmes. Larger organisations that foster a partnership strategy and provide additional resources can enable medium-sized enterprises to be more proactive in adopting cybersecurity measures more effectively.

Training and preparedness also play a critical role in managing cyber-risks within supply chains, yet they were often underfunded or supported by this type of business. For Mzileni and Ncubukezi (2022), cybersecurity readiness requires basic training and awareness, especially for employees who might inadvertently introduce vulnerabilities through phishing or other unintentional actions. In highlighting this, Mzileni and Ncubukezi (2022) contended that many SMEs lacked the resources for foundational security measures, leading to limited internal awareness of cybersecurity best practices. This lack of preparedness was echoed by many of the medium-sized enterprise managers, who cited the importance of fostering internal awareness to address cyber-risks ethically and effectively, underscoring that cyber preparedness was not merely technical but also a matter of organisational culture and responsibility.

In conclusion, medium-sized enterprises faced notable challenges in managing cybersecurity within supply chains due to resource constraints, limited regulatory support, and gaps in awareness. For writers including Ajuzie (2019), Franke and Meland (2019), McLilly (2020), Zeiringer et al. (2022), and Mthiyane et al. (2022), SMEs could improve their resilience by adopting more proactive CRMi strategies, which might include outsourcing cybersecurity functions, leveraging cloud-based solutions, and collaborating within supply networks. Furthermore, this type and size of business could also strengthen regulatory support and increasing awareness of affordable CRMi solutions could empower medium-sized enterprises to manage cybersecurity risks more effectively, ensuring they were secure participants within increasingly interconnected supply chains.

5.2.6 Summary on the level of preparedness against cyber-risks

The findings support the existing academic literature on CRMi as to how medium-sized enterprises view and approach cybersecurity. Many medium-sized enterprises in this study

lacked formal, dedicated CRM strategies, opting instead to integrate cybersecurity into broader risk management frameworks. The perception among medium-sized enterprise managers that they were "too small" to be targeted highlighted a fundamental misunderstanding of cyber-risks, which academic literature identifies as a critical issue. Therefore, the medium-sized enterprises need to be made aware that their size does not exempt them from attacks. In fact, as seen in the interviews, their limited security measures made them more attractive to opportunistic cybercriminals. Addressing this misconception is crucial for improving the overall cybersecurity posture of medium-sized enterprisess, ensuring they adopt adequate risk management practices to protect against a wide range of threats.

5.3 Cyber-risk mitigation and cyber-risk insurance

Cybersecurity preparedness in medium-sized enterprises presented unique challenges due to limited resources, varying levels of awareness, and differing approaches to cyber-risk mitigation (CRMi) and cyber-risk insurance (CRI). Themes that emerged from the study were associated with the adoption of CRMi strategies, resource constraints, employee training and awareness, and technological tools, which will be presented below.

5.3.1 Employee training and awareness as a risk mitigation strategy

Drawing on the empirical results in Chapter Four revealed that managers consistently identified employee behaviour in particular as to being susceptibility to phishing. Several of the participants cited recent incidents that triggered ad-hoc or reactive training initiatives, while other interviewees used their onboarding sessions or phishing simulations to address this problem. Interestingly, there was an admission that training was irregular and not fully embedded into ongoing employee development processes.

Employee training and awareness programmes emerged as critical elements in medium-sized enterprises' CRMi strategies, with many interviewees acknowledging the importance of ongoing education. Medium-sized enterprises have arguably viewed employee training and awareness programmes as crucial components of their cybersecurity strategies, as cyber threats tend to increasingly target human vulnerabilities, and employee behaviour becomes central to cybersecurity defences. Therefore, these medium-sized enterprises had adopted

a range of training practices, from proactive, structured programmes to inconsistent, reactive measures, highlighting the challenges of fostering a sustained culture of cybersecurity awareness. While many medium-sized enterprises recognised the value of employee training, the degrees and levels of commitment did vary. Some medium-sized enterprises had initiated training during onboarding, covering data security and IT protocols, and incorporated ongoing, mandatory, and optional sessions, including practical phishing simulations. The interviewed medium-sized enterprise managers believed these programmes emphasised vigilance, proactive behaviour, and personalised engagement to address key risks, particularly phishing, thereby fostering a culture of responsibility and resilience against cyber threats.

This proactive approach aligns with Renaud (2016) and Kalhoro et al. (2021), who argued that while SMEs strive to enhance information system security and use IoT technology to improve product quality and service delivery, employees are often recognised as the weakest link in cybersecurity. However, research by Consoli et al. (2020) and Carías et al. (2021) highlighted that, while training is valuable, the format and content often lack comprehensive organisational coverage among SMEs, which may limit its effectiveness. As a result, targeted training is essential for mitigating risks such as phishing and social engineering attacks.

There was also a need for continuous, structured training programmes that adapt to evolving risks, with Labunets et al. (2020) and Schlesinger (2018) advocating for flexible training strategies that kept pace with emerging threats, ensuring employees remain vigilant. Some of the medium-sized enterprise managers reflected this best practice by integrating structured training programmes into their CRMi efforts. However, inconsistencies in training across medium-sized enterprises revealed critical gaps in their cybersecurity planning. The reliance on employee vigilance alone, as seen in some medium-sized enterprises was inadequate for a secure cybersecurity posture. This is supported by Zeiringer et al. (2022), who noted that SMEs often struggled to establish consistent cybersecurity behaviours among all staff members. Binkhorst (2020) highlighted the importance of closing the knowledge gap between cybersecurity experts and non-experts to ensure training was accessible and effective for all employees.

For the medium-sized enterprise managers in this study, there was an acknowledgement that there was a persistent gap in effectively communicating potential risks while fostering a

consistent staff vigilance to these threats. To address this, training initiatives designed to ensure cybersecurity practices are necessary, which also need to be embedded into the business. This strategy of tailoring training programmes within a medium-sized enterprise design around specific business needs is supported by Dimitrov and Rasheva-Yordanova (2019), who advocate for skills-focused training that accounts for SMEs' resource constraints. Dimitrov and Rasheva-Yordanova (2019) argue that such training is more practical and implementable for SMEs, as opposed to focusing on specialised, technical knowledge which may exceed their capacity to apply the strategy effectively. By prioritising practical skills development, medium-sized enterprises might be better positioned to enhance their operational capabilities, whereas overly technical training risks being inaccessible and underutilised, limiting its impact.

To emerge was also the importance associated with external collaboration to enhance training effectiveness. Ajuzie (2019) and Such et al. (2015) suggested that partnerships with external experts could improve training programmes by incorporating advanced insights on cybersecurity threats. However, many of these medium-sized enterprises in this study conducted training internally, rarely leveraging external expertise, which may have limited its effectiveness given the complexity of modern cyber threats. This reluctance to seek external collaboration potentially left medium-sized enterprises underprepared for sophisticated cyber-risks that evolved rapidly.

In summary, both the interviews and existing literature underscored the importance of employee training in CRMi strategies for medium-sized enterprises. While some medium-sized enterprises in this study had progressed in integrating training as a core component of cybersecurity, many continued to rely on reactive and inconsistent approaches. To improve resilience, medium-sized enterprises however needed structured, proactive training models that incorporated external expertise and practical, hands-on applications. By preparing employees as the first line of defence against cyber-risks, medium-sized enterprises can strengthen their overall cybersecurity posture in an increasingly challenging threat landscape.

5.3.2 Backup strategies and data recovery

The earlier findings in Chapter Four, including in sections 4.3 and 4.4, revealed that managers tended to describe backup procedures and processes as one of the few cybersecurity practices adopted. These practices often involved physical tapes stored offsite or multi-stage backups. Some of the interviewees indicated that they used alternative systems as contingency options, though reliance on manual or physical processes was common. These strategies and practices adopted reveal a significant gap between existing backup routines and the adoption of more advanced solutions like a cloud-based approach.

The findings in the study highlighted backup plans as a cornerstone of cyber resilience for medium-sized enterprises. Several firms in this study emphasised the use of physical backup tapes as a primary method for safeguarding against data loss, with some businesses even removing tapes from the premises to protect data from physical disasters such as fires. The study found that there were medium-sized enterprises who had implemented multi-stage backup procedures as their main cybersecurity strategy, while other businesses had opted for secondary recovery options or standby sites. There were a few medium-sized enterprises involved in this research who had employed more agile approaches, utilising external backup services to share and operate data and applications on alternative systems, including competitor systems, if necessary. These backup strategies collectively provided an essential layer of data security, and conducting frequent restore activities further enhanced preparedness for recovery from potential cyber incidents.

Despite these measures, academic literature including Schlesinger (2018) and Radanliev et al. (2018) suggests that physical backups alone may leave SMEs exposed to additional vulnerabilities. Their studies recommend adopting advanced, cloud-based backup solutions to strengthen data protection. Cloud-based backups offer multiple advantages over traditional physical methods, including protection against a wider range of threats, such as ransomware and natural disasters, and features like automated and encrypted backups. Cloud solutions also provide faster recovery times and stronger security compared to physical tapes, which can be susceptible to theft, accidental loss, or damage during transport.

For instance, there were medium-sized enterprises which did not account for the risk of cybercriminals compromising backup tapes, reflecting a potential weakness in their data protection strategies. This finding aligns with Zeiringer et al. (2022), who observed that some

SMEs tend to rely on basic risk mitigation strategies, often overlooking more advanced threats. By transitioning to cloud-based backup systems, these SMEs could enhance their data security and improve their response capabilities during cyber incidents.

While Kapoor et al. (2018) in their qualitative research study were not directly addressing backup strategies, the topic became prominent when preparing for cyber incidents and actions necessary after an attack in the form of data recovery. Kapoor et al. (2018) argue that every SME must be prepared for potential cyber incidents by taking actions such as continuous testing, verification, and the use of backups to restore data and systems to normal business operations. To address this, they developed an SME-specific Incident Response Framework that is simple yet powerful enough to guide SMEs effectively. This framework is both practical and helpful in informing SME responses to data breaches.

These findings are particularly interesting because, while organisations often prioritise technical measures in practice, their best-practice advice tends to emphasise prioritising measures that address user-related factors. Although Kapoor et al. (2018) did not focus directly on backup strategies, their qualitative research underscored the importance of data recovery as a vital element of cyber incident preparation and response. For Kapoor et al. (2018) there is a need for SMEs to adopt proactive measures, such as continuous testing, verification, and maintaining reliable backups, to restore data and systems quickly after an attack. Building on this, Kapoor et al. (2018) identified challenges including overreliance on technical measures, inconsistent breach responses, and a lack of learning mechanisms to improve resilience. To address these issues, Kapoor et al. (2018) proposed a structured, SME-specific incident response framework with clear procedures for the management of security breaches, data recovery, and fostering organisational resilience, enabling the businesses to be better prepared for and recover from a cyber incident.

To overcome this lack of knowledge and understanding, it is therefore necessary for medium-sized enterprises to adopt a more robust strategy of relying on backup solutions and adopt more advanced technologies like cloud-based backups, alongside developing comprehensive and proactive approaches to incident response. This includes structured processes for breach response and a focus on learning from past events, which could help medium-sized enterprises mitigate risks more effectively and ensure they are better prepared for future incidents.

5.3.3 Zero trust policies and authorisation control

Interview evidence, as discussed in sections 4.5.1 and 4.5.2, showed that several medium-sized enterprises had begun embedding zero trust principles into their daily operations, from role-based access restrictions to verification of remote maintenance devices, as a direct response to concerns over unauthorised network access.

The adoption of zero trust policies emerged as a significant theme in interviews with medium-sized enterprise managers, highlighting a proactive approach to minimising cyber-risks through stringent access controls. Several medium-sized enterprise managers described implementing zero trust policies by focusing on restricting user access based on job roles and ensuring that no device could connect to the company network without prior authorisation. This included remote devices, such as those used by maintenance personnel, which required verification before gaining network access. Similarly, devices used by remote employees were routinely checked for malware to enhance network security.

This emphasis on zero trust aligns closely with current cybersecurity best practices, particularly for medium-sized enterprises that lack the robust perimeter defences typically available to larger enterprises. Tam et al. (2021) advocated for zero trust models as an effective strategy for mitigating internal threats and preventing unauthorised access, noting their growing relevance in distributed work environments—a trend accelerated by the COVID-19 pandemic. Kalhoro et al. (2021) further support this approach, emphasising that role-based access controls and regular device monitoring are vital components in reducing the risk of security breaches.

For medium-sized enterprises that have not yet implemented zero trust models, the absence of comprehensive cyber policies leaves critical systems and sensitive data highly vulnerable to security breaches. Despite the recognised benefits, implementing zero trust models presents significant challenges for medium-sized enterprises. Al-Dosari and Fetais (2023) argue that the financial investment required to fully adopt zero trust architectures represent a substantial barrier for SMEs, especially those with limited IT budgets. A zero-trust approach demands investment not only in advanced technologies but also in continuous process development, making it difficult for smaller organisations to regularly update and upgrade their infrastructure.

To address these challenges, both the interviews and the existing literature, including Tam et al. (2021), recommend a phased approach to adopting zero trust policies. Rather than implementing a full-scale architecture immediately, SMEs could begin by securing their most critical systems and gradually expanding zero trust practices across other areas of the organisation. This incremental adoption strategy allows SMEs to implement robust security measures in a manageable way, balancing costs and resource limitations effectively. By progressively building a zero-trust environment, medium-sized enterprises can strengthen their cybersecurity resilience without overwhelming their capacities, thus creating a sustainable path toward comprehensive cybersecurity.

5.3.4 Cloud-based solutions for cyber-risk mitigation

The findings from sections 4.5.3 and 4.5.4 illustrated the varied attitudes of medium-sized enterprises toward cloud adoption, ranging from enthusiastic uptake for operational and cybersecurity benefits to pronounced caution over maintaining cybersecurity sovereignty and avoiding the risks associated with shared infrastructure.

While attitudes toward cloud adoption varied among the medium-sized enterprise managers in this study, the findings indicated a growing recognition of cloud-based services as being a potential practical solution for cyber-risk mitigation (CRMi). Several organisations expressed their intentions to transition to platforms like Microsoft Dynamics, citing benefits such as enhanced remote access, streamlined data management, and improved scalability. Other medium-sized enterprise managers emphasised the cybersecurity advantages of cloud services, including real-time threat detection, automated backups, and resilience during cyber incidents, ultimately aiming to achieve both operational efficiency and robust cyber defence. Some of the participants in the medium-sized enterprises also reported adopting cloud-based solutions specifically to meet the cybersecurity requirements of their supply chain partners, particularly for secure data sharing, remote access, and alignment with international standards necessary for supplier approval. This approach of adopting cloud-based solutions aligns with McLilly (2020), who noted that cloud adoption can help smaller firms meet large partners' expectations. Supporting this, Ajuzie (2019) highlighted the collective and shared-service models as scalable, cost-effective options for this size of business.

However, not all medium-sized enterprise managers shared this enthusiasm for cloud adoption: some expressed concerns about the increased risks associated with cloud platforms, viewing them as attractive targets for attackers due to their shared infrastructure and widespread usage. This apprehension aligns with Rawindaran et al. (2021), who found that SMEs often hesitated to trust cloud services due to perceived vulnerabilities. Data sovereignty also remained a key concern; for example, some medium-sized enterprises were apprehensive about storing sensitive information on foreign servers, echoing issues discussed by McLilly (2020) regarding control over data storage locations. Despite these reservations, studies by Quesada (2016), Saber (2016), McLilly (2020) and Ncubukezi (2020) emphasised the strategic advantages of cloud adoption for SMEs. For Quesada (2016) the advancements in cloud monitoring can support new business models and proactive cybersecurity, helping SMEs shift away from purely reactive measures. This was supported by Ncubukezi (2020) who proposed a proactive cloud-based risk assessment model, arguing that tools like Monte Carlo simulations and Bayesian analysis can make advanced risk management practical for smaller businesses. Furthermore, Mlakar et al. (2021) advocated for cost-effective "Security as a Service" models, allowing SMEs to maintain IT continuity without straining limited resources, a recommendation echoed by McLilly (2020) and Saber (2016), who suggested that outsourcing complex cybersecurity functions to cloud providers could alleviate the burden on SMEs' internal teams.

The risks of cloud adoption have also been acknowledged, with Franke and Meland (2019) pointing to the potential for business interruptions due to cloud outages and ransomware attacks, especially in sectors like manufacturing and IT, underscoring the dual nature of cloud services. While cloud platforms offered significant benefits in scalability and cost, the solution also introduced risks that medium-sized enterprises needed to actively manage. Pfeifer (2021) recommended that SMEs reduce cybersecurity complexity by leveraging external cloud-based expertise but emphasised the importance of carefully vetting providers to ensure compliance with data protection standards like GDPR, which was also supported by Pfister and Lehmann (2023).

In summary, cloud-based solutions can offer medium-sized enterprises invaluable benefits in scalability, cost reduction, and enhanced security capabilities but also introduce new vulner-

abilities. While some medium-sized enterprises viewed cloud adoption positively for its operational and cybersecurity advantages, others remained cautious, citing concerns over increased risks and data sovereignty. The academic literature, including Quesada (2016), Schmitz and Pape (2020), and Rawindaran et al. (2021), supports these mixed attitudes, underscoring the benefits of cloud adoption while emphasising the need for comprehensive CRMi. For medium-sized enterprises to fully leverage cloud technologies, a balanced approach is essential, which includes careful provider vetting, adherence to data protection standards, and a proactive stance toward managing potential cloud-specific risks.

5.3.5 Dependence on external expertise

The interview in sections 4.4.3 and 4.5.4 highlighted that many medium-sized enterprises saw external expertise as essential to managing cybersecurity risks, particularly where internal skills and resources were lacking. Therefore, integration of external expertise emerged as a critical finding when managing cybersecurity risks for many of the medium-sized enterprises. These managers recognised the limitations of their in-house capabilities and often relied on external consultants to bridge these gaps. For example, some of the medium-sized enterprise managers reported hiring consultants following significant cyber incidents to assess vulnerabilities and develop mitigation strategies, which provided valuable support in understanding and addressing specific cybersecurity risks. Other managers emphasised the need for specialised skills that their internal teams lacked, and some collaborated with service providers for 24/7 monitoring and incident response that their small-scale operations could not handle independently.

This reliance on outsourcing is well-supported in academic literature. Mthiyane et al. (2022) recommend outsourcing as a cost-effective solution for SMEs, allowing the business to access essential skills without incurring the high costs of building a dedicated in-house team. Schlesinger (2018) further highlighted that outsourcing can rapidly enhance an SME's cybersecurity posture by leveraging specialised expertise, which is increasingly critical given the complexities of the digital environment.

However, reliance on external consultants presents certain challenges. Renaud (2016) warned that SMEs must carefully assess the relevance and applicability of guidance from external experts. Some of the medium-sized enterprise managers echoed this, noting that

while external advice was beneficial, it needed to align closely with their unique business needs, underscoring the importance of internal knowledge to effectively assess and apply third-party recommendations. Additionally, medium-sized enterprises expressed concerns about granting remote access to external entities, which could introduce vulnerabilities if not properly managed. This aligns with Alahmari and Duncan (2020), who caution that outsourcing can introduce new risks related to data sharing and remote access, particularly if these elements are not securely managed.

The need to balance internal capabilities with external support emerged as a recurring theme in this study. Schlesinger (2018) argued that while external consultants are essential for SMEs that lack cybersecurity expertise, maintaining core internal competencies is equally crucial for a well-rounded defence strategy. The importance of proactive risk assessment was also particularly important for those SMEs who had experienced a cyberattack. Rawindaran et al. (2021) reinforced that organisations tended to benefit significantly from the intervention of external consultants when such interventions were part of a broader, risk-based approach.

Despite the clear benefits of external expertise, medium-sized enterprises face challenges in selecting the right cybersecurity companies or support. Osborn and Simpson (2018) note that cybersecurity providers often prioritise larger enterprises, which can leave SMEs feeling underserved. Some medium-sized enterprises' managers expressed similar concerns, remarking that service providers sometimes failed to understand the specific needs of smaller-scale operations, potentially resulting in suboptimal cybersecurity strategies. This indicated the urgent need for cybersecurity providers to develop tailored services that address the distinct challenges of medium-sized enterprises rather than repurposing solutions designed for larger enterprises, to ensure effective and relevant cybersecurity support.

External support also plays a crucial role in regulatory compliance. Medium-sized enterprises often rely on consultants to navigate complex regulatory requirements, such as NIST standards. From a theoretical perspective, Aurelien (2021) and Rawindaran et al. (2021) contended that external consultants can help SMEs achieve compliance while ensuring that these regulations translate into practical security improvements. This assistance is particularly vital for medium-sized enterprises that may find regulatory demands too complex to manage independently.

Based on above, there was evidence that external expertise in cybersecurity was critical for the medium-sized enterprises. While outsourcing can effectively address knowledge and resource gaps, the solution requires careful evaluation to ensure that external guidance aligns with specific business needs. Medium-sized enterprises demonstrated the advantages of leveraging external consultants to enhance cybersecurity, comply with regulations, and develop structured CRMi strategies. However, challenges such as dependency on third parties, third-party risks, and the need for internal knowledge to evaluate and implement external advice should not be overlooked. A balanced approach is therefore needed which integrates external support with internal capability development. This is essential for building resilience against evolving cybersecurity threats.

5.3.6 Cyber security compliance and certification

Evidence from the interviews, particularly in sections 4.3.2 and 4.5.5, showed that perspectives on adopting formal cybersecurity certifications such as ISO 27001 and TISAX varied considerably, which was shaped by client requirements, perceived complexity, and prior incident experience.

Some of the medium-sized enterprises had pursued certifications primarily due to client requirements or prior cyber incidents, reflecting a more compliance-driven approach. For instance, medium-sized enterprises obtained TISAX certification to satisfy client demands, which also resulted in improved IT security measures. Other organisations had adopted both TISAX and ISO 27001 after experiencing ransomware attacks, illustrating how negative experiences often prompt proactive cybersecurity actions. This strategy aligns with Ashby et al. (2018), who found that client pressure is a significant driver of compliance efforts in SMEs, pushing them to adopt formal certifications.

While some of the medium-sized enterprises displayed more reluctance to pursue certifications unless directly required by clients, other managers expressed a willingness to comply only if prompted by client demand, questioning the necessity of certifications and emphasising the perceived robustness of their existing security processes. This hesitancy is consistent with findings by Mijnhardt et al. (2016), who observe that standards like ISO 27001 are often seen as overly complex for SMEs. They suggest simplified frameworks, such as the CHOISS model, as more practical alternatives for smaller businesses with limited resources. Rae and

Patel (2019) further support these concerns and highlight a growing gap between escalating cybersecurity threats and the low adoption rates of formal certifications among SMEs. For Rae and Patel (2019), the authors proposed alternative approaches, such as a cybersecurity rating scheme that assesses behaviours and risk levels, to make cybersecurity insights more accessible to SMEs without the high burden of formal certification. This aligns with the perspectives of those medium-sized enterprises favouring practical, cost-effective solutions over complex compliance models, seeing them as more attainable ways to address cybersecurity risks.

Client demands served as a significant motivator for some medium-sized enterprises to adopt certifications. However, as discussed earlier in sections 5.2.5 and 5.5.4, these pressures could also stem from broader supply chain or contractual requirements. In the context of certification, some of the medium-sized enterprises had pursued ISO 27001 specifically to meet client expectations, while other businesses prioritised cost-efficiency and minimal compliance measures unless certification became a necessity.

This perspective echoes the findings of Nelson and Madnick (2017a), who noted that many companies assess cybersecurity spending considering competing priorities, weighing the cost and benefits carefully before committing to formal certifications. In supporting this, Eilts (2020) and Alahmari and Duncan (2020) indicated that limited resources are a common obstacle for SMEs trying to improve cybersecurity readiness. These authors (e.g., Eilts, 2020; Alahmari & Duncan, 2020) suggest that SMEs may benefit more from accessible frameworks, such as the NIST Cybersecurity Framework, which provides practical guidance without necessitating formal certification. This approach resonates with medium-sized enterprises that favour flexible, informal security practices over rigid compliance structures, seeking more adaptable methods for maintaining cybersecurity while managing costs.

Ultimately, client pressure, past incidents, and resource constraints significantly influence the variation in certification adoption among SMEs. In supporting this, Eilts (2020) and Alahmari and Duncan (2020) support the notion that SMEs benefit more from simplified, accessible cybersecurity approaches rather than strict certifications, which can be costly and complex. Consistent with the findings from Chapter Four, many of the medium-sized enterprises in this study, the development of customised, flexible, and cost-effective cybersecurity strategies appeared to be the most practical path for building resilience against cyber threats.

5.3.7 Adoption of cyber-risk insurance and emergency preparedness

As presented in Chapter Four, sections 4.6.2 and 4.7.1, the interviews indicated that there was a mixed approach to adopting cyber-risk insurance (CRI) among medium-sized enterprises. For some firms, CRI became essential after a significant cyberattack. Labunets et al. (2020) support combining CRI with internal security measures, suggesting that a balanced approach to risk management is most effective. In contrast, in this study several of the medium-sized enterprises had been hesitant to adopt CRI. Those organisations that had experienced minor cyberattacks tended to prefer to strengthen internal security measures, including the usage of additional data backups and firewalls. Part of the reason for relying on internal solutions, such as emergency planning and internal procedures, was a perception of CRI as being reactive rather than proactive. This perspective of being reactive echoes findings by Nieuwesteeg and Waard (2018) and Kavčič and Delak (2019), who noted that high premiums and inconsistent coverage often deterred SMEs from adopting CRI. This was supported by Zeller and Scherer (2023) who argued that insurers frequently charged these businesses the full cost of risk mitigation services, such as self-protection, to policyholders, making policies financially unappealing for many medium-sized enterprises. Zeller and Scherer (2023) also highlighted that overly specific and expensive insurance options further made CRI unattractive for SMEs, underscoring the need for insurers to develop more accessible and cost-effective policies tailored to SME needs. This reluctance to adopt CRI is further compounded by financial considerations. To address this, several medium-sized enterprises suggested that funds might be better allocated to enhance cybersecurity infrastructure. Schlesinger (2018) noted similar reluctance among SMEs, due to underestimating financial risks and limited awareness of the scope and benefits of CRI, advocating a similar solution.

A significant challenge for medium-sized enterprises was a general lack of understanding regarding CRI coverage. The findings reflect observations by Labunets et al. (2020), who indicated that CRI without clarity on what the insurance specifically covered was a common issue and that SMEs frequently relied on brokers, sometimes resulting in underinsurance. Binkhorst (2020) suggested that clearer communication about CRI's benefits could help SMEs better understand its value as part of an integrated cybersecurity strategy. For Eilts

(2020) CRI alone was insufficient for comprehensive protection, and therefore recommended the NIST Framework, integrating CRI with proactive measures such as employee training, system updates, and thorough risk assessments was needed.

Complementing these considerations, several medium-sized enterprise managers highlighted contingency planning as crucial for maintaining operations during cyber incidents. This perspective aligned with Schlesinger (2018) and Consoli et al. (2020), who stressed the importance of preparedness and documented recovery processes in effective cybersecurity strategies.

Based on above, while CRI can offer essential financial protection for medium-sized enterprises, the adoption did often vary based on cost, perceived value, and understanding of coverage. Consistent with the evidence from Chapter Four, many of the medium-sized enterprises integrated CRI effectively, and while there was some residual hesitancy, the focus was on strengthening internal security measures and contingency planning. This bridging of the gap would require enhanced education on CRI, simplified policies, and promoting CRI as part of a broader, proactive cybersecurity strategy. These observations underline the importance of aligning insurance choices with broader security investments to ensure both financial stability and operational resilience. This theme will be expanded in section 5.4.4, to provide further analysis on how these approaches can be combined to create a balanced risk management strategy.

5.3.8 Summary of the approaches and perspectives associated with cyber-risk mitigation and cyber-risk insurance

This study found that the experiences and perception of these medium-sized enterprise managers related to CRMi strategies were that while limited resources, employee awareness, and supply chain risks were significant considerations, there were some limitations between existing theoretical frameworks and actual practices. The medium-sized enterprises in this study tended to adopt a reactive approach, which focused on internal measures and addressed the risks only after incidents occurred. Existing academic debate, including Consoli et al. (2020) and Eilts (2020), emphasise the need for more proactive strategies, such as formal risk assessment models, cyber-risk insurance, and outsourcing cybersecurity functions. Moreover, both authors advocate that SMEs should implement formalised CRMi strategies,

invest in employee training, and consider the benefits of CRI as part of a comprehensive risk management approach to improve cybersecurity. Although these medium-sized enterprises indicated an increasing awareness of the need for robust CRMi, they still faced certain challenges in implementing comprehensive quantitative risk assessment tools and providing consistent training.

5.4 The relationship between specific risks and cyber-risk mitigation strategies

Cybersecurity risks pose a potential but significant threat to medium-sized enterprises, which requires robust risk mitigation strategies to be adopted and implemented. The interviews in this study revealed that the medium-sized enterprise managers' approaches to addressing phishing, ransomware, and other cyber threats were influenced and informed by internal and external factors.

5.4.1 Proactive vs. reactive cyber-risk mitigation strategies

As reflected in Chapter Four, sections 4.3.1 and 4.5.1, the interviews revealed that some medium-sized enterprise managers continued to rely on reactive strategies even after experiencing past cyber incidents or addressing regulatory compliance, other businesses, which mainly had not experienced a cyberattack, were only just beginning to consider adopting a proactive cybersecurity approach. This included one medium-sized enterprise that had adopted international standards like ISO 27001 and TISAX, driven by regulatory compliance and the past experience of suffering from a cyberattack. This finding was aligned with the findings of Stahl et al. (2003), who indicated that SMEs often adopted cybersecurity measures reactively, typically following a cyber incident. However, this reactive behaviour can leave the SME vulnerable to potential threats, which underscores the need for a more comprehensive risk management strategy in small and medium sized businesses. For those medium-sized enterprises who had taken a proactive cybersecurity stance by investing in preventive measures, the focus was on avoidance of potential costly operational disruptions. This investment reflected an understanding that the costs associated with a cyberattack could far exceed the expense of prevention. This perspective is aligned with Kazemargi and Spagnoletti (2020), who argued that cybersecurity should be integrated with overall business strategy, especially in those sectors like manufacturing and retail, as they have begun to be increasingly more digitalised.

By embedding cybersecurity into broader operations, Armenia et al. (2021) highlight that this can improve the decision-making process by providing a holistic overview of risk and its mitigation. Supporting this, Ashby et al. (2018) emphasise that integrating strategy with risk management can enable SMEs to address threats proactively, reducing disruptions and aligning mitigation with their long-term goals. This comprehensive integration can ensure that cybersecurity efforts strengthen overall business performance while fostering resilience and competitiveness.

However, many of the interviewed medium-sized enterprise managers continued to rely heavily on reactive strategies, including qualitative assessments, rather than adopting quantitative risk management tools. This reliance on qualitative assessments limited their ability to fully develop preventive strategies.

Freund and Jones (2014) highlighted the potential benefits of adopting quantitative frameworks like the Factor Analysis of Information Risk (FAIR), which can support informed decision-making regarding cybersecurity investments. Arguably, by helping SMEs identify critical risks and allocating resources more effectively, such frameworks can reduce reliance on external consultants and encourage the development of internal capabilities. In summary, these findings indicate that some medium-sized enterprises had to resort to hiring external consultants following cyber incidents, underscoring their preference for external assistance over internal capability development.

Nelson and Madnick (2017a) proposed that SMEs should integrate cybersecurity into their innovation processes. Viewing cybersecurity not merely as a cost but as a strategic asset would enable SMEs to protect valuable assets while fostering growth and maintaining a competitive edge. However, the interviews revealed a continuing divide between medium size businesses adopting a strategic view and those relying mainly on reactive responses.

In summary, and consistent with the earlier findings in Chapter Four, the interviews indicated differences of opinion and practices between adopting a proactive and reactive cybersecurity approach. Those proactive medium-sized enterprises were often driven by regulatory compliance or past cyber incidents, whereby strategies and measures like firewalls, intrusion detection systems, and international standards such as ISO 27001 had been adopted, indicating an understanding that prevention costs less than cyberattacks. These businesses

had aligned their cybersecurity with the overall medium-sized enterprise's strategy, enhancing decision-making, fostering resilience, and maintaining competitiveness (Armenia et al., 2021; Ashby et al., 2018; Kazemargi & Spagnoletti, 2020).

5.4.2 Identified potential cyber-risks and perceived vulnerabilities

As discussed in Chapter Four, medium-sized enterprises' risk perceptions were often shaped by a combination of operational realities and underlying misconceptions. This section builds on those findings detailed in the previous chapter, by detailing how specific vulnerabilities, ranging from geopolitical threats to internal technical weaknesses and human error, translate into distinct risk profiles. The outcomes show how these risks influence the balance between reactive and proactive cyber-risk mitigation approaches.

From the interviews with the medium-sized enterprise managers, there was an indication that this type of business may encounter cyber threats due to external factors, their internal vulnerabilities, and employee behaviours, all of which substantially affected their cybersecurity strategy.

Some of the interviewees expressed a heightened awareness about cyberattacks being influenced by the current global political climate, especially threats from state-sponsored actors. The interviewees pointed out that the extent of these risks was often under-represented in the media, which led several medium-sized enterprise managers to indicate an increased lack of awareness in the sector as to the potential threat. This was particularly relevant in sectors like manufacturing, where the shift toward automation and the emergence of complex global supply chains has introduced new security challenges. Strupczewski (2021) highlights how political tensions and state-sponsored threats had led to an increased level of risks, particularly to SMEs, which while part of the global supply chain is not fully prepared to manage and minimise the risk of a cyberattack.

To mitigate these external risks, several managers recommended adopting the "Zero Trust" model (which is aligned to Tam et al., 2021), as presented in section 5.3.3. This theme of internal vulnerabilities within medium-sized enterprise infrastructure emerged as another recurring concern for these managers. Some of the medium-sized enterprise managers described using sensors to monitor network activity, which helped identify weaknesses like open network ports. However, despite efforts to close these gaps, the reliance on qualitative

risk assessments left them susceptible to human error, underscoring the need for more data-driven, quantitative tools to manage internal risks.

A related concern was the growing risk associated with remote work, particularly during the pandemic, when employees frequently accessed systems from unsecured personal devices. To mitigate these risks, some medium-sized enterprises implemented restrictions on USB devices and unauthorised technologies, attempting to safeguard critical systems against potential breaches. Dayalan (2017) and Grocke (2017) support these observations, depicting SMEs as being “soft targets” due to their limited defences. Both Dayalan (2017) and Grocke (2017) have independently highlighted phishing and ransomware attacks as common threats faced by SMEs, which often lack advanced security systems, especially in terms of Bring your own device (BYOD) working. Supporting this, Rawindaran et al. (2021) further emphasise that SMEs that have now often increased reliance on remote access have amplified their vulnerability to phishing and similar cyber threats, particularly in the context of decentralised work environments.

Human factors and employee behaviour were identified as being critical areas of vulnerability in these medium-sized enterprises. The interviewees highlighted that employees were susceptible to phishing, which led them to continuously monitor remote network access. As discussed in section 5.3.1, improving training and awareness is essential to reduce risks linked to human error. This section’s findings reinforced the need for managers linking phishing susceptibility and inconsistent monitoring to a need for sustained awareness programmes. Kapoor et al. (2018) also note that SMEs often lack the capacity for consistent monitoring and effective response, underscoring the importance of embedding employee awareness into overall CRMi strategies.

In the area of operational risks, the interviews revealed that ransomware was seen as being a significant concern for The interviewees highlighted that employees were susceptible to phishing, which led them to continuously monitor remote network access. s. Some of the interviewees identified how encryption-based attacks could potentially corrupt network data, paralyse business functions, and severely impact productivity and revenue. This was contextualised by some of the medium-sized enterprise managers noting that a single day of downtime might be manageable, but also recognising that the theft of critical data could lead to long-term reputational damage. One medium-sized enterprise manager recalled the severe

disruption caused by a ransomware attack, which underscored the need for systematic monitoring and vulnerability scanning as part of daily cybersecurity activities. Despite this, several medium-sized enterprises still held the belief that their small size made them unlikely targets, a perception that influenced their decisions on investment and the importance of cybersecurity. Kapoor et al. (2018) supported this observation, noting that SMEs often failed to fully recognise the likelihood or potential impact of cyberattacks, which resulted in a preference for short-term planning over long-term strategic measures. One medium-sized enterprise exemplified this mindset by planning for only a two-day disruption due to a cyberattack, focusing solely on potential sales losses in their customer relationship management system. McLilly (2020) similarly observed that such limited understanding of potential threats created significant gaps in SMEs' preparedness.

To summarise the above, the interviews with the medium-sized enterprise managers revealed that cybersecurity challenges stemmed from external threats, internal vulnerabilities, and employee behaviours, influencing their reactive strategies. Part of the threats could be attributed to potential State-sponsored cyber activities, amplified by global political tensions, which were seen as being under-represented in the media. These unreported threats left these medium-sized enterprises inadequately informed or aware of the risks, particularly in sectors like manufacturing. As to internal weaknesses and vulnerabilities, there was an over-reliance on qualitative assessments and employee being susceptibility to phishing, further highlighted the need for comprehensive training and data-driven tools. This section has also indicated that operational risks, such as ransomware, were significant threats, which could lead to disruptions that threatened productivity and reputation. The interviews revealed that many medium-sized enterprises underestimated their risk exposure, therefore tended to favour short-term strategies over being proactive, adopting long-term strategies. However, to build resilience, medium-sized enterprises may need to adopt advanced models like "zero trust" ethos, improve the existing monitoring systems, and provide robust training programmes, thereby moving from reactive to proactive approaches to meet further cyberattacks.

5.4.3 Qualitative versus quantitative risk assessment

Building on the risk perception patterns discussed in Chapter Four and in section 5.4.2, there is evidence that medium-sized enterprises' choice of risk assessment methodology significantly shaped their cybersecurity posture. This section explores the tension between qualitative and quantitative approaches, showing how the continued reliance on subjective assessments can limit the ability to identify, prioritise, and respond to cyber risks effectively.

As noted above in the previous section, the interviews with the medium-sized enterprise managers revealed a reliance on qualitative risk assessment methods, with minimal usage of quantitative approaches in evaluating potential cyber threats. The interviewees emphasised their use of qualitative methods to categorise cyber-risks, based on the perception that this form of assessment enables the categorisation into a three-part scale: high, medium, or low, based on the perceived severity of a cyberattack. This reliance on qualitative evaluation highlighted a significant vulnerability, as the method placed cybersecurity decision-making on the subjective judgement of the manager rather than on a structured data analysis. While qualitative assessments can provide a general view of risk, the method lacks the precision necessary for effective resource allocation and long-term planning. This dependence on subjective judgement contradicts the original studies of Ishikawa (2017), Schmitz and Pape (2020) and Armenia et al. (2021), who reported that SMEs needed to take a more balanced, data-informed approach to risk management.

The debate between qualitative and quantitative risk assessment centered on the trade-off between cost, resource availability, and whether a medium-sized enterprise sought simplicity or precision in analysis. The qualitative method provided an easily implementable solution, while the quantitative approach offered data-driven insights that enabled more informed decision-making but required a greater amount of data. Armenia et al. (2021) highlighted the limitations of qualitative approaches in assessing cyber-risks, despite their ease of use and interpretation, and introduced the SME Cyber-Risk Assessment (SMECRA) tool as a solution. Meanwhile, Armenia et al. (2021) proposed that a quantitative model could help SMEs better evaluate risks and understand the financial implications of cyber incidents. By integrating qualitative methodologies with quantitative metrics, SMECRA offered a structured framework for effective resource allocation. Ishikawa (2017) supported this duality, by advocating Monte Carlo simulations to quantify potential losses, enabling SMEs to identify

risk areas and make well-informed mitigation decisions. These two approaches presented by Armenia et al. (2021) and Ishikawa (2017) challenge the widespread reliance on qualitative methods in SMEs to address the potential gap in their cybersecurity.

As previously mentioned, several of the medium-sized enterprises in this study continued to rely on basic qualitative tools, such as colour-coded matrices, to indicate perceived severity levels of cyber-risks. While these qualitative techniques provided some level of visual clarity, the methodology does not provide the detailed account of the potential financial implications or any guidance as to strategic resource allocation. Schmitz and Pape (2020) noted that SMEs would benefit from simplified quantitative tools tailored to their specific resource limitations. In explaining this, Schmitz and Pape (2020) advocate the incorporation of numerical data and expert input, observing such tools could help bridge the gap between qualitative assessments and the practical, data-driven decisions essential for robust cybersecurity.

Overconfidence in employee capabilities, as discussed in section 5.4.2, may also reduce the effectiveness of purely qualitative assessments by fostering a false sense of security and underestimating the potential for human error. This outcome underscores the importance of supplementing qualitative assessments with objective and measurable data.

Interestingly, the interviews also revealed that some of the medium-sized enterprise managers had focused on minimising immediate impacts, such as short-term sales losses, rather than adopting a comprehensive, data-driven approach to assess the broader and long-term financial consequences of cyber incidents. This short-term strategy tends to be aligned with a reactive approach, which was criticised by McLilly (2020), who noted that SMEs often rely on qualitative assessments that fail to capture the full scope of potential risks. To address this, Strupczewski (2021) and Al-Dosari and Fetais (2023), advocate for integrating quantitative tools to move beyond simplistic, immediate categorisations of risk. Such quantitative tools can provide SMEs with the means to evaluate risks more comprehensively, enabling a deeper understanding of the financial and operational impacts of cyber incidents.

While some medium-sized enterprise managers adopted a mixed approach to risk assessment by combining qualitative and quantitative methodologies, this approach was often driven by external pressures from supply chain partners requiring it as a prerequisite. Some managers noted that, while they had not yet adopted formal certifications or CRI, external demands were shaping their risk assessment practices, prompting them to combine internal

evaluations with measurable compliance standards when necessary. Others, however, focused solely on maintaining robust internal processes, questioning the value of integrating formal certifications or externally driven metrics unless explicitly required. Malhotra (2015), Ishikawa (2017), and Armenia et al. (2021) independently highlighted the benefits of combining methods, as seen in models like SMECRA, which integrate qualitative insights with quantitative metrics.

When consistently applied, this mixed approach can offer a more comprehensive understanding of risks, allowing medium-sized enterprises to transition from surface-level evaluations to data-driven, informed decision-making. However, as McLilly (2020) highlighted, recent trends have increasingly shifted toward a stronger emphasis on quantitative methods, reflecting the growing demand for precise, measurable risk management strategies.

Based on the above, the findings indicate that most of the medium-sized enterprises heavily relied on qualitative assessments for cyber-risk evaluation, which limited their ability to fully understand and address cyber threats. In contrast literature, including Ishikawa (2017) and Armenia et al. (2021), advocates for integrating quantitative methods, such as Monte Carlo simulations and tailored risk assessment tools like SMECRA, to enhance the precision and depth of risk evaluations. Adopting a strategy that combines qualitative and quantitative assessments would enable SMEs to allocate resources more strategically, improve cybersecurity resilience, and transition from a reactive to a proactive approach in risk management. This shift aligns with broader recommendations for medium-sized enterprises to adopt a more structured, data-driven approach that moves beyond basic assessments and addresses the complexities of modern cyber threats effectively.

5.4.4 The cost-benefit analysis of cybersecurity investments

Extending the discussion from section 5.4.3 on how assessment methods influence strategic choices, the interview findings outlined in Chapter Four also revealed that medium-sized enterprises approached cybersecurity decision-making through a cost-benefit lens. The balance between financial investment, perceived value, and the choice of technical versus insurance-based solutions shaped how each business structured its overall cyber-risk mitigation strategy.

The medium-sized enterprises in this study demonstrated diverse approaches to cybersecurity investments, reflecting the need to balance preventive measures with financial methodologies like cyber-risk insurance (CRI). While CRI was often viewed as an integral component of a comprehensive risk management strategy, particularly when aligned with industry standards and additional insurance services, many medium-sized enterprises prioritised tangible investments such as firewalls, encryption, and employee training. This preference reflects a traditional risk management approach, as noted by Franke and Meland (2019), where immediate, visible solutions were favoured due to perceived reliability and cost-effectiveness. Cost concerns had also led to some of the medium-sized enterprises to explore alternative solutions like cloud-based Security as a Service (SECaaS), which can offer scalable protection tailored to the firms' budgets. However, there were still concerns about data sovereignty and control over sensitive information presented challenges, as highlighted by Pfister and Lehmann (2023) and McLilly (2020).

Several medium-sized enterprises indicated that their reluctance to adopt CRI was seen as a trade-off because they chose to allocate resources to internal security infrastructure while maintaining contingency plans to address potential disruptions. This preference was driven by the perception that CRI premiums were disproportionately high compared to its coverage. These medium-sized enterprise managers expressed a scepticism about insurers' willingness to pay claims, further deterring adoption. These findings align with Nieuwesteeg and Waard (2018) and Schlesinger (2018), who contend that SMEs often hesitate to invest in CRI due to high premiums and limited understanding of policy specifics. This lack of clarity regarding CRI policies, as noted by Labunets et al. (2020), underscores the need for greater transparency and education to ensure SMEs can make informed decisions.

However, those medium-sized enterprises who had experienced significant cyberattacks highlighted the benefits of CRI in providing financial stability and proactive services, such as regular security updates offered by insurers. One medium-sized enterprise's approach, which combined internal security measures, external expertise, and CRI, served as a model for integrating diverse cybersecurity components. This balanced approach reflects recommendations by Vieira et al. (2020), who argued that integrating financial safeguards with robust security measures enhances resilience against cyber threats. Furthermore, this synergy

between CRI and preventive measures demonstrates the value of a holistic cybersecurity strategy, capable of addressing both immediate risks and long-term resilience.

Based on the above, the cost-benefit analysis remains a critical factor in medium-sized enterprise cybersecurity decision-making. While many medium-sized enterprise businesses prioritised tangible preventive measures, CRI can provide essential financial protection when integrated with broader risk management strategies. Alternatives such as SECaaS can offer a solution for medium-sized enterprises to enhance cybersecurity while managing costs, but to achieve this requires the insurance sector to address the perceived concerns around data sovereignty. However, by adopting a balanced strategy that combines preventive investments with CRI, medium-sized enterprises can mitigate financial and operational risks, achieving both immediate protection and long-term resilience in an increasingly interconnected digital landscape.

5.4.5 Summary as to relationships between specific risks and cyber-risk mitigation strategies

Some medium-sized enterprises adopted proactive strategies to mitigate cyber-risks, but many still relied on reactive strategies driven by regulatory requirements or past incidents. Academic literature from Nelson and Madnick (2017a) and Kazemargi and Spagnoletti (2020) suggested that aligning cybersecurity with business strategies and implementing proactive measures, such as regular risk assessments, preventive technologies, and employee training, could significantly enhance medium-sized enterprises' resilience. A shift from a cost-centric perspective to a strategic view of cybersecurity was proposed to help SMEs to mitigate risk more effectively and capitalise on digital opportunities more securely. However, many of the medium-sized enterprises in this study continued to depend on qualitative assessments and basic internal measures, limiting their ability to fully understand and mitigate cyber threats. To improve resilience, these medium-sized enterprises were encouraged to enhance awareness, adopt comprehensive cybersecurity frameworks, and incorporate more quantitative risk assessments.

Ishikawa (2017) and Armenia et al. (2021) both emphasised the value of integrating quantitative methods, such as Monte Carlo simulations, or respective tailored risk assessment tools like SMECRA, to increase the accuracy of risk evaluations. A combination of both qualitative

and quantitative methods could enable SMEs to allocate resources more effectively, improve their cybersecurity resilience, and transition from a reactive to a proactive risk management approach.

The attitude towards cybersecurity investments amongst the medium-sized enterprise managers was complex, driven by concerns over cost, perceived value, and the efficacy of cyber-risk insurance (CRI). Some of the medium-sized enterprise managers remained sceptical, citing high premiums and perceived inadequate coverage, while other interviewees recognised CRI's value as part of a broader cybersecurity strategy. The literature, such as Ishikawa (2017), Schmitz and Pape (2020), Vieira et al. (2020), and Armenia et al. (2021), encourages SMEs to adopt a balanced approach, integrating CRI with direct preventive actions to ensure both immediate defence and financial resilience.

5.5 Medium-sized enterprise managers' perception of cyber-risk insurance and its role as a potential solution within cyber-risk mitigation strategies

The reported incidents of cyberattacks and the reliance on digital infrastructure highlighted the need for effective cyber-risk mitigation (CRMi) amongst German manufacturing medium-sized enterprises. Cyber-risk insurance (CRI) is a potential option for mitigating or insuring against a cyberattack, by offering financial protection and support services. However, the perception of CRI among medium-sized enterprise managers did vary, often influenced by concerns over cost, value, and its integration into existing practices.

5.5.1 Challenges in understanding cyber-risk insurance coverage

Building on the discussion in section 5.4.4 about cost–benefit considerations in cybersecurity investments, the interviews also highlighted that decision-making around cyber-risk insurance (CRI) was shaped as much by understanding and perception as by financial evaluation. As discussed in sections 4.4.2 and 4.4.3, these challenges were also evident in the interviews, where the managers expressed uncertainty. These uncertainties included the extent of their policy coverage, diverging views on CRI's value, and a tendency to prioritise tangible security investments or contingency planning over insurance. Several managers noted that they preferred direct control through internal measures, while others acknowledged the reassurance and stability that CRI could offer, particularly after experiencing an incident.

The challenge for medium-sized enterprise managers was not only to understand and adopt the correct CRIs, but also to navigate widely differing perceptions of their value, with some seeing CRI as essential, while other interviewees remained sceptical due to high premiums and coverage limitations. This outcome included clarity as to the scope of the insurance coverage, with many managers uncertain about what was actually covered under their policies. Beyond understanding the terms, there were also varied perspectives and reasons for adopting CRI, reflecting distinct levels of risk tolerance and resource availability among medium-sized enterprises. While some managers saw CRI as essential for financial protection, other participants remained sceptical due to high premiums and perceived limitations in coverage. This finding supported Nieuwesteeg and Waard (2018), who observed that many medium-sized enterprises were deterred by the cost of CRI and potential loopholes or gaps insurers might use to limit coverage. In contrast, some medium-sized enterprises managers viewed CRI more favourably, likening it to traditional forms of insurance, such as fire insurance, which offered both psychological reassurance and financial protection. This positive view aligns with Schlesinger (2018), who argued that CRI provides significant reassurance and essential risk mitigation for medium-sized enterprises.

Some of the medium-sized enterprise managers were unclear about the specifics of the policy, even though they might have had CRI coverage for years. Some interviewees assumed that their policy covered IT forensics, data recovery, and business interruption but lacked certainty on the restrictions or limitations. Other managers questioned whether their property insurance extended to major cyber incidents like data loss. This lack of clarity presented a significant risk, as these medium-sized enterprises could find themselves under-protected during a cyberattack, indicating the need for greater transparency and education as to policy terms. This theme was studied by Labunets et al. (2020), Nieuwesteeg and Waard (2018) and Schlesinger (2018), who indicated that many SMEs were dependent on insurance brokers without fully understanding the policy details, which could lead to gaps in the coverage. For Labunets et al. (2020), SMEs often entered insurance agreements without a thorough understanding of what was covered. To address this, Nieuwesteeg and Waard (2018) and Schlesinger (2018) recommend that SMEs work closely with insurers to ensure they fully understand their coverage, especially regarding threats like ransomware and operational downtime.

There was a scepticism as to insurers' willingness to pay claims, which presented another challenge to the medium-sized enterprises. One of the medium-sized enterprise managers expressed their concerns about potential loopholes insurers might exploit to reject claims, which was compounded by the high premiums associated with CRI. As a result, some medium-sized enterprises chose to prioritise investment in security technology over CRI. This preference for tangible measures reflected a belief that direct security investments offered more control and immediate benefits, particularly given the complexity of insurance products.

In contrast, there were some medium-sized enterprises who were advocates of CRI, particularly after experiencing a cyberattack. For these firms there was an emphasis on the importance of gaining immediate assistance and coverage for the business interruption. Some managers even compared CRI to traditional forms of insurance, such as fire coverage, framing it as an essential safeguard for maintaining business stability. The proactive services offered by some insurers, such as regular security assessments and IT forensics, were also seen as beneficial for identifying and mitigating threats before they escalated.

A recurring theme among many of the interviewees was a preference for direct investments in cybersecurity infrastructure over CRI. In this context, McLilly (2020) suggested a cost-effective alternative, such as adopting cloud-based Security as a Service (SECaaS). The findings indicate one medium-sized enterprise allocated funds to security technology instead of insurance premiums, believing this provided better long-term value. For other medium-sized enterprises there was a prioritisation of seeking contingency planning over CRI. This included the usage of robust backup systems and a preference for traditional business interruption insurance for more conventional risks, like fire.

In summary, while CRI could be a valuable inclusion for a medium-sized enterprise by provide a comprehensive cybersecurity strategy by offering financial protection and facilitating business continuity, the medium-sized enterprises in this study in the main remained hesitant to seek CRI, due to the high premiums, uncertainty as to the insurance coverage, and a scepticism towards the likelihood of a payout. To address this, Nieuwesteeg and Waard (2018), Schlesinger (2018) and Labunets et al. (2020) independently suggest that improved transparency, clearer communication regarding CRI coverage, and the integration of the CRI

with broader cybersecurity strategies could assist medium-sized enterprises to navigate these challenges and enhance resilience.

5.5.2 Cyber-risk insurance as part of a broader cybersecurity strategy

Building upon the previous discussions of medium-sized enterprises' reluctance toward CRI adoption due to cost concerns, scepticism about insurers, this section shifts the focus to the strategic value of CRI. Rather than framing CRI as a standalone or reactive measure, this section explores its potential as a complementary element in comprehensive cybersecurity strategies.

As discussed in section 4.4.4, the interview findings revealed that some medium-sized enterprises had begun to view CRI as part of a multi-layered risk management approach, while others continued to treat it as an optional add-on or even an unnecessary expense. This divergence was often shaped by differences in incident history, risk tolerance, and the maturity of existing security measures.

A key theme emerging from the study was the importance of integrating CRI into a broader cybersecurity framework. medium-sized enterprise managers expressed diverse opinions on this integration, with some emphasising the sufficiency of existing preventive measures, such as employee training and adherence to industry standards, while others highlighted the limitations of such measures in addressing financial risks. For medium-sized enterprises that adopted CRI, the reported benefits extended beyond financial protection. Managers highlighted services provided by insurers, such as proactive security assessments and system updates, which strengthened their overall security posture and helped mitigate future threats. This perspective aligns with Franke and Meland (2019) and Rejda and McNamara (2017), who advocate for CRI as a critical layer in multi-dimensional risk management.

Additionally, the findings revealed a gap in understanding among medium-sized enterprises regarding the role of CRI within their cybersecurity strategies. Many managers admitted to being unaware of the full scope of their policies, underscoring the need for clearer communication and education. This echoes Labunets et al. (2020), who stress the importance of transparency from insurers in articulating policy terms and benefits.

Interestingly, the study highlighted a preference among some medium-sized enterprises to focus their resources on internal security measures, such as hardware upgrades and other

preventive practices, as these were perceived to deliver immediate, measurable benefits. However, this approach often underestimated the role of CRI in enhancing overall resilience. When integrated with preventive strategies, CRI addresses risks that internal measures alone may not fully mitigate, providing a more comprehensive approach to managing cybersecurity threats.

In conclusion, the integration of CRI as a supportive layer within cybersecurity frameworks offers medium-sized enterprises a pathway to strengthen both financial and operational resilience. Closing knowledge gaps through improved communication and positioning CRI as a complement, rather than a competitor, to preventive measures can help medium-sized enterprises appreciate its strategic value. By doing so, CRI adoption can be reframed as a proactive and essential element of a holistic cybersecurity approach.

5.5.3 Summary of medium-sized enterprise managers' perceptions of cyber-risk insurance and its role in cyber-risk mitigation strategies

The examination of cyber-risk insurance (CRI) in the context of CRMi, informed by interviews with medium-sized enterprise managers from the German manufacturing sector together with the current academic debate, indicated that although several businesses recognised the importance of CRI, these entities exhibited reluctance to implement it until a substantial cyber incident had occurred. This reactive strategy differed from proactive initiatives that prioritised the incorporation of CRI into a comprehensive cybersecurity framework. The theme of cost-benefit analysis emerged from the interviews, which had significantly influenced medium-sized enterprise' decisions, leading to many of the managers preferring internal security measures over seeking CRI. However, the potential financial and operational consequences of cyberattacks underscored the critical need for CRI as a means of managing these risks.

For some medium-sized enterprises, the decision to adopt CRI was also influenced by external requirements, particularly from large clients and supply chain partners who increasingly demanded proof of coverage and formal cybersecurity certifications as part of contractual agreements. These external pressures can encourage medium-sized enterprises to align their cybersecurity policies with recognised standards, making CRI not only a risk management tool but also a means of maintaining critical business relationships.

As supply chains have become increasingly interconnected, cyber threats are becoming more prevalent. This has prompted large organisations to require their clients and suppliers to adopt CRI and obtain formal certifications. In response, medium-sized enterprises have begun to proactively embrace CRI and align their cybersecurity policies with international standards. This trend highlights the growing recognition of CRI as a critical component of robust cybersecurity strategies, supported by its alignment with standardised practices and its role in mitigating cyber-risks within interconnected networks.

5.6 Medium-sized enterprises' preparedness against cybercrime risk and the managers' attitudes to cyber-risk mitigation measures and business success

In the current digital age, medium-sized enterprises are facing the dual challenge of protecting their operations against cyber-risks while maintaining productivity and financial commitments. As businesses have become increasingly reliant on their IT infrastructure and automated processes, there has also been an increase in vulnerability to cyberattacks. This section examines the preparedness of cyber-risk mitigation (CRMi) in addressing the risk that a medium-sized enterprise may fail to achieve its business objectives. It also explores how such enterprises can manage cyber-risks while sustaining business performance, with particular attention to IT dependency, external pressures, and the role of CRMi in business success.

5.6.1 Dependence on IT infrastructure and production automation

As highlighted in section 4.6.1, the interviews with the German medium-sized enterprise managers underscored the strong reliance on IT infrastructure and automation. The findings in Chapter Four revealed the challenges associated with the operational benefits of technological but also the vulnerabilities of a cyberattack. The medium-sized enterprise managers indicated that there were varied approaches which had been adopted, demonstrating a lack of a consensus amongst these organisations in the manufacturing sector.

One approach to emerge from the interviews was the incorporation of redundancy within their IT infrastructure as a contingency strategy. Several medium-sized enterprises had hot-standby systems across multiple production sites to ensure business continuity in case of server failures or cyberattacks. This strategy of redundancy aligns with the findings of Pfister

and Lehmann (2023), who emphasised the importance of resilient infrastructure in safeguarding operations against technological disruptions or a cyberattack outage. By establishing redundant production infrastructure, these medium-sized enterprises were focused on reducing downtime and maintaining continuity, reflecting an understanding of operational risks tied to increasing IT dependency. Other medium-sized enterprises had decided to use different monitoring tools like network sensors to identify potential vulnerabilities within their systems. Although the network sensors offered a comprehensive overview of network activity, these medium-sized enterprises often lacked a formal CRM strategy, instead relying on a broader security strategy, but not necessarily cyberattack focused which left potential risks unaddressed.

The increased use of automation in external processes, such as electronic data interchange (EDI) and e-invoicing, emerged as another potential target for a cyberattack, which were identified in the interviews. The interviewees indicated there was awareness of cyberattack vulnerabilities which had emerged due to the reliance on automated connections. This awareness and potential threat are supported by Kazemargi and Spagnoletti (2020), who argue that while digitalisation improves efficiency, this technology has led to SMEs becoming increasingly exposed to external threats.

The integration of automation into maintenance and production processes has also introduced complexities to the cybersecurity landscape. Some of the medium-sized enterprise managers had adopted remote troubleshooting for production networks, which enabled efficient operational management but introduced new security challenges. Where these solutions involved cloud connectivity or raised data sovereignty considerations are presented in section 5.3.4.

A consistent theme to emerge from the study was the medium-sized enterprises' awareness of the vulnerabilities that had arisen from both the technological infrastructure and human factors. This outcome highlights that securing infrastructure must be accompanied by addressing human-related vulnerabilities, illustrating the dual challenge medium-sized enterprises face in protecting both systems and employee practices in an increasingly decentralised work environment.

In summary, automation and digital connectivity have enhanced operational efficiency for medium-sized enterprises but have also introduced significant cyber-risks, requiring comprehensive management. The interviews revealed a wide range of strategies for mitigating these risks, from redundancy in infrastructure to network monitoring, yet pointed to a general need for more structured CRM strategies that fully incorporate cybersecurity measures. The discussion above supports the notion that aligning IT with broader business strategies, combined with a proactive and holistic approach to cyber-risk management, is crucial for medium-sized enterprises. Such alignment would allow these organisations to enhance resilience within an increasingly automated and interconnected digital landscape, reducing vulnerabilities while maximising the benefits of technological integration.

5.6.2 External pressures driving cyber-risk mitigation strategies

As discussed in section 4.6.2 of Chapter Four, supplier and client requirements emerged in the earlier analysis as one of the most consistent external forces shaping medium-sized enterprises' cybersecurity strategies. These pressures were especially significant in industries handling sensitive data and requiring high operational security standards. Chapter Four findings showed that manufacturing sector medium-sized enterprises were particularly exposed to such pressures, with supplier audits and contractual demands acting as de facto cybersecurity benchmarks.

Unlike internal drivers, supplier requirements often compelled the medium-sized enterprises to revise internal processes to meet contractual obligations, particularly concerning data protection and cybersecurity accountability. This dynamic is particularly evident in sectors like manufacturing, where client selection increasingly depends on demonstrable security practices. Larger business partners often demand rigorous security standards, compelling medium-sized enterprises to implement formal CRMi measures to maintain accountability and secure their positions within critical supply chains. This requirement was confirmed by Renaud (2016), who found that larger companies may exclude SMEs that have experienced cyberattacks from their supplier networks.

For SMEs, cybersecurity accountability is not just about compliance; it is crucial for building trust and sustaining business relationships. Despite this, several medium-sized enterprises

admitted they currently did not follow specific cybersecurity standards, as no such requirements were in place. However, they acknowledged the need to explore appropriate standards for their business in the future. This aligns with Quesada (2016), who argue that regulatory demands and compliance pressures are primary drivers of cybersecurity initiatives in SMEs, along with Renaud and Weir (2016), who emphasise the risk of exclusion from supply chains for SMEs failing to meet cybersecurity expectations. However, navigating these external demands introduces complexities, particularly when accountability requires transparency.

Several medium-sized enterprises expressed concerns about disclosing sensitive information during security audits, highlighting the risks of exposing proprietary information, such as data locations or security protocols, to external parties. This tension reflects findings by Labunets et al. (2020), who observed that SMEs often face challenges balancing transparency with the protection of sensitive data, especially when vulnerabilities must be disclosed as part of accountability measures. In competitive industries, such transparency may inadvertently compromise intellectual property or operational integrity, forcing SMEs to carefully navigate the trade-off between accountability and safeguarding their proprietary assets.

The evolving nature of supplier-driven pressures has highlighted the importance of strategic, proactive adaptation to cybersecurity requirements. Unlike reactive approaches that follow direct cyber incidents, there were external pressures that demanded sustained investment in CRMi, with accountability being central to the business partnership.

Chapter Four documented medium-sized enterprises' cautious stance toward supplier-mandated transparency; this study suggests that proactive CRMi integration can reframe these pressures as strategic opportunities rather than compliance burdens**.** Such a proactive stance, as Schlesinger (2018) notes, strengthens resilience and trust within supply chains.

To summarise the above, supplier-driven pressures can uniquely shape the cybersecurity strategies of medium-sized enterprises by emphasising accountability and transparency as essential components of maintaining business relationships. These demands can introduce not only compliance obligations but also challenges in balancing transparency with the protection of sensitive data. The findings of this study highlight the importance of medium-sized enterprises aligning their CRMi practices with supply chain accountability to ensure long-term viability in increasingly cybersecurity-conscious industries.

5.6.3 The role of cyber-risk mitigation in business success: direct and indirect contributions

As indicated in section 4.7.3 in Chapter Four, the connection between CRMi and business performance was already a contested theme during the earlier analysis, with some medium-sized enterprise managers in the manufacturing sector perceiving minimal direct business benefits from cybersecurity investments. The current findings reinforce this divide, showing that medium-sized enterprise managers expressed widely varying views on CRMi's direct and indirect contributions.

Some of the interviewees in this study downplayed CRMi's direct role in business success, stating that they did not perceive a strong correlation between cybersecurity and traditional success metrics such as customer satisfaction, delivery performance, or productivity. For these medium-sized enterprises, CRMi was not seen as a bridge between risk management and business success, reflecting a belief that cybersecurity investments did not visibly drive business growth or improve measurable outcomes.

In contrast, only a few interviewees highlighted a direct link between CRMi and business success, emphasising the importance of customer trust and reputation protection. These interviewees argued that cybersecurity could serve as a unique selling proposition (USP), particularly as customers increasingly valued secure operations. They viewed CRMi as essential for safeguarding financial stability and brand reputation, which in turn reinforced its role as an integral component of long-term success. Nelson and Madnick (2017a), along with Stahl (2003), supported this view, contending that effective CRMi, when integrated with innovation strategies, could provide a competitive advantage. This finding also relates to the outcomes in section 5.4.1, where proactive CRMi was linked to resilience and operational stability. This reinforces the argument that trust, and reliability can drive long-term success, a view shared by the medium-sized enterprise managers, who regarded CRMi as a critical driver of business reputation and customer trust, and as a potential source of strategic advantage.

Stahl et al. (2003) suggested that CRMi contributes indirectly to business success by preventing disruptions and retaining customer trust, which resonates with the views of several of the managers, who emphasised the ethical responsibility to protect their customers. Several managers echoed this perspective, emphasising the ethical responsibility to protect not only

customers but also suppliers from cyber threats, viewing it as essential for ensuring the company's long-term viability.

Some of the interviewees also noted that a significant cyberattack could severely disrupt production, thereby impacting overall business performance. These perspectives reflect an understanding that, while CRMi may not be a visible driver of immediate success, it creates the conditions necessary for maintaining productivity, continuity, and customer confidence. Franke and Meland (2019) supported this view, noting that business interruption due to cyberattacks poses a significant risk, particularly for SMEs in the manufacturing sector. This observation aligns with concerns among the medium-sized enterprises about the potential financial impacts of cyberattacks on productivity and revenue. Armenia et al. (2021) demonstrated through dynamic simulation that SMEs' risk profiles benefit from CRMi investments, suggesting that reducing cyber-risk is essential for sustaining productivity and achieving long-term success.

The relationship between CRMi and innovation also emerged as a key theme in both the interviews and academic literature. De Oliveira et al. (2019) found a direct link between business success and innovation, suggesting that CRMi could be an indicator of a company's ability to adopt new technologies while managing associated cyber-risks. This indicates that a company's success increasingly depends on its capacity to innovate securely. However, findings from the interviews showed that many managers struggled to connect CRMi with business success metrics, focusing instead on more traditional success indicators. He et al. (2020) and Wang et al. (2024) both explored the relationship between cybersecurity and innovation. While they found that companies often reduce their innovation efforts immediately following a cyberattack, both studies contend that, over time, companies tend to increase their innovation efforts post-attack, incorporating stronger CRMi to manage future threats effectively. This advice underscores the notion that companies should view CRMi not as an obstacle to growth but rather as a facilitator of secure innovation and progress.

The discussion above collectively highlighted the multifaceted role of CRMi in business success, including direct contributions, such as enhancing customer trust and differentiating the business in the market, as well as indirect benefits, like safeguarding productivity and ensuring business continuity. While some medium-sized enterprise regarded CRMi merely as a

protective measure or an operational cost, others recognised its potential as a strategic asset supporting sustainable business growth. Nonetheless, a gap remained in fully integrating CRMi into broader business strategies, as evidenced by the mixed perceptions among the interviewed medium-sized enterprises and the existing academic debate that emphasises the need for more proactive and aligned CRMi investments.

5.6.4 Summary of medium-sized enterprises' preparedness against cybercrime risk and the managers' attitudes to cyber-risk mitigation measures and business success

The comparative analysis of German medium-sized enterprise managers' perspectives on cyber-risk mitigation compared to the current academic literature reveals a complex relationship between cybersecurity and business success. While many of the company's managers in this study viewed CRMi as an essential protective measure, there was a lack of consensus as to whether this initiative directly contributed to traditional success indicators like productivity and revenue growth. There was, however, a consensus that CRM did play an important indirect role by safeguarding operations, protecting reputations, and ensuring long-term business continuity. The study found that external pressures from clients and suppliers drove many medium-sized enterprises to adopt CRMi measures, as cybersecurity increasingly became a competitive requirement in industries handling sensitive data. Even though concerns were expressed about the costs and transparency of cybersecurity practices, these medium-sized enterprises recognised the need to integrate CRM into their broader business strategies to remain viable in an increasingly digitised economy. From a theoretical perspective, Nelson and Madnick (2017a), De Oliveira et al. (2019) and Hoppe et al. (2021) support the view that cybersecurity should not be seen in isolation but as part of a comprehensive risk management strategy contributing to long-term success.

5.7 Summary of the Discussion Chapter

This chapter has explored the preparedness of German manufacturing medium-sized enterprises against potential cyber-risks through the adoption of cyber-risk mitigation (CRMi) strategies and the role cyber-risk insurance (CRI) can provide as a framework for these businesses to follow. By drawing on the interviews with the medium-sized enterprise managers and existing literature, the findings have revealed an array of diverse approaches and per-

ceptions toward CRMi and CRI, which are shaped by resource constraints, external pressures, and the complexities of aligning cybersecurity with broader business strategies. One element that emerged from the discussion was the variation in preparedness amongst these medium-sized enterprises. While some companies demonstrated structured and proactive CRMi strategies, such as the conducting of risk assessments and utilising multi-layered protection strategies, other businesses relied on reactive, ad hoc approaches.

This disparity in preparedness aligns partially with Osborn and Simpson's (2018) conclusion that larger SMEs with dedicated IT departments are more likely to engage in robust CRMi. However, even those medium-sized enterprises with a lower cyber-risk engagement were generally aware of the importance of basic cybersecurity measures, challenging the earlier assumptions by Renaud (2016) that SMEs routinely neglect fundamental cybersecurity protocols. This finding has underscored the importance of organisational size and resource availability, as suggested by Zeiringer et al. (2022), in determining the sophistication of CRMi strategies and the need to consider the resourcing aspect of the business. However, there are still medium-sized enterprises who have underestimated their vulnerability to a cyberattack, which is highlighted by a critical need for greater awareness and tailored support, as emphasised by Kapoor et al. (2018) and McLilly (2020).

The influence of external pressures, particularly from supply chain partners, has emerged as a significant driver or motivator for adopting CRMi. Larger business partners often required medium-sized enterprises to meet stringent cybersecurity standards, effectively compelling these enterprises to enhance their CRMi strategies and approaches. This finding is reflective of Renaud and Weir (2016), who argued that supply chain dependencies elevate the need for accountability and transparency in cybersecurity practices. However, several medium-sized enterprises in this study expressed concerns over balancing the need for transparency demanded through conducting audits and their need to protect sensitive data, a tension also noted by Labunets et al. (2020). These external pressures, while promoting higher standards, revealed a challenge for medium-sized enterprises in maintaining operational security while meeting contractual obligations.

Another critical aspect explored was the perception of CRI as a component of CRMi strategies. While several medium-sized enterprises in this study valued CRI for its financial and operational protection, particularly after experiencing a severe cyberattack, other managers

viewed this requirement with scepticism. This scepticism could be linked to concerns about high premiums, limited coverage of the insurance policy, and a lack of clarity as to the terms. These sentiments echoed Nieuwesteeg and Waard's (2018) observation that the cost and complexity of CRI policies deterred many SMEs from seeking insurance coverage. However, the proactive services provided by insurers, such as risk assessments and security updates, highlighted the potential of CRI to complement internal CRMi measures, as advocated by Franke and Meland (2019). This proactive approach underscored the relevance of promoting the perceived value of CRI and its actual benefits through providing the opportunity for the insurer to better align their product with those of the SME, as advocated by Labunets et al. (2020) and Schlesinger (2018).

The relationship between CRMi and business success was another recurring theme. Many of the medium-sized enterprises in this study saw CRMi as being an expense rather than a strategic enabler, with limited recognition of its role in supporting business growth or gaining a competitive advantage. This finding contradicts Nelson and Madnick (2017a), who asserted that integrating CRMi with innovation can enhance organisational resilience and performance. However, some of these German-based manufacturing medium-sized enterprises identified indirect benefits of CRM, such as retaining customer trust and protecting their reputation, which is aligned with the findings of Armenia et al. (2021) that effective risk management strengthens long-term organisational viability. There was also a need for CRMi to be adopted to be a part of the traditional success metrics, highlighting the necessity for medium-sized enterprises to integrate cybersecurity more holistically into their business strategies.

The rapid adoption of automation and increased IT dependency has further complicated the adoption of CRMi in German-based manufacturing medium-sized enterprises. While automation can enhance business efficiency, it also introduces certain vulnerabilities, particularly in terms of the interconnectedness of the medium-sized enterprises' networks and remote working environment. Several medium-sized enterprises have addressed these risks through infrastructure redundancies and network monitoring strategies, reflecting Pfister and Lehmann's (2023) emphasis on building resilient systems. However, reliance on reactive measures, such as post-incident recovery, has highlighted an ongoing challenge of aligning

CRMi with the demands of increasingly digitised operations. The findings underscore the importance of aligning cybersecurity strategies with technological advancements, as advocated by Kazemargi and Spagnoletti (2020), to ensure both operational efficiency and security are maintained.

The study has also highlighted that human vulnerability is a critical feature in cybersecurity. Employee susceptibility to phishing and social engineering attacks was a common concern, prompting some of the medium-sized enterprises to implement training programmes and simulation activities. These efforts align with Dimitrov and Rasheva-Yordanova (2019), who emphasise the importance of tailored and practical training for SMEs to be implemented. However, inconsistent training across these medium-sized enterprises revealed a persistent problem in fostering a cybersecurity-awareness organisational culture, as noted by Muhirwe and White (2016). This finding points to the need for continuous and adaptive training programmes that keep pace with evolving threats, as advocated by Labunets et al. (2020) and Schlesinger (2018).

In summary, this chapter has illustrated the diverse levels of preparedness and perceptions of CRMi adoption amongst German medium-sized enterprises, emphasising the interplay of resource constraints, external pressures, and organisational priorities. While many of these medium-sized enterprises in this study demonstrated a baseline level of cybersecurity awareness, proactive and integrated CRMi strategies remained limited, constrained by the financial implications and perceived risks. CRI, though recognised for its potential benefits, was also seen with a degree of scepticism due to concerns about value and transparency, highlighting an opportunity for insurers to better align their products with medium-sized enterprise's needs. The findings also revealed an underutilisation of CRMi as a strategic enabler for business success, suggesting a need for greater alignment between cybersecurity measures and broader organisational goals. As medium-sized enterprises navigate the complexities of digitisation and automation, integrating CRMi into business frameworks does emerge as a vital approach needed to enable these businesses to become more resilient to potential cyberattacks and sustained growth in an increasingly interconnected landscape.

6 Chapter Six
Conclusions

6.1 Introduction

This chapter will present the outcome of the study, drawing together the existing knowledge as presented in the literature review (Chapter Two), together with the findings (Chapter Four), along with the outcomes of the previous chapter, the discussion, to set out the contribution to both academic and professional knowledge. The chapter will present how the aim of the study has been achieved together with the research objectives and related questions. To make this explicit, Section 6.5.5 revisits the research objectives to demonstrate how they have been achieved. Following this, the contribution from an academic and then professional perspectives will be presented. Finally, the chapter will lay out the limitations of this study before presenting themes for future research.

6.2 Aim of the research

The aim of the study was to investigate the attitudes and strategies adopted by German manufacturing medium-sized enterprise managers in response to the growing cyber-risks due to advantaged attack methods driven by the increased usage of digitalisation.
Based on this aim, the study sought to explore the perceptions and experiences of these medium-sized enterprise managers toward cyber-risk mitigation (CRMi), examining the frameworks, measures, and strategies they have effectively been adopted, including the use of cyber-risk insurance (CRI), to mitigate or limit the consequences of cyberattacks. Before conducting the main study, an extensive literature review was conducted, as it was originally assumed that medium-sized enterprises were not taking sufficient measures to combat cybercrime threats. Part of the rationale for this original perception was based on the complexity and difficulty of interpreting available mitigating cyberattack guidelines, such as certification schemes including ISO 27001. Part of the assumption was also connected to the medium-sized enterprises' financial position, skill sets, and physical resources, which were expected to represent a barrier in the context of the medium-sized enterprises' CRMi strategies. To understand this, the study addressed the following research questions:

- RQ1: What are the risk mitigation strategies adopted in German manufacturing medium-sized enterprises to mitigate against a cyberattack?

- RQ2: What is the relationship between specific risk factors and risk mitigation strategies within medium-sized enterprises?
- RQ3: How do medium-sized enterprise managers consider cyber-risk insurance as a vital option within their risk mitigation strategies?

By addressing these research questions, the study intended to enhance the understanding of how the availability of CRI influenced the CRMi strategies in German-based manufacturing medium-sized enterprises, particularly in protecting against tangible and intangible financial losses. Reflecting this, the CRI was critically reviewed from three dimensions:

- highlighting the significance of highly relevant data in cyber-risk management and risk mitigation decisions,
- comparing the associated cost and return of a cyber-risk management investment against the cost and efficiency of cyber-risk insurance,
- incorporating the key metrics of risk mitigation into the medium-sized enterprises' risk and financial systems to effectively measure and manage profitability and financial stability.

6.3 Overview of the study

6.3.1 Theoretical foundation

This study was based on adopting a social constructivist approach. The focus was to understand the perceptions of medium-sized enterprise managers about cyber-risk and how these were informed or influenced. This aligns with Burr and Dick's (2017) work on the evolution of certainties within organisations due to cyberattacks and risk. Therefore, initially, a narrative literature review was conducted to establish the existing knowledge regarding the social construction of knowledge related to cyber security awareness (CSA), cyber-risk mitigation (CRMi), cyber-risk insurance (CRI), and business success within medium-sized enterprises.

Building on the concept of cybersecurity awareness and reflective of the constructivist approach adopted in the study (Ajzen, 1991; Chaudhary et al., 2023), the focus was on the existing knowledge gaps associated with CSA within German-based manufacturing medium-sized enterprises and the technological threats and types of avoidance behaviour (Liang & Xue, 2009; Carpenter, 2019). However, it needs to be acknowledged that "security behaviour" and "attitudes of managers and employees" could be affected by the existing social

norms in the business, which can influence the success or failure of CSA. Therefore, this study has reviewed CSA as a preeminent method to mitigate cyber threats (Armenia et al., 2021), by investigating how the end-user manager can reduce their human-related vulnerabilities (Muhirwe & White, 2016), then examined how organisations manage to instil the necessary knowledge about cybersecurity in their staff, thereby providing an overall understanding of CSA and strengthening the medium-sized enterprise against malicious attacks through cyber-risk mitigation (CRMi) strategies.

Once the integration of CSA into the overall cyber-risk management process was fully understood, this study then focused on how German manufacturing medium-sized enterprises define their processes to mitigate or limit cyber-risks. While the literature provided a rich insight into the available technical concepts and strategies (Nykänen & Kärkkäinen, 2016; Osborn & Simpson, 2015; Pawar, 2016; Saber, 2016; Such et al., 2015), the challenge was that these managers were getting a subjectively false sense of security (Stahl et al., 2003). Therefore, this study specifically explored whether these managers from German manufacturing medium-sized enterprises had adopted a broader approach, which involves balancing practical experience with a perceived level of risk, to potentially mitigate against risk which is unique to their organisation or business. Furthermore, this study examined whether the managers' adoption of CRMi strategies had enhanced their awareness of potential cyber-risks (Strupczewski, 2021).

This study also scrutinised and evaluated cyber-risk insurance (CRI) as one option amongst the various CRMi techniques to determine whether the German manufacturing medium-sized enterprises sector strategies mitigated the risk of unexpected financial losses that could result from reputational damage, loss of productivity, or being liable for damages to third parties (Rejda & McNamara, 2017). Furthermore, the study investigated the challenges faced by these medium-sized enterprises in determining the necessary coverage for their tangible and intangible assets (Franke & Meland, 2019) and the available CRI products or portfolios in the insurance market (Kavčič & Delak, 2019). In achieving this, the study focused on understanding whether those medium-sized enterprises who had taken out CRI had concerns about the high costs of premium payments and the uncertainty about whether their policies were financially beneficial (Nieuwesteeg & Waard, 2018).

Finally, this study endeavoured to explore the link between CRMi and business success. Previous studies, including de Oliveira et al. (2019), established a primary connection between success and innovation, identifying CRMi-measures as innovative skills and technology (de Oliveira et al., 2019), indicating that business capacity to adopt new technological advancements was a key factor for success while also recognising the need to be aware of potential cyber-risks. Reflecting this, the study investigated the managers' perceptions of how CRMi strategies and cyber security investments enabled business success to be achieved while mitigating a cyberattack.

6.3.2 Research gaps and empirical approach

Based on the study's theoretical work, research questions and search strings used in the systematic literature review, the following research gaps were identified:

- Research gap 1: Limited research exists on the actual level of preparedness against cyber-risks, especially in the German manufacturing context.
- Research gap 2: There is insufficient insight into the cyber-risk mitigation strategies currently adopted by German medium-sized enterprises.
- Research gap 3: Limited understanding exists regarding the role of cyber-risk insurance within German medium-sized enterprises and what risks are effectively covered by existing insurance policies.

The study's fieldwork consisted of conducting semi-structured interviews with nine managers from German manufacturing medium-sized enterprises, which worked in a wide range of production areas within this sector. There were three companies who operated in the metal processing, two organisations who provided electrical and semi-conductor components, together with managers who oversaw plant engineering, print technology, wood processing, and confectionary manufacturing activities. The interviews were recorded, and transcripts were analysed using a content analysis approach, as advocated by Miles and Huberman (1994), before being manually coded.

The Mayring's method was followed as advocated by Mayring and Fenzl (2014); Mayring (2004, 2022) served as the basis for the qualitative analysis of the interviews. Initially, the outcome of the literature review guided the development of the first series of codes. From

these deductive categories, the study employed an inductive method to understand the subjective interpretation of each interviewee assigned to the terms “CSA”, “CRMi”, “CRI”, and “business success”. A descriptive qualitative method to interview the managers of these German-based manufacturing medium-sized enterprises was conducted through semi-structured interviews, which allowed the interviewees to share their experiences and insights regarding CRMi.

6.4 Findings and conclusions

This section will set out how the three research gaps, as presented in section 2.10, were answered and how the research aim was achieved.

6.4.1 Conclusion related to research gap 1: Limited research exists on the actual level of preparedness against cyber-risks, especially in the German manufacturing context

In answering the first research gap, the results from the interviews showed that German medium-sized enterprises were reasonably well prepared against the current cyber-risks at time of data-collection. This outcome differs from earlier results published in international literature, such as those by Renaud (2016) or Osborn and Simpson (2018). While this outcome could be due to these studies being over six years old, the findings could also be attributed to the medium-sized enterprises surveyed in this study not being micro-enterprises that comprise 10 or fewer workers but rather employing between 50 to 250 employees, therefore indicating increased awareness of potential cyber-threats. As noted by Osborn and Simpson (2017), larger SMEs are more likely to invest in CRMi. However, the levels of preparedness amongst the medium-sized enterprises did vary. While basic strategies were taken in all analysed medium-sized enterprises, only a smaller number of businesses had dedicated, structured CRMi-strategies. These medium-sized enterprises tended to be larger in size, had a dedicated IT department, and, in at least one of the analysed businesses, had also assigned CRMi individual responsibility within their organisational structure. This confirmed the findings of Zeiringer et al. (2022), who identified employee numbers as a good indicator for SMEs’ CRMi-engagement. However, based on following the categories recommended by Zeiringer et al. (2022), in this study, none of the medium-sized enterprises analysed fell into the collective category of neglecting fundamental cybersecurity issues, but some only took basic CRMi-measures.

The level of knowledge amongst the managers interviewed as to cyber-risks varied. There was, however, a general level of knowledge and an awareness about cyber-risks within their companies. However, even for those medium-sized enterprises that had a lower level of engagement in CRMi, the businesses did not identify any problems associated with the information about cyber-risks or the lack of related mitigation measures used but were confused about the potential implications of engaging with cyber-risk insurance, confirming the original work of Renaud and Weir (2016) and Grocke (2017).

Amongst the medium-sized enterprises in this study, the representatives with lower levels of preparedness against cyberattacks also indicated that they did not see their company as likely to be targeted for cyberattacks, which was based on the size of the company. This perception indicated that there were minimal financial resources being invested, which had resulted in a limited data-secure storage solution being implemented and being a potential issue in the future. The original notion proposed by Renaud (2016) that SMEs might serve as a backdoor for cybercriminals to access other business partners in their supply chain was not mentioned during the interviews. This is interesting, as the interviews indicated that there was an indication that in the future, this may become a requirement for suppliers and clients for medium-sized enterprises to engage with CRMi. There was also a critical awareness that CRMi was becoming increasingly an important facet within the supply chain and that all actors may need to engage with CRMi throughout their business interactions.

6.4.2 Conclusion on results related to research gap 2: There is insufficient insight into the cyber-risk mitigation strategies currently adopted by German medium-sized enterprises

In answering the second research gap, communication was repeatedly mentioned throughout the interviews as an important non-technological aspect associated with CRMi in the German-based manufacturing medium-sized enterprises. This finding is in line with Binkhorst (2020) and the earlier work by Thompson (2012). Bell (2017) advocated for the effective introduction of CRMi-strategies and measures, citing the flat hierarchical structures and good internal communications of the medium-sized enterprises in this study as enabling this. For Bell (2017), communication was seen as an important CRMi-aspect in these SMEs, particularly in terms of strengthening the human factor in an CRMi strategy. This included ensuring

that any complex technical barriers to conveying messages, such as adopting a zero-trust approach to employees opening an email containing links to malicious webmail sites or malware hidden within an attachment, were prohibited.

As to the usage of technical measures such as firewalls, backups, or VPNs, most of the medium-sized enterprises in this study opted for a payment-requirement solution. Only one medium-sized enterprise in this study opted for a freeware firewall solution, which they attributed to a previous cybersecurity attack. This finding confirms Rawindaran et al. (2021), who indicated the trade-off between costs and ease of use when deciding on which cybersecurity solution.

When assessing the medium-sized enterprise's cyber-risk situation, those interviewed indicated the highest level of preparedness and tended to use some form of structured tools for assessing risks. These tools included medium-sized enterprises meeting requirements for certification based on existing cybersecurity schemes or using risk assessment instruments, such as questionnaires, when determining the type of cyber-risk insurance (CRI). External consultants were also used, who use structured risk assessment instruments. These approaches are similar to solutions suggested by Rawindaran et al. (2021) and Aurelien (2021). Although not identified in this study, those medium-sized enterprises with higher levels of preparedness against cyber-risks also use scenario and war-gaming studies to assess the effectiveness of their CRMi-strategies and tactical measures to address the threats if and when they occurred.

The use of cloud-based cyber-risk management was less common amongst these German medium-sized enterprises. Only one medium-sized enterprise in this study used a cloud-based, on-demand CRMi-solution, challenging McLilly's (2020) original assertion. Likewise, the use of AI-based CRMi-solutions, as proposed by Ncubukezi (2020), could not be identified or found in this study.

Only one medium-sized enterprise had experienced a major and financially harmful ransomware, which had led to the CRMi strategy being adopted, including both certification and CRI, the usage of an external consultancy, and implementing a cloud-based CRMi-solution. This partly confirms the findings by Oxford Analytica (2021) that ransomware attacks are a major driver for companies to engage with CRMi in general, with Kenneally (2021) highlighting the link between CRI and an increase in ransomware attacks.

6.4.3 Conclusion on results relevant to research gap 3: Limited understanding exists regarding the role of cyber-risk insurance within German medium-sized enterprises and what risks are effectively covered by existing insurance policies

The third research question was to investigate how the role of cyber-risk insurance (CRI) was perceived by German medium-sized enterprise managers. The decision-makers interviewed for this study mentioned interruptions in production and/or sales as the main measurement for assessing potential damage from cyberattacks. This confirms the findings from the work presented by Franke and Meland (2019), as the study indicated that business interruption was a major concern for the manufacturing and production industries, whereas the loss of customer data was considered more important compared to the initial costs for financing the insurance. What did not emerge was the awareness or concerns associated with the hijacking of the IT infrastructure or cryptocurrency mining activities.

A major outcome of this study regarding CRI was the dissatisfaction amongst the decision-makers in the medium-sized enterprises as to the availability and types of insurance. The interviews revealed that the primary reason for their dissatisfaction was not only the high costs of insurance premiums, but also their concerns about whether the coverage would be sufficient or if the costs would be excessive.

6.4.4 Conclusion to cyber-risk mitigation and business success

In analysing the study's data, the interviews highlighted a critical intersection between cyber-risk mitigation (CRMi), innovation, and business success. As identified in the literature review presented in Chapter Two, the relationship between cybersecurity measures and organisational performance has received considerable debate. Nelson and Madnick (2017b), for example, demonstrated a direct connection between higher levels of CRMi and increased innovation, thereby indicating a direct linkage for enabling business success. Conversely, He et al. (2020) observed that organisations that were affected by a cyberattack often scaled back their innovation activities, although He at al. (2020) advocate for a proactive approach through increased CRMi efforts to foster resilience and safeguard future innovation, a perspective supported by Wang et al. (2024). Based on this literature, a strong link between CRMi, innovation and business success was expected to emerge from the empirical findings. For instance, the findings of this study aligned with Wang et al.'s (2024) proposition, which

was particularly relevant for medium-sized enterprise Five. After experiencing a severe cyberattack, medium-sized enterprise Five had adopted the most comprehensive CRMi strategy, reflecting a proactive approach to manage and mitigate any future cyberattack. This robust strategy not only attempted to mitigate against future risks but also created an environment conducive to innovation, ultimately contributing to a business's sustained success.

However, this was an exception, as for most of the interviewed medium-sized enterprises such a strategic connection between CRMi and innovation was not evident. These insights underscored the importance of viewing CRMi not only as a defensive mechanism but as a strategic enabler that can drive innovation and support long-term business objectives. By adopting and enhancing CRMi practices, organisations can not only protect their operations but also unlock opportunities for growth and gain a competitive advantage, emphasising the dual role of cybersecurity as both a safeguard and a catalyst for attaining business success. While the literature indicated that CRMi could serve as a driver for innovation and strategic growth, the interview data suggest that most medium-sized enterprises still regard cybersecurity in operational or compliance terms, thus falling short of leveraging it for business success.

6.5 Conclusions in relation to the initial research questions

The identified gaps as presented above will now be further contextualised below, commencing with considering the risk mitigation strategies adopted in medium-sized enterprises as to cyber-risk mitigation.

6.5.1 Conclusions related to research question 1: What are the risk mitigation strategies adopted in German manufacturing medium-sized enterprises to mitigate against a cyberattack?

The results from the study showed that there were different levels of preparedness against cyber-risks in these German medium-sized enterprises, resulting in different approaches and perspectives to cyber-risk mitigation (CRMi). All the medium-sized enterprises in the study implemented a basic technical mitigation measurement, including the use of firewalls, backups, VPNs, and staff awareness training. Some of the medium-sized enterprises had also instigated restrictions on automated data exchange with outside organisations. There were several medium-sized enterprises that had adopted analogue CRMi-measurements,

measures that attempted to involve mitigating against redundant production facilities due to a cyberattack and preventing supply-chain problems or production interruptions from occurring. Those medium-sized enterprises with a lower level of preparedness, which implemented basic measures on an ad hoc basis, tended to have a no-structure approach due to the costs and lack of awareness. Where there was an awareness about the potential risks and costs of CRMi, the main cybersecurity measures used tended to be delegated to the IT department or individuals tasked with IT maintenance but may not have engaged in a formal CRMi.

Finally, those representatives from medium-sized enterprises who had smaller revenue turnover and limited employee numbers tended to see their business as not being a potential target for cyberattacks.

6.5.2 Conclusions related to research question 2: What is the relationship between specific risk factors and risk mitigation strategies within medium-sized enterprises?

The medium-sized enterprises in this study did not demonstrate that CRMi strategies or individual CRMi measures specifically addressed a wide range of risk factors. Generally, the most common risk factors identified were related to targeted automated cyberattacks, particularly denial-of-service (DOS) threats delivered via malicious emails. Two specific challenges emerged from the findings as particularly difficult for the interviewed experts to address.

The first challenge involved low-level attacks, such as malicious emails sent to employees. medium-sized enterprises attempted to mitigate this risk through cyber-risk awareness training, which was typically provided as part of the onboarding process. In medium-sized enterprises with higher levels of cyber-risk preparedness, continuous monitoring and testing were implemented. For example, employees' awareness was periodically assessed by sending simulated phishing emails that replicated cyberattacks containing suspicious links or attachments.

The second challenge related to the potential threats posed by employees using personal devices to access the medium-sized enterprises' IT systems. To mitigate this risk, many medium-sized enterprises adopted policies prohibiting the use of personal devices for work-related tasks. This measure was aimed at safeguarding the company's IT infrastructure from

potential vulnerabilities introduced through personal devices connected to less secure home networks.

While these mitigation strategies were effective in addressing these specific risk factors, the findings suggest that medium-sized enterprises' CRMi measures were primarily focused on these two challenges, with limited evidence of strategies targeting other cyber risks.

6.5.3 Conclusions related to research question 3: How do medium-sized enterprise managers consider cyber-risk insurance as a vital option within their risk mitigation strategies?

The German medium-sized enterprise managers were aware of cyber-risk insurance (CRI); however, only a minority had some form of CRI. There was a general sceptical attitude towards CRI. Underlying this was the uncertainty about the perceived value of CRI and the level of coverage that would be required for the company. While loss of production or sales were considered, and the medium-sized enterprise managers in general did assess the potential financial damage, other consequences were difficult to determine and assess for both the insurance companies and the medium-sized enterprise. The medium-sized enterprises' managers also expressed their concern about the high cost of insurance and the stringent requirements for CRMi measures, which are prerequisites for insurance. Eventually, the managers rationalised this decision based on the necessary high levels of CRMi-measurements needing to be taken and the potential cost, making self-insurance more beneficial.

6.5.4 Emerging contribution as to German medium-sized enterprises preparedness against cybercrime risk and the managers' attitudes to cyber-risk mitigation strategies to attain intangible business success

In addressing this research gap, the study findings remain inconclusive; however, productivity and company image can be adversely affected by a cyberattack. In reaching this conclusion, while the interviews captured the perceptions, it was not possible to quantify the perceived value, reduced relative costs, or loss of revenue which could occur following a cyberattack. The findings in this study did contradict Oliveira et al. (2019), who stated that SMEs typically link business success to the effective implementation of innovative technology and therefore often stressed the importance of this as a key success factor. In this study, the managers acknowledged that the exploitation of their network in information systems

could be vulnerable to malicious cyberattacks, which could lead to technical and economic issues such as loss of revenue, profitability, and negative financial productivity (Anderson & Moore, 2006). However, the managers in this study struggled to establish a connection between CRMi's beneficial effects and the critical success factors that could contribute to the overall success of a business in the event of a cyberattack.

6.5.5 Revisiting the research objectives

The following subsection explicitly revisits the research objectives to demonstrate how each has been achieved. In doing so, it shows how the objectives informed the study, how they were addressed through the literature review, empirical investigation, and discussion, and how they underpin the answers to the research questions and contributions to knowledge:

1. To critically identify from the current academic debate what cyber-risk mitigation strategies (CRMi) are adopted to manage potential cyber threats.

   This has been achieved through the systematic literature review (Chapter Two), which synthesised the state of knowledge on CRMi strategies in SMEs and surfaced the core debates and limitations that informed the research gaps (Section 2.10). The review highlighted, in particular, that CRMi is a critical issue for SMEs, that many organisations remain under-prepared due to limited resources and expertise, and that cyber-risk insurance (CRI) is increasingly considered as one element of CRMi strategies, though its role and effectiveness remain contested. Taken together, these findings directly addressed research gap 1 by clarifying the current level of academic debate and the absence of comprehensive insight into SMEs' preparedness against cyber-risks.

2. To critically analyse, from the findings generated from German manufacturing medium-sized managers, the strategies adopted to manage and mitigate potential cyberattacks.

   The objective was fulfilled by the empirical results (Chapter Four) and their critical interpretation in the discussion (Chapter Five), which provided detailed insights into the measures actually implemented within German manufacturing medium-sized enterprises. The interviews revealed a spectrum of preparedness levels, ranging from basic technical safeguards (e.g. firewalls, backups, VPNs, email screening, and

onboarding awareness training) to structured approaches involving incident reporting systems, restricted device usage, and formalised monitoring. At the most advanced level, some firms had developed dedicated cyber-risk strategies, sought certification, and even combined internal expertise with external consultancy. Importantly, the analysis showed that managerial attitudes strongly shaped these strategies: in less-prepared enterprises, CRMi remained reactive and ad hoc, whereas in better-prepared enterprises, decision-makers adopted a proactive stance, recognising CRMi as a strategic investment linked to operational resilience. In this way, the analysis directly addressed research gap 2, providing much-needed insight into the strategies currently adopted by German medium-sized enterprises.

3. To critically evaluate, from the findings, how German manufacturing medium-sized managers mitigate against potential cyberattacks.

   Achievement of this objective is demonstrated in the integrative evaluation presented in the discussion (Chapter Five) and reinforced in the conclusions (Sections 6.4–6.5). In these sections, the findings were systematically contrasted with the literature to assess patterns of preparedness and mitigation across different enterprises. The evaluation revealed that while all firms adopted basic technical safeguards, only a subset had developed structured CRMi strategies, often linked to certification or cyber-risk insurance, and that attitudes toward insurance were marked by scepticism due to perceived cost and limited value. The analysis further demonstrated that managerial orientation and resource availability strongly influenced whether mitigation remained reactive or became strategically embedded in organisational processes. In this way, the study addressed Research Gap Three by clarifying how managers in German medium-sized enterprises operationalise mitigation strategies and by highlighting the wide variation in their depth, structure, and effectiveness.

4. To provide a new critical academic insight into how German-based manufacturing medium-sized enterprises mitigate against potential cyberattacks.

   This objective is realised through the study's contributions to knowledge (Section 6.6) and, most significantly, through the development of the proposed CRMi framework (Sections 6.7–6.14). The framework integrates the empirical findings with prior litera-

ture to produce an academically grounded yet managerially actionable model tailored to the German manufacturing SME context. Its three pillars: base risk management, CRMi strategies (including CSA), and operational success, demonstrate how mitigation measures extend beyond technical safeguards to encompass organisational resilience, employee awareness, and preparedness for residual risks. By explicitly linking CRMi to business continuity, competitive advantage, and long-term business success, the framework provides a novel academic contribution and a practical tool for managers. In this way, the study offers the critical new insight required by this objective, positioning CRMi not merely as defensive practice but as a strategic enabler of sustainable performance in German manufacturing medium-sized enterprises.

Collectively, these outcomes demonstrate that the research objectives have been achieved in full. Each objective has been explicitly addressed through the systematic literature review, empirical investigation, and integrative evaluation, thereby directly closing the research gaps identified in Chapter Two. In doing so, the objectives also underpin the answers to the research questions (Sections 6.5.1–6.5.3) and provide the foundation for the study's original contributions to academic and professional knowledge (Sections 6.6–6.14).

6.6 Contribution to knowledge

This study makes four substantive contributions to academic knowledge in the field of medium-sized enterprise cybersecurity. Firstly, the study's contribution to addressing a major empirical gap by offering in-depth insights directly from senior decision-makers in German manufacturing medium-sized enterprises, perspectives that are largely absent from the predominantly desk-based literature. Secondly, the outcome of the study demonstrates that resource constraints, cost-benefit logic, and limited cyber-risk mitigation capacity shape medium-sized businesses' decision-making in ways not fully captured by existing frameworks. In doing so, the study expands the current discourse by highlighting the underestimation of intangible risks such as reputational harm and the absence of structured mitigation strategies in many medium-sized enterprises. Thirdly, this project challenges prevailing assumptions about cyber-risk insurance, arguing that existing models often fail to meet the practical needs of medium-sized enterprises in terms of affordability, transparency, and alignment with medium-sized enterprise-specific risk profiles. Fourthly, and most critically, the study introduces

a dedicated cyber-risk mitigation framework tailored specifically to the operational realities of German manufacturing medium-sized enterprises. This framework integrates cyber-risk insurance, formal mitigation strategies, and return on security investment (ROSI) within a coherent structure that is both academically grounded and managerially actionable. To the best of the author's knowledge, this is the first empirical study to synthesise medium-sized enterprises-specific constraints, perceptions of risk, and insurance adoption into a practical framework, providing a distinct contribution to the literature and offering valuable implications for scholars, business leaders, and policymakers alike. The remainder of this section expands upon these contributions in greater detail, beginning with the academic significance of the study's empirical findings.

6.6.1 Contribution to academic knowledge

Based on the above, this study has provided a new and critical insight from senior management and leadership perspectives, which have hitherto often been unavailable from both an academic and professional perspective. Part of this uniqueness can be attributed to the access and willingness to disclose the challenges of cybersecurity without breaching business confidentiality. Reflecting this challenge, even at the outset of this research project, these participants were initially reluctant to participate, but once contacted and assured of the ethical rigour of the study and its respect for their confidentiality, they were happy to present their viewpoint. This reluctance could be related to the fact that there has been minimal primary-based research, with most studies being deskbound projects. There are several key contributions that have emerged from the findings, which include the intangible loss of reputation, which was not really considered, as only the production downtime and financial loss were seen as important. Unlike existing literature such as AL-Dosari and Fetais (2023), Pfister and Lehmann (2023), Hoppe et al. (2021), Alahmari and Duncan (2020), and Kalhoro et al. (2021), which have been mainly deskbound studies, this qualitative research project focused on medium-sized businesses in the German manufacturing sector. AL-Dosari and Fetais (2023), in their systematic literature review, focused on investigating the potential usage of an IT risk-management framework for SMEs. The study by AL-Dosari and Fetais (2023) concluded that there was a critical need for SMEs to adopt some form of IT risk-management methodology. In another systematic literature review-based study, Pfister and Lehmann (2023) noted that firstly, there was limited research related to digitalisation in SMEs,

but then concluded that the focus on digital management solutions could potentially provide long-term cost savings but neglected the threat of cyber-risk management. In partly addressing this omission earlier, Alahmari and Duncan (2020) indicated that the cyber-risk culture in SMEs was predominately informed and influenced by IT experts. However, in reaching this conclusion, Alahmari and Duncan (2020) also called for more in-depth empirical research. Finally, Kalhoro et al. (2021) focused on cloud-based solutions to contend that there was a significant misunderstanding in SMEs as to the potential of cybersecurity threats; however, in this systematic literature review, the study was unable to provide the empirical evidence as to the reasons and the underlying rationale for this conclusion. These current omissions in this theme of cybersecurity in medium-sized enterprises represent a significant gap in knowledge, which for Germany is critical to understand, as this form of business is seen as the core economic driver and main employer in the country. To date, there has been little research into this sector or size of business in terms of the implications of cybersecurity from a senior leadership or management viewpoint. There was a sense of self-assuredness amongst the leadership and management of conducting a risk assessment, an acceptance of the potential risks, and a perspective on the likelihood of advanced AI and ransomware being used.

In reaching this conclusion, this study firstly challenges the notion of Renaud (2016), who contended that SMEs do not take sufficient measures to manage cyber-risks, which is why they are targeted by cyber criminals, but only at a lower level. The contention is based on the premise that SMEs that suffer from cyberattacks could be cut off as suppliers by larger companies. In this study, the cyberattacks were related to low-level activities such as phishing. However, even with this form of cyberattack activity, large organisations in Germany were not inclined to reject suppliers due to these forms of security breaches. This finding therefore extends Renaud and Weir's (2016) work, which was focused on cyber-risks, as this research found that formal cyber-risk mitigation networks amongst other medium-sized enterprises were not a common approach adopted, even though they were critically aware of risks but had instigated a few basic measures to minimise the potential impact.

This finding rejects Renaud's (2016) original notion that external actors are also important for cyber-risk preparedness, particularly those who act as suppliers for larger companies. Renauld’s (2016) study contended that SMEs needed to have cyber-risk mitigation (CRMi)

measures and argued for the need to gain cyber-risk certification. The justification for Renaud (2016) was that this certification was based on the premise that a cyberattack might serve as a backdoor for cybercriminals to gain access to other business partners in the supply chain, but this was not mentioned or identified during the interviews. This study also challenges Renaud's (2016) conclusion that SMEs do not take sufficient cyber-risk management measures, but instead this study found that they were targeted by cyber criminals, but only at a low level. The medium-sized enterprises in this study found that their business activities were not necessarily the main target of an attack and that cyber criminals were not interested in using medium-sized enterprises as a back door to attack larger enterprises. This study instead extends Dayalan's (2017) research that SMEs do not take sufficient measures, as this qualitative project identified an awareness of the potential risks and associated costs of CRMi, which was then compared by the management team to the investment requirements (Ishikawa, 2017). This is important, as Kazemargi and Spagnoletti (2020) noted that while Industry 4.0 has been widely investigated in large enterprises, there has been limited research about how SMEs with limited financial resources make investment decisions in strategic cyberattack technologies. Part of the reason for this lack of investment in this study could be attributed to the initial cost or expense required, together with the lack of perceived necessity.

This study acknowledges Armenia et al.'s (2021) findings that there are tools that can be used to assess cyber-risks that can enable SMEs to identify possible options that can be designed to assist in identifying and classifying potential risks. This information can then be used by SMEs to prioritise cyber-risk investments to evaluate residual risks, but this study found that this was not seen as essential by the medium-sized enterprises analysed. The interviews revealed that instead, the evaluation process was often taken at a departmental level.

The study also contradicts Osborn and Simpson (2018), who noted that medium-sized companies with 10–249 employees, which was the focus of this study, had more control over their IT networks and devices. This study found that there was limited control over the IT infrastructure and responsibility for cyber-risk activities. Instead, the responsibilities and evaluation process were primarily devolved to an individual employee or department level. In

reaching this conclusion, this study extends the current understanding that cyber-risk training is fundamental but is departmental or individualised and focused on phishing attacks, which does build on and challenges the small number of existing studies such as Carías et al. (2021) and Quesada (2016). Carías et al. (2021), who argued that a cyber resilience framework for SMEs was essential to have, including a checklist of actions, ranging from the development of a cyber resilience strategy to the development of staff training programmes. This had originally been examined by Quesada (2016), who found that employees and owners of SMEs tended to lack formal and extensive cyber-risk management training or awareness, which this study from a German perspective also supports. Saber (2016) carried out research on cyber-risk management activities in SMEs and recommended this size of business needed to introduce proactive CRMi policies, including ensuring that staff training was adequate. Developing on this theme, Consoli et al. (2020) focussed on the development of training programmes for SMEs' owners and employees, which was informed by the earlier work of Consoli and Kovatcheva (2019), who proposed a new cybersecurity training programme for SMEs, but in this study the extensive nature of these training programmes was seen as being too excessive, irrelevant, and expensive.

The importance of reinsuring these forms of activities closely aligns with the debate surrounding training and the risk of cyberattacks. Armenia et al. (2021) and Heidt et al. (2019) found that SMEs tended to manage their own cybersecurity risk and tended to seek cyber-risk insurance (CRI) based on an economic evaluation of the potential and residual risk of the event occurring. These studies, along with this study, indicated that the size of the organisation often informed and influenced their cybersecurity status based on evaluating the investment required and the possible impact of the risk profile. This partly supports but also addresses McLilly (2020), who concluded that since SMEs have limited resources, they tended to outsource cyber-risk management; however, in this study there was a reluctance among the medium-sized enterprises' managers to adopt CRI due to the need to share their business activities with external entities. Scepticism about the value of CRI also emerged from the interviews, which is partly supported by Kavčič and Delak (2019), who found that CRI products for SMEs in the USA represented 85%–90% of CRI activities, while in Europe it was only 5%–9%. Part of the reason for this limited engagement in insuring against this form of risk was based on the clients' self-assessment, the potential data loss and liability for breaches of confidentiality, and the associated legal costs along with damages caused. More

recently, Zeller and Scherer (2023), in studying risk mitigation services in relation to CRI and the potential usage of optimal contract design and price structure, found that when pricing a single contract, the insurer would always shift the full cost of self-protection services to the insured; however, this was often rejected due to the high price or cost associated with the self-insurance services or if a portfolio option was followed. In this study, CRI was seen as being irrelevant and not providing the insurance needed amongst medium-sized enterprise decision-makers as to the available insurance offers. Part of the rationale was based on existing insurance policies tending to be designed to be too specific and comprising complete or portfolio coverage, which was too expensive. Therefore, these medium-sized enterprises did not consider existing insurance offers to be of good financial value. This therefore updates Vieira et al.'s (2020) assertion that the uncertainty about the value for money of insurance policies requires insurance companies to identify these major challenges related to cyber-risk, which further requires the insurance industry to provide solutions to assist SMEs to better understand risks and areas of potential exposure. The usage of cyber security certification can be seen as an external tool for mitigating potential cyber-risks. However, medium-sized enterprises in this study did not actively pursue cyber security certification, only seeking insurance when it was deemed necessary for their business, such as a requirement or prerequisite for providing a supply chain or demonstrating CRMi competence to potential or existing clients. The usage of questionnaires provided by cyber insurers was seen by the interviewees in this study as a form of certification, as the managers compared their current activities with the risk prevention strategies used by the insurers. However, this mechanism could not only be seen as being a summarised internal security indicator but also confirmed the medium-sized enterprises' scepticism about CRI.

This study found a common reluctance among the medium-sized enterprises to share resources, such as cloud-based solutions to mitigate again cyberattacks, but also a rejection of collaboration by sharing resource-based strategies amongst German-based manufacturing medium-sized enterprises. As medium-sized enterprises are now moving to external storage and AI technology solutions, Ncubukezi (2020) suggested that cyber-risk management tools have begun to adopt a cloud approach, which is now being tailored for the needs of SMEs. This usage of cloud-based solutions has led to the emergence of cyberattacks targeting IT systems, but in this study, this trend was less common amongst these German medium-sized

enterprises. Part of the reason can be attributed to these German-based medium-sized enterprises being less reliant on the usage of cloud-based solutions, with only one business using on-demand CRMi-technology, which challenges McLilly's (2020) original assertion of the growth of cloud-based solutions in SMEs. Likewise, the usage of AI-based CRMi-solutions, as proposed by Ncubukezi (2020), could not be found. Again, part of the reason could be attributed to the overall reluctance to use, rely on, or even communicate about cyber-risks with external entities outside of the company. This lack of engagement of cyber-risk security measures also resulted in a reluctance to communicate with other medium-sized enterprises in their sector, which are often their competitors. This finding challenges the original work of Ajuzie (2019), who carried out case study research amongst SMEs, and contended that information exchange was present amongst SMEs to provide collective solutions and information exchange forums.

6.6.2 Contribution to professional knowledge

6.6.2.1 General

Drawing on the findings and outcome of the previous section above and informed by the Discussion and Findings chapters, this section will focus on the professional contribution. In achieving this, the key contributions from an academic viewpoint will be presented from a professional perspective.

The first professional contribution is that this study found these medium-sized enterprises did not perceive insuring again cyberattack risks was critical. There was instead a perspective that the type of attacks could be mitigated against and then minimised within the company through staff awareness training, for example, as to phishing attacks. The potential of any other cyber activities that could compromise the overall business activity or extend to impact on external businesses was seen as not credible. It was only after a cyberattack that the medium-sized enterprise leadership recognised the need for insurance. Part of this perspective was also related to the initial outlay or cost. Reflecting this, this study contends that the insurance companies need to provide more competitive but also medium-sized enterprise-designed portfolios which are specifically tailored to the sector. Therefore, the insurance sector should be aware that cybersecurity for medium-sized enterprises is complex and is often constrained by finance and resources.

Related to this, is the second professional contribution which was associated with the cyberattacks being perceived to be predominately focused on large organisations in the German manufacturing sector, with the medium-sized enterprises leadership dismissing the notion that they could be used as a "backdoor". To address this, this study contends that the sector should consider making cybersecurity insurance a mandatory or prerequisite requirement for medium-sized enterprises when supplying these larger organisations.

It seems, as mentioned above, that only after a cyberattack did enhanced cybersecurity became a priority. The consensus was that medium-sized enterprises saw cybersecurity as being more of an issue for large multinational companies, as they were seen as being too small an actor for targeted attacks. While these medium-sized enterprises acknowledged that they had been targeted, the cyberattack activities were predominantly phishing attacks on a personal employee basis. To address these forms of low-level attacks, medium-sized enterprises had put in place employee awareness-training; however, this may be inadequate.

With the mandatory insurance against cyberattacks, which could be enforced in the future by the large organisations in the supply chain, there is a need for the usage of KPIs to be aligned with meeting cybersecurity performance and goals, which is the third professional contribution. To address this, this study contends that a cyber-risk mitigation (CRMi) framework is needed for the German-based manufacturing medium-sized enterprises, which will be presented below. In creating a CRMi framework for medium-sized enterprises, the process involves identifying potential risks, implementing strategies to mitigate against these risks occurring, while ensuring that the business can sustain or improve its success despite potential cyber threats. Through following this framework and recommendations, managers can then decide on the most appropriate cybersecurity strategies and metrics to limit financial loss. The CRMi plans can also minimise the risk while also working within budgetary constraints in terms of meeting the expected return on security investment (ROSI). In next section 6.7 below, the framework and associated strategies will be set out.

6.7 Cyber-risk mitigation framework for German manufacturing medium-sized enterprises

The purpose of this study was to establish a conceptual framework model for cyber-risk mitigation (CRMi) before making recommendations for German manufacturing medium-sized enterprises for providing future cybersecurity solutions. Based on the findings of the study, a

new CRMi framework for medium-sized enterprises was created that can be used to inform future CRMi strategies in the German manufacturing sector. The CRMi framework offers German-based manufacturing medium-sized enterprises guidelines to address the challenges associated with managing cyber security risks by providing mitigation strategies and managerial execution plans. These plans enable the development of robust cyber security initiatives to protect the existing critical infrastructure while also reflecting and acknowledging the limited resources available in medium-sized enterprises. It should be noted that this framework does not intend to replace any of the existing certifications within the ISO system but rather to represent a methodology which can be followed by Germany's medium-sized enterprises to assess cyber-risks and an indication of potential mitigation measures (Mijnhardt et al., 2016). As indicated in the literature review and in this study, insurance was seen as an important aspect; the development of this framework and methodology also provides an insight into how this adaptation can protect and ensure medium-sized enterprise business continuity in the event of a cyberattack. To illustrate this, Table 6-1 below sets out the outline of this cybersecurity framework.

6.8 Overview of the proposal framework

The proposed CRMi framework was created based on the findings generated from this study, together with the conceptual theories and concepts outlined in the literature review in section 2.2, 2.7 and 2.9 of Chapter Two. The framework has been designed to assist in identifying the relationship between theoretical concepts and practical experience to provide an assurance of accuracy, efficacy, and performance. To achieve this, the CRMi framework integrates several concepts that act as a common language for enhancing cyber-risk management and mitigation techniques.

6.9 Approach, concept and objectives of the CRMi framework

The proposed CRMi framework comprises three main pillars:

- Base risk management pillar (medium-sized enterprise organisation's assets and threats)
- CRMi pillar (CSA plus CRMi techniques and strategies)
- Operational success pillar (potential residual losses, KPI, KSF and business success)

Through the integration of these three domains, this forms a unified approach that can enhance CRMi in German manufacturing medium-sized enterprises. As a result, this approach can assist in building on existing industry practices to help medium-sized enterprises achieve overall risk control by ensuring that all steps and activities are carried out in accordance with the prescribed agreed guidelines. By adopting this framework, the strategy supports the interpretation of the concepts associated with mitigating and minimising cyber-risks. To explain the modelled concepts, the framework provides different features, with each definition presented offering a unique solution and data characteristic properties. This is represented in the graphical visualisation and description of Figure 6-1 below:

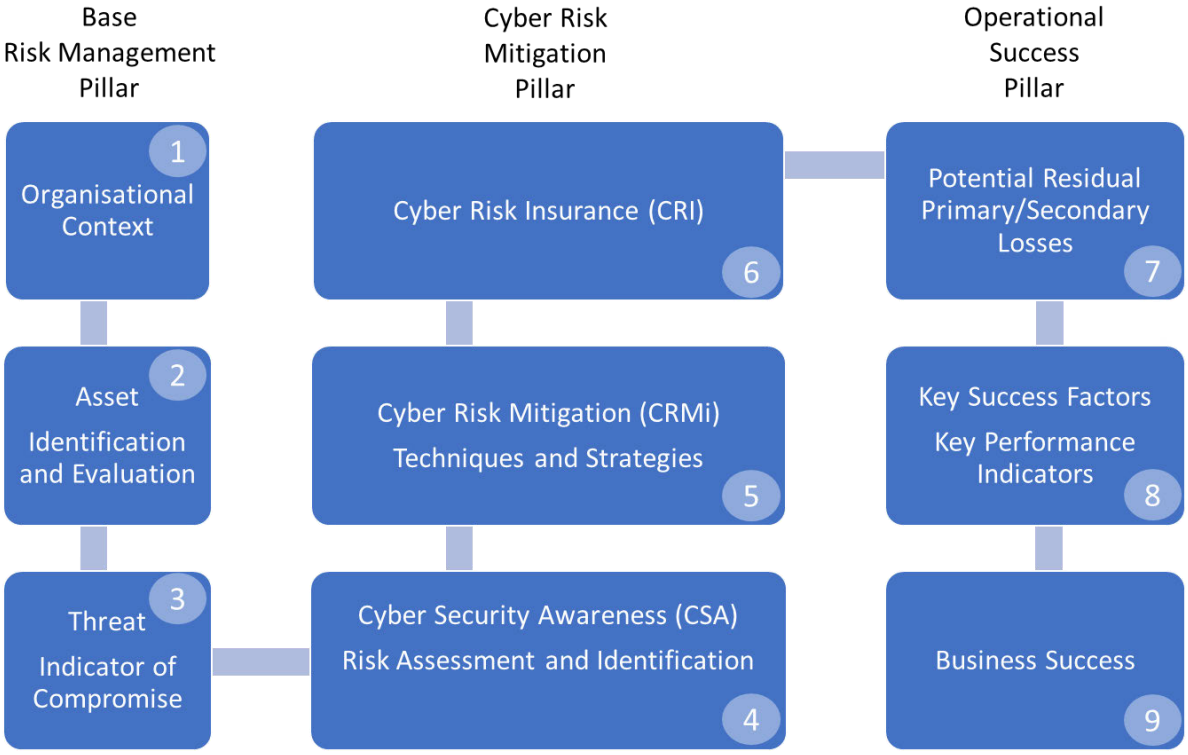


Figure 6-1: Outline of CRMi framework

Based on figure 6-1, the CRMi framework reflects five major objectives:

- To establish a closer linkage and communication between the CRMi processes and activities at the C-suite level of the organisation. This included the processes and activities at the system and operational levels within the organisation;

- The incorporating of internal and external stakeholders, such as employees and business partners, such as suppliers, are essential in the overall construction of an effective CRMi;
- To be effective, the CRMi preparatory activities need to facilitate a more efficient and cost-effective execution of the CRMi framework at both a system and operational levels;
- To demonstrate how the CRMi framework can be implemented in the established recovery management strategy when managing a cyber-risk; and
- To align all CRMi activities with the overarching goal of the business to attain success.

6.10 Technical specification

With German manufacturing medium-sized enterprises being part of a global supply chain, this study contends that the same CRMi process steps and processes adopted by larger organisations need to be followed (Manuj & Menzer, 2008; Musa, 2012). However, in the realm of cyber security, the entire process, from the supply of goods through the manufacture of the goods through their distribution and sale, can vary in terms of the potential risk response (i.e. the decision as to adequate solutions, ranging from risk avoidance to risk mitigation to risk transfer through taking out cyber-risk insurance).

To contextualise this, the amount of lost business, and the time taken to detect the risk can disrupt the supply chain performance, consequently response time is critical (El Baz & Ruel, 2021). Therefore, for manufacturing medium-sized enterprises, CRMi objectives need to be adaptable and provide suitable mitigation processes which are reflective of the potential losses to materials, finances, and reputation. To ensure the continuity exists in the supply chain and the mitigation processes are suitably adaptable, Musa (2012) suggests that supply chains should be closely monitored and continuously reviewed.

In this study, all interviewed German medium-sized enterprises operated in the manufacturing industry and used some form of cyber-physical systems (CPS). Participants commonly worked within supply chains, networked, and connected with larger organisations, often online and externally in cyberspace. Figure 6-2 illustrates how the CPS environment functions in a typical medium-sized enterprise and the potential effects of cybersecurity risks.

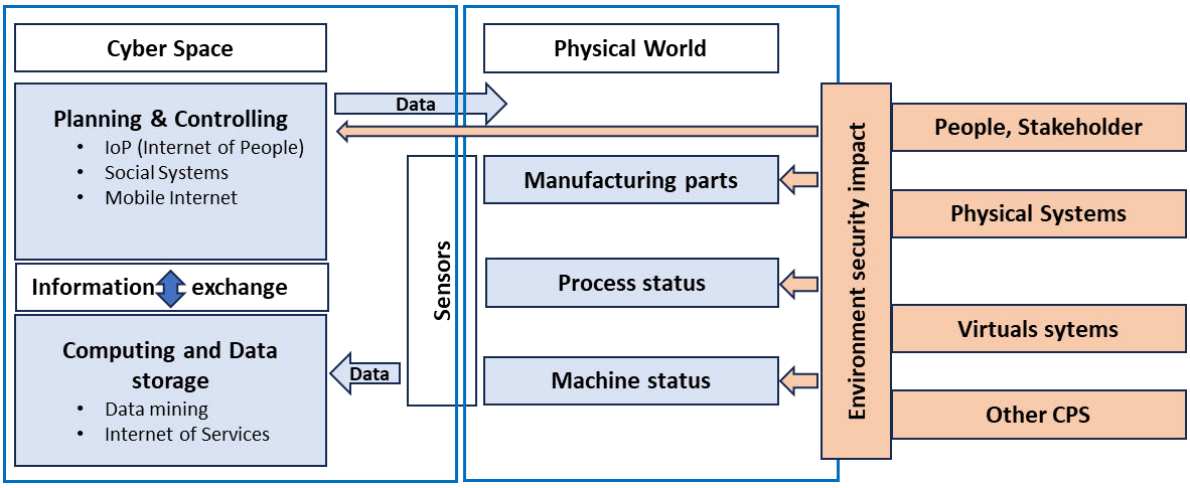


Figure 6-2: Cyber Physical System

6.11 Base risk management pillar (Step 1- 3)

This section will present how the base risk management pillars operate in terms of managing the cyber-risk of German manufacturing medium-sized enterprises, including the prescribed standards and controls which should be adopted to mitigate against or reduce cybersecurity threats, commencing with Step 1.

6.11.1 Medium-sized enterprise organisational context (Step 1)

As outline above, the CPSs are critical, and their interconnectedness can make a medium-sized enterprise vulnerable to potential cyberattacks. However, by identifying the security requirements of the CPS, this can enable the business to indicate relevant risks and then consider a suitable solution to minimise the cyber-risk, which requires the CPS not only to focus on reducing the severity of the risk, but also on enhancing the medium-sized enterprises' overall business success. In reviewing a generic risk management process, which was largely followed by the medium-sized enterprises in this study, it became clear that with cyber-risk, there was a need to have mitigation strategies established to prevent, detect, and provided remediation solutions which are then embedded permanently into the communication and monitoring layer of the business, as outlined below in 6-3:

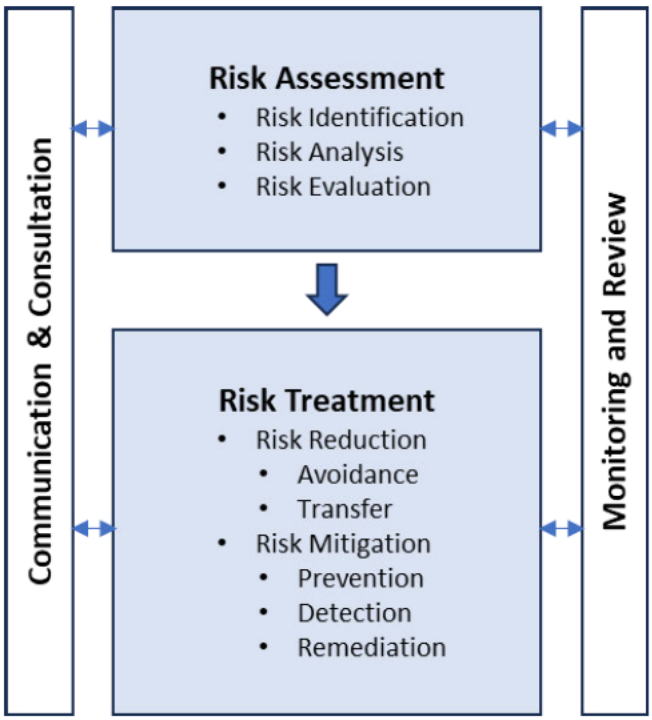


Figure 6-3: Generic Risk Management Process

To contextualize this further, Table 6-1 below illustrates the core mitigation strategies and steps that need to be taken to address and evaluate the performance of risk mitigation strategies.

Table 6-1: Organisational Context (Step 1)

Topic *(Responsibility)*	Input	Technique and Steps	Output
Internal and external actors. *(Manager, IT-department).*	Grouping of actors into internal (manager, staff) and external stakeholders (people or companies involved in service delivery outside the organisation).	Identify actors and their roles. Examine job profile, roles, duties and responsibilities of actors.	A defined list of actors and their role.
		Responsibility for cybersecurity lies ultimately with top-management. Responsibility for implementation of CRMi-measures is delegated to a dedicated Cybersecurity Officer within the IT Department.	Ensured vendor and service provider compliance documentation. IT Department provides regular reports to top-management on policies and strategies based on identified gaps and emerging threats and CRMi measure effectiveness. Enhanced cybersecurity oversight and continuous improvement.

Table 6-1: Organisational Context (Step 1)			
Topic *(Responsibility)*	Input	Technique and Steps	Output
Topic continued.	Clarify key external stakeholder categories such as cloud service providers, supply chain partners, and consultants.	Regularly review and update the list of actors to reflect changes in the business environment and evolving cyber threats.	Comprehensive and current documentation of internal and external actors.
Risk monitoring.	IT networks, systems and applications.	Conduct continuous network monitoring to detect and respond to suspicious activities.	Detection of security breaches or anomalies.
		Integration of periodic dynamic role reviews to adjust responsibilities based on evolving cyber threats.	Up-to-date cybersecurity role assignments and CRMi strategies.
Incident Reporting.	Cyber incidents (e.g., phishing attempts, malware detections, ransomware).	Establish a system for employees and stakeholders to report and analyse security incidents to learn from them and improve defences.	Established incident management framework including: • Centralised Incident reporting system • Structured incident analysis (root causes and potential preventive measures).
		Lessons learned from incident analysis are integrated directly into policy updates and training programs.	Continuous improvement in incident response and organisational learning.
Cybersecurity Policies.	Policy and Procedure documents.	Revise and update security policies and procedures based on lessons learned from internal and available public information from external security incidents.	Revised policies recommending enhanced access controls, improved user training, or new security technologies.
		Develop and implement an internal communication strategy to promote awareness of roles and responsibilities and enhance incident reporting procedures.	Increased organisational awareness and proactive cybersecurity culture.
Governance and Compliance.	IT security policy, cyber standards and regulatory requirements.	Appoint a cybersecurity officer responsible to oversee the cybersecurity strategy. Ensure alignment with industry standards and regulatory	Integrate CRMi strategies into the overall risk management framework of the organisation. Conduct audits and prepare detailed reports for man-

Table 6-1: Organisational Context (Step 1)			
Topic *(Responsibility)*	Input	Technique and Steps	Output
Topic continued.	*Input continued.*	requirements (e.g., ISO 27001, NIST).	agement and the cybersecurity officer, outlining findings and recommendations.
		Regularly audit vendor compliance to maintain strong cybersecurity postures.	Continuous compliance checks and mitigation of third-party risks.

Table 6-1: Organisational Context (Step 1)

6.11.2 Asset identification and evaluation (Step 2)

Step 2 focuses on the asset identification and evaluation stages. Here the assets are valued based on the medium-sized enterprise's focus to attain a stable and reliable business functions. These assets can be principally divided into two groups: those that are tangible e.g. hardware; and intangible properties, e.g., patents, industrial designs, and copyrights, along with technical aspects, such as non-disclosed know-how, commercial secrets, inventions, and manufacturing pro-cesses. This concept involves identifying and evaluating assets used within the medium-sized enterprise and the extent to which they could be adversely affected by a cyberattack, as shown in Table 6-2:

Table 6-2: Asset identification and evaluation (Step 2)			
Topic *(Responsibility)*	Input	Technique and Steps	Output
Assets *(Security Analyst and IT Manager).*	An overview and list of medium-sized enterprise's tangible and intangible properties, their core functionalities and subcomponents.	Assets profiling. Review of asset inventory, security policy, interviewing security analyst and physical observation of assets.	Description of assets, functions, and subcomponents owners, criticality and asset goals.
	Existing IT asset profile including hardware, software, data, and network resources.	Combine asset control principles with the organisation's security policies to ensure comprehensive asset management.	Enumeration of security goals and principles that each asset must achieve for sustained operations of the organisation.
	Asset profile along with its objectives (e.g. availability, accountability, confidentiality).	Employ asset criticality ranking to determine criticality level and impact (low to high) from unauthorised access.	Consistent, clear classification of assets by their criticality to organisational processes and functions.

Table 6-2: Asset identification and evaluation (Step 2)

6.11.3 Threat Indicator of compromise (Step 3)

With the third step, medium-sized enterprises should be aware of the data associated with cyberattacks, known as indicators of compromise (IOC). Tounsi and Rais (2018) divided these attributes of IOC into three distinct sub-classes. The sub-classes included a series of indicators associated with the network, such as IP and hostnames, including URLs and domain names, along with email attachments.

These potential cybersecurity issues and facets are summarised below in Table 6-3:

Table 6-3: Threat Indicator of compromise (Step 3)

Topic *(Responsibility)*	Input	Technique and Steps	Output
Threat *(Security analysist).*	Organisational assets and list of vulnerabilities provided by a list of software and hardware weaknesses (Common Weakness Enumeration, CWE).	Organisation to determine vulnerability profile and its ranking. Regularly conduct vulnerability assessments in systems, processes, and people to identify weaknesses in the IT infrastructure. Integrate a vulnerability management program for continuous monitoring, prioritisation, and periodic reviews.	A comprehensive vulnerability profile ranking vulnerabilities in assets.
	Organisational assets and list of threats provided by a list of attack pattern and its classification.	Gather and determine potential threats (malware, phishing, insider threats, physical theft). Use threat intelligence from various sources to analyse potential cyber threats on assets. Integrate advanced threat intelligence platforms for real-time monitoring and dynamic threat landscape awareness.	A comprehensive threat profile detailing potential threats to assets.

Table 6-3: Threat Indicator of compromise (Step 3)

6.12 Cyber-risk mitigation pillar (Steps 4 to 6)

Navigating the cybersecurity landscape requires a progression from establishing cyber security awareness to implementing risk mitigation strategies, which is set out in Steps 4 to 6. This includes the option of risk transfer in the form of securing cyber-risk insurance as a potential means to limit the financial repercussions. The following section outlines how each stage builds upon the previous one to form a comprehensive cyber-risk mitigation strategy, commence with Step 4.

6.12.1 Cyber security awareness (Step 4)

Cybersecurity awareness provides the means to evaluate and identify potential cyber threats and the associated risks. The medium-sized enterprise can implement training programmes for the entire staff and initiate various awareness campaigns to promote cybersecurity best practice, enable employees to become aware and knowledgeable of potential cybersecurity issues, reduce human error, and ultimately minimise the number of incidents caused by employee mistakes, such as falling for phishing scams. Through this awareness programme, the medium-sized enterprises security strategy can enable employees to become the first line of defence, as outlined below in Table 6-4:

Table 6-4: Cyber Security Awareness (Step 4)

Topic *(Responsibility)*	Input	Technique and Steps	Output
Awareness *(Manager and entire staff).*	Information from the organisation on protection, detection, incident response, and recovery measures.	All employees must be made aware of cyber-risks through training, starting with training in the onboarding phase.	A policy including an incident-reporting guideline.
	Importance of non-punitive reporting culture.	Staff should be made aware that reporting cases of trespass (e.g. accidental opening of attachment) will not result in negative consequences.	Enhanced reporting culture encouraging proactive communication of security incidents.
	Continuous updates and education on cyber-risks.	Employees should be subscribed to newsletters informing about up-to-date cyber-risk situations.	Ongoing employee awareness of current cybersecurity threats and best practices.

Table 6-4: Cyber Security Awareness (Step 4)

6.12.2 Cyber-risk mitigation (Step 5)

With the fifth step, creating a cyber-risk mitigation framework involves several key steps to ensure that the medium-sized enterprise can identify, assess, and respond to cyber threats effectively. While this study showed that medium-sized enterprises were taking initial steps to mitigate and transfer risk to varying degrees, effective cyber resilience could only commence when the business had established a clear cyber-risk baseline, where progress could be assessed and measured. By establishing a baseline, medium-sized enterprises can mitigate against risk by understanding their level of cyber security and maturity and how this relates to resourcing decisions together with their resilience strategies.

6.12.2.1 Preventive actions

The framework indicates the importance of implementing controls to prevent cyberattacks occurring, such as the usage of firewalls, intrusion detection systems (IDS), and antivirus software. Furthermore, these proposed actions of technical and directional nature can significantly reduce the risk of cyber incidents and enhance the overall security of the medium-sized enterprise, as shown below in Tables 6-5 and 6-6:

Table 6-5: Preventive cyber-risk mitigation techniques (Technical, Step 5)

Topic *(Responsibility)*	Input	Technique and Steps	Output
Regular software updates and patch management. *(IT and Security).*	Gather and prioritize known vulnerabilities from internal/ external sources. Software/Hardware Inventory. Details on available patches including organisational policies and procedures.	Run test patches in a controlled environment to validate that they do not disrupt operations or cause unexpected issues. Deploy and roll out patches to production systems based on priority and in alignment with the patch management policy. Verify the successful application of patches and communicate the results to relevant stakeholders. Ensure operating systems and software components are kept up to date with available updates and patches, including mobile devices.	Updated software: Systems with the latest patches to mitigate known vulnerabilities and improve security and functionality. Compliance reports. Improved security posture with reduced risk of exploitation. Patch logs and system stability reports. Alerts and notifications. Remediation of vulnerabilities that were previously identified, resulting in a lower risk profile for the organisation.

Table 6-5: Preventive cyber-risk mitigation techniques (Technical, Step 5)			
Topic *(Responsibility)*	Input	Technique and Steps	Output
Implementing multi-factor authentication (MFA).		Implement MFA to add an extra layer of security beyond just passwords.	Enhanced authentication security reducing risk of unauthorised access.
Encryption *Topic continued*	Software/Hardware (SW/HW) tools or devices used to perform the encryption, such as encryption libraries, dedicated HW, or integrated SW solutions.	Convert sensitive data to ensure its protection from unauthorised access. *Technique and Steps continued.*	Secure storage locations for encrypted data, ensuring data confidentiality. *Output continued.*
Network Traffic Control.	Security Policies which define acceptable network behaviour and security requirements.	Monitor, control and secure data packets. Utilizing firewalls and antivirus software on the central IT-system as well as on all individual devices to safeguard against external threats. Using antivirus software or endpoint detection and response on all systems, including on mobile devices. Filters must be set centrally by the IT-administrator(s).	Network traffic that is monitored, filtered, and secured against unauthorised access and threats. Access Control Logs and Incident Report which report on detected and mitigated security incidents. Reaching endpoint security, ensuring devices are secure and compliant with organisational policies. Security Alerts and Notifications: Real-time alerts about detected threats, suspicious activities, and potential security breaches. Updated Security Policies based on new threats, vulnerabilities, and lessons learned from incidents.
Regular security audits and penetration testing.	Information about potential threats, vulnerabilities, and attack patterns. User Credentials and digital certificates.	Perform periodic security audits and penetration tests to identify and address vulnerabilities within the system.	Comprehensive audit reports, detailing the findings of the security audit, including identified vulnerabilities, compliance gaps, and areas for improvement. Potential methods to remediate vulnerabilities An evaluation of the identified risks and their potential impact on the organisation.

Table 6-5: Preventive cyber-risk mitigation techniques (Technical, Step 5)			
Topic *(Responsibility)*	Input	Technique and Steps	Output
	Network Architecture including configurations.		Action plan next steps and measures to achieve compliance certification. Improved security posture: Enhance security measures and policies based on findings from audits and penetration tests.
Access rights.	A list of all levels of access rights must be kept.	Implement strict access controls and authentication mechanisms (e.g., MFA) to ensure only authorised personnel access sensitive systems. Apply least privilege principles and revoking unnecessary privileges.	Up-to-date list detailing user rights and access levels.
Certification	Certification policy and standards.	Execute a certification process to attain cybersecurity certifications like ISO 27001 or NIST.	Achieved certifications supporting CRMi strategy development.
E-Mail security.	Internal cybersecurity policy.	Set filters for suspicious Emails and direct them to a mailbox separate from the company's IT-system.	Trained employees aware of handling suspicious emails, reduced phishing risks.
Use of devices outside company premises.	Remote work policies.	Ensure data backups, encryption, and VPN usage. Restrict use of personal storage devices.	Secure remote access to company IT-system only via VPN. No use of private storage or other peripheral devices.
Disaggregation of IT-systems.	IT system architecture.	Segregate IT systems to separate user and admin rights. Restrict personal use of company devices.	Enhanced security through system segregation and minimised risk exposure.
Technical Preventive Controls *(IT Security Team).*	Security policies, patch management tools, and encryption standards. Network traffic monitoring solutions.	Implement continuous patch management for software and hardware vulnerabilities. Enforce encryption and multi-factor authentication (MFA). Monitor network traffic and implement proactive security	Reduced risk exposure through strengthened technical defences. Minimised attack surface with enhanced system hardening.

Table 6-5: Preventive cyber-risk mitigation techniques (Technical, Step 5)

Table 6-6: Preventive cyber-risk mitigation techniques (Directional, Step 5)			
Topic *(Responsibility)*	Input	Technique and Steps	Output
Employee training awareness and education. *(Trainers/experts or qualified instructors).*	Training materials, schedule, and metrics to measure training effectiveness. Training needs based on employee skill gaps. Employee input on training preferences.	Conducting regular training sessions to educate employees on recognising phishing attempts, using secure passwords, and following best practices for cybersecurity. Draft a secure password policy with mandatory renewals. Perform regular phishing simulations to educate employees on recognising and responding to phishing attacks. Integrate directional preventive controls, including security drills, and response simulations to enhance resilience.	Knowledgeable and skilled staff who is compliant with organisational standards, thereby contributing to the overall success and security of the organisation. Training records and compliance certifications. Improved performance and behavioural changes: enhance employee performance and productivity and adherence to company policies and procedures. Risk reduction with decreased likelihood of errors, security breaches, and non-compliance due to better-informed employees.
Incident Response Planning.	Internal policy	Develop and maintain an incident response plan. Conduct targeted incident response exercises and regular updates to align with evolving threats.	Effective and quick responses to security breaches.
Regular Audits and Assessments.		Conduct periodic security audits and assessments. Assess effectiveness of technical and directional preventive controls to identify gaps.	
Directional Preventive Controls *(Security Leadership & HR).*	Employee training programmes, security policies, and response planning frameworks.	Strengthen organisational resilience by integrating cybersecurity awareness into onboarding and training. Regularly update security policies and conduct simulated attack exercises. Conduct periodic security risk assessments focused on human factors and process improvements.	Improved incident preparedness and response. Increased employee engagement in cybersecurity practices. Reduced likelihood of breaches due to human error.

Table 6-6: Preventive cyber-risk mitigation techniques (Directional, Step 5)

6.12.2.2 Detective actions

An important aspect of Step 5, is the detection of potential cyber-risks and the mitigation techniques which could be used to identify and respond to this form of attack. These detection techniques can help the medium-sized enterprise to identify and respond to cyber threats promptly, whereby minimising the potential impact to the overall business activity, as shown in Table 6-7:

Table 6-7: Detective cyber-risk mitigation techniques (Step 5)

Topic *(Responsibility)*	Input	Technique and Steps	Output
Intrusion Detection Systems (IDS). *(IT or security personnel).*	Data on incoming and outgoing: • Network Traffic & logs, • System Activity, • User Activity & anomaly user behaviour, • Feeds about known threats.	IDS in order to monitor network and system activities for malicious activities or policy violations from unauthorised access and attacks. Monitors individual host systems for signs of intrusion.	Alerts and notifications when such activities are detected including classification in severity and urgency (e.g., critical to low). Incident and summary reports on status and detected threats. Recommendations for actions to be taken.
Endpoint Detection and Response.		Continuously monitor endpoints for signs of malicious activities and to facilitate rapid response to detected threats.	
Vulnerability Scanning.	IP Addresses: • names of the systems or devices, • Application URLs, • Usernames and Passwords.	Regularly scanning systems and networks for known vulnerabilities to ensure they are identified and addressed promptly.	List of identified vulnerabilities. Information about the systems, applications, or devices affected by each vulnerability. Suggested actions to mitigate or resolve each identified vulnerability. Detailed reports on incident causes, recommendations to prevent recurrence, and process improvement strategies.
Root Cause Analysis.	Incident data. System and process data. Statements from involved people.	Conducting thorough investigations to determine the root cause of security incidents. This helps in understanding how the incident occurred and identifying measures to prevent recurrence.	

Table 6-7: Detective cyber-risk mitigation techniques (Step 5)

6.12.2.3 Corrective actions

Linked to the above is the use of corrective cyber-risk mitigation techniques, which should involve the actions that are needed to address and limit the impact of the cyberattack. Implementing these corrective measures can help the medium-sized enterprise to effectively respond to and recover from a cyber incident, whereby minimising its influence and strengthening overall business security.

Table 6-8: Corrective cyber-risk mitigation techniques (Step 5)

Topic *(Responsibility)*	Input	Technique and Steps	Output
Inventory of IT-system. *(IT department)*	Inventory of all hard- and software components.	Update IT-inventory including mobile devices and tools such as VPN-software used by employees when working from outside company premises.	Refreshing the IT inventory yields numerous benefits, from maintaining operational efficiency and enhanced security to optimised resource allocation.
	Building automation technology including sensors and actuators for production (IoT devices).	These systems including any devices using IoT-technology must also be inventoried and their linkage to other IT-systems be analysed.	
Reaction to incident. *(IT department)*	Ransomware scenarios, incident response protocols.	Develop scenarios for responding to successful cyberattacks. Avoid ransom payments, rely on backups, consult experts for system restoration.	Minimised impact of attacks, effective incident containment, and rapid recovery.
Data backup and recovery plans.	Procedures for regular backups, test recoveries, secure storage media.	Establish a list of which data require back-up and at what frequency. Checks if backup storage media is separated from main IT-system and kept in secure location or in a cloud storage, which are all not directly linked to company IT-system.	Reliable data recovery to restore corrupted data following incidents, reduced data loss risks.
Communication and Reporting.	Stakeholders, employees, customers, and regulatory bodies. List of past incidents.	Communicate incidents transparently, outline response steps taken.	Maintained trust and transparency with stakeholders.
Third-Party Risk Management.	Vendor information. Data connection and exchange scripts.	Assess and manage risks associated with third-party vendors and partners in the overall supply chain.	Risk, compliance and performance reports help to make informed decisions, ensure compliance, and maintain

Table 6-8: Corrective cyber-risk mitigation techniques (Step 5)			
Topic *(Responsibility)*	Input	Technique and Steps	Output
Input continued	Technical evaluations of third-party systems.	*Technique and Steps continued.*	the overall security and performance of their third-party relationships.
Incident Response Plan.	Threat intelligence, incident alerts, policies, asset inventory, roles/contacts, forensic data, risk assessments.	Develop, implement and regularly update response plans to address incidents when they occur.	Enhanced readiness to contain and recover from incidents effectively.
Business Continuity (BCP) and Disaster Recovery (DRP) plan.	Draft BCP and DRP documents.	Develop, maintain, and test BCPs and DRPs through regular drills.	Continuity of critical business functions (BCP) and effective post-incident recovery of IT systems and data (DRP).
Third-Party Assessments.	Knowledgeable third-party security experts.	Evaluate organisation's incident response plans and remediation efforts through third-party assessments.	Objective evaluation of security posture with recommendations for improvement.

Table 6-8: Corrective cyber-risk mitigation techniques (Step 5)

6.12.3 Cyber-risk insurance (Step 6)

The sixth step is related to cyber-risk insurance (CRI). CRI is a critical component in the strategy to mitigate the financial impact caused by a cyberattack. Having CRI potentially provides the medium-sized enterprise with a financial safety net to cover losses related to data breaches, cyberattacks, and other information security breaches.

Table 6-9: Cyber-risk mitigation through cyber-risk insurance (Step 6)			
Topic *(Responsibility)*	Input	Technique and Steps	Output
Questionnaire *(Management)*	Series of questions insurance companies use to assess the organisation's cybersecurity posture and risk level.	Answering questions on the • firm's IT system, • network infrastructure, • and data management, • existing cybersecurity measures, • any malware defences, • access and administration privileges.	Overall assessment of vulnerability to cyberattacks and the effects on business. Conditions linked to the insurance will also inform management about necessary cyber-risk mitigation measures.

Table 6-9: Cyber-risk mitigation through cyber-risk insurance (Step 6)			
Topic *(Responsibility)*	Input	Technique and Steps	Output
Understanding Cyber-risk insurance (CRI).	Policy coverage limits and general conditions offered with regard to: • Data breaches, • Business interruption, • Cyber extortion payments, • Legal Expenses, • Incident response.	Checking offered insurance conditions and limits against potential losses from company assets compromised by various cyberattack scenarios.	Achieving clarity about what are the coverage elements of a CRI and to what monetary extent there are losses, expenses, and services covered from various cyber incident scenarios.
Mitigation benefits.		Verify if CRI offers financial protection, access to expertise, risk assessment support, and regulatory compliance.	Understanding CRI benefits in terms of risk reduction, loss mitigation, and qualitative service improvements.
Cost benefit analysis.	Offered policy terms and conditions. Risk Management Policy. Expense budget.	Assess Return on Security Investment (ROSI) by evaluating the potential financial impact of cyber incidents against insurance costs.	Guidance on the financial justification for CRI investment based on ROSI, risk reduction, operational efficiency, business resilience and strategic value (business continuity, reputation etc.).

Table 6-9: Cyber-risk mitigation through cyber-risk insurance (Step 6)

6.13 Operations success pillar (Steps 7 to 9)

Medium-sized enterprises that effectively identify their risk profile and implement measures to manage, mitigate, and transfer that risk, such as through comprehensive cyber-risk mitigation (CRMi) strategies, are better positioned to recover from the initial impact of a cyberattack. By adopting a sophisticated and holistic approach to cybersecurity, medium-sized enterprises can not only mitigate risks but also enhance their reputation as trusted business partners within the supply chain and the broader cybersecurity ecosystem. Business success, in this context, can be viewed as the ability to avoid or reduce potential losses resulting from cyberattacks.

In Step 7, the focus shifts to addressing residual losses, which are seen as a critical aspect in determining whether the business is successful after CRMi has been applied. Residual losses represent a key indicator in assessing the effectiveness of these measures and their influ-

ence on business continuity. Subsequently, this study emphasises the importance of adopting and using key success and performance indicators to achieve and sustain a level of enhanced business success.

6.13.1 Potential residual primary/secondary losses (Step 7)

Freund and Jones (2014), in their quantitative cybersecurity risk assessment approach, defined various types of cyber breaches that can lead to different claiming scenarios. Drawing on Freund and Jones' (2014) work, the framework proposed in this study is that cyber-risks can be segmented into six forms of losses, then further grouped dependent on whether those losses have a direct or indirect impact on the medium-sized enterprise. Direct losses can primarily affect the perceived value and replacement costs associated with the manufacturing assets involved, whereas indirect secondary losses refer to those downstream activities, such as competitive advantage, fines, or reputational damage.

Understanding the distinction between these losses is critical for medium-sized enterprises to effectively manage and mitigate the risks associated with a cyberattack. Through adopting this strategy, a medium-sized enterprise can repair or replace damaged systems and data, minimise indirect losses, such as a loss of customer trust and potential damage to brand reputation, which could lead to decreased sales and could adversely overall business performance.

The practical relevance of this segmentation was reinforced by the interview data generated from the German manufacturing medium-sized enterprise managers. These managers consistently identified business interruption losses caused by a system downtime as their primary concern, highlighting their openness to strategies focused on mitigating these tangible financial negative outcomes. These managers also emphasised the importance of managing the costs associated with repairing or replacing damaged systems and data. Other issues included secondary or indirect losses such as diminished customer trust, brand reputation damage, decreased sales, and client churn.

There were secondary costs, such as compliance requirements and the need for enhanced cybersecurity measures, which were often overlooked by these medium-sized enterprises. To address this gap, CRMi strategies must holistically target both direct and indirect losses, ensuring that they are designed to mitigate to meet acceptable levels while also reducing

the likelihood of future cyberattacks occurring again. Although cyber-risk insurance was not a high priority for the interviewed medium-sized enterprise managers, the strategy was recognised as being a potential mechanism to support the minimisation of both primary and secondary losses, especially after a severe cyberattack. Such insurance could provide economic benefits and business stability, fulfilling a critical need for medium-sized enterprises facing significant risk exposure.

6.13.2 Critical success factors and key performance indicators (Step 8)

Based on the findings of this study, key performance indicators (KPIs) and measurements of productivity were seen as an important theme, including ensuring that orders can be taken, sales can occur through to the supply and storage of raw materials. To contextualise this, Table 6-10 through the cyber-risk mitigation (CRMi) framework provides a mitigation strategy to address potential cyber-risks by identifying several key critical success factors (CSF) and positive outcomes.

Table 6-10: CSF and KPI (Step 8)

Critical success factors (CSFs)	Positive result of cyber-risk mitigation (CRMi)
Data Integrity and Confidentiality.	Protecting sensitive information from breaches and unauthorised access. This is crucial for maintaining trust with customers and partners.
Financial Stability.	Protecting the organisation's financial health by reducing direct financial losses, legal fees, and remediation costs.
Innovation and Growth.	Securing digital assets and ensuring the integrity of intellectual property. This can lead to a competitive advantage in the market.
Ensuring Business Continuity.	Helping to prevent disruptions caused by cyberattacks. This ensures that critical business operations can continue without significant downtime, which is essential for maintaining productivity and supply commitments.
Customer Trust and Loyalty.	Enhances customer's expectations regarding personal and financial information to be secure. This is critical for long-term success and customer retention.
Compliance and Regulatory Requirements.	Ensures compliance with business partner and regulatory requirements with regard to data protection and cybersecurity, thereby avoiding legal penalties and potential reputational damage. Many industries already demand to acquire an industry-recognised certification (e.g., TISAX).
Strategic Risk Management.	Allows for better strategic planning by identifying potential threats and implementing measures to counter them, aligning with long-term organisational goals.

Table 6-10: CSF and KPI (Step 8)

In summary, Table 6-10 above indicates how CRMi can directly support the various critical success factors by safeguarding key aspects of the medium-sized enterprise, which range from protecting data and ensuring compliance to maintaining customer trust and enabling continuous innovation.

As to the key performance indicators (KPIs), based on the study's outcome, there were various metrics to consider, including quality checks, meeting plan figures, sustainability, innovation, and a more advanced return on security investment (ROSI). Based on the framework, a medium-sized enterprise could use a range of relevant performance indicators to delineate the perceived value creation of their products and services, along with the relative costs of achieving this value. Adopting this CRMi-based approach enables KPIs to reflect the skills and resources available, serving as a differentiating factor in assessing the enterprise's performance, as shown in Table 6-11:

Table 6-11: CRMi positively influencing KPIs (Step 8)	
Key performance indicators (KPIs)	CRMi positively influences KPIs
Financial Impact.	Reduction in financial losses higher than security investments. This results in significant cost savings and better financial performance (ROSI).
System Uptime Percentage.	Enhances higher IT systems uptime and availability as the likelihood of downtime due to cyberattacks is reduced.
Data Breach Frequency.	Preventive cybersecurity measures reduce the frequency of data breaches. Fewer breaches indicate a more secure CRMi.
Productivity Metrics.	Improved cybersecurity translates into fewer disruptions and higher productivity levels for machinery output and employee efficiency.
Innovation Rate.	Encourages new product and service launches by securing digital assets and intellectual property.
Compliance Rates.	Precautionary investments in cybersecurity lower costs and possible fines for fulfilling any future certification, insurance obligations, or compliance with regulatory standards.
Incident Response Time.	Preventive, detective and corrective CRMi can detect and respond to incidents more quickly. This leads to a lower average incident response time, minimising potential damage and service disruption.
Employee Awareness and Training Completion Rate.	Higher completion rates of these programmes indicate a well-informed workforce capable of identifying and mitigating cyber-risks.

Table 6-11: CRMi positively influencing KPIs (Step 8)	
Key performance indicators (KPIs)	CRMi positively influences KPIs
Brand Sentiment Score.	Enhances an organisation's reputation, leading to positive brand sentiment and ultimately reflecting the organisation's perceived reliability and trustworthiness in the market.

Table 6-11: CRMi positively influencing KPIs (Step 8)

In summary, Table 6-11 CRMi can indicate through the various KPIs how to enhance the system's reliability, improving response times, ensuring compliance, protecting financial interests, and maintaining customer satisfaction and trust.

6.13.3 Business success (Step 9)

In the final step, business success is measured by the medium-sized enterprise's ability to generate a positive return on investment or profit. The question of how CRMi can contribute to the business success of medium-sized enterprises in the German manufacturing industry was outlined in the various stages, as presented above. In achieving business success CRMi can play a critical role in ensuring the long-term success and stability of the medium-sized enterprise in the event of a cyberattack. To achieve this, KPIs and CSFs can be used to anticipate and predict potential cybersecurity issues for the medium-sized enterprise, business partners, and other stakeholders. Business success can be achieved through fostering innovation and growth, but needs the prioritisation of operational resilience and protection of tangible and intangible assets. However, the challenge for medium-sized enterprises, as identified in this study, was the limited IT security management resources, and the lack of third-party involvement. Therefore, to meet future higher regulatory requirements, medium-sized enterprises may need to seek and adhered to cyber-risk insurance requirements through certification processes, and this proposed framework provide a potential additional roadmap.

6.14 Summary on the proposed cyber-risk mitigation framework

The cyber-risk mitigation (CRMi) framework as presented in this section, and throughout the study, is arguably essential for German-based manufacturing medium-sized enterprises to adopt, as the methodology can provide a structured approach to managing the growing risks

associated with a cyberattack and the potential outcomes. Cybercriminals are increasingly targeting medium-sized enterprises today, which is due not only to the ever-changing digital landscape and reliance on technology but also to the recognised lack of adequate protection. But by implementing a robust CRMi strategy, as advocated by this study, this proactive approach does provide several benefits that can help the medium-sized enterprise avoid becoming a victim of a cyberattack.

The proposed CRMi framework should firstly be adopted in German-based manufacturing medium-sized enterprises to protect the various business activities against cyber-threats such as data breaches, the usage of malware, and ransomware attacks. By identifying system vulnerabilities, these medium-sized enterprises can take suitable proactive measures to secure sensitive information, including customer, supplier, and financial data. The adoption of this methodology will also better prepare medium-sized enterprises to respond to cyber-related incidents if and when they occur, minimise potential damage, and speed up recovery times.

One of the key benefits available to these manufacturing medium-sized enterprises through the adoption of the proposed methodology is that it can provide and maintain business continuity throughout and following a cyberattack. Without proper cybersecurity measures in place, even a minor breach can lead to significant disruptions, halting business operations and potentially leading to financial and reputational damage. Through protecting critical assets, this proposed framework can reduce downtime and speed up the restoration of services. This continuity is crucial for maintaining customer trust, securing the reputational profile of the medium-sized enterprise, and avoiding costly interruptions.

Thirdly, from a financial perspective, business interruptions can become critical for medium-sized enterprises, as a cyberattack can negatively influence the financial stability of the business. This study indicates that the proposed CRMi framework can assist in maintaining long-term cost savings through reducing the associated expenses of recovering the business activities following a cyberattack.

The next and fourth benefit is having a comprehensive cybersecurity plan designed to safeguard the company's reputation. Data breaches and security incidents can severely damage a company's image, leading to a loss of customer trust and business. By protecting customer

data and maintaining high levels of security, medium-sized enterprises can build and maintain trust with their clients, partners, and other stakeholders, ensuring their reputation remains intact. From a German manufacturing medium-sized enterprise's perspective, there has been the increasing need to attain certain certifications, often requiring modifications to the existing delivery strategies when providing goods and services to larger business partners or being a part of a supply chain. Investing in proactive cybersecurity measures can assist medium-sized enterprises in attaining these accreditations. By being compliant, these medium-sized enterprises not only avoid potential financial losses but also demonstrate their commitment to data protection, further boosting trust amongst customers and partners.

Beyond any regulatory or business benefits, the fifth advantage associated with the cyber-risk framework is the enhancement of the operational efficiency of the medium-sized enterprise. By streamlining security processes, medium-sized enterprise business managers can make better use of resources and improve their overall IT infrastructure. This can lead to more informed decision-making regarding technology investment and staffing levels, thereby optimising the way cybersecurity is managed within the business.

The next and sixth advantage of implementing the proposed cyber-risk mitigation framework is the potential competitive advantage the methodology can offer. In an increasingly security-conscious market, businesses can demonstrate strong cybersecurity practices, which may lead to winning new contracts and clients, especially those from larger organisations that require partners to meet high standards of cyber resilience.

The seventh benefit is that this framework promotes employee cyber awareness and engagement. A comprehensive cyber-risk strategy often includes employee training embedded into the existing security best practices and awareness policies, thereby potentially reducing the risk of human error and data breaches. This can also mean that employees are made aware of the importance of cybersecurity, enhancing overall vigilance and reducing risk.

A well-structured cybersecurity framework offers a scalable and adaptable opportunity. As medium-sized enterprises grow, their cyber-risk mitigation strategies need to be able to be scaled up, ensuring that the company remains protected as it grows. The framework also has the flexibility to adapt to emerging threats, providing ongoing protection against new risks that arise as the cyberthreat landscape evolves, which is the eighth benefit.

Finally, the ninth benefit is having a robust cybersecurity framework, which can enhance the financial appeal to stakeholders. Stakeholders are increasingly focused on cybersecurity as a critical consideration when making informed financial decisions. This framework can demonstrate to stakeholders a strong commitment to managing cyber-risks, making the manufacturing medium-sized enterprise more attractive to potential investors. Furthermore, by protecting intellectual property and proprietary technology, these medium-sized enterprises can secure their innovations and avoid the costly consequences of cyber espionage or theft.

In conclusion, the proposed CRMi framework is crucial for German manufacturing medium-sized enterprises to adopt, in terms of enabling business activities to be protected against cyber threats, ensuring business continuity, reducing costs, safeguarding the company's reputation, ensuring regulatory compliance, improving operational efficiency, and enhancing competitiveness. The methodology also promotes a culture of security within the organisation and ensures the business remains agile in the face of ever-evolving cyber-risks, making the methodology an essential component for innovation and growth leading to long-term business success.

However, during this study, the interview partners had difficulty seeing and connecting CRMi strategies to the potential benefits of attaining business success. While there was a recognition of the benefits and the crucial role that CRMi can provide, the connection to long-term success and stability was not fully understood. While the medium-sized enterprises in this study showed an understanding as to how cybersecurity has grown in importance, there was also an acknowledgement of needing to prioritise operational resilience to protect their tangible and intangible assets. However, at the same time, there was limited IT security management resources allocated and a reluctance to engage with their competitors to share costs or to use third-party intelligence and cloud administrators.

6.15 Limitations of this study

The study attempted to provide a new perspective to understand the challenges faced by German based medium-sized enterprises in the manufacturing sector; however, there are several limitations. A key limitation was the difficulty in identifying willing interview partners for this study, which resulted in nine medium-sized enterprises participating. Part of the rea-

son for this can be attributed to the limited awareness and expertise, coupled with the perceived fear of reputational damage, security issues, and eventually potential legal concerns, which made the medium-sized enterprises hesitant to initially discuss their cybersecurity risks. However, as the interviews progressed, the medium-sized enterprise managers began to disclose before providing a critical insight into their experiences. These findings not only highlighted the key issues and challenges associated with CRMi, but also illustrated how cybersecurity protocols are implemented, and the underlying prioritisation of these solutions.

As this study was focused on providing a critical and rich insight into the operational priorities, perspectives, and challenges associated with cyberattacks, a generalised outcome was rejected. Although initially consideration was given to providing a generalised outcome, due to the limited access of the participants a larger sample size was not feasible, and therefore the study rejected a quantitative approach due to the limited number of medium-sized enterprise businesses prepared to participate. A quantitative study again was not feasible, but instead this project developed a new theoretical insight rather than validating pre-existing theory.

Another limitation of the study was the acknowledgement that the researcher was the only person who conducted the interviews and then analysed the data, which could potentially limit the findings. To address this, the researcher constantly reviewed the interview transcripts and the recording, in order to be immersed in the data. The researcher acknowledges that this approach could potentially taint or bias the data; however, the researcher actively pursued opportunities to discuss the findings with the participants, fellow doctorate candidates, and supervisors to constantly review and challenge the data analysis and its conclusions.

6.16 Areas of future research

Consideration was given to conducting a quantitative project, but as this study was focused on providing a critical and rich insight into the operational experiences, perspectives, and challenges associated with cyber-risk mitigation (CRMi) strategies in German-based manufacturing medium-sized enterprises, a generalised approach was rejected. Even though the initial motivation was to determine how CRMi can contribute to business success, it became

evident during the interviews that the participants did not perceive this connection as directly relevant to their operational priorities. However, this lack of focus on the link between CRMi and business success highlights a significant gap for future research, reinforcing the importance of this theme being explored further.

Although this study gave useful theoretical insights into cyber-risks, it was not possible to use a larger sample size because participants were not easy to get in touch with. This meant that a quantitative approach could not be used. The small number of medium-sized enterprise manufacturing businesses prepared to participate also resulted in the development of a new theoretical perspective rather than validating a pre-existing theory or methodology. Reflecting this, future research could expand on this study, by employing a larger, more diverse range of medium-sized enterprises to assess how CRMi strategies and frameworks directly influence business activities, including providing a sustainable success, such as profitability, growth, and innovation.

Another limitation of this study is that the researcher single-handedly collected and analysed the interview data, which could potentially create bias or restrict the outcome of the study. Although the researcher took steps to mitigate bias by rigorously reviewing interview transcripts and recordings, he did draw on his peers and supervisors to validate interpretations to enhance the reliability of the project. Future research could consider incorporating multiple researchers or reviewers to ensure a broader and more objective analysis of how CRMi can mitigate against potential cyber-risks.

Finally, future studies should explore the direct and indirect influence that CRMi can have on a business, including its sustainable success, by focusing on operational resilience, customer trust, profitability, and market competitiveness. Consideration may include conducting a longitudinal study to understand the long-term effects of CRMi strategies on business performance.

6.17 Summary of the Conclusion Chapter

This research has set out to evaluate the preparedness of German manufacturing medium-sized enterprises against cybercrime risks, by exploring how senior managers perceived the role of cyber-risk mitigation (CRMi) in a German-based medium-sized enterprise. An in-depth analysis of the findings related to the research questions led to the development of a

conceptual CRMi framework, which enabled the project to achieve its intended purpose. The outcome of the project has provided a significant contribution to both academic knowledge and practical business application, thereby offering new insights into cybersecurity practices, challenges, and opportunities for manufacturing medium-sized enterprises.

In addressing the study's aim, this project found that while these German manufacturing medium-sized enterprises generally demonstrated awareness of cyber-risks, their levels of preparedness and sophistication in addressing these potential threats varied. Most of the medium-sized enterprises had implemented basic cybersecurity initiatives such as firewalls, backups, VPNs, and employee training programmes. However, the extent of the effectiveness of these strategies was often dependent on the size of the company, available resources, and the leadership's prioritisation of cybersecurity. Part of the reason for this approach could be attributed to these medium-sized enterprises being constrained by financial and resource limitations, which had led to the ad hoc approaches to cybersecurity, exposing them to potential cyberattacks. This outcome was supported by Renaud (2016), who argued that medium-sized enterprises are largely unprepared for cyber threats and are therefore often used by cyberattackers as a backdoor to target larger organisations.

This study did show, however, that these German medium-sized enterprises did not completely neglect cybersecurity. While their focus tended to be on mitigating low-level threats such as phishing attacks or advanced threats like ransomware, supply chain vulnerabilities were not seen as a priority. This supports the findings by Mijnhardt et al. (2016), who similarly highlighted gaps in medium-sized enterprise preparedness against sophisticated cyber-threats.

This study has also uncovered a blend of technological and non-technological strategies employed by medium-sized enterprises to manage potential cyber-risks. Staff awareness training was seen and recognised as a fundamental aspect of a medium-sized enterprises' cybersecurity defence, particularly against external phishing activities, which aligns with Consoli et al.'s (2020) findings. However, the adoption of advanced solutions, such as AI-based or cloud-driven CRMi tools, was limited, reflecting concerns about cost, complexity, and a lack of perceived necessity (McLilly, 2020; Ncubukezi, 2020). Many of these medium-sized enterprises had delegated cybersecurity responsibilities to IT departments or individual employees, rather than integrating CRMi across the entire business, as advocated by Osborn and

Simpson (2018). The study found, however, that only when the medium-sized enterprises had experienced a cyberattack had this experience led to the business adopting a proactive cyber-risk strategy. This finding aligns with Armenia et al. (2021), who noted that medium-sized enterprises often prioritise response over prevention in their cybersecurity efforts, until a cyberattack occurs.

A key finding of the study was the widespread scepticism toward cyber-risk insurance (CRI). Although the medium-sized enterprise managers in this study were aware of CRI, the adoption rates were relatively low due to high premiums, the lack of understanding of the insurance coverage, and the stringent requirements for eligibility. Many of these medium-sized enterprise managers perceived themselves as being too small to be targeted by sophisticated attacks, reinforcing the belief that CRI was unnecessary. This scepticism aligns with Kavčič and Delak's (2019) contention that European SMEs tend not to be proactive in adopting CRI. To address this, the findings of this study indicated that insurers must develop tailored, cost-effective products to meet the specific needs of these SMEs. Furthermore, policymakers might consider mandating cybersecurity insurance or standards as a prerequisite for participating in large supply chains, whereby enhancing sector-wide resilience (Pfister & Lehmann, 2023).

At the commencement of the study, the relationship between CRMi and business success was seen as a critical theme. However, while some of those interviewed demonstrated a clear connection between robust CRMi strategies and sustained growth, many of the managers struggled to link cybersecurity directly to business outcomes such as profitability and competitiveness. This finding supports Wang et al.'s (2024) assertion that CRMi can serve a dual purpose, both as a defensive mechanism and a strategic enabler of business success, but needs to be recognised as such.

However, as the study progressed, the project led to the creation of a proposed conceptual CRMi framework that was specifically designed for German manufacturing medium-sized enterprises. The framework emphasises key areas for the medium-sized enterprise to focus on, such as risk identification and assessment, cost-effective mitigation strategies, and the alignment with business KPIs to evaluate ROSI and performance. The methodology also provides guidance on integrating CRI into broader risk management strategies. By following this

framework, medium-sized enterprises can enhance their cybersecurity strategies while ensuring operational and strategic objectives are met.

Reflecting on the above, this study has made several important contributions to academic knowledge. Firstly, the study has provided a new empirical insight from a senior manager perspective working in German manufacturing medium-sized enterprises, thereby addressing a critical gap in the literature, which has often relied on deskbound studies (e.g., AL-Dosari & Fetais, 2023; Pfister & Lehmann, 2023). By capturing these managerial perspectives, the research has provided a new insight into the decision-making processes, challenges, and attitudes toward CRMi measures in this economically vital sector. Secondly, the findings have revealed the main challenges faced by medium-sized enterprises in terms of cybersecurity. While Renaud (2016) contended that SMEs are not accurately prepared, these German medium-sized enterprises did demonstrate some basic preparedness but lacked advanced CRMi strategies or approaches. This finding indicates that these medium-sized enterprises had a continuum readiness to address a cyberattack rather than a binary strategy of being prepared. Thirdly, this study underscores the medium-sized enterprises' reluctance to adopt advanced CRMi tools, such as AI-driven or cloud-based solutions, due to cost concerns and preferences for localised control. These findings add to the original work of Ncubukezi (2020) and McLilly (2020), who emphasised the potential need for advanced cyber-risk technologies but did not address the barriers to their adoption. Fourthly, this study identified the associated scepticism toward CRI, which adds to the existing academic debate (e.g. Vieira et al., 2020), which has highlighted the potential of CRI; this study has revealed the underlying hesitancy to adopt this form of technological solution, including costs, coverage, and the perceived necessity, as being critical barriers. Finally, the study reinforces the link between CRMi and business innovation, supporting the argument of Wang et al. (2024) that cybersecurity fosters resilience and growth.

From a practical perspective, the study offers actionable recommendations for medium-sized enterprises, insurers, and policymakers. The development of a tailored CRMi framework, as created in this study, provides medium-sized enterprises with a practical roadmap for identifying risks, implementing cost-effective mitigation strategies, and aligning cybersecurity efforts with business objectives. This framework is designed to balance resource limitations with the need for robust security, whereby enabling medium-sized enterprises to

achieve ROI while minimising financial loss and operational disruptions (Heidt et al., 2019; Kazemargi & Spagnoletti, 2020;).

The findings also highlight the need for insurers to create medium-sized enterprise-specific CRI products that address financial and operational constraints. Policymakers are encouraged to consider mandatory cybersecurity standards or insurance requirements for medium-sized enterprises in larger supply chains, ensuring sector-wide security and compliance is attained (Pfister & Lehmann, 2023).

Furthermore, this study emphasises the importance of continuous employee training programmes to address evolving cyber-threats. Proactive approaches, such as phishing simulations, can improve staff vigilance and reduce human error (Consoli et al., 2020; Quesada, 2016). Finally, the integration of CRMi with innovation initiatives offers medium-sized enterprises a pathway to resilience and competitive differentiation, enabling these businesses to capitalise on growth opportunities in a rapidly changing digitalised economy.

Despite these contributions, this study is not without its limitations. A key challenge for this study was the difficulty in securing willing interview partners, resulting in a sample of nine medium-sized enterprises. This limitation could be attributed to the participants' perceived fear of reputational damage, concerns about security and legal implications, and a general reluctance to discuss cybersecurity risks openly. However, once the interviews had begun, the participants became more open, offering critical insights into their experiences and challenges with CRMi.

Building on this study, future research should address the limitations of this study and further explore the relationship between CRMi and business success, which was the initial focus of the project. While this study originally sought to examine this link, the participants did not prioritise the connection during the interviews, highlighting a critical gap that indicates the need for further research. Expanding the sample size and employing a quantitative approach would also enable broader generalisability and statistical validation to occur. Future research could also explore the adoption of advanced CRMi technologies like AI-driven tools and cloud solutions, focusing on their potential to enhance both cybersecurity and organisational performance, together with the benefits associated with collaborative activities. Finally, consideration should be given to researching the tailoring of insurance products and regulatory mandates by insurers and policymakers.

6.18 Personal reflection

The decision to pursue my PhD was an easy one; for over a decade, it had been my dream to delve deeper into a specific subject scientifically. I began the PhD program at the University of Gloucestershire with great enthusiasm. However, unforeseen changes in my personal and professional life, compounded by the profound impact of COVID-19 on my economic and social circumstances, forced me to set aside my dreams and reassess my path. As years of unproductivity passed, I found myself on the verge of giving up. The PhD course leader sent me an alert letter, inquiring about my willingness to continue as the maximum period of study was nearing its end. Deciding to remain in the programme required deep introspection to rediscover my motivation for pursuing this goal. Recognising that I had never abandoned a project, no matter how challenging, and with only a year and a half remaining, my determination to complete the programme intensified. This journey of perseverance became a defining chapter in my life.

After enrolling, I initially believed that with my intellect and willingness to study hard while maintaining a full-time job, I could successfully complete the programme within the remaining time. I quickly realised how mistaken I was. During the second residency, it became clear that my writing and research would be scrutinised at a much higher level of professionalism. Research, which had once felt like an extension of my prior academic and corporate experiences, now required a deeper level of rigour and critical analysis.

This doctoral journey was not merely an academic exercise; it transformed me personally and professionally. I honed my writing and critical thinking skills, cultivated patience and perseverance, and, most importantly, learned the value of constructive criticism. These qualities will undoubtedly serve me in future endeavours, whether academic, professional, or personal.

When I began exploring the topic of cyber-risk mitigation in German manufacturing medium-sized enterprises, I approached it with an open mind. Although my background in mathematical analytics and (re)insurance provided a strong foundation, I entered the research process with no preconceived notions about the subject. I sought to learn from managers of mid-sized companies who were navigating the complex integration of intelligent digital technologies into manufacturing processes, addressing increasingly sophisticated cyber threats, and deciding on appropriate mitigation strategies.

Initially, I was both hopeful and excited about recruiting participants for my study. However, I quickly encountered challenges. Cybersecurity and preparedness are deeply confidential topics for most companies, making it exceedingly difficult to find enough managers willing to share their experiences openly. Despite these obstacles, I persevered and managed to gather valuable insights from those who agreed to participate. Their perspectives illuminated the diverse approaches medium-sized enterprises take to balance the pressing need for cybersecurity with their unique corporate philosophies and traditions.

The findings from my study revealed not only the challenges medium-sized enterprises face but also the untapped opportunities for further education and research in this field. The conversations I had with participants were inspiring—they reflected a group of professionals who were not only passionate about their work but also pragmatic in their approach to cyber-risk mitigation. Their commitment to their organisations, combined with a clear understanding of cybersecurity's importance, offered valuable insights into the intersection of technology, strategy, and tradition.

This research has deepened my appreciation for the process of inquiry and the contributions it can make to both academic and professional domains. It has reinforced my passion for exploring complex problems and generating new knowledge. Furthermore, the study has sparked my interest in potentially expanding this line of research in the future. The themes and topics uncovered during my study present numerous opportunities for further exploration, particularly as cybersecurity continues to evolve in response to emerging threats.

Looking back, this journey was not just about earning a doctoral degree—it was about resilience, growth, and rediscovery. It reminded me of the importance of staying true to my goals, even when the path forward seemed uncertain. Completing this research study has not only strengthened my skills but also renewed my belief in the transformative power of education. I am grateful for the challenges I encountered along the way, as they have shaped me into a more determined and reflective researcher.

This experience has been profoundly rewarding, and I am excited to see how the knowledge and skills I have gained will contribute to my future endeavours. I now understand that the pursuit of knowledge is not a destination but a lifelong journey—one that I am proud to continue.

References

Abl. of the EU L 124/36 of 20.05.2003, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32003H0361

Adamos, K., Filippopoulos, I., Stergiopoulos, G., & Gritzalis, D. (2023). A Survey on National Cyber Emergency Plans. *European Conference on Cyber Warfare and Security*, 22(1), 1-11.

Ajuzie, G. (2019). *Cybercrime prevention among small businesses in the greater houston area: A qualitative exploratory case study.* Doctoral Dissertation. University of Phoenix.

Ajzen, I. (1991). The Theory of planned behavior. *Organizational Behavior and Human Decision Processes*. *50*(2), 179-211.

Aken, J. E. V. (2004). Management research based on the paradigm of the design sciences: the quest for field-tested and grounded technological rules. *Journal of management studies*, 41(2), 219-246.

Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. *2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA)*. IEEE.

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber riskc. Journal of Financial Stability, 60, 100989.

AL-Dosari, K., & Fetais, N. (2023). Risk-management framework and information-security systems for small and medium enterprises (SMES): A meta-analysis approach. *Electronics*, 12(17), 3629.

Allianz. (2021). *Allianz Riskbarometer*. Retrieved 23.06.2023 from https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2021.pdf

Allianz. (2023). *Allianz Riskbarometer*. Retrieved 23.06.2023 from https://www.allianz.com/en/press/news/studies/230117_Allianz-Risk-Barometer-2023.html

Alvesson, M., & Deetz, S. (1999). *Doing critical management research*. Sage.

Anderson, R., & Moore, T. (2006). The economics of information security. S*cience*, *314*(5799), 610-613.

Antman, E. M., Lau, J., Kupelnick, B., Mosteller, F., & Chalmers, T. C. (1992). A comparison of results of meta-analyses of randomized control trials and recommendations of clinical experts: treatments for myocardial infarction. *Jama*, 268(2), 240-248.

Armenia, S., Angelini, M., Nonino, F., & Palombi, G. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support, 147*, 113580.

Armenia, S., Franco, E. F., & Nonino, F. (2019). Towards the definition of a dynamic and systemic assessment for cybersecurity risks. *Systems research and behaviourl science*, *36*(4), 404-423.

Ashby, S., Bryce, C., & Ring, P. (2018). *Risk and the strategic role of leadership*. City University of London.

Astor, M., Rammer, C., Klaus, C., & Klose, G. (2016). *Endbericht: Innovativer Mittelstand 2015-Herausforderungen, Trends und Handlungsempfehlungen für Wirtschaft und Politik*. ZEW-Gutachten und Forschungsberichte.

Aurelien, J. (2021). *Exploring Effective Defensive Cybersecurity Strategies for Small Businesses - Doctoral Dissertation*. Colorado Technical University.

Babbie, E. R. (2020). *The practice of social research*. Cengage Au.

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*(3), 393-410.

Bartsch, M., Gentemann, L., Kob, T., Krösmann, C., Mille, M., Petri, A., Ritter, T., Rost, P., Schmidt, S., & Schulz, M. (2018). Spionage, Sabotage und Datendiebstahl–Wirtschaftsschutz in der Industrie. *Studienbericht*, 60.

Baxter, J., & Eyles, J. (1997). Evaluating qualitative research in social geography: establishing 'rigour'in interview analysis. *Transactions of the Institute of British geographers*, *22*(4), 505-525.

Becker, S., Bryman, A., Ferguson, H., & Ferguson, T. H. (Eds.). (2012). *Understanding research for social policy and social work: themes, methods and approaches*. Policy Press.

Bell, S. (2017). Cybersecurity is not just a'big business' issue. *Governance Directions*, *2017*, 536-539.

Bent, S., Shojania, K. G., & Saint, S. (2004). The use of systematic reviews and meta-analyses in infection control and hospital epidemiology. A*merican journal of infection control*, 32(4), 246-254.

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, *63*(4), 531-540.

BERA (2018). *Ethical Guidelines for Educational Research*, Fourth edition (2018). Retrieved 25.06.2024 from https://www.bera.ac.uk/publication/ethical-guidelines-for-educational-research-2018

Binkhorst, V. (2020). I*mproving Cyber Risk Communication: Mental Models of VPN in a professional services firm in the Netherlands*.

Bitkom (https://www.bitkom.org/sites/main/files/2023-01/221125StudieIndustrie-40-1.pdf)

Blaikie, N. (2007). *Approaches to social enquiry: Advancing knowledge*. Polity.

Boell, S. K., & Cecez-Kecmanovic, D. (2015). On being 'systematic'in literature reviews in IS. *Journal of Information Technology*, 30(2), 161-173.

Boletsis, C., Halvorsrud, R., & Pickering, J. B. (2021). *Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment* Proceedings of the 16th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISIGRAPP 2021),

Boote, D. N., & Beile, P. (2005). Scholars before researchers: On the centrality of the dissertation literature review in research preparation. *Educational researcher*, 34(6), 3-15.

Braun, V., & Clarke, V. (2023). Toward good practice in thematic analysis: Avoiding common problems and be (com) ing a knowing researcher. *International journal of transgender health*, *24*(1), 1-6.

Bravo-Moreno, A. (2003). Power games between the researcher and the participant in the social inquiry. *The Qualitative Report*, 8(4), 624-639.

Brinkmann, S., & Kvale, S. (2005). Confronting the ethics of qualitative research. *Journal of Constructivist Psychology*, 18(2), 157-181.

Brocke, J. v., Simons, A., Niehaves, B., Niehaves, B., Reimer, K., Plattfaut, R., & Cleven, A. (2009). Reconstructing the giant: On the importance of rigour in documenting the literature search process. *ECIS*, 2206-2217.

Brown, S., Fox, S., Hewage, C., & Khan, I. (2022). Threat modelling of cyber physical systems: A real case study based on window cleaning business. *SN Computer Science*, *3*, 139.

Bryman, A. (2017). Quantitative and qualitative research: further reflections on their integration. *In Mixing methods: Qualitative and quantitative research*, (pp. 57-78). Routledge.

Bryman, A. (2016). *Social research methods*. Oxford University Press.

Bryman, A., & Bell, E. (2015). *Business research methods*, Oxford University Press: Oxford, UK.

Bryman, A. and Bell, E. (2017) *Business Research Methods*. Ethical Considerations Oxford University Press: Oxford, UK

BSA (2017). Statement of Ethical Practice (2017). Retrieved 25.06.2024 from. https://www.britsoc.co.uk/media/24310/bsa_statement_of_ethical_practice.pdf

BSI. (2024). *CERT-Bund-Reports - Offene SSDP-server*. Bundesamt für Sicherheit in der Informationstechnik. Retrieved 05.04.2024 from https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/CERT-Bund-Reports/HowTo/Offene-SSDP-Server/Offene-SSDP-Server_node.html#:~:text=Das%20Simple%20Service%20Discovery%20Protocol,SSDP%20verwendet%20Port%201900%2Fudp.

Burr, V. (2015). *Social constructionism*. Routledge.

Burr, V., & Dick, P. (2017). Social constructionism. *The Palgrave handbook of critical social psychology*, 59-80.

BVMV. (2022). *Der Mittelstand ist Garant für Stabilität und Fortschritt*. Der Mittelstand BVMV e.V. Retrieved 20.09.2022 from https://www.bvmw.de/de/der-verband/%C3%BCber-uns/zahlen-fakten

Carías, J. F., Borges, M. R., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). Systematic approach to cyber resilience operationalization in SMEs. *IEEE access*, *8*, 174200-174221.

Carías, J. F., Arrizabalaga, S., & Labaka, L. (2021). Cyber resilience self-assessment tool (CR-SAT) for SMEs. *IEEE Access*, *9*, 80741-80762.

Carmines, E. G., & Zeller, R. A. (1979). *Reliability and validity assessment*. Sage publications.

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems*, *44*.

Cartagena, S., Gosrani, V., Grewal, J., & Pikinska, J. (2020). Silent cyber assessment framework. *British Actuarial Journal*, 25, e2.

Cebula, J. J., & Young, L. R. (2010). A taxonomy of operational cyber security risks. *Software Engineering Institute, Carnegie Mellon University*

Charmaz, K. (2014). Constructing grounded theory.

Chaudhary, S., Gkioulos, V., & Goodman, D. (2023, February). *Cybersecurity Awareness for Small and Medium-Sized Enterprises (SMEs)*: Availability and Scope of Free and Inexpensive Awareness Resources. In Computer Security. ESORICS 2022 International Workshops: CyberICPS 2022, SECPRE 2022, SPOSE 2022, CPS4CIP 2022, CDT&SECOMANE 2022, EIS 2022, and SecAssure 2022, Copenhagen, Denmark, September 26–30, 2022, Revised Selected Papers (Vol. 13785, p. 97). Springer Nature.

Cipriani, A., & Geddes, J. (2003). Comparison of systematic and narrative reviews: the example of the atypical antipsychotics. *Epidemiology and psychiatric sciences*, 12(3), 146-153.

Cohen, L., Manion, L., & Morrison, K. (2013). The ethics of educational and social research. In *Research methods in education,* (pp. 99-128). Routledge.

Cohen, M. A., & Lee, H. L. (2020). Designing the right global supply chain network. *Manufacturing & Service Operations Management*, 22(1), 15-24.

Colicchia, C., & Strozzi, F. (2012). Supply chain risk management: a new methodology for a systematic literature review. *Supply Chain Management: an International Journal*, 17(4), 403-418.

Collins, J. A., & Fauser, B. C. (2005). Balancing the strengths of systematic and narrative reviews. *Human reproduction update*, 11(2), 103-104.

Consoli, A., & Kovatcheva, E. (2019). Cybersecurity Training for SME: Filling The Gap or Corporate Strategy? In *ICERI2019 Proceedings* (pp. 10434-10443). IATED.

Consoli, A., Kovatcheva, E., & Nesurini, A. M. (2020, //). *CYBER-SECURITY AWARENESS FOR SME MANAGERS* 13th annual International Conference of Education, Research and Innovation - ICERI2020 Proceedings,

Conteh, N. Y., & Royer, M. D. (2021). The unprecedented rise in cybercrime and the role of the human vulnerability factor. In *Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention* (pp. 32-43). IGI Global.

Cook, D. J., Greengold, N. L., Ellrodt, A. G., & Weingarten, S. R. (1997). The relation between systematic reviews and practice guidelines. *Annals of internal medicine*, 127(3), 210-216.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on risk and insurance-Issues and practice*, *47*(3), 698-736.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: Choosing among five approaches*. Sage publications.

Crotty, M. (1998). *The foundations of social research: Meaning and perspective in the research process.* Sage publications.

Crowther, D., & Lancaster, G. (2012). *Research methods*. Routledge.

Cyber, X. (2019). *Global ICS & IIoT Risk Report. A data-driven analysis of vulnerabilities in our industrial and critical infrastructure*. CyberX Labs.

Dash, B., Ansari, M. F., Sharma, P., & Ali, A. (2022). Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review. *International Journal of Software Engineering & Applications (IJSEA)*, *13*(5)

Dayalan, M. (2017). Cyber Risks, the Growing Threat. *International Journal of Novel Research and Development*, *2*(9)

de Oliveira, L. S., Soares Echeveste, M. E., Cortimiglia, M. N., & Gularte, A. C. (2019). Open innovation in regional innovation systems: Assessment of critical success factors for implementation in SMEs. *Journal of the Knowledge Economy*, *10*, 1597-1619.

Dijkers, M. P. (2009). The value of "traditional" reviews in the era of systematic reviewing. American *Journal of Physical Medicine & Rehabilitation*, 88(5), 423-430.

Dimitrov, W., & Rasheva-Yordanova, K. (2019). Toward Overcoming The Disproportion Between The Demand For Professionals And The Provision Of Training In Cybersecurity. In *Proceedings of EDULEARN19 Conference 1st-3rd July 2019* (pp. 1656-1664). IATED.

Dixon-Woods, M., Agarwal, S., Jones, D., Young, B., & Sutton, A. (2005). Synthesising qualitative and quantitative evidence: a review of possible methods. *Journal of health services research & policy*, 10(1), 45-53.

Dutta, N., Jadav, N., Tanwar, S., Sarma, H. K. D., Pricop, E., Dutta, N., Jadav, N., Tanwar, S., Sarma, H. K. D., & Pricop, E. (2022). Introduction to cybersecurity. In N. Dutta, N. Jadav, S. Tanwar, H. Kumar, D. Sarma, & E. Pricop (Eds.), *Cyber Security: Issues and Current Trends* (pp. 1-16). Springer.

Easterby-Smith, M. T., & Thorpe, R. R. & Lowe, A.(2002) *Management Research: An Introduction*. Sage

Easterby-Smith, M., Thorpe, R., & Jackson, P. R. (2012). *Management research*. Sage.

Easterby-Smith, M., Jaspersen, L. J., Thorpe, R., & Valizade, D. (2021). *Management and business research*. Sage.

Eilts, D. (2020). *An empirical assessment of cybersecurity readiness and resilience in small businesses - A dissertation report submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Information Systems*. College of Computing and Engineering Nova Southeastern University.

EIOPA. (2019). *Cyber Risk for Insurers - Challenges and Opportunities*. Luxemburg: EIOPA.

El Baz, J., & Ruel, S. (2021). Can supply chain risk management practices mitigate the disruption impacts on supply chains' resilience and robustness? Evidence from an empirical survey in a COVID-19 outbreak era. *International Journal of Production Economics*, *233*, 107972.

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, *17*(5), 474-491.

ENISA. (2016). Cyber Insurance: Recent Advances, Good Practices and Challenges. European Union Agency for Network and Information Security (ENISA).

Falkner, E. M., & Hiebl, M. R. (2015). Risk management in SMEs: a systematic review of available evidence. *The Journal of Risk Finance*, *16*(2), 122-144.

Farao, A., Panda, S., Menesidou, S. A., Veliou, E., Episkopos, N., Kalatzantonakis, G., Mohammadi, F., Georgopoulos, N., Sirivianos, M., & Salamanos, N. (2020). *SECONDO: A platform for cybersecurity investments and cyber insurance decisions. In Trust, Privacy and Security in Digital Business*: 17th International Conference, TrustBus 2020, Bratislava, Slovakia, September 14–17, 2020, Proceedings 17 (pp. 65-74). Springer.

Fink, A. (2019). *Conducting research literature reviews: From the internet to paper*. Sage publications.

Franke, U., & Meland, P. H. (2019). Demand side expectations of cyber insurance. In *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)* (pp. 1-8). IEEE.

Frels, R. K., & Onwuegbuzie, A. J. (2013). Administering quantitative instruments with qualitative interviews: A mixed research approach. *Journal of Counseling & Development*, *91*(2), 184-194.

Freund, J., & Jones, J. (2014). *Measuring and managing information risk: a FAIR approach*. Butterworth-Heinemann.

Garzoni, A., De Turi, I., Secundo, G., & Del Vecchio, P. (2020). Fostering digital transformation of SMEs: a four levels approach. *Management Decision*, *58*(8), 1543-1562.

Gill, J. and Johnson, P. (2002) *Research Methods for Managers*. Third Edition, Sage Publications Ltd., New York.

Gill, J., & Johnson, P. (2010). R*esearch methods for managers*. Sage Publications.

Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action. *MIS quarterly*, *41*(3), 703-A716.

Goodwin, D., Mays, N., & Pope, C. (2020). Ethical issues in qualitative research. *Qualitative research in health care*, 27-41.

Google. (2022). *Google Scholar*. Retrieved 15.11.2022 from https://scholar.google.com/

Gray, J. R., & Grove, S. K. (2020). *Burns and Grove's The Practice of Nursing Research-E-Book: Appraisal, Synthesis, and Generation of Evidence*. Elsevier Health Sciences.

Greenhalgh, T. (1997). How to read a paper: Papers that summarise other papers (systematic reviews and meta-analyses). Bmj, 315(7109), 672-675.

Grocke, D. (2017). Emerging cybersecurity threats in large and small firms. *Bulletin (Law Society of South Australia)*, *39*(3), 20-22.

Guba, E. G. (1990). The paradigm dialog. Sage Publications Inc.

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research*, (pp. 105–117). Sage Publications, Inc.

Hahn, A. (2016). Operational technology and information technology in industrial control systems. In E. J. Colbert & A. Kott (Eds.), *Cyber-security of SCADA and other industrial control systems* (pp. 51-68). Springer.

Hammersley, M. (1990). *Reading ethnographic research: A critical guide*. Routledge.

Hart, C. (2018). *Doing a literature review: Releasing the research imagination*. Sage Publications.

Hatch, M. J., & Cunliffe, A. L. (2006). *Organization Theory: Modern, Symbolic and Postmodern Perspectives*. Oxford University Press.

He, C. Z., Frost, T., & Pinsker, R. E. (2020). The impact of reported cybersecurity breaches on firm innovation. *Journal of Information Systems*, *34*(2), 187-209.

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the security divide between SME and large companies: How SME characteristics influence organizational IT security investments. *Information Systems Frontiers*, 21, 1285-1305.

Hermann, M. (1986). Effects of Speech and Interview Materials on Profiles of Leaders at a Distance: A Validation Exercise. *Report prepared for Defense Systems, Inc. as part of Contract DSI-85-1240*

Higgins, J. P., & Green, S. (2008). *Cochrane Handbook for Systematic Reviews of Interventions*. The Cochrane Collaboration.

Holsti, O. R. (1969). *Content analysis for the social sciences and humanities*. Addison-Wesley.

Hoppe, F., Gatzert, N., & Gruner, P. (2021). Cyber risk management in SMEs: insights from industry surveys. *The Journal of Risk Finance*, 22(3/4), 240-260.

Hubbard, D. W., & Seiersen, R. (2023). *How to measure anything in cybersecurity risk*. John Wiley & Sons.

Huberman, M. (1995). Networks that alter teaching: Conceptualizations, exchanges and experiments. *Teachers and teaching,* 1(2), 193-211.

Idahosa, M. D. (2020). *Strategies for Implementing Successful IT Security Systems in Small Businesses - Doctoral Dissertation*. Walden University.

IHK-Bayern. (2023). *Firmendaten im Internet*. Industrie- und Handelskammern in Bayer. Retrieved 10.09.2023 from https://firmen-in-bayern.de/sites/fitby/imprint.aspx

Ishikawa, T. (2017). *A Study on Evaluation Methodology of Cybersecurity Investment - Doctoral Dissertation*. Kyushu University.

ISO. (2022). *ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. International Organization for Standardization.

ISO/IEC 2700. (2022). *Information securtiy, cybersecurity and privacy protection - Information security managmeent systems - Requirements*. International Organization for Standardisation.

IT Governance. (2023). *Cyber Security Solutions*. Retrieved 20.06.2023 from https://www.itgovernance.co.uk/cyber-security-solutions

Jackson, K., & Bazeley, P. (2019). *Qualitative data analysis with NVivo*. Sage Publications.

Jain, S. (2022). *The Significance of Cyber Insurance in the Manufacturing Sector* - CXO Outlook. CXO Outlook. Retrieved 20.03.2023 from https://www.gajshield.com/index.php/resources/gajshield-blogs/292-the-significance-of-cyber-insurance-in-the-manufacturing-sector-3

Jbair, M., Ahmad, B., Maple, C., & Harrison, R. (2022). Threat modelling for industrial cyber physical systems in the era of smart manufacturing. *Computers in Industry*, *137*, 103611.

Jimenez-Sanchez, K. (2017). *Insurance can help strengthen cyber resilience as risks evolve*. Swiss Re. Retrieved 20.03.2023 from https://www.reinsurancene.ws/insurance-can-help-strengthen-cyber-resilience-as-risks-evolve-swiss-re/

Johnson, B. T. (1989). *DSTAT: Software for the meta-analytic review of research literatures*. Hillsdale, NJ: Lawrence Erlbaum.

Kalhoro, S., Rehman, M., & Ponnusamy, V. (2021). Extracting key factors of cyber hygiene behaviour among software engineers: A systematic literature review. *IEEE Access*, *9*, 99339-99363.

Kapoor, K., Renaud, K., & Archibald, J. (2018). *Preparing for GDPR: helping EU SMEs to manage data breaches*. AISB 2018: Symposium on Digital Behaviour Interventions for Cyber-Security, Liverpool.

Kavčič, T., & Delak, B. (2019). State of the cyber insurance products within Slovenian insurance companies. *Online Journal of Applied Knowledge Management*, *7*(2), 56-68.

Kazemargi, N., & Spagnoletti, P. (2020). IT investment decisions in industry 4.0: evidences from SMEs. In *Digital Business Transformation: Organizing, Managing and Controlling in the Information Age* (pp. 77-92). Cham: Springer International Publishing.

Kejwang, B. (2022). Effect of cybersecurity risk management practices on performance of insurance sector: A review of literature. *International Journal of Research in Business and Social Science*, *11*(6), 334-340.

Kemmis, S., McTaggart, R., Nixon, R., Kemmis, S., McTaggart, R., & Nixon, R. (2014). Introducing critical participatory action research. *The action research planner: Doing critical participatory action research*, 1-31.

Kenneally, E. (2021). Ransomware: a Darwinian opportunity for cyber insurance. *Connecticut Insurance Law Journal*, 28(1), 165. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3849120 https://cilj.law.uconn.edu/wp-content/uploads/sites/2520/2022/04/Ransomware-Kenneally-CILJ-Vol.-28.1.pdf

Khan, F., Kim, J. H., Mathiassen, L., & Moore, R. (2021). Data breach management: an integrated risk model. *Information & Management*, *58*(1), 103392.

Kim, L. (2022). Cybersecurity: Ensuring confidentiality, integrity, and availability of information. In *Nursing Informatics: A Health Informatics, Interprofessional and Global Perspective* (pp. 391-410). Springer.

King, N. (2004). 21——using templates in the thematic analysis oftext——. *Essential guide to qualitative methods in organizational research*, *256*.

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering*. Keele University - Department of Computer Science.

Kivimaa, K. (2017). *How to increase SME's trust in Cloud Service Providers - MSc-thesis*. School of Computing, National College of Ireland.

Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: factors of success. *Entrepreneurship and Sustainability Issues*, *6*(4), 2081.

Klotz, A., & Prakash, D. (2008). *Qualitative methods in international relations*. Springer.

Klykken, F. H. (2022). Implementing continuous consent in qualitative research. *Qualitative Research*, 22(5), 795-810.

Kosub, T. (2015). Components and challenges of integrated cyber risk management. *Zeitschrift für die gesamte Versicherungswissenschaft*, *104*, 615-634.

Kraus, B. (2019). Relational constructivism and relational social work. In The Routledge handbook of critical social work (pp. 93-104). Routledge.

Krippendorff, K. (2018). *Content analysis: An introduction to its methodology*. Sage publications.

Kumar, S., Biswas, B., Bhatia, M. S., & Dora, M. (2021). Antecedents for enhanced level of cyber-security in organisations. *Journal of Enterprise Information Management*, *34*(6), 1597-1629.

Labunets, K., Pieters, W., & Eeten, M. v. (2020). The Cyber Insurance Landscape. In *Security Risk Models for Cyber Insurance* (pp. 11-26). Taylor & Francis.

Ladhani, S., & Williams, H. C. (1998). The management of established postherpetic neuralgia: a comparison of the quality and content of traditional vs. systematic reviews. *British Journal of Dermatology*, 139(1), 66-72.

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659-671.

Lee, S. Z. (2020). A basic principle of physical security and its link to cybersecurity. *International Journal of Cyber Criminology*, *14*(1), 203-219.

Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science*, 9.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS quarterly*, 71-90.

Lincoln, Y. S., Lynham, S. A., & Guba, E. G. (2011). Paradigmatic controversies, contradictions, and emerging confluences, revisited. *The Sage handbook of qualitative research*, 4(2), 97-128.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Sage.

Locke, E. A. (2007). The case for inductive theory building. *Journal of management*, *33*(6), 867-890.

Lutkevitch, B. (2021). *What is risk mitigation?* Retrieved 15.07.2023 from https://www.techtarget.com/searchdisasterrecovery/definition/risk-mitigation

Malhotra, Y. (2015). *Risk, Uncertainty, And, Profit for the Cyber Era: Model Risk Management of Cyber Insurance Models Using Quantitative Finance and Advanced Analytics - Post-Doctoral Research Thesis on Finance, Risk, and, Quant Modeling Beyond the Global Financial Crisis*. State University of New Your.

Manuj, I., & Mentzer, J. T. (2008). Global supply chain risk management strategies. International *Journal of physical distribution & logistics management*, 38(3), 192-223.

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*, *24*, 35-61.

Marshall, C., Rossman, G. B., & Blanco, G. L. (2021). *Designing Qualitative Research*. SAGE Publications.

Mayring, P. (2004). Qualitative content analysis. *A companion to qualitative research*, 1(2), 159-176.

Mayring, P. (2015). *Qualitative Inhaltsanayse - Grundlagen und Techniken* (12 ed.). Beltz.

Mayring, P. (2022). *Qualitative Content Analysis - A Step-by-Step-Guide*. SAGE.

Mayring, P., & Fenzl, T. (2014). Qualitative inhaltsanalyse. In *Handbuch Methoden der empirischen Sozialforschung* (pp. 543-556). Springer.

Mayring, P., Fenzl, T., & Letz, F. (2024). QCAmap // a software Qualitative Content Analysis. Association for Supporting Qualitative Research ASQ. Retrieved 02.02.2024 from https://www.qcamap.org/ui/en/home

McLilly, L. (2020). *Exploring a Cost-Benefit Cloud-Based On-Demand Cybersecurity Service Solution for Small Businesses: A Quantitative Examination - A Dissertation Presented in Partial Fulfillment of the Requirements for the Degree of Doctor of Computer Science*. Colorado Technical University.

Mijnhardt, F., Baars, T., & Spruit, M. (2016). Organizational characteristics influencing SME information security maturity. *Journal of Computer Information Systems*, *56*(2), 106-115.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook Sage*.

Mitchell, M. L., & Jolley, J. M. (2010). Research design explained: Instructor's edition (7th ed.). Wadsworth/Cengage Learning.

Mlakar, I., Jeran, P., & Šafran, V. (2021, //). *A Cost-Effective Security Framework to protect micro enterprises: PALANTIR e-commerce use case* 2021 9th International Symposium on Digital Forensics and Security (ISDFS),

Moher, D., Tetzlaff, J., Tricco, A. C., Sampson, M., & Altman, D. G. (2007). Epidemiology and reporting characteristics of systematic reviews. *PLoS medicine*, *4*(3), e78.

Moses, J. W., & Knutsen, T. L. (2019). *Ways of knowing: Competing methodologies in social and political research*. Bloomsbury Publishing.

Mthiyane, Z. Z. F., Poll, H. M. v. d., & Tshehla, M. F. (2022). A Framework for Risk Management in Small Medium Enterprises in Developing Countries. *Risks*, *10*, 173.

Muhirwe, J., & White, N. (2016). CYBERSECURITY AWARENESS AND PRACTICE OF NEXT GENERATION CORPORATE TECHNOLOGY USERS. *Issues in Information Systems*, *17*(2)

Mulrow, C. D. (1994). Systematic reviews: rationale for systematic reviews. *Bmj*, 309(6954), 597-599.

Mulrow, C. D., & Cook, D. (Eds.). (1998). *Systematic reviews: synthesis of best evidence for health care decisions*. ACP Press.

Musa, S. N. (2012). *Supply chain risk management: identification, evaluation and mitigation techniques* Linköping University Electronic Press].

Mzileni, I., & Ncubukezi, T. (2022). Impact of information security threats on small businesses during the Covid-19 pandemic. In *Proceedings of the 21st European Conference on Cyber Warfare and Security* (Vol. 21, pp. 401-410). University of Chester.

Ncubukezi, T. (2020). A proposed: integration of the Monte Carlo model and the Bayes network to propose cyber security risk assessment tool for small and medium enterprises. *International Journal of Computer Science and Information Systems*, 18(3), 152-155. https://www.academia.edu/download/63013467/19_Paper_01032035_IJCSIS_Camera_Ready_pp152-15520200419-112605-ej13bf.pdf

Nelson, N., & Madnick, S. (2017a). Studying the tension between digital innovation and cybersecurity. In *3rd International Conference on Information Systems Security and Privacy*. Association for Information Systems.

Nelson, N., & Madnick, S. (2017b). *Trade-offs between digital innovation and cyber-security - Working Paper CISL 2017-03*. Massachusetts Institute of Technology.

Nieuwesteeg, B., & Waard, B. d. (2018). The law and economics of cyber insurance contracts: a case study. *European European Review of Private Law*, *26*(3), 371-420.

NIST. (2012). *Guide for Conducting Risk Assessments, NIST Special Publication 800-30*. National Institute of Standards and Technology.

NIST. (2018). *Cybersecurity Framework*. National Institute of Standards and Technology (NIST). Retrieved 15.06.2023 from https://www.nist.gov/cyberframework

Nola, R., & Sankey, H. (2014). *Theories of scientific method: an introduction*. Routledge.

NSA. (2018). *NSA'S Top Ten Cybersecurity Mitigation Strategies*. National Security Agency. Retrieved 12.07.2023 from https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf

Nunes, S. R. (2018). Value focused assessment of cyber risks to gain benefits from security investments.

Nykänen, R., & Kärkkäinen, T. (2016). Supporting cyber resilience with semantic wiki. In *Proceedings of the 12th International Symposium on Open Collaboration* (pp. 1-8). Association for Computing Machinery.

OECD (2021), *The Digital Transformation of SMEs, OECD Studies on SMEs and Entrepreneurship*, OECD Publishing, Paris, https://doi.org/10.1787/bdb9256a-en.

Oppenheim, A. N. (2000). *Questionnaire design, interviewing and attitude measurement*. Bloomsbury Publishing.

Osborn, E., & Simpson, A. (2015). Small-scale cyber security. In *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing* (pp. 247-252). IEEE.

Osborn, E., & Simpson, A. (2017). On small-scale IT users' system architectures and cyber security: A UK case study. *Computers &Security*, *70*, 27-50.

Osborn, E., & Simpson, A. (2018). Risk and the small-scale cyber security decision making dialogue—a UK case study. *The Computer Journal*, *61*(4), 472-495.

Ouda, A. J., Yousif, A. N., Hasan, A. S., Ibrahim, H. M., & Shyaa, M. A. (2022). The impact of cloud computing on network security and the risk for organization behaviors. *Webology*, *19*(1), 195-206.

Oxford Analytica. (2021). *The cyber insurance market will grow rapidly*. Oxford Analytica. https://doi.org/10.1108/OXAN-DB262447

Oxford Analytica. (2023). *Germany cyberattacks underline risk landscape*. Oxford Analytica.

Oxman, A. D., & Guyatt, G. H. (1993). The science of reviewing research a. *Annals of the New York Academy of Sciences*, 703(1), 125-134.

Paquet-Clouston, M., & García, S. (2023). On the Dynamics behind Profit-Driven Cybercrime: From Contextual Factors to Perceived Group Structures, and the Workforce at the Periphery. *Global Crime*, *24*(2), 122-144.

Pawar, S. A. (2016). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International Journal of Ifnromation Management Data Insigts*, *2*(1), 10080.

Pfeifer, M. R. (2021). IT security in SMEs—Threats and Chances for Supply Chains. *Journal of Supply Chain and Customer Relationship Management*, *2021*, 435883.

Pfister, P., & Lehmann, C. (2023). Returns on digitisation in SMEs—a systematic literature review. *Journal of Small Business & Entrepreneurship*, *35*(4), 574-598.

PIE. (2023). *Small Business Insurance*. PIE Insurance. Retrieved 20.03.2023 from https://www.pieinsurance.com/small-business-insurance

Quesada, I. (2016). *Seccord - Deliverable 5.5 Catalogue Year 3.* Aljosa Pasic (ATOS).

Radanliev, P., De Roure, D., Cannady, S., Mantilla Montalvo, R., Nicolescu, R., & Huth, M. (2018). Analysing IoT cyber risk for estimating IoT cyber insurance. In *Living in the Internet of Things: Cybersecurity of the IoT-2018. IET Conference Proceedings,* pp. 1-9. The Institution of Engineering and Technology.

Rae, A., & Patel, A. (2019). Defining a new composite cybersecurity rating scheme for smes in the uk. In *International Conference on Information Security Practice and Experience,* (pp. 362-380). Springer.

Raina, S. (2023). *Geopolitical Instability Raises Threat of 'Catastrophic Cyberattack in Next Two Years'*. World Economic Forum. Retrieved 10.06.2023 from https://www.weforum.org/press/2023/01/geopolitical-instability-raises-threat-of-catastrophic-cyberattack-in-next-two-years/

Randolph, J. (2019). A guide to writing the dissertation literature review. *Practical assessment, research, and evaluation*, 14(1), 13.

Rawindaran, N., Jayal, A., Prakash, E., & Hewage, C. (2021). Cost Benefits of Using Machine Learning Features in NIDS for Cyber Security in UK Small Medium Enterprises (SME). *Future Internet*, *13*(8), 186.

Rejda, G. E., & McNamara, M. J. (2017). Principles of Risk Management and Insurance, 13th edition. Pearson Education.

Renaud, K. (2016). *How smaller businesses struggle with security advice*. Elsevier.

Renaud, K., & Weir, G. R. S. (2016). Cybersecurity and the Unbearability of Uncertainty. *Cybersecurity and Cyberforensics*, Amman.

Rumrill Jr, P. D., & Fitzgerald, S. M. (2001). Using narrative literature reviews to build a scientific knowledge base. *Work*, 16(2), 165-170.

Saber, J. A. (2016). *Determining small business cybersecurity strategies to prevent data breaches - Doctoral dissertation*. Walden University.

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2020). *Research methods for business students*, (8th ed.). Pearson Education.

Schenkenhofer, J. (2022). Hidden champions: A review of the literature & future research avenues. Management Review Quarterly, 72(2), 417-482.

Scheuermann, J. E. (2016). *The internet of things: Is your cyber insurance protecting you*? Retrieved 10.07.2023 from https://www.klgates.com/the-internet-of-things--is-your-cyber-insurance-protecting-you-11-30-2016/#_ftn8

Schlesinger, M. (2018). Optimal Models for Cyber Insurance for the SME/SMB Markets. *Int'l J. Data Protection Officer, Privacy Officer &Privacy Couns*, *18*(2:4), 18-26.

Schmitz, C., & Pape, S. (2020). LiSRA: Lightweight Security Risk Assessment for decision support in information security. *Computers & Security*, *90*, 101656.

Shaw, I. (2023). Ethics and the practice of qualitative research. In *Research and Social Work in Time and Place*, (pp. 277-288). Routledge.

Silverman, D. (2021). *Doing qualitative research*. Sage Publication.

Silverman, D. (2024). *Interpreting qualitative data*. Sage Publication.

Stahl, B. C., Lichtenstein, Y., & Mangan, A. (2003). The limits of risk management: A social construction approach. *Communications of the International Information Management Association*, *3*(3), 15-22.

Statista(2024, https://de.statista.com/statistik/daten/studie/164300/umfrage/arten-von-computerkriminalitaet-in-unternehmen-in-deutschland/)

Strupczewski, G. (2021). Defining cyber risk. *Safety science*, *135*, 105143.

Such, J. M., Vidler, J., Seabrook, T., & Rashid, A. (2015). *Cyber security controls effectiveness: a qualitative assessment of cyber essentials. Technical Report SCC-2015-02*. Security Lancaster, Lancaster University.

Suri, H. (1998). *A Critique of Contemporary Methods of Research Synthesis*. Paper presented at the AARE Annual Conference, Adelaide.

Tam, T., Rao, A., & Hall, J. (2021). The good, the bad and the missing: a narrative review of cyber-security implications for Australian small businesses. *Computers & Security*, *109*, 102385.

Tanenbaum, S. J. (2005). Evidence-based practice as mental health policy: Three controversies and a caveat. *Health Affairs*, 24(1), 163-173.

Thompson, P. B. (2012). Ethics and risk communication. *Science Communication*, *34*(5), 618-641.

Tøndel, I. A., Meland, P. H., Omerovic, A., Gjære, E. A., & Solhaug, B. (2015). Using cyber-insurance as a risk management strategy: Knowledge gaps and recommendations for further research. *SINTEF Rapport*, *A27298*

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. C*omputers & Security*, 72, 212-233.

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management*, 14(3), 207-222.

Trochim, W. M. (2006). *The qualitative debate*. Socialresearchmethods.

University of Gloucestershire Research Ethics Handbook, 2024. Research Ethics: A Handbook of Principles and Procedures. Last updated: 12 March 2024. Retrieved on 26.7.2024 from https://www.glos.ac.uk/information/knowledge-base/research-ethics-a-handbook-of-principles-and-procedures/

Unluer, S. (2012). Being an insider researcher while conducting case study research. *Qualitative Report*, *17*, 58.

Vieira, A. C., Insua, D. R., Baylon, C., & Awondo, S. (2020). Risk Management Models for Cyber Insurance. In *Security Risk Models for Cyber Insurance* (pp. 49-82). Chapman and Hall/CRC.

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security–what goes where? Information & Computer Security. *Computers & Security*, *26 (1)*, 2-9.

Wang, J., Ho, C. Y. C., & Shan, Y. G. (2024). Does cybersecurity risk stifle corporate innovation activities? *International Review of Financial Analysis*, *91*, 103028.

Weare, C., & Lin, W.-Y. (2000). Content analysis of the World Wide Web: Opportunities and challenges. *Social science computer review*, *18*(3), 272-292.

Weber, R. P. (1990). *Basic content analysis*. Sage.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS quarterly*, xiii-xxiii.

Wicki-Birchler, D. (2020). The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime? *International Cybersecurity Law Review*, *1*, 63-72.

Willig, C. (2013). *Introducing qualitative research in psychology*. McGraw-Hill education.

Woiceshyn, J., & Daellenbach, U. (2018). Evaluating inductive vs deductive research in management studies: Implications for authors, editors, and reviewers. *Qualitative research in organizations and management: An International Journal*, *13*(2), 183-195.

World Economic Forum Global Risk Report 2024 19th edition, https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf?utm_source=chatgpt.com

Wrede, D., Stegen, T., & Graf von der Schulenburg, J.-M. (2020). Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market. *The Geneva Papers on risk and insurance-Issues and practice*, 45, 657-689.

Yin, R. K. (2018). *Case study research and applications*. Sage Publications.

Yousefi, A. (2020). *AI-Enabled Cyber Insurance Platform for Small Businesses - Master Thesis*. Macquaire University - Sydney.

Zeiringer, J. P., Durst, S., & Thalmann, S. (2022). Show Me What You Do and I Will Tell You Who You Are: A Cluster Typology of Supply Chain Risk Management in SMEs. *Journal of Theoretical and Applied Electronic Commerce Research*, *17*(1), 345-359.

Zeller, G., & Scherer, M. (2023). Risk mitigation services in cyber insurance: optimal contract design and price structure. *The Geneva Papers on Risk and Insurance. Issues and Practice*, *48*(2), 502.

Zwilling, M. (2022). Trends and Challenges Regarding Cyber Risk Mitigation by CISOs—A Systematic Literature and Experts' Opinion Review Based on Text Analytics. *Sustainability*, *14*(3), 1311.

Annex 1: Cover letter sent to selected medium-sized enterprises

Anschreiben an selektierte mittelständische Unternehmen	Cover letter to selected medium-sized enterprises
Sehr geehrte Damen und Herren, mit dieser Anfrage möchte ich Sie um Ihre Unterstützung für meine Forschungsarbeit zum Thema „Cyber-Risikominderungsstrategien für den deutschen produzierenden Mittelstand“ bitten. Dieses Forschungsprojekt wurde von mir bei einer renommierten Universität im Rahmen eines PhD-Programms eingereicht und ist genehmigt. Inhaltlich zielt diese Forschungsarbeit darauf ab, Cyber-Risiko-Minderungs-Praktiken in deutschen produzierenden mittelständischen Unternehmen zu untersuchen. Da die Fertigungen stetig durch neue Technologien unter dem Label Smart Industry oder Industrie 4.0 transformiert werden, sind die meisten dieser Technologien entweder selbst digital oder auf digitale Konnektivität angewiesen. Dieser technologische Wandel bringt jedoch eine grundlegende Verschiebung von Cyber-Risiken und -Sicherheit mit sich, da Geräte miteinander ver-	Ladies and Gentlemen, With this request, I would like to ask for your support for my research work on the topic of “Cyber-Risk mitigation strategies for German manufacturing medium-sized enterprises”. This research project has been submitted by me to a reputed university under a PhD program and was approved. In terms of content, this research aims to investigate cyber-risk mitigation practices in German manufacturing medium-sized enterprises. As manufacturing is constantly being transformed by new technologies under the Smart Industry or Industry 4.0 label, most of these technologies are either digital themselves or rely on digital connectivity. However, this technological change brings with it a fundamental shift in cyber-risk and security as devices become interconnected and in-

bunden und Informationen und Kontrolle sowohl innerhalb als auch in unterschiedlichem Maße außerhalb der Organisation des Unternehmens übertragbar werden. Diese Probleme gilt es weiter zu erforschen, um sowohl unbeabsichtigte als auch beabsichtigte Sicherheitsvorfälle zu verhindern. Ohne geeignete Cyber-Risikomanagement-Prozesse und Minderungstechniken könnten daher die Geschäftsergebnisse und der zukünftige Erfolg deutscher mittelständische Unternehmen in der verarbeitenden Industrie gefährdet sein.	formation and control become transferable both within and, to varying degrees, outside the company's organization. These issues need to be further researched to prevent both unintentional and intentional security incidents. Therefore, without appropriate cyber-risk management processes and mitigation techniques, the business results and future success of German medium-sized enterprises in the manufacturing industry could be at risk.
Basierend auf einem qualitativen Forschungsdesign – d. h. persönliche Befragung von Managern und Fachexperten auf Unternehmensebene – sollen einzigartige Einblicke in die cyberphysischen Systeme und unternehmensspezifische Normen, Strategien und individuelle Erfahrungen zur Risikomitigation von Cyberrisiken erforscht und Lösungen generiert werden.	Based on a qualitative research design – i.e. personal surveys of managers and specialist experts at company level - unique insights into cyber-physical systems and company-specific standards, strategies and individual experiences for risk mitigation of cyber-risks are to be researched and solutions generated.
Die Untersuchung soll mit Risikomanagern, IT-System-Verantwortlichen und/oder Mitglieder der Geschäftsführung aus mittelständischen Unternehmen des verarbeitenden Gewerbes durchgeführt werden. Dabei sollen Unternehmen aus dem mittleren Segment speziell betrachtet werden.	The study is to be conducted with risk managers, IT system managers and/or members of management from medium-sized enterprises in the manufacturing industry. Organisations from the medium-sized segment are to be considered in particular.
Die Kernfrage dieser Studie zielt darauf ab, ob mittelständische Unternehmen, die Mitigation-Techniken und Cyber-Versicherungen zur Minderung	The key question of this study is whether medium-sized enterprises that use mitigation techniques and cyber-risk insurance to mitigate cyber-risks are more successful than those that do not.

von Cyber-Risiken nutzen, erfolgreicher sind als diejenigen, die dies nicht tun. Zusätzlich zu der oben umrissenen zentralen Forschungsfrage sollen aufgrund der Interviews ebenfalls folgende Fragen geklärt werden können - Wie ist die Cyber-Risikowahrnehmung und das -Risikomanagement im deutschen produzierenden Mittelstand? - Wie praktiziert der deutsche Mittelstand Cybersicherheit im Kontext von IoT und/oder vernetzten Produktionsanlagen? - Welche Beziehung besteht zwischen spezifischen Risikofaktoren und Risikominderungsstrategien in mittelständische Unternehmen? - Wie sieht der deutsche Mittelstand die Rolle der Cyber-Risikoversicherung im Rahmen der Cyber-Risikominderung? Hierzu ist angedacht ein Interview auf Basis grundsätzlicher Fragen zu führen. Hinsichtlich der unten genannten Themenblöcke wird ein Zeitrahmen von 1 - 1½ Stunden geschätzt. Die persönliche Befragung kann mit Ihrem Einverständnis im Unternehmen stattfinden, aber auch mittels Videokonferenz durchgeführt werden. Folgende Themenkomplexe sollen besprochen werden: - Einführungsabschnitt: (Vorstellung, Unternehmen, Rolle des Befragten) - Praktiken des Cyber-Risikomanagements und -strategie	In addition to the central research question outlined above, the following questions should also be clarified based on the interviews. - What is cyber-risk perception and risk management in German medium-sized manufacturing companies? - How do German medium-sized companies practice cybersecurity in the context of IoT and/or networked production systems? - What is the relationship between specific risk factors and risk mitigation strategies in medium-sized enterprises? - How do German medium-sized companies see the role of cyber-risk insurance in the context of cyber-risk reduction? For this purpose, it is planned to conduct an interview based on basic questions. With regard to the topic blocks mentioned below, a time frame of 1 - 1½ hours is estimated. With your consent, the personal survey can take place in the company, but can also be carried out via video conference. The following topics should be discussed: - Introductory section: (Introduction, company, role of interviewee) - Cyber-risk management practices and strategy

- Cyber-Risiko und Industrie 4.0/IoT (vernetzte Produktionsanlagen, IoT) - Cyber-Risikomanagement und Geschäftserfolg (Erfolgsfaktoren) - Cyber-Versicherung (Risikodeckung, Einbindung Cyber-Risiko-management-Strategie)	- Cyber-risk and Industry 4.0/IoT (connected production systems, IoT) - Cyber-risk management and business success (success factors) - Cyber-risk insurance (risk coverage, integration of cyber-risk management strategy)
Ich würde mich sehr freuen, wenn ich Sie als Interviewpartner gewinnen könnte und Ihr Unternehmen mich bei dieser Forschungsarbeit unterstützen würde. Die Interviews würde ich gerne im zweiten und dritten Quartal dieses Jahres durchführen.	I would be very happy if I could get you as an interview partner and if your company would support me in this research work. I would like to conduct the interviews in the second and third quarters of this year
Alle Informationen aus dem Interview werden streng vertraulich behandelt und im Rahmen der Analyse vollständig anonymisiert. Gerne bin ich auch bereit, die komprimierten Ergebnisse als Dank mit Ihnen zu teilen. Das Forschungsprojekt sollte bis Mitte 2025 abgeschlossen sein.	All information from the interview is treated as strictly confidential and completely anonymized as part of the analysis. I would also be happy to share the compressed results with you as a “Thank You”. The research project should be completed by mid-2025.
Für Fragen und weitere Informationen bzgl. Terminabsprache, Interviewleitfaden etc. stehe ich Ihnen gerne unter der angegebenen E-Mail-Adresse beziehungsweise der Mobilnummer zur Verfügung. Besten Dank & Freundliche Grüße Herbert Sedlmair	If you have any questions or require further information regarding appointments, interview guidelines, etc., please do not hesitate to contact me at the e-mail address or mobile number provided. Many thanks & kind regards Herbert Sedlmair

Annex 2: Interview consent form

Einwilligungserklärung Interview	**Interview consent form**
Ich erkläre hiermit mein Einverständnis zur Nutzung der personenbezogenen Daten, die im Rahmen des folgenden Gesprächs erhoben wurden: • Datum des Interviews: …… • Name der zu interviewenden Person: …….. • Kurzbeschreibung des Forschungsprojekts: Untersuchung von Cyber-Risikominderungsstrategien bei den deutschen produzierenden Mittelstand. • Durchführende Hochschule: University of Gloucestershire, School of Business and Technology (Das Forschungsprojekt wurde im Rahmen eines PhD-Programms eingereicht und genehmigt). • Leiter des Projekts: Herbert Sedlmair	I hereby declare my consent to the use of the personal data collected during the following interview: • Date of the interview: ..... • Name of the person to be interviewed: …… • Brief description of the research project: Cyber-Risk mitigation strategies for German manufacturing medium-sized enterprises. • Performing university: University of Gloucestershire, School of Business and Technology (The research project was submitted and approved as part of a PhD program). • Head of the project: Herbert Sedlmair
Die Daten werden im Rahmen eines mündlichen Gesprächs erhoben, das mit einem Aufnahmegerät aufgezeichnet wurde. Zum Zwecke der Datenanalyse werden die mündlich erhobenen Daten verschriftlicht (Transkription), wobei die Daten anonymisiert und die Tonaufnahme nach der Transkription gelöscht werden. Eine Identifizierung der interviewten Person ist somit ausgeschlossen.	The data is collected as part of an oral conversation that was recorded using a recording device. For the purpose of data analysis, the data collected orally is written down (transcription), whereby the data is anonymized and the audio recording is deleted after transcription. An identification of the person interviewed is therefore impossible.
Kontaktdaten, die eine Identifizierung der interviewten Person zu einem späteren Zeitpunkt ermöglichen würden, werden aus Dokumentationsgründen in einem separaten Schriftstück lediglich den	For documentation reasons, contact details that would enable the person interviewed to be identified at a later date will only be made available to the reviewers of the scientific work in a separate document.

Gutachter:innen der wissenschaftlichen Ausarbeitung zur Verfügung gestellt. Nach dem Abschluss des Projekts werden diese Daten gelöscht. Der Speicherung der personenbezogenen Daten zu Dokumentationszwecken kann durch die interviewte Person jederzeit widersprochen werden. Die Teilnahme an dem Gespräch erfolgt freiwillig. Das Gespräch kann zu jedem Zeitpunkt abgebrochen werden. Das Einverständnis zur Aufzeichnung und Weiterverwendung der Daten kann jederzeit widerrufen werden. _____ Vorname und Name in Druckbuchstaben _____ Datum, Ort Unterschrift	After the project is completed, this data will be deleted. The interviewee can object to the storage of personal data for documentation purposes at any time. Participation in the interview is voluntary. The conversation can be canceled at any time. Consent to the recording and further use of the data can be revoked at any time. _____ First and last name in block letters _____ Date, place signature

Annex 3: Interview guide

Interviewfragebogen:

Videokonferenz am [Datum]

Beginn:

Ende:

Interview questionnaire:

Video conference on [date]

Start:

End:

Deutsch	English
0 Einführungsabschnitt	**0 Introductory Section**
0.1 Kurze Vorstellung des Interviewers und des Dissertationsvorhabens.	0.1 Short introduction of the interviewer and the dissertation project.
0.2 Fragen zum Befragten.	0.2 Questions about the interviewee.
0.2.1 Name (Anonymität wird zugesichert).	0.2.1 Name (anonymity will be assured).
0.2.2 Beruflicher Hintergrund und Erfahrung (technische oder kaufmännische Ausbildung, Industrieerfahrung, Firmenerfahrung).	0.2.2 Professional background and experience (technical or business education, experience within industry, experience within company).
0.2.3 Rolle des Befragten im Unternehmen. Welchen Zuständigkeitsbereich verantworten Sie im Unternehmen?	0.2.3 Role of interviewee in company (owner/employee/level of management). Which area of responsibility are you responsible for in the company?
0.2.4 Inwieweit sind Sie in den größeren Cyber-Risiko-Management (CRM) - Prozess involviert?	0.2.4 To what extent are you involved in the larger cyber-risk-management (CRM) process?

Deutsch	English
0.3 Unternehmen: Kurzbeschreibung des Unternehmens (Branche, Produkte, Mitarbeiterzahl, Anteil B2B/B2C-Kunden, typische Größe von B2B-Kunden, Geschäftsprozesse).	0.3 Company: Short description of business (sector, products, number of employees, share of B2B/B2C-clients, typical size of B2B-clients, business process).
0.4 Wie sieht die IT-Infrastruktur des Unternehmens aus?	0.4 What is the company's IT infrastructure?
0.5 Was sind die Leistungs-/Erfolgskennzahlen des Unternehmens?	0.5 What are the company's performance/success measures?
0.5.1 Können Sie die kritischen Erfolgsfaktoren im Geschäftsprozess des Unternehmens beschreiben? (Umsatz, Kosten und Investitionen und/oder Fähigkeiten und Ressourcen?)	0.5.1 Can you describe the critical success factors in the business process of the company ((sales, costs, and investments and/or skills and resources?)
1 Praktiken des Cyber-Risikomanagements	**1 Cyber risk management practices**
1.1 Wie hat Ihr Unternehmen Cybersicherheitsrichtlinien im Risikomanagementprozess implementiert?	1.1 How has your company implemented cybersecurity guidelines in risk management process?
1.2 Wie hoch ist das Cyber-Risiko in Ihrem Unternehmen und inwieweit ist CRM in den RM-Prozess integriert?	1.2 What is the cyber risk in your organization and to what extent is CRM integrated into the RM process?
1.3 Können Sie bitte erläutern, wie IT- und Cyber-Risiken monetär quantifiziert werden und wie dies die Priorisierung von Risiken im Managementprozess beeinflusst?	1.3 Can you please explain how IT and cyber risk exposure are quantified in monetary terms and how this influences the prioritization of risk in the management process?
1.4 Wie gut sieht der Interviewpartner das Unternehmen gegen Cyber-Risiken gewappnet?	1.4 How well does the interview partner consider the company to be prepared against cyber-risks?
1.5 Welche Cyber-Risiken sieht der Interviewpartner als Bedrohung für sein Unternehmen an?	1.5 Which cyber risks does the interview partner consider to be a threat for their company?

Deutsch	English
1.6 Wurde Ihr Unternehmen bereits Opfer eines Cyber-Angriffs?	1.6 Has the interviewee's company already been a victim of a cyberattack?
1.6.1 Wenn ja, wie haben Sie reagiert und diese Vorfälle aufgezeichnet (auch aufgezeichnete Beinaheunfälle)?	1.6.1 If yes, how have you reacted and have you recorded those incidents (also near misses recorded)?
2 Cyber-Risikostrategien und ihre Komponenten	**2 Cyber- risk strategies and what is involved**
2.1 Können Sie bitte etwas über die Cyber-Risikostrategie Ihres Unternehmens sagen? (Falls nicht vorhanden, können Sie bitte die Gründe erläutern?)	2.1 Can you please talk about your company's cyber risk strategy? (In case of none, can you please explain the reasons?)
2.2 Geben Sie unabhängig von der Antwort auf 2.1 bitte Informationen darüber an, welche Maßnahmen das Unternehmen ergreift, um Cyber-Risiken zu managen oder zu mindern?	2.2 Regardless of answer to 2.1, please provide information on which measures the company takes to manage or mitigate cyber risk?
2.3 Welche der unter 2.2 genannten Maßnahmen sind die wichtigsten?	2.3 Out of measures mentioned under 2.2, which are the most important ones?
2.4 Wie bewertet das Unternehmen im Umgang mit anderen Unternehmen (Lieferanten, Kunden) deren Cyber-Risiko-Exponierung, Minderungsmaßnahmen oder CRM-Strategien?	2.4 When dealing with other companies like suppliers or clients, how does the company assess their cyber-risk exposure, and what mitigation measures and strategies are adopted?
2.5 Was sind die Hauptprobleme für das Unternehmen im Zusammenhang mit Cyber-Risiken?	2.5 What are the main problems for the company in context of cyber-risks?
2.6 Welchen potenziellen finanziellen Schäden ist das Unternehmen im Zusammenhang mit Cyber-Risiken ausgesetzt?	2.6 What is the potential financial damage the company is exposed to in the context of cyber risks? (intangible assets, business interruption)?
2.7 Wie hoch sind die geschätzten Kosten für das Cyber-Risikomanagement und die Minderungsmaßnahmen des Unternehmens?	2.7 What are the estimated costs of the company's cyber risk management and mitigation measures?

Deutsch	English
2.8 Für Fragen zu Richtlinien/Maßnahmen wäre es hilfreich, alle verfügbaren schriftlichen Unterlagen zu erhalten.	2.8 For questions about policies/measures, it would be useful to receive any written documentation available.
3 Cyber-Risiko und Industrie 4.0/IoT	**3 Cyber risk and industry 4.0/IoT**
3.1 Wie ist Ihre Einschätzung zu Cyber Risiko und Industrie 4.0, moderne vernetzte Produktionsanlagen?	3.1 What is the interview partners assessment regarding cyber risk and industry 4.0, modern networked production facilities?
3.2 Ist Ihr Unternehmen von diesem Problem betroffen?	3.2 Is the company affected by this issue?
3.2.1 Wenn ja, erläutern Sie bitte, wie und welche Strategien/Maßnahmen es in diesem Zusammenhang gibt?	3.2.1 If yes, please explain how and what policies/measures exist in this context?
3.3 Wie schätzen Sie das Cyber-Risiko und Internet of Things (IoT)-Geräte ein?	3.3 What is the interview partners assessment regarding cyber risk and Internet of Things (IoT)-devices?
3.3.1 Wenn ja, erläutern Sie bitte, wie und welche Strategien/Maßnahmen in diesem Zusammenhang existieren?	3.3.1 If yes, please explain how and what policies/measures exist in this context?
3.4 Welche Cyber-Verflechtungen mit anderen Unternehmen (Supply Chain) gibt es?	3.4 What are the cyber interdependencies with other companies (supply chain)?
4 Cyber-Risikomanagement und Geschäftserfolg	**4 Cyber-risk management and business success**
4.1 Wie trägt Cyber Risk Management Ihrer Meinung nach zum Geschäftserfolg bei?	4.1 How does the interviewee consider cyber risk management to contribute to business success?

Deutsch	English
4.2 Wo steht Cyber Risk Management im Kontext mit anderen Unternehmens-erfolgsfaktoren?	4.2 Where does cyber risk management stand in context with other business success factors?
4.3.1 Welche Faktoren beeinflussen Ihrer Meinung nach die CRM- und Mitigations-Strategien positiv hinsichtlich des Erfolgs Ihres Unternehmens?	4.3 Which factors do you believe positively influence the CRM and -Mitigation strategies the success of your company?
4.3.1 Inwieweit stimmen diese Faktoren Ihrer Meinung nach mit den wahrgenommenen Haupterfolgsfaktoren des Unternehmens überein?	4.3.1 To what extent do you think that these factors match with the perceived the company's key success factors?
5 Cyber-Versicherung (CRI)	**5 Cyber-risk insurance (CRI)**
5.1 Welche Erfahrungen hat das Unternehmen mit dem Einkauf von CRI gemacht?	5.1 What is the company's experience with purchasing CRI?
5.2 Wenn es keinen CRI gibt und keine Anschaffungspläne bestehen, was sind die Gründe dafür?	5.2 If there is no CRI and there are no plans to buy any, what are the reasons for this?
5.3 Welche Arten von Risiken sind (sollten) in bestehenden oder geplanten CRI abgedeckt werden?	5.3 What types of risks are (intended to be) covered in existing or planned CRI?
5.4 Hat das Unternehmen bereits Schadenleistungen aus einer CRI erhalten?	5.4 Has the company already received claims payments from CRI?
5.5 Wo sehen Sie CRI als Element der Cyber-Risikomanagement-Strategie?	5.5 Where does the interview partner see CRI as an element of cyber risk management strategy?
5.6 Wie schätzen Sie das Verhältnis zwischen Versicherungskosten und CRI-gedeckten Schadenskosten ein?	5.6 How does the interview partner assess the relationship between insurance costs and damage costs covered by CRI?

Deutsch	English
5.7 Wie wird bei einer Cyber-Versicherung die Versicherungsprämie in Relation zur wahrgenommenen eigenen Sicherheit gesetzt?	5.7 How is the insurance premium for cyber-risk insurance set in relation to the perceived security?
5.8 Wie schätzt der Interviewpartner ein akzeptables Verhältnis zwischen Kosten für Cyber-Risikomanagement und -Mitigation und Cyber-Risikoversicherung ein?	5.8 How does the interview partner assess an acceptable relationship between costs for cyber risk management and mitigation and cyber-risk insurance?
5.9 Wie, glauben Sie, stabilisiert oder verbessert der Cyber-Versicherungsschutz Ihren Geschäftserfolg?	5.9 How do you think cyber-risk insurance protection stabilizes or improves your business success?
5.10 Welche Risiken hält der Interviewpartner für beherrschbar durch die CRM-Strategie und -Maßnahmen eines Unternehmens und welche Restrisiken sollten durch CRI abgedeckt werden?	5.10 What risks does the interview partner considered to be manageable by a company's CRM-strategy and measures and what residual risks should be covered by CRI?
6 Abschluss des Interviews	**6 Conclusion of the interview**
6.1 Inwieweit spielen potenzielle Cyber-Risiken und nachfolgende Cybersicherheitsinvestitionen eine Rolle bei der Entscheidung über zukünftige Geschäftsprioritäten oder Investitionen?	6.1 To what extent play potential cyber risks and subsequent cybersecurity investments a role when deciding upon future business priorities or investments?
6.2 Welche weiteren Themen im Zusammenhang mit Cyber-Risiko hält der Interviewpartner für wichtig bei Cyber-Risiko und mittelständischen Unternehmen?	6.2 What are other topics in the context of cyber risk, which the interview partner considers to be important of cyber risk and medium-sized enterprises?

Annex 4: Transcripted interview (Example No. 5)

German Original Interview Text	English Translation
00:00:12 HS Ja, vielleicht darf ich anfangen, Herr xxxx. Vielen Dank, dass Sie sich für das Interview Zeit genommen haben. Ich hoffe es geht Ihnen gut und Ihr Unternehmen hat ein erfolgreiches Geschäftsjahr 2023 hinter sich. Für 2024 ist die Prognose zu der wirtschaftlichen Entwicklung in Deutschland verhalten hoffe aber, dass Ihr Unternehmen weiterhin gute Geschäftsaussichten hat **00:00:58 Befragter** Ja, also wir können dem Klagen eigentlich nicht zustimmen. Also wir sind im Jahr 2023 über 20% gewachsen. Das rasante Wachstum wurde durch zunehmende Rohstoffpreiserhöhungen begleitet, die an den Kunden im Wesentlichen durchgereicht wurden. Da wir mit den wichtigsten Industriekunden langfristige Lieferverträge eingegangen sind, sollte sich das Wachstum, wenn auch abgeschwächt, fortsetzen. Die Tendenz zu neuen, trinkwasserkonformen bleifreien Werkstoffen und zu Ausgaben im Wassermanagement setzt sich weiter fort. Wir als xxxx nehmen hier eine führende Rolle in der Sanitär-Branche ein.	**00:00:12 HS** Yes, perhaps I may begin, Mr. xxxx. Thank you very much for taking the time for this interview. I hope you are doing well and that your company has had a successful financial year in 2023. For 2024, the forecast for economic development in Germany is subdued, but I hope that your company continues to have good business prospects. **00:00:58 Respondent** Yes, we can't really agree with the complaints. We grew by over 20% in 2023. The rapid growth was accompanied by increasing raw material price hikes, which were essentially passed on to the customer. As we have entered into long-term supply contracts with our most important industrial customers, growth should continue, albeit at a slower pace. The trend towards new, drinking water-compliant lead-free materials and expenditure on water management is continuing. Our company xxxx plays a leading role in the sanitary industry in this area.
00:02:23 HS	**00:02:23 HS**

Ja, kurz zu meiner Person. Ich bin gelernter Versicherungsmathematiker und seit 30 Jahren in der Rückversicherung tätig. Und insofern ist dieses Thema auch natürlich indirekt ein Thema für die Rückversicherungsbranche, vor allem wenn es um Akkumulationen geht.	Yes, briefly about myself. I am a trained actuary and have been working in the reinsurance industry for 30 years. And in this respect, this topic is, of course, indirectly an issue for the reinsurance industry, especially when it comes to accumulations.
Aber abseits von meiner beruflichen Karriere ist mein Forschungsthema Cybersicherheit und Mitigations-Strategien bei mittelständischen Unternehmen. Da diese Unternehmen im Gegensatz zu den ganz großen Unternehmen vielleicht begrenzte Mittel haben, sowohl in der Mitarbeiterzahl als vielleicht auch von den Geldmitteln, die zur Verfügung stehen, um diese Cyberthemen abdecken zu können, ist das Cyberrisiko Management von besonderem Interesse.	But apart from my professional career, my research topic is cybersecurity and mitigation strategies in medium-sized enterprises. Since these organisations, in contrast to very large companies, may have limited resources, both in terms of the number of employees and perhaps the financial resources available to cover these cyber topics, cyber-risk management is of particular interest. In this respect, I have taken on the task of speaking to you in management and recording your expertise in this interview.
Insofern habe ich mir die Aufgabe gemacht mit Ihnen in der Geschäftsführung zu sprechen und Ihre Expertise in diesem Interview aufzunehmen.	
Speziell möchte ich in meiner Promotionsarbeit der Frage nachgehen, inwieweit Cyber Risiko und Unternehmenskennzahlen, also Erfolgskennzahlen zusammenspielen können. Also inwieweit das eine das andere bedingt oder vielleicht ausschließt. Also das, das ist so ein bisschen kurz, erklärt der Hintergrund meiner Arbeit, die ich mir vorgestellt habe. Ich habe schon etliche Interviews geführt. Es ist in der Tat interessant, welche Bandbreite es gibt und bin natürlich sehr gespannt, was sie mir heute zu Ihrem Unternehmen erzählen.	In my thesis, I would particularly like to investigate the question of the extent to which cyber-risk and company metrics, i.e., success metrics, can interact. So, to what extent does one cause, or perhaps exclude, the other? That provides a brief overview of my work's background, as I envision it. I've already conducted a number of interviews. It's actually interesting what a range there is and I'm of course very excited to hear what you tell me about your company today.
Ich habe Ihnen bereits mitgeteilt, dass erstens dieses Interview aufgezeichnet wird, weil ich nicht so schnell mitschreiben kann, und zweitens wird alles anonymisiert. Des Weiteren, gehen diese Gespräche nirgends ein, die werden gelöscht, es wird dieses Gespräch nur in Stichpunkten zusammengefasst, Überbegriffe gebildet, um dann über	I have already told you that, firstly, this interview will be recorded because I cannot take notes so quickly, and secondly, everything will be anonymized. Furthermore, these conversations do not go anywhere, they are deleted, this conversation is only summarized in bullet points, umbrella terms are formed in order to then use certain analytical methods to get the content, a message, an explanation, a tendency from all these interviews.

bestimmte Analyseverfahren dann aus all diesen Interviews eine Nachricht, eine Erklärung, eine Tendenz rauszuhören. Also noch mal herzlichen Dank, dass sie sich bereit erklärt haben und ja, insofern wollte ich Ihnen vorab diesen Fragebogen senden, damit Sie ein bisschen wissen, worum es geht. **00:05:33 Befragter** Vielen Dank. Das war auch gut so, denn ich musste mich mit meinem IT- Leiter zusammensetzen um einige Spezifika zu Cyber aufzunehmen.	So, thank you again for agreeing to do so and yes, I wanted to send you this questionnaire in advance so that you know a little bit about what it's about. **00:05:33 Respondent** Thank you. That was a good thing, because I had to sit down with my IT manager to get some specifics about cyber.
00:05:51 HS Okay. Dann steigen wir in das Interview ein und meine erste Frage wäre nach Ihrem beruflichen Hintergrund **00:06:04 Befragter** Gut, also ich habe mit einer Lehre angefangen und anschließend an der Technisch Hochschule meinen Abschluss in Betriebswirtschaft gemacht. Meine erste berufliche Stelle war im Marketing und Vertrieb. Nach einer Zwischenstation als Direktor in einer metallverarbeitenden Firma habe ich vor knapp 14 Jahren meine Karriere in der jetzigen Firma begonnen und bin seit einigen Jahren Geschäftsführer und CEO.	**00:05:51 HS** Okay. Then we'll get into the interview and my first question would be about your professional background **00:06:04 Respondent** Well, I started with an apprenticeship and then graduated from a technical college with a degree in business administration. My first job was in marketing and sales. After a stopover as a director in a metal processing company, I started my career in my current company almost 14 years ago and have been managing director and CEO for several years now.
00:06:40 HS Welchen Zuständigkeitsbereich verantworten Sie im Vorstand?	**00:06:40 HS** Which area of responsibility are you responsible for on the Management Board?

00:06:50 Befragter Als alleiniger Geschäftsführer verantworte ich alle Bereiche im Unternehmen.	**00:06:50 Respondent** As the sole managing director, I am responsible for all areas of the company.
00:07:00 HS Inwieweit sind Sie in den größeren CRM-Prozess involviert? **00:07:30 Befragter** Das Unternehmen setzt dabei sowohl auf präventive als auch reaktive Maßnahmen. Das Unternehmen ist frei von Sicherheitslücken und potenziellen Sicherheitsrisiken zu halten, ist für das gesamte Unternehmen unerlässlich und eine stetige Betriebserfordernis/-aufgabe. Präventive Maßnahmen sollen das Risiko von Sicherheitsverletzungen reduzieren. Durch die Einführung von neuen Tools, Erkennungsstrategien und Reaktionsplänen halten wir eine starke Barriere aufrecht. Darüber hinaus geben wir unseren Mitarbeitern durch verpflichtende und optionale Schulungen sowie Angriffssimulationen, bspw. Phishing, die nötigen Werkzeuge an die Hand, um signifikante Attacken zu identifizieren und ein schnelles Melde- und Reaktionswesen umzusetzen. Mitarbeitersensibilität und Risikotransparenz sind für das Unternehmen die wichtigsten präventiven Maßnahmen in der Bekämpfung von Cyberkriminalität, Wirtschaftsspionage und Betrugsversuchen. Reaktive Maßnahmen sind im Gegenzug dazu bestimmt, die Erkennungsrate und Reaktionsfähigkeit der Unternehmung auf einem hohen Niveau zu gewährleisten und die Widerstandsfähigkeit während einer Cyberattacke beständig zu halten. Dazu setzen wir auf flächendeckende Sicherheits- und Schwachstellenscanner und ein Event- und Vorfalls-Manage-	**00:07:00 HS** To what extent are you involved in the larger CRM process? **00:07:30 Respondent** The company relies on both preventive and reactive measures. Keeping the company free of security gaps and potential security risks is essential for the entire company and is a constant operational requirement/task. Preventive measures are intended to reduce the risk of security breaches. By introducing new tools, detection strategies, and response plans, we maintain a strong barrier. In addition, we provide our employees with the necessary tools through mandatory and optional training, as well as attack simulations, e.g., phishing, to identify significant attacks and implement a rapid reporting and response system. Employee sensitivity and risk transparency are the most important preventive measures for the company in combating cybercrime, industrial espionage and attempted fraud. In return, reactive measures are intended to ensure the company's detection rate and responsiveness are at a high level and to maintain its resilience during a cyberattack. To do this, we rely on comprehensive security and vulnerability

mentsystem sowohl auf den zentralen, als auch auf den regional genutzten Endpunkten der IT-Infrastruktur. Nebst automatisierten Erkennungsmechanismen, wird dadurch auch eine systematische Reaktion auf Angriffsversuche ermöglicht.	scanners and an event and incident management system on both the central and regional endpoints of the IT infrastructure. In addition to automated detection mechanisms, this also enables a systematic response to attempted attacks.
00:08:53 HS Können Sie bitte Ihr Unternehmen kurz beschreiben, zum Beispiel welche Produkte hergestellt werden, wie viele Mitarbeit sie haben und welche Unternehmen ihre Produkte abnehmen und wie allgemein die Geschäftsprozesse sind? **00:09:20 Befragter** Also, das Unternehmen hatte im Geschäftsjahr eine Bilanzgröße von ca. 27,4 Mio. Die Umsatzerlöse beliefen sich auf knapp 58 Mio. Für 2024 erwarten wir eine Steigerung um 10 Mio. auf 68 Mio. Der Umsatz wird zu 70% im Inland, zu 25% im EU-Ausland sowie 5% im Nicht EU-Ausland erzielt. Wir beschäftigen derzeit knapp 200 Mitarbeiter. Davon sind mehr als die Hälfte in der Produktion beschäftigt. Im Büro arbeiten etwa 60 Personen. Das Unternehmen ist mittlerweile zu einem führenden Hersteller von Verbindungselementen, Baugruppen und Systemen in der Trinkwasserversorgung sowie Sanitär- und Haustechnik geworden. Die Struktur und Organisation des Unternehmens gliedert sich in die vier Geschäftsbereiche, Water, Industry, Clean, Digital (iQ water solutions)	**00:08:53 HS** Can you please briefly describe your company, for example which products are manufactured, how many employees do you have and which companies buy your products and what are the general business processes? **00:09:20 Respondent** So, the company had a balance sheet size of around 27.4 million in the financial year. Sales revenue amounted to almost 58 million. For 2024, we expect an increase of 10 million to 68 million. 70% of sales will be domestic, 25% achieved in other EU countries, and 5% in non-EU countries. We currently employ almost 200 people. Of these, more than half are employed in production. About 60 people work in the office. The company has now become a leading manufacturer of fasteners, assemblies, and systems for drinking water supply as well as sanitary and building technology. The structure and organisation of the company are divided into four business areas: Water, Water Industry, Clean, Digital (iQ water solutions) In the water sector, we develop, produce and sell our own products for drinking water supply exclusively through specialist wholesalers, with foreign business in the Benelux and Scandinavia being carried out by independent, locally operating companies.

Im Bereich Water entwickeln, produzieren und vertreiben wir Eigenprodukte in der Trinkwasserversorgung ausschließlich über den Fachgroßhandel, wobei das Auslandsgeschäft in Benelux und Skandinavien durch unabhängige, lokal operierende Gesellschaften wahrgenommen wird. Die zweite tragende Säule bildet der Bereich Industry. Mit der Herstellung und Montage von Komponenten und Baugruppen beliefert man global agierende Unternehmen in der Sanitär- oder Haustechnik. Der Geschäftsbereich Clean ist aus dem Geschäftsbereich Water herausgelöst worden, um ihm eine höhere Autarkie und Selbständigkeit zu geben. Dieser Geschäftsbereich bündelt alle Aktivitäten zur Reinigung und Desinfektion von Trinkwasser sowie Trinkwasseranlagen. Zur Beschleunigung der Entwicklungsaktivitäten nutzt man Räumlichkeiten in einem Digital Hub in Dortmund u. a. getragen durch das Fraunhofer- Institut IML (Anm.: Institut für Materialfluss und Logistik) und ISST (Anm.: Institut für Software- und Systemtechnik). Das Unternehmen bedient sich hier dem System der zwei Kulturen. Das heißt, die Organisation des Unternehmens findet sich einerseits in einer klassischen Hierarchie wieder. Andererseits nutzt man die agilen Managementmethoden und -strukturen. Wir arbeiten in einem dualen Betriebssystem. Während wir unsere hierarchische Struktur für unser Basis- und Bestandsgeschäft einsetzen, Water und Industry, nutzen wir die agile Networkorganisation, um Marktchancen schnell zu erkennen und umzusetzen (Clean und Digital). Außerdem wurden hierüber agile Projekte implementiert, von denen auch das Bestandsgeschäft wie z.B. die Produktion profitiert Wir produzieren nur im Inland. Im Ausland unterhalten wir lediglich Verkaufsstellen.	The second supporting pillar is the “Industry” sector. With the production and assembly of components and modules, we supply global companies in sanitary or household technology. The Clean division was separated from the Water division in order to give it greater self-sufficiency and independence. This business area bundles all activities for the cleaning and disinfection of drinking water and drinking water systems. To accelerate development activities, space in a digital hub in Dortmund is used, among other things. supported by the Fraunhofer Institute IML (note: Institute for Material Flow and Logistics) and ISST (note: Institute for Software and Systems Engineering). The company uses the system of two cultures here. This means that, on the one hand, the organization of the company is reflected in a classic hierarchy. On the other hand, agile management methods and structures are used. We work in a dual operating system. While we use our hierarchical structure for our basic and existing business, Water and Industry, we use the agile network organization to quickly identify and implement market opportunities (Clean and Digital). In addition, agile projects were implemented, from which existing business such as production also benefits We only produce domestically. We only have sales outlets abroad.

00:12:53 HS In ihrem Unternehmen spielen digitale Prozesse und automatisierte Produktionsverfahren eine wichtige Rolle. Wie sieht die IT-Infrastruktur des Unternehmens aus?	**00:12:53 HS** Digital processes and automated production methods play an important role in your company. What does the company's IT infrastructure look like?
00:13:09 Befragter Die Produktentwicklung und Vermarktung der neuen digitalen Systeme und Dienstleistungen unter dem neuen Markennamen „iQ“, findet in einem Digital Hub am Sitz des Fraunhofer Instituts in Dortmund statt. Der Umsatz im laufenden Geschäftsjahr lag mit EUR 57,8 Mio. 29% über Vorjahresniveau. Das rasante Wachstum wurde begleitet durch zunehmende Rohstoffpreiserhöhungen, die den Kunden durchgereicht wurden. Mit den wichtigsten Industriekunden bestehen langfristige Lieferverträge. Die Tendenz zu neuen, trinkwasserkonformen Werkstoffen (bleifrei) setzt sich weiter fort. Das Unternehmen nimmt hier eine führende Rolle in der Sanitär-Branche ein. Im Bereich Digital wurden überwiegend Projektumsätze im Software-Bereich realisiert. Aufgrund der komplexen und langfristigen Entwicklungs-Vorleistung hatten wir dies auch bereits vorausschauend moderat eingeplant. Dieser Geschäftsbereich ist auch nicht auf kurzfristige Umsatzerfolge ausgerichtet. Die Digitalisierung der Wasserwirtschaft wird vor allem durch langfristige, aber dafür nachhaltige Geschäftsmodelle getrieben. Trotz unterschiedlicher Marktmechanismen im Industriegeschäft und Water Eigenprogramm nutzen wir beide Geschäftsbereiche durch sinnvolle und ergänzende Sy-	**00:13:09 Respondent** The product development and marketing of the new digital systems and services under the new brand name “iQ” take place in a digital hub at the headquarters of the Fraunhofer Institute in Dortmund. At EUR 57.8 million, sales in the current financial year were 29% above the previous year's level. The rapid growth was accompanied by increasing raw material price increases that were passed on to customers. Long-term supply contracts exist with the most important industrial customers. The trend towards new materials that are compatible with drinking water (lead-free) continues. The company plays a leading role in the sanitary industry. In the digital area, project sales were predominantly realized in the software area. Due to the complex and long-term development pre-performance, we had already planned this moderately in advance. This business area is also not geared towards short-term sales success. The digitalization of the water industry is primarily driven by long-term but sustainable business models. Despite different market mechanisms in the industrial business and our own Water programme, we use both business areas through sensible and complementary synergies to ensure cost leadership in the industrial business and quality leadership in our

nergien, um sowohl im Industriegeschäft die Kostenführerschaft und im Eigenprogramm die Qualitätsführerschaft zu sichern. Mit „Digital“ streben wir eine zukünftige Technologieführerschaft an und Clean schließt die Lücke zur Trinkwasserversorgung mit nachhaltigen Lösungen, ohne dass sich diese vier Geschäftsbereiche hier in einem Widerspruch befinden.	own program. With “digital,” we strive for future technology leadership and Clean closes the gap in drinking water supply with sustainable solutions, without these four business areas being in contradiction.
Die Digitalisierung bleibt ein dominanter Treiber zur Transformation der Wirtschafts- und Arbeitswelt. Um die Chancen der Digitalisierung zu nutzen, ist eine leistungsfähige und flächendeckende Infrastruktur erforderlich. Wir haben dies frühzeitig erkannt und bereits vor einigen Jahren mit einem neuen Konzept die notwendigen Voraussetzungen geschaffen.	Digitalization remains a dominant driver for the transformation of the economic and working worlds. In order to take advantage of the opportunities offered by digitalization, a powerful, comprehensive infrastructure is required. We recognised this early on and created the necessary conditions with a new concept a few years ago.
Die Digitalisierung des Unternehmens wird als Chance gesehen und ist im vollen Gange. Zeitgleich werden Führungskräfte und Belegschaft auf die organisatorischen Herausforderungen vorbereitet. Die Brücke zwischen Digitalisierung und agiler Organisation bildet dabei unser digitaler Transformationsprozess.	The digitalization of the company is seen as an opportunity and is in full swing. At the same time, managers and employees are prepared for the organisational challenges. Our digital transformation process forms the bridge between digitalization and agile organisations.
Die digitale Transformation wird ein wesentlicher Beschleuniger für unser agiles Netzwerk - sowohl extern als auch intern. Wir planen für die nächsten Jahre eine Vervielfachung der interdisziplinären Initiativen. Eine CoP (Anm.: Community of Practice) fungiert als Katalysator und Unterstützer der Initiativen. Die wichtigsten Digitalisierungsprojekte haben wir in einem „Big Picture“ dargestellt.	Digital transformation will be a key accelerator for our agile network, both externally and internally. We are planning to multiply the number of interdisciplinary initiatives in the next few years. A CoP (Anm.: community of practice) acts as a catalyst and supporter of the initiatives. We have presented the most important digitization projects in a “big picture.”.
Führungskräfte, Belegschaft und CoP‘s werden eingehend auf die Arbeitsweise und Kultur vorbereitet. Wir haben hierzu ein Regelwerk erarbeitet und die interne Stelle eines „Transformation Managers“ geschaffen. Zur Steuerung und Koordination der Digitalisierungsprojekte haben wir zusätzlich die Funktion „Head of Digital Transformation“ eingerichtet.	Managers, staff, and CoPs are thoroughly prepared for the way we work and the culture. We have developed a set of rules for this and created the internal position of a “Transformation Manager”. To control and coordinate digitalization projects, we have also set up the “Head of Digital Transformation” function.

Die seinerzeit erarbeitete Unternehmensstrategie „xxxxx2025“ wurde unter der Führung einer renommierten Strategieberatung einem Strategy-Review unterzogen und in Teilen angepasst.	The corporate strategy “xxxxx2025” that was developed at the time was subjected to a strategy review and partially adjusted under the leadership of a renowned strategy consultancy.
00:17:05 HS Was sind die Leistungs-/Erfolgskennzahlen des Unternehmens? **00:17:21 Befragter** Wie in fast jedem produzierenden Unternehmen sind Umsatz, Deckungsbeitrag, Gewinn und Produktivitätskennzahlen auch für uns sehr wichtig. Dazu kommt dann halt noch die Einhaltung der Qualität. Gerade in der Produktion haben wir die KPIs in der Datenerhebung und Berichterstattung verfeinert. Das wäre u.a. der Durchsatz, also die Anzahl der produzierten Einheiten einer spezifischen Maschine. Dazu auch die Zykluszeit, die zur Herstellung eines Produkts benötigt wird. Sollten Produktionslinien umgestellt werden ist in der Fertigungsbranche auch die Umstellungszeit wichtig. Auf Maschinenebne sind die Ausfallzeitraten von Geräten für uns ein wichtiger Indikator. Die Ausfallzeiten von Geräten beinhalten sowohl geplante Ausfallzeiten als auch ungeplante. Auch die Ausfallzeit bis Inbetriebnahme oder Wiederinbetriebnahme zeigt an wie gut die Effektivität der Wartung von Maschinen sowie die Effektivität der Maschinen selbst ist. Durch effektive präventive Wartung kann die Ausfallzeit reduziert werden	**00:17:05 HS** What are the company's performance/success metrics? **00:17:21 Respondent** As in almost every manufacturing company, sales, contribution margin, profit, and productivity indicators are also very important for us. Then there is the maintenance of quality. Especially in production, we have refined the KPIs for data collection and reporting. This would include, among other things, the throughput, i.e., the number of units produced by a specific machine. This also includes the cycle time required to produce a product. If production lines are changed, the changeover time is also important in the manufacturing industry. At the machine level, equipment downtime rates are an important indicator for us. Equipment downtime includes both planned downtime and unplanned downtime. The downtime until launching or re-launching also shows how effective the maintenance of machines is, as well as the effectiveness of the machines themselves. Effective preventive maintenance can reduce downtime, creating a better manufacturing process. Companies want to keep this rate as low as possible.

und so ein besserer Herstellungsprozess geschaffen werden. Unternehmen wollen diese Quote so niedrig wie möglich halten. Im wirtschaftlichen Bereich sind noch die Nachfrageprognose, die Produktionserfüllung und die eingesparten Kosten jeweils ein wichtiger Faktor, letzteres auch weil in einer Formel die geschätzten Reparaturkosten, der daraus resultierende Produktionsverlust sowie die Kosten für die präventive Wartung zusammengeführt werden.	In the economic area, demand forecast, production fulfilment, and the costs saved are each important factors, the latter also because the estimated repair costs, the resulting production loss, and the costs for preventative maintenance are combined in a formula.
00:18:57 HS Welche dieser Faktoren würden Sie als die kritischen Erfolgsfaktoren im Geschäftsprozess des Unternehmens beschreiben? (Umsatz, Kosten und Investitionen und/oder Fähigkeiten und Ressourcen?)	**00:18:57 HS** Which of these factors would you describe as the critical success factors in the company's business process? (Sales, costs and investments and/or skills and resources?)
00:19:12 Befragter Natürlich ist die Gesamtkapitalrentabilität oder die im Jargon bekannte „Manufacturing KPI Return On Assets“ die zentrale finanzielle Metrik neben denen, die sich auf die Fertigung beziehen. Weil, wenn Sie keine Einnahmen haben, sind Sie auch kein Unternehmen! Dazu kommen noch die Herstellungskosten pro Einheit. Der Wert ist für uns sehr wichtig, da er die Gesamtkosten, also alle Kosten, die mit der Produktion zusammenhängen misst und diese dann durch die Anzahl der gefertigten Einheiten teilt.	**00:19:12 Respondent** Obviously, return on assets, or the jargon known as manufacturing KPI return on assets, is the key financial metric alongside those relating to manufacturing. Because if you don't have revenue, you're not a business company! Then comes the manufacturing cost per unit. This value is very important to us because it measures the total costs, i.e., all costs associated with production, and then divides these by the number of units produced.
00:19:46 HS Kommen wir zu den Praktiken des Cyber-Risikomanagements. Wie hat Ihr Unternehmen Cybersicherheitsrichtlinien im Risikomanagementprozess implementiert?	**00:19:46 HS** Let’s move on to cyber-risk management practices. How has your company implemented cybersecurity policies in the risk management process?

00:20:08 Befragter Seit einigen Jahren, also nach dem Hackerangriff, stützen wir uns dabei auf einen risikobasierten Ansatz, der sich an dem international anerkannten Standard der ISO 27001 orientiert. Als TISAX (Anm.: Trusted Information Security Assessment Exchange) zertifiziertes Unternehmen nutzen wir die dort eindeutig definierten Prozesse und organisatorische Zuständigkeiten, um auch den gestiegenen Anforderungen der Cybersicherheit gerecht zu werden und Risiken, wie Ransomware, angemessen zu begegnen. Informationssicherheit ist in der IT-Organisation etabliert und die berichten direkt an mich. Mit Direktionsrecht allen Mitarbeitern gegenüber – außer mir - ausgestattet, besteht Interventionsrecht im Fall von Sicherheitsverstößen oder unmittelbarem Handlungsbedarf. In einer Vielzahl von erlassenen und regelmäßig überwachten Sicherheitsrichtlinien werden das grundlegende Verhalten von Benutzern festgelegt, technische Erfordernisse definiert und Prüfmaßnahmen eingefordert. Dazu gehört ebenfalls das Ausnahmemanagement für abweichende temporäre Anforderungen und etwaige Grundprinzipien wie „Segregation of Duties“, „Need to know“ und „Least privilege access“. Abgerundet wird dieses Maßnahmenpaket durch eine Cybersicherheitsversicherung und eine vertragliche definierte und Vorfall-bezogene forensische Unterstützungsleistung durch einen externen Partner. Technische Maßnahmen sorgen mit der neuesten Hard- und Software sowie adäquaten Informationssicherheitsprozessen für eine solide Basis, um die Informationssicherheit zu gewährleisten.	**00:20:08 Respondent** For several years now, i.e., after the hacker attack, we have relied on a risk-based approach that is based on the internationally recognised standard ISO 27001. As a TISAX (Note: Trusted Information Security Assessment Exchange) certified company, we use the processes and organisational responsibilities clearly defined there to meet the increased cybersecurity requirements and adequately address risks such as ransomware. Information security is established in the IT organisation, and they report directly to me. Equipped with the right to direct all employees - except me - there is a right to intervene in the event of safety violations or an immediate need for action. In a multitude of issued and regularly monitored security guidelines, the basic behaviour of users is defined, technical requirements are defined, and testing measures are required. This also includes exception management for deviating temporary requirements and any basic principles such as “Segregation of Duties”, “Need to Know,” and “Least Privilege Access." This package of measures is rounded off by cybersecurity insurance and a contractually defined and incident-related forensic support service from an external partner. Technical measures with the latest hardware and software, as well as adequate information security processes, ensure a solid basis for ensuring information security.

Vor dem Hintergrund der sich extrem schnell wandelnden Marktveränderungen wurde durch die Geschäftsführung seinerzeit das Risk-Management-System neu definiert. Sicherlich geht es vornehmlich darum, potenzielle Risiken rechtzeitig zu erkennen, um umgehend und angemessen darauf reagieren zu können. Die Geschäftsführung hat sich dazu entschlossen, den bereits erkannten Marktrisiken durch entsprechende Vorkehrungen frühzeitig entgegenzuwirken. In den Planungsprämissen der Budgetplanung werden die erwarteten potenziellen Risiken erfasst und dem Beirat bzw. Gesellschafter im Rahmen der Budgetgenehmigung vorgelegt. Die Geschäftsführung informiert den Beirat bzw. Gesellschafter regelmäßig über den Fortgang durch ein aktives Risk-Management. Die Gefahr einer Unterbrechung von Lieferketten durch den Ukraine-Krieg wird für unser Unternehmen bis auf einzelne, wenige Komponenten derzeit als nicht kritisch eingestuft. Durch ausreichend hohe Eigenlagerbestände sowie ein bei uns geführtes Halbzeug-Konsignationslager sehen wir die Produktions- und Lieferfähigkeit als weiterhin unkritisch.	Against the background of extremely rapidly changing market changes, the management redefined the risk management system. The main aim is certainly to identify potential risks in good time in order to be able to react to them promptly and appropriately. The management has decided to counteract the market risks that have already been identified at an early stage by taking appropriate precautions. The expected potential risks are recorded in the planning premises of the budget planning and presented to the advisory board or shareholders as part of the budget approval. The management regularly informs the advisory board and shareholders about the progress of active risk management. The risk of supply chains being interrupted by the war in Ukraine is currently not classified as critical for our company, with the exception of a few individual components. Due to sufficiently high stock levels and a semi-finished consignment warehouse, we maintain that we continue to view production and delivery capability as uncritical.
00:23:43 HS Wie hoch ist das Cyber-Risiko in Ihrem Unternehmen? **00:23:50 Befragter** Die Frage kann ich nicht beantworten.	**00:23:43 HS** How high is the cyber-risk in your company? **00:23:50 Respondent** I can't answer that question.
00:24:07 HS	**00:24:07 HS**

Können Sie bitte erläutern, wie IT- und Cyber-Risiken monetär quantifiziert werden und wie dies die Priorisierung von Risiken im Managementprozess beeinflusst? **00:24:30 Befragter** Wir haben keinen quantitativen Ansatz um die Cyber-Risiken in Relation zu unseren materiellen und immateriellen Assets zu bestimmen. Wir verwenden mehr eine qualitative Risiko-Matrix, die die möglichen Auswirkungen durch verschiedene Angriffswege in Farben von grün bis rot darstellt. Dabei klassifizieren wir die Angriffswege als „Zugriff über das Internet“, „Physischer Zugriff auf das Netzwerk“, „E-Mail-Phishing“ und „Zugriff über das interne Netzwerk“.	Can you please explain how IT and cyber-risks are quantified in monetary terms and how this influences the prioritisation of risks in the management process? **00:24:30 Respondent** We do not have a quantitative approach to determining cyber-risks in relation to our tangible and intangible assets. We use more of a qualitative risk matrix that shows the potential impact of different attack vectors in colours ranging from green to red. We classify the attack paths as "Access via the internet", "Physical access to the network", "Email phishing" and "Access via the internal network".
00:25:17 HS Welchen potenziellen finanziellen Schäden ist das Unternehmen im Zusammenhang mit Cyber-Risiken ausgesetzt? **00:25:30 Befragter** Wir hatten ja einen Hackerangriff und dadurch hat sich eine reelle Zahl ergeben. Jetzt, nach Kauf einer Cyberversicherung, wäre die Netto-Belastung für das Unternehmen wesentlich geringer und im Hinblick auf unser zu erwirtschaftendes Nettoergebnis auch verträglicher. Aber genaue Zahlen möchte ich Ihnen aus Vertraulichkeitsgründen nicht sagen.	**00:25:17 HS** What potential financial losses is the company exposed to in connection with cyber-risks? **00:25:30 Respondent** We had a hacker attack, and that resulted in a real figure. Now, after purchasing cyber-risk insurance, the net burden for the company would be significantly lower and also more acceptable in terms of our net profit. But I don't want to give you exact figures for reasons of confidentiality.
00:25:40 HS	**00:25:40 HS**

Können Sie bitte etwas über die Cyber-Risikostrategie Ihres Unternehmens sagen? (Falls nicht vorhanden, können Sie bitte die Gründe erläutern?) **00:25:55 Befragter** Gegen IT-Risiken ist das Unternehmen weitgehend gewappnet. Wir verfügen über eine Cyber-Versicherung und unterziehen uns regelmäßig einem Security-Check durch den Versicherer. Ein umfassender Versicherungsschutz wurde in Abstimmung mit dem Versicherungsmakler vereinbart. Darüber hinaus haben wir ein Notfallkonzept erarbeitet. Mitarbeiterschulungen zum Umgang und zur Sensibilisierung potenzieller Gefahren finden zyklisch statt.	Can you please say something about your company's cyber-risk strategy? (If not available, can you please explain why?) **00:25:55 Respondent** The company is largely armed against IT risks. We have cyber-risk insurance and regularly undergo a security check by the insurer. Comprehensive insurance coverage has been agreed upon in consultation with the insurance broker. We have also drawn up an emergency plan. Employee training courses on dealing with and raising awareness of potential risks take place on a regular basis.
00:26:11 HS Welche Maßnahmen ergreift Ihr Unternehmen, um Cyber-Risiken zu managen oder zu mindern? **00:26:30 Befragter** Wir machen eine Aufzeichnung der gesamten Hardware und Software im Unternehmen. Typischerweise umfasst dies Softwarelizenzen und Geräte innerhalb und außerhalb des Netzwerks sowie IoT, ICS usw. Unternehmensressourcen können sich ständig ändern: Geräte werden hinzugefügt und ausgemustert, physische Maschinen werden auf virtuelle Maschinen migriert, Benutzer kommen und gehen und verschiedene Stakeholder installieren und aktualisieren Software (mit oder ohne Genehmigung).	**00:26:11 HS** What measures does your company take to manage or mitigate cyber-risks? **00:26:30 Respondent** We keep a record of all hardware and software in the company. Typically, this includes software licenses and devices on and off the network, as well as IoT, ICS, etc. Enterprise resources can change constantly: devices are added and retired, physical machines are migrated to virtual machines, users come and go, and different stakeholders install and update software (with or without permission).

Auf dieser Basis treffen wir wichtige Entscheidungen über IT-Sicherheits-Strategien für die einzelnen Elemente des Netzwerks. Ziel des Unternehmens muss es schon sein, eine insgesamt akzeptable Risikolage herzustellen. Auch erreichen wir mit NAC (Anm.: Network Access Control) eine Netzwerktransparenz und Zugriffsverwaltung. Das heißt durch gesetzte Richtlinien hinsichtlich Zugriffes auf Geräten von Benutzern in unseren Unternehmensnetzwerken, wie zum Beispiel „Zero Trust“ können wir die Risiken auf diese Weise über die Benutzerzugriffsberechtigungen nach Bedarf und abhängig von der beruflichen Rolle jeder Person steuern und bewerten. Bezüglich einer möglicher Kompromittierung von Daten von außen haben wir durch Trennung kritische Netzwerke und Dienste durch Firewalls und andere Netzwerkabwehrmaßnahmen getroffen, um bei einem Hackerangriff den unzulässigen Datenverkehr zu blockieren und Inhalte einzuschränken. Nach dem Hackerangriff haben wir auch unseren Disaster-Recovery-Plan überarbeitet. Die dadurch leidvoll erfahrenen Einschränkungen in der Geschäftskontinuität sollten uns zukünftig nicht mehr widerfahren. Das ausgearbeitete Dokument befasst sich mit Datenschutz, Datenwiederherstellung, Offsite-Backups, Systemwiederherstellung, Konfigurationen und Protokollen. Damit wir auch zukünftig Cyberangriffe wirksam abwehren, fordert der Plan zudem regelmäßige Überprüfungen der gesamten IT-Sicherheit hinsichtlich Identifizierung etwaiger Lücken im System und organisatorischer Maßnahmen diese zu schließen bzw. zu minimieren.	On this basis, we make important decisions about IT security strategies for the individual elements of the network. The company's goal must be to create an overall acceptable risk situation. We also achieve network transparency and access management with NAC (Note: Network Access Control). This means that by setting policies regarding access to users' devices on our corporate networks, such as "Zero Trust", we can control and assess risks via user access permissions as needed and depending on each person's job role. Regarding possible compromise of data from outside sources, we have implemented firewalls and other network defence measures to block unauthorised data traffic and restrict content in the event of a hacker attack by separating critical networks and services. After the hacker attack, we also revised our disaster recovery plan. We should no longer experience the painful restrictions on business continuity that we will experience in the future. The prepared document covers data protection, data recovery, offsite backups, system recovery, configurations, and protocols. So that we can continue to effectively ward off cyberattacks in the future, the plan also calls for regular reviews of the entire IT security to identify any gaps in the system and organisational measures to close or minimise them. With regard to suppliers and customers, i.e., with regard to possible entry points or endpoints, we have subjected them to special monitoring so that an attacker cannot exploit possible vulnerabilities or security problems with endpoints for security attacks.

Bezüglich Lieferanten und Kunden, also hinsichtlich möglicher Eintrittspunkte oder Endpunkte, haben wir die einer besonderen Überwachung unterzogen, damit ein Angreifer mögliche Schwachstellen oder /Sicherheitsprobleme bei Endpunkten nicht für Sicherheitsangriffe ausgenutzt werden können.	
00:29:20 HS Wie gut sehen Sie das Unternehmen gegen Cyber-Risiken gewappnet? **00:29:30 Befragter** Nach den getroffenen Maßnahmen, wie also vorhin beschrieben, fühlen wir uns relativ sicher. Auch wegen der Unterstützung durch den Cyber-Versicherer, der uns regelmäßig über die aktuellen Sicherheitsanforderungen und durch seinen Service auf dem Laufen hält.	**00:29:20 HS** How well prepared do you think the company is against cyber-risks? **00:29:30 Respondent** After the measures we have taken, as described earlier, we feel relatively secure. Also because of the support from the cyber insurer, who regularly keeps us up to date with the latest security requirements and their service.
00:29:57 HS Welche Cyber-Risiken sehen Sie als Bedrohung für ihr Unternehmen an? **00:30:11 Befragter** Mit dem getätigten Ransomware Angriff hatten wir eben die katastrophalen Ausmaße eines Hackerangriffs erfahren. Ansonsten sind es die Phishing-Angriffe, in denen Hacker versuchen die Mitarbeiter zur Weitergabe von vertraulichen Informationen - also wie Anmeldedaten oder vertrauliche Unternehmensinformationen - weiterzugeben. Der Weg ins IT-Netzwerk führt ja oft über die Mitarbeiter!	**00:29:57 HS** Which cyber-risks do you see as a threat to your company? **00:30:11 Respondent** With the ransomware attack, we just experienced the catastrophic extent of a hacker attack. Otherwise, it's phishing attacks in which hackers try to trick employees into passing on confidential information, such as login details or confidential company information. The way into the IT network often leads via the employees!

Dafür hat sich ja meines Wissens der Begriff Social- Engineering oder Social- Hacking auch in der IT-Sicherheit eingebürgert, da auch hier das menschlichen Verhaltens von Mitarbeiter ausgenutzt wird, um sicherheitstechnisch relevante Daten zu gewinnen. Dabei gehen die Täter das vermeintlich schwächtes Glied der Sicherheitskette an, um über Vertrauen, Hilfsbereitschaft, Angst oder Respekt vor Autorität aus, einen unserer Mitarbeiter gezielt zu manipulieren.	As far as I know, the term social engineering or social hacking has also become established in IT security, as the human behaviour of employees is also exploited here in order to obtain security-relevant data. The perpetrators target the supposedly weakest link in the security chain in order to manipulate one of our employees through trust, helpfulness, fear, or respect for authority.
00:31:23 HS Wie bewertet das Unternehmen im Umgang mit anderen Unternehmen (Lieferanten, Kunden) deren CR-Exponierung, Minderungsmaßnahmen oder CRM-Strategien? **00:31:35 Befragter** Ja, hatte ich ja vorhin auch schon gesagt, wir haben uns auf die Eintrittspunkte oder Endpunkte und deren möglichen Schwachstellen konzentriert. Gerade bei intelligenten Lieferketten, die Material just in time dahin bringen, wo es benötigt wird, sind im produzierenden Gewerbe zunehmend so selbstverständlich wie intelligente Steuerketten, die wissen, wann sie das nächste Mal gewartet werden müssen. Damit wir unsere Maschinendaten gut vor Hackerangriffen schützen, sind wir sehr vorsichtig bei dem doch geringen Datenaustausch geworden.	**00:31:23 HS** When dealing with other companies (suppliers, customers), how does the company assess their CR exposure, mitigation measures or CRM strategies? **00:31:35 Respondent** Yes, as I said earlier, we focused on the entry points or end points and their potential weaknesses. Intelligent supply chains in particular, which bring material just in time to where it is needed, are increasingly as common in the manufacturing industry as intelligent control chains that know when they next need to be serviced. In order to protect our machine data from hacker attacks, we have become very careful with the small amount of data exchanged.
00:32:24 HS Wie hoch sind die geschätzten Kosten für das Cyber-Risikomanagement und die Minderungs-maßnahmen des Unternehmens?	**00:32:24 HS** What is the estimated cost of the organization's cyber-risk management and mitigation efforts?

00:32:23 Befragter Wir geben jährlich einen Millionenbetrag für die Aktualisierung der IT-Landschaft aus. Einen eigenen Kostenblock für die IT- bzw. Cybersicherheit haben wir nicht.	**00:32:23 Respondent** We spend millions annually updating the IT landscape. We do not have a separate cost block for IT or cyber security.
00:32:40 HS Wurde Ihr Unternehmen bereits Opfer eines Cyber-Angriffs? 00:32:45 Befragter Ja, wir hatten uns in falscher Sicherheit gewogen und einen ziemlich heftigen Cyberangriff erfahren. Wir haben dann relativ schnell gemerkt, dass die Folgen dieses Cyberangriffs buchstäblich vernichtend für unser Unternehmen sein könnten. Ein Mitarbeiter hatte im Mai letzten Jahres den Rechner gestartet und schnell gemerkt, dass etwas nicht stimmt. Als die Systeme hochgefahren wurden kam dann schon die Meldung der Hacker. Die Angreifer hatten fast die komplette Server-Landschaft des Unternehmens mit Hilfe eines Ryuk-Trojaner lahmgelegt, und zwar so richtig. Alle unsere Mitarbeiter konnten keine E-Mails mehr verschicken, keine Kundentermine mehr einsehen und die Produktion kam zum Erliegen. Umgerechnet 650.000 Euro in Bitcoins sollte die Firma zahlen, damit die Hacker die Systeme wieder freigeben. Nach internen Absprachen und auch Konsultation mit den Sicherheitsbehörden hatten wir beschlossen, dass die Zahlung eines Lösegelds für uns nicht in Frage kommt und wir auch nicht mit den Tätern verhandeln wollen. Was folgte, war eine Betriebsunterbrechung von mehr als einem Monat. Weil auch die Backups fast vollständig verschlüsselt wurden, mussten alle Systeme von unseren	**00:32:40 HS** Has your company already been the victim of a cyberattack? **00:32:45 Respondent** Yes, we had a false sense of security and experienced a pretty serious cyberattack. We then realised relatively quickly that the consequences of this cyberattack could be literally devastating for our company. An employee started the computer in May of last year and quickly noticed that something was wrong. As soon as the systems were booted up, the report from the hackers came. The attackers had almost paralysed the company's entire server landscape with the help of a Ryuk Trojan. All of our employees could no longer send emails or view customer appointments, and production came to a standstill. The company had to pay the equivalent of 650,000 Euros in Bitcoins so that the hackers would release the systems again. After internal discussions and consultation with the security authorities, we decided that paying a ransom was out of the question for us and that we also did not want to negotiate with the perpetrators. What followed was a business interruption lasting more than a month. Because the backups were almost completely encrypted, all systems had to be reinstalled by our

internen Spezialisten neu aufgesetzt werden. Ein Großteil der Stammdaten wie Kundendaten, Maschinendaten, Verträge etc. ging größtenteils verloren. All das musste von den Mitarbeitern aufwendig von Hand neu eingeben werden. Doch das war nur die interne Sicht der Dinge. Nur wenige Kunden hatten Verständnis für die dramatische Lage gezeigt und uns wegen Produktionsausfall und Lieferausfällen mit Vertragsstrafen in erheblicher Größenordnung konfrontiert. So kamen neben den eh schon hohen Kosten für die Wiederherstellung der Systeme auch die Vertragsstrafen noch dazu. Durch den Cyber-Angriff ist uns also ein beträchtlicher Schaden entstanden, der knapp an unserer Existenz gekratzt hat. In jedem Fall habe ich eine gewisse Stressresistenz entwickelt. Als Unternehmer ist es ja so, dass man eben etwas unternimmt, wenn es ein Problem gibt. Nach der Cyberattacke konnte ich aber nichts tun, sondern musste mich darauf verlassen, dass die Spezialisten das Richtige unternehmen. Ich war also gezwungen, eine größere Gelassenheit zu entwickeln.	internal specialists. A large part of the master data, such as customer data, machine data, contracts, etc., was largely lost. The employees had to laboriously re-enter all of this by hand. But that was only the internal view of things. Only a few customers had shown understanding of the dramatic situation and confronted us with contractual penalties of considerable magnitude due to loss of production and delivery. In addition to the already high costs of restoring the systems, there were also contractual penalties. The cyberattack caused us considerable damage, which barely scratched our existence. In any case, I have developed a certain resistance to stress. As an entrepreneur, you just do something when there is a problem. After the cyberattack, there was nothing I could do but rely on the specialists to do the right thing. So, I was forced to develop greater calm.
00:35:42 HS Und wie haben Sie im Nachgang auf diesen Cyber-Vorfall reagiert? **00:035:49 Befragter** Ja also, wie ich eingangs schon gesagt habe, wir haben das Cyberrisiko für lange Zeit verdrängt.	**00:35:42 HS** And how did you subsequently react to this cyber incident? **00:035:49 Respondent** So yes, as I said at the beginning, we have ignored cyber-risk for a long time. Of course, we knew that the threat of cybercrime was to be expected in the manufacturing sector in Germany - including small and medium-sized companies. But when it comes to your own business, you are much more confident and think that this won't happen to us.

Natürlich wussten wir, dass im produzierenden Gewerbe in Deutschland – auch bei den kleinen und mittelgroßen Unternehmen - mit der Bedrohung durch Cyberkriminalität zu rechnen ist. Aber wenn es jedoch um den eigenen Betrieb geht, ist man wesentlich zuversichtlicher und denkt, das wird uns schon nicht passieren. Im Nachgang haben wir diesen Angriff nochmals analysiert und versucht, die Schwachstelle in unseren Computersystemen zu analysieren. Vor allem sollte herausgefunden werden, wie wir uns zukünftig gegen solch hochprofessionellen Angriffen von Cyberkriminellen mit Ransomware schützen können, damit wir eine Verschlüsselung und Diebstahl von Daten und eventuellen Firmengeheimnissen nicht nochmal durchmachen müssen. Als wesentliche Maßnahmen zur IT-Sicherheit haben wir den Turnus bei den Sicherheitskopien erhöht und auch den Ablageort außerhalb des Unternehmens bestimmt. Sicherheitsupdates werden jetzt automatisch wöchentlich erstellt und ohne Netzzugang aufbewahrt, damit sie bei einem Angriff nicht in Mitleidenschaft gezogen werden. Zudem haben wir die Vergabe an Administratoren-Rechte auf wenige Mitarbeiter eingeschränkt die Firewalls aktualisiert und verstärkt und für E-Mails eine „Sandbox“ eingerichtet, wo alle verdächtigen Emails landen und außerhalb des firmeneigenen Netzwerks geöffnet werden können. Auch haben wir das Thema Risikomanagement auf die Agenda gesetzt und ein schriftliches Konzept für den Notfall, also ein Notfallkonzept, erstellt, damit wir bei einem massiven Angriff auf fertige Abläufe zugreifen können. Dazu haben wir einen externen Dienstleister miteingebunden. Und bei allen technisch und administrativ aufwendigen Vorkehrungen, oft kommen die Hacker doch auf den vermeintlich einfachsten Wegen ins System: über E-Mails.	Afterwards, we analysed this attack again and tried to identify the vulnerability in our computer systems. Above all, we should find out how we can protect ourselves against such highly professional attacks by cyber criminals with ransomware in the future so that we don't have to go through encryption and theft of data and possible company secrets again. As key IT security measures, we have increased the frequency of backup copies and also determined the storage location outside the company. Security updates are now automatically created on a weekly basis and kept off the network so that they are not affected in the event of an attack. We have also limited the allocation of administrator rights to a few employees, updated and strengthened firewalls and set up a “sandbox” for emails where all suspicious emails end up and can be opened outside the company network. We have also put the topic of risk management on the agenda and created a written emergency concept so that we can access ready-made processes in the event of a massive attack. For this purpose, we involved an external service provider. And despite all the technically and administratively complex precautions, hackers often get into the system in the seemingly easiest way: via email.

00:38:37 HS Kommen wir nun zum dritten Block der Fragen, bezüglich ihres Cyber-Risikos in dem Industrie 4.0/IoT Umfeld. Wie ist Ihre Einschätzung zu Cyber Risiko und Industrie 4.0, moderne vernetzte Produktionsanlagen?	**00:38:37 HS** Let's now move on to the third block of questions regarding your cyber-risk in the Industry 4.0/IoT environment. What is your assessment of cyber-risk and Industry 4.0, modern networked production facilities?
00:38:49 Befragter Eine der größten Herausforderungen in naher Zukunft stellt die Digitalisierung der Branche dar. Hierin liegen aber auch unseres Erachtens nach den bedeutendsten Chancen für unser Unternehmen. Wir haben frühzeitig erkannt, dass die Digitalisierung einen Paradigmenwechsel erfordert und bei einer erfolgreichen Transformation erhebliche Marktpotenziale bietet. Hierzu wurde seinerzeit eine umfassende Markt- und Unternehmensanalyse durchgeführt und die sich abzeichnenden Veränderungen durch die Digitalisierung auf Prozesse, Produktion, Markt- und Verbraucherverhalten und deren Folgen ausführlich beschrieben. In einer Digitalisierungs-Roadmap haben wir gemeinsam mit dem Fraunhofer Institut die wichtigsten Maßnahmen erarbeitet. Diese werden jetzt sukzessive umgesetzt. Im Bereich der Produktion liegt für uns der Fokus auf der Schaffung von mehr Intelligenz in den Prozessen, z. B. durch eine digital unterstützte Auftragsabwicklung, intel-	**00:38:49 Respondent** One of the biggest challenges in the near future is the digitalization of the industry. In our opinion, this also represents the most significant opportunity for our company. We recognised early on that digitalization requires a paradigm shift and, if the transformation is successful, offers significant market potential. For this purpose, a comprehensive market and company analysis was carried out, and the emerging changes due to digitalization in processes, production, market, and consumer behaviour and their consequences were described in detail. Together with the Fraunhofer Institute, we have developed the most important measures in a digitalization roadmap. These are now being implemented gradually. In the area of production, our focus is on creating more intelligence in the processes, e.g., through digitally supported order processing, intelligent containers, and the use of 3D printers. At the same time, the collaboration between digital technologies and

ligente Behälter und den Einsatz von 3D-Druckern. Gleichzeitig ist für uns die Kollaboration von digitalen Technologien und unseren Mitarbeitern von großer Bedeutung, zum Beispiel im Kontext von Robotik und automatischen Transporten.	our employees is of great importance to us, for example, in the context of robotics and automatic transport.
Weiteres Potenzial sehen wir in der ganzheitlichen Digitalisierung der Verwaltung. Von digitaler Belegerkennung über digitale Fertigungsaufträge bis zur digitalen Kundenakquise haben wir in nahezu allen Bereichen Initiativen gestartet. Unsere Kunden nehmen vor allem die Entwicklungen im Bereich unserer intelligenten Produkte und Geschäftsmodelle wahr.	We see further potential in the holistic digitalization of administration. From digital document recognition to digital production orders to digital customer acquisition, we have launched initiatives in almost all areas. Our customers are particularly aware of developments in the area of our intelligent products and business models.
Mit „iQ Water Solutions“ haben wir eine neue Marke aufgebaut und entwickeln gemeinsam mit starken Partnern unser Portfolio an digitalen Produkten weiter. Cloud- und Plattformtechnologien kommen hier zum Einsatz, um unseren Kunden umfassende Lösungen aus der Verbindung von digitalen, datenbasierten Services mit unserer starken Basis, den physischen Produkten, zu bieten.	With “iQ Water Solutions,” we have built a new brand and are further developing our portfolio of digital products together with strong partners. Cloud and platform technologies are used here to offer our customers comprehensive solutions by combining digital, data-based services with our strong base of physical products.
Den Querschnitt bildet die agile Organisation im Zentrum unseres Handelns. Sie vernetzt alle Digitalisierungsbereiche wie Produktion, Produkte, Prozesse und Geschäftsmodelle und ist die Basis für die erfolgreiche Umsetzung.	The cross-section is the agile organisation at the centre of our actions. It connects all areas of digitalization, such as production, products, processes, and business models, and is the basis for successful implementation.
Neben Ersatz- und Neuinvestitionen werden wir umfangreich in Digitalisierungsprojekte investieren.	In addition to replacement and new investments, we will invest extensively in digitalization projects.
Wir sind nach DIN EN 9001:2015 sowie dem Energiemanagement-System ISO 50001 zertifiziert.	We are certified according to DIN EN 9001:2015 and the energy management system ISO 50001. (Note: DIN EN 9001:2015 is the world's most successful and best-known management system for quality management. Companies that implement the requirements of the standard increase their customer satisfaction and efficiency. They strengthen their competitiveness and grow faster.)
(Anm.: DIN EN 9001:2015 ist das weltweit erfolgreichste und bekannteste Managementsystem für Qualitätsmanagement. Unternehmen, die die Anforderungen der Norm umsetzen, erhöhen ihre Kundenzufriedenheit und ihre Effizienz. Sie stärken ihre Wettbewerbsfähigkeit und wachsen schneller.)	

00:42:21 HS Ist Ihr Unternehmen von diesem Problem betroffen? Und welche Strategien/Maßnahmen gibt es in diesem Zusammenhang?	**00:42:21 HS** Is your company affected by this issue? And what strategies/measures are there in this context?
00:42:30 Befragter In unserer Eigenwahrnehmung in puncto Informationssicherheit bei den vernetzten Produktionsmaschinen machen wir uns derzeit keine großen Sorgen. Natürlich kann da bei einem Hackerangriff im produzierenden Gewerbe viel passieren, vor allem, wenn die Maschinen quasi die Fertigung selbst organisieren und intelligente Roboter Menschen bei der Fertigung zur Hand gehen, also ganz im Sinne von Industrie 4.0. Natürlich ist man geneigt, bei dieser positiven Selbsteinschätzung sowie der internen Meinung, die Firma ist unter dem Radar von Hackern, sich zu überschätzen. Vielleicht würde bei einem Stresstest das Ergebnis nicht schön ausfallen und eventuell unsere Systeme gehackt, Daten manipuliert und Maschinen in den Stillstand geführt werden. Das Problem scheint ja auch zu sein, dass die Systeme auch dann keine Warnung ausgeben, wenn Anomalien auftreten. Wichtig ist, dass wir in Stufe eins den Eingangsbereich des Unternehmens Cyber-sicherheitstechnisch gesichert haben, damit die Möglichkeiten leicht in unser Netzwerk einzudringen oder an Passwörter von Angestellten zu gelangen erstmal ausreichend verhindert wird. Bei Phishing-Mails darf man natürlich die Schulung der ganzen Belegschaft nicht vergessen, da hier ja immer eine menschliche Schwachstelle besteht in unser System einzudringen und dann einen Angriff auf alle möglichen Datenbanken und Maschinensteuerungen der Unternehmen auszuführen.	**00:42:30 Respondent** In our own perception of information security for networked production machines, we are currently not particularly worried. Of course, a lot can happen in the event of a hacker attack in the manufacturing industry, especially when the machines virtually organise production themselves and intelligent robots help people with production, in the spirit of Industry 4.0. Of course, given this positive self-assessment and the internal opinion that the company is under the radar of hackers, one is inclined to overestimate oneself. Perhaps the result of a stress test would not be good, and our systems might be hacked, data manipulated, and machines brought to a standstill. The problem also seems to be that the systems do not issue a warning even when anomalies occur. It is important that in level one we have secured the company's entrance area with cyber security so that the possibility of easily breaking into our network or obtaining employee passwords is sufficiently prevented.

So, was ich gelesen habe sind allein über Phishing-Mails und gefälschte Webseiten vielfach an die Zugangsdaten von Mitarbeiter oder gaben diese durch Klicken auf Links die Möglichkeit für Cyberkriminelle leicht Schadsoftware im Firmensystem zu installieren. In reaktiven Maßnahmen waren die Unternehmen aber scheinbar doch in der Lage die „physische Sicherheit“ weitestgehend wieder herzustellen.	When it comes to phishing emails, you should of course not forget to train the entire workforce, as there is always a human vulnerability to break into our system and then carry out an attack on all possible databases and machine controls of the company. From what I've read, there are often phishing emails and fake websites that give employees access to data or give cybercriminals the opportunity to easily install malware in the company system by clicking on links. However, through reactive measures, the companies were apparently able to largely restore “physical security”.
00:44:59 HS Wie schätzen Sie das Cyber-Risiko und Internet of Things (IoT)-Geräte ein? **00:45:11 Befragter** Eine zentrale Herausforderung ist die Harmonisierung der verschiedenen Protokolle. Es gibt mehrere IoT-Kommunikationsprotokolle, die in der Kommunikation zwischen Geräten im IoT-Netzwerk verwendet werden. IoT-Protokolle sollen sicherstellen, dass Informationen, die von einem Gerät oder Sensor stammen, von einem anderen Gerät, Gateway oder Service gelesen und interpretiert werden können. Wenn die Übertragungsprotokolle keine Sicherheit beinhalten, besteht die Gefahr, dass die Daten während der Übertragung manipuliert werden. Dies führt zu dem Problem, dass Analysen auf diesen veränderten Daten basieren und zu falschen Schlussfolgerungen führen. Nehmen wir vorausschauende Wartung von Maschinen in unserem Unternehmen als Beispiel. Werden falsche Daten durch ein Datenleck übertragen, wird der Algorithmus, der zum Beispiel zukünftige Szenarien für die Ausfallrate der Maschine berechnen soll,	**00:44:59 HS** How do you assess cyber-risk and Internet of Things (IoT) devices? **00:45:11 Respondent** A key challenge is the harmonisation of the various protocols. There are several IoT communication protocols used for communication between devices in the IoT network. IoT protocols are designed to ensure that information coming from one device or sensor can be read and interpreted by another device, gateway, or service. If the transmission protocols do not include security, there is a risk that the data will be manipulated during transmission. This leads to the problem that analyses are based on, which leads to incorrect conclusions.

so geändert, dass er falsche Werte generiert, was für mich wieder zu zusätzlichen Kosten führt. Zum Beispiel, indem man einen Wartungsmechaniker zu oft verwendet oder zusätzliche Kosten an sich nimmt, weil ich Ausfälle nicht richtig vorhersagen kann.	Let's take the predictive maintenance of machines in our company as an example. If incorrect data is transmitted due to a data leak, the algorithm that is supposed to calculate future scenarios for the machine's failure rate, for example, is changed so that it generates incorrect values, which again leads to additional costs for me. For example, using a maintenance mechanic too often or incurring additional costs because I cannot correctly predict failures.
00:46:33 HS Wenn ja, erläutern Sie bitte, wie und welche Strategien/Maßnahmen in diesem Zusammenhang existieren?	**00:46:33 HS** If yes, please explain how and what strategies/measures exist in this context?
00:46:39 Befragter Es ist wichtig, vernünftige Sicherheitsmechanismen umzusetzen und sie während des gesamten Lebenszyklus von IoT-Projekten dauerhaft zu erneuern. Dazu gehört zum Beispiel die zertifikatbasierte Authentifizierung, die Sicherstellung, dass auch Geräte in Bezug auf die IT-Sicherheit abgedeckt werden und immer wieder überprüft werden, ob die Zertifikate und Authentifizierungsmechanismen gültig sind und dass die Daten während der Übertragung nicht geändert wurden. Umgekehrt bedeutet dies, dass erneuerbare Sicherheit in IoT-Lösungen umgesetzt werden müssen. Leider erleben wir immer wieder, dass eine Lösung einfach umgesetzt wird, weil sie schnell erfolgen muss und Cybersicherheit als zentraler Faktor entlang des gesamten Lebenszyklus im IoT-Sektor vernachlässigt wird. Auf der anderen Seite gibt es die Möglichkeit, durch Segmentierung von Netzen – also die gezielte Nicht-Vernetzung – eine gewisse Sicherheit zurückzugewinnen. Das geht	**00:46:39 Respondent** It is important to implement sensible security mechanisms and continually renew them throughout the lifecycle of IoT projects. This includes, for example, certificate-based authentication, ensuring that devices are also covered in terms of IT security and that it is continually checked whether the certificates and authentication mechanisms are valid and that the data has not been changed during transmission. Conversely, this means that renewable security must be implemented in IoT solutions. Unfortunately, we often neglect cybersecurity as a central factor throughout the entire life cycle of the IoT sector, simply because we need to implement a solution quickly. On the other hand, there is the possibility of regaining a certain level of security through segmentation of networks, i.e., targeted non-networking. Of course, this goes far beyond the individual components and also includes the strategic aspect. The so-

aber natürlich weit über die einzelne Komponente hinaus und beinhalte auch den strategischen Aspekt. Die sogenannte Zwiebel- Architektur kann helfen, die steigende Komplexität zu beherrschen. Hierbei wird in den obersten Schichten ein einzelner Zugangspunkt eingerichtet, der gut abgesichert sein muss. Alle darunter liegenden Systeme und Komponenten reagieren auf Bedrohungen, wie es ihre Ressourcen, Rechenzeit und Speicher, erlauben. Damit gewinnt man Kontrolle zurück und kann im Notfall an dem zentralen Knoten reagieren.	called onion architecture can help manage increasing complexity. This involves setting up a single access point at the top layers, which must be well secured. All underlying systems and components respond to threats as their resources, computing time, and memory allow. This gives you back control and allows you to react at the central node in an emergency.
00:48:27 HS Welche Cyber-Verflechtungen mit anderen Unternehmen (Supply Chain) gibt es? **00:48:37 Befragter** Wir haben ein ERP-System (Anm.: Enterprise Resource Planning) und ein integraler Bestandteil von Geschäftsprozessen ist der elektronischer Datenaustausch (EDI, Electronic Data Interchange). Das gilt auch beim Warentransfer zwischen den Betrieben, wo jetzt in unserem Fall nicht so gewaltige Mengen an Informationen ausgetauscht werden. Besonders in den Zeiten von Industrie 4.0 fällt es schon schwer, ohne diese Standards Informationen zwischen den einzelnen Betrieben einer Fertigungskette auszutauschen. Das Supply-Chain-Management-System (SCM) leistet die nötige Hilfe hier im Datenaustausch. Allerdings muss man bezüglich der Anbindung des SCM an das ERM schon aufpassen. Bevor man mehrere Betriebe einer Fertigungskette über ein SCM-System miteinander verbindet, muss man genau die Sicherheit der Daten prüfen, da diese auch gehackt werden können. Niemand teilt gerne mit fremden Unternehmen die Details seiner Fertigungsstrecken, des Warenflusses oder gar über die Häufigkeit von technischen	**00:48:27 HS** What cyber connections with other companies (supply chain) are there? **00:48:37 Respondent** We have an ERP system (note: Enterprise Resource Planning), and an integral part of business processes is electronic data interchange (EDI, Electronic Data Interchange). This also applies to the transfer of goods between companies, where, in our case, not such huge amounts of information are exchanged. Especially in the age of Industry 4.0, it is difficult to exchange information between the individual companies in a production chain without these standards. The supply chain management system (SCM) provides the necessary help in data exchange. However, you have to be careful about connecting the SCM to the ERM. Before you connect several companies in a production chain via an SCM system, you must carefully check the security of the data, as it can also be hacked. Nobody likes to share the details of their production lines, the flow of goods, or even the frequency of technical

Problemen und Fertigungsfehlern. Allerdings sind auch die Vorteile in einem schnellen Austausch relevanter Informationen zu sehen, die alle Betriebe innerhalb unserer Wertschöpfungskette schnell auf Veränderungen reagieren lässt. Anstatt aber alle Daten allen Teilnehmern zur Verfügung zu stellen, wählen wir nur einzelne, relevante Datensätze, wie etwa Lagerbestände oder Kapazitätsdaten, aus und speisen diese über unser ERP-System ein. So können Sicherheitsbedenken minimiert werden, während die Unternehmen die meisten Vorzüge des Supply-Chain-Managements genießen können.	problems and manufacturing errors with third-party companies. However, the advantages can also be seen in the rapid exchange of relevant information, which allows all companies within our value chain to react quickly to changes. Instead of making all data available to all participants, we only select individual, relevant data sets, such as inventory levels or capacity data, and feed them into our ERP system. This means security concerns can be minimised while companies enjoy the most benefits of supply chain management.
00:50:40 HS Widmen wir uns im vierten Block nun dem Cyber-Risikomanagement und Geschäftserfolg. Wie trägt Cyber-Risiko Management Ihrer Meinung nach zum Geschäftserfolg bei? **00:50:52 Befragter** Wenn wir uns intern im Management über Risikomanagement unterhalten, sind wir uns schon bewusst, dass mit zunehmender Automatisierung und Netzwerktechnik wir eine andere Geschwindigkeit an den Tag legen müssten und auch einen Sinneswandel im Unternehmen vollziehen müssten, um auch zukünftig das Risiko und auch das Cyberrisiko besser beherrschbar zu machen. Dazu kommt, dass hinsichtlich der Risikoeinschätzung ein Mangel besteht, es unklare Zuständigkeiten gibt und letztlich, wie angesprochen, wir uns die fehlenden Ressourcen schlicht nicht leisten können.	**00:50:40 HS** In the fourth block, let's now focus on cyber-risk management and business success. How do you think cyber-risk management contributes to business success? **00:50:52 Respondent** When we talk about risk management internally in management, we are already aware that with increasing automation and network technology, we would have to move at a different speed and also have to change our minds in the company in order to better manage risk and cyber-risk in the future and make it manageable. In addition, there is a lack of risk assessment, there are unclear responsibilities, and ultimately, as mentioned, we simply cannot afford the missing resources.

Gerade das Thema Datensicherheit in der Produktion sorgt immer wieder für unklare Zuständigkeiten, da schieben sich die Abteilungen die Verantwortung zu häufig gegenseitig zu. Die IT fühlt sich nicht für die Maschinensicherheit verantwortlich und die operativen Mitarbeiter fühlen sich nicht als IT-Spezialisten. Das liege nicht zuletzt an der zunehmenden Digitalisierung der Produktionsprozesse, weil ja auch IT und produktionsnahe Steuerung immer mehr verschmelzen.	The issue of data security in production in particular often leads to unclear responsibilities, with departments too often shifting responsibility to each other. IT does not feel responsible for machine safety, and operational employees do not feel like IT specialists. This is not least due to the increasing digitalization of production processes, because IT and production-related control are increasingly merging.
Zugegebener Maßen fehlt uns im Management da häufig auch die Expertise, um die richtigen Schritte in der IT-Sicherheit zu gehen. Also, es sind längst nicht immer nur die Mitarbeiter, die mit ihrem Verhalten im Betrieb für eine mangelhafte IT-Sicherheit sorgen, da müssen wir uns im Management schon auch an der Nase packen, wenn es um Fehleinschätzung zu bestehende Risiken geht und die daraus resultierenden möglichen Folgen, personeller wie finanzieller Art.	Admittedly, we in management often lack the expertise to take the right steps in IT security. So, it's not always just the employees who are responsible for inadequate IT security through their behaviour in the company; we in management also have to take action when it comes to misjudgement of existing risks and the resulting risks possible consequences, both personnel and financial.
Ich meine, wenn wir unser Unternehmen anschauen, da kommt im Schnitt etwa eine IT-Kraft auf 50 Mitarbeiter. Das liegt für Mittelständler in unserer Größe mit 200 Beschäftigten schon vermutlich über dem Durchschnitt. Die IT-Angestellten kümmern sich um die gesamten IT-Systeme des Betriebes inklusive des Maschinenparks und müssen alles am Laufen halten. Das heißt, für Prävention und die ständige Verbesserung der IT-Sicherheit bleibt dann kaum noch Zeit.	I mean, if we look at our company, there is an average of one IT person for every 50 employees. This is probably above average for medium-sized companies of our size, with 200 employees. The IT employees take care of the company's entire IT systems, including the machinery, and have to keep everything running. This means that there is hardly any time left for prevention and constant improvement of IT security.
Aber schon richtig, um der wachsenden Gefahr durch Cyberangriffe zu begegnen muss IT-Sicherheit mehr Managementaufgabe werden und hierfür ein Konzept mit klaren Regeln und Methoden erarbeiten. Die Informationssicherheit im Unternehmen muss einen Top-Down-Ansatz verfolgen.	But it is true that in order to counter the growing threat of cyberattacks, IT security must become more of a management task and a concept with clear rules and methods must be developed. Information security in the company must pursue a top-down approach.
00:53:49 HS	**00:53:49 HS**

Wo steht Cyber Risk Management im Kontext mit anderen Unternehmenserfolgsfaktoren? **00:53:57 Befragter** Wie wir an dem Schaden nach dem Hackerangriff gesehen haben, greift es sowohl in den Produktions- als auch in den wirtschaftlichen, sprich finanziellen Bereich ein und verändert dort jeweils die Kennzahlen.	Where does cyber-risk management stand in the context of other business success factors? **00:53:57 Respondent** As we have seen from the damage caused by the hacker attack, it affects both production and the economy, i.e., the financial area, and changes the key figures there.
00:54:17 HS Welche Faktoren beeinflussen Ihrer Meinung nach die CRM- und Mitigations-Strategien positiv hinsichtlich des Erfolgs Ihres Unternehmens? **00:54:30 Befragter** Da die finanziellen Mittel gerade in unserem kleineren Produktionsbetrieb ja endlich sind, musste nach kleinen aber relativ wirksamen IT-Sicherheitskonzepten gesucht werden. Ansatzpunkte haben wir in der Maschinensicherheit durch Firewalls etc. gefunden als auch in der Ausbildung und Kommunikation mit den Mitarbeitern. Im Rahmen unseres Informationssicherheits-Managements (ISMS) lässt sich schon mit eigentlich selbstverständlichen technischen Maßnahmen eine verbesserte Sicherheit gegen Hacker erzielen. Zum Beispiel, indem wir die Betriebssysteme aktuell halten, regelmäßig Sicherheitsupdates einspielen und eine Zwei-Faktor-Authentifizierung für unsere Mitarbeitenden eingeführt haben.	**00:54:17 HS** In your opinion, what factors positively influence the CRM and mitigation strategies with regard to the success of your company? **00:54:30 Respondent** As financial resources are limited, especially in our small production company, we had to look for small but relatively effective IT security concepts. We found starting points in machine security through firewalls, etc., as well as in training and communication with employees. As part of our information security management system (ISMS), improved security against hackers can be achieved with technical measures that are actually self-evident. For example, we keep our operating systems up to date, regularly install security updates, and have introduced two-factor authentication for our employees.

Des Weiteren, sensibilisieren wir alle Mitarbeiter bezüglich Phishing-Kampagnen und für die Gefahren, die dort lauern. Und wir motivieren Geschäftsführung und IT-Verantwortliche mehr miteinander zu reden. Managemententscheidungen können nur so gut sein, wie die Informationen, auf denen sie beruhen.	Furthermore, we sensitise all employees to phishing campaigns and the dangers that lurk there. And we motivate management and IT managers to talk to each other more. Management decisions can only be as good as the information on which they are based.
00:55:58 HS Inwieweit stimmen diese Faktoren Ihrer Meinung nach mit den wahrgenommenen Haupterfolgs-faktoren des Unternehmens überein?	**00:55:58 HS** In your opinion, to what extent do these factors correspond to the perceived main success factors of the company?
00:56:12 Befragter Ich denke schon, dass es hier eine Überlagerung gibt. Letztlich trägt die kontinuierliche Sicherheit des Unternehmens zur Erfüllung der strategischen Zielgrößen, wie Geschäftserfolg und Kundenzufriedenheit, Service- und Produktzufriedenheit bei. Hierarchisch darunter kann das dann weiter aufgeteilt werden auf technologische Faktoren, die die Maschinen und Produktion betreffen als auch die wirtschaftlichen Zielgrößen. Ganz wichtig ist meines Erachtens auch die Zufriedenheit der Mitarbeiter. Denn ohne Mitarbeiter geht es selbst in Industry 4.0 nicht. Ich meine auch, dass wir es gewohnt sind in einem sicheren Umfeld zu leben. Ist ein Unternehmen instabil auch aufgrund hoher IT-Risiken, ist es für Lieferanten, Kunden und Mitarbeiter wirklich nicht interessant. Die Reputation des Unternehmens ist somit auch entscheidend.	**00:56:12 Respondent** I think there is an overlap here. Ultimately, the continuous security of the company contributes to the fulfilment of strategic targets such as business success, customer satisfaction, service, and product satisfaction. Hierarchically, this can then be further subdivided into technological factors that affect machines and production as well as economic targets. In my opinion, employee satisfaction is also very important. Because even Industry 4.0 cannot work without employees. I also think that we are used to living in a safe environment. If a company is unstable, also due to high IT risks, it is really not interesting for suppliers, customers, and employees. The company's reputation is therefore also crucial.
00:57:23 HS	**00:57:23 HS**

Gerne würde ich im Rahmen des CRI auch die Funktion der Cyber-Versicherung (CRI) beleuchten. Welche Erfahrungen hat das Unternehmen mit dem Einkauf von CRI gemacht?	I would also like to shed light on the cyber-risk insurance (CRI) function as part of the CRI. What experience has the company had with purchasing CRI?
00:57:37 Befragter Gegen IT-Risiken ist das Unternehmen weitgehend gewappnet. Wir verfügen über eine Cyber-Versicherung und unterziehen uns regelmäßig einem Security-Check. Ein umfassender Versicherungsschutz wurde in Abstimmung mit dem Versicherungsmakler vereinbart. Darüber hinaus haben wir ein Notfallkonzept erarbeitet. Mitarbeiterschulungen zum Umgang und zur Sensibilisierung potenzieller Gefahren finden zyklisch statt. Die Mitarbeiter sind dennoch nach dem erfolgten Hackerangriff sehr, sehr aufmerksam. Da bekommen wir auch regelmäßig Warnungen über neue Bedrohungen, die ich an meine Mitarbeiter weiterleite. Und genauso regelmäßig fragen einige extra bei mir nach, ob diese Mail tatsächlich von mir kommt und ob sie das darin enthaltene Dokument wirklich öffnen dürfen. Wer einen solchen Angriff und die Folgen einmal miterlebt hat, ob nun als Mitarbeiter oder als Firmenchef, verfällt danach nicht wieder in Routine. Das ist, um es noch mal ganz deutlich zu sagen, ein dramatisches Ereignis. Insofern resultiert das beschriebene Verhalten sicher zu 80 Prozent aus dem heilsamen Schock von damals. Und ansonsten schulen wir stetig im Berufsalltag.	**00:57:37 Respondent** The company is largely protected against IT risks. We have cyber-risk insurance and regularly undergo a security check. Comprehensive insurance coverage was agreed upon in consultation with the insurance broker. We have also drawn up an emergency plan. Employee training courses on dealing with and raising awareness of potential risks take place on a regular basis. Nevertheless, employees are very, very attentive following the hacker attack. We also regularly receive warnings about new threats, which I pass on to my employees. And just as regularly, some of them ask me whether this email actually comes from me and whether they can really open the document it contains. Anyone who has experienced such an attack and its consequences before, whether as an employee or as a company boss, does not fall back into a routine afterwards. To put it bluntly, this is a dramatic event. In this respect, 80 percent of the behaviour described is certainly the result of the healing shock of that time. And apart from that, we are constantly training in our day-to-day work.
00:59:06 HS	**00:59:06 HS**

Welche Arten von Risiken sind (sollten) in bestehenden oder geplanten CRI abgedeckt werden? **00:59:16 Befragter** Ja also, im Detail weiß ich das ad hoc nicht. Ich denke, es sind nach einem Angriff die IT-Forensik und die Wiederherstellung der Daten gedeckt, als auch die finanziellen Kosten durch die Betriebsunterbrechung sowie Kosten, die durch Information von Kunden und Vertragspartnern, also Krisenkommunikation anfallen. Ich glaube, dass auch ein Deckungsbaustein Lösegeldforderungen bis zu einem bestimmten Betrag abgedeckt ist.	What types of risks are (should be) covered in existing or planned CRI? **00:59:16 Respondent** Yes, well, I don't know in detail ad hoc. I think IT forensics and data recovery are covered after an attack, as well as the financial costs of business interruption and the costs of informing customers and contractual partners, i.e., crisis communication. I believe that a cover module for ransom demands is also part of the insurance, up to a certain amount.
00:59:53 HS Hat das Unternehmen bereits Schadenleistungen aus einer CRI erhalten? **01:00:02 Befragter** Nein, das haben wir nicht.	**00:59:53 HS** Has the company already received claims payments from a CRI? **01:00:02 Respondent** No, we have not.
01:00:10 HS Wo sehen Sie CRI als Element der Cyber-Risikomanagement-Strategie? **01:00:20 Befragter** Grundsätzlich ist ja eine versicherungstechnische Abdeckung von Risiken eine gute Sache, vor allem wenn es um eine Übernahme von Schäden geht, die für das Unternehmen sehr schmerzhaft oder sogar existenzbedrohend wären. Wenn ich mir zum Bei-	**01:00:10 HS** Where do you see CRI as an element of cyber-risk management strategy? **01:00:20 Respondent** In principle, insurance coverage for risks is a good thing, especially when it comes to covering damages that would be very painful or even threaten the company's existence. For example, if I imagine fire damage and the resulting damage caused by a business interruption, then these are events that would be difficult for us to withstand

spiel Brandschäden vorstelle und der dadurch verursachte Schaden durch eine Betriebsunterbrechung, dann sind das Ereignisse, die wir in unserer Bilanz nur schwer aushalten könnten. Und dafür finde ich zum Beispiel die Versicherungsprämie für die Sachdeckung angemessen. Bei der Cyberversicherung verhält sich das anders. Ich gebe Ihnen hierzu ein Beispiel. Wir hatten damals bereits ein Angebot vorliegen und dann kam der Hackerangriff. Heute muss man sagen: Die Police hätte uns ohnehin nicht viel geholfen, weil dort Schäden bis maximal 50.000 Euro abgedeckt gewesen wären. Mit dem Wissen von heute ist das natürlich viel zu wenig. Das heißt nicht automatisch, dass eine Cyberversicherung nicht hilft, aber nach der Erfahrung, die wir damals mit der Ransomware-Attacke machen mussten, hätten wir uns vorher mit einer solchen Police mehr beschäftigen müssen und zumindest unsere Abschätzung der materiellen und immateriellen Werte den Deckungsangeboten einer Cyberversicherung gegenüberstellen müssen. Das Thema Cyberversicherung sind wir übrigens wieder, sobald wir nach dem Angriff einen klaren Kopf hatten, angegangen. Inzwischen haben wir eine passende Versicherung gefunden und abgeschlossen.	on our balance sheet. And I think the insurance premium for property coverage, for example, is appropriate. Things are different with cyber-risk insurance. I'll give you an example of this. We already had an offer at the time, and then the hacker attack came. Today we have to say: The policy wouldn't have helped us much anyway because it would have covered damage up to a maximum of 50,000 Euros. With today's knowledge, this is, of course, far too little. That doesn't automatically mean that cyber-risk insurance doesn't help, but based on the experience we had with the ransomware attack, we should have looked more into such a policy beforehand and at least based our assessment of the material and intangible values on the coverage offered have to face cyber-risk insurance. By the way, we tackled the topic of cyber-risk insurance again as soon as we had a clear head after the attack. We have now found and taken out suitable insurance.
01:02:05 HS Wie schätzen Sie das Verhältnis zwischen Versicherungskosten und CRI-gedeckten Schadenskosten ein? **01:02:14 Befragter** Die aktuelle Police deckt jetzt Schäden bis hin zur Abwicklung des Unternehmens ab. Um eine solche Police zu bekommen, mussten wir im Unternehmen ja bestimmten	**01:02:05 HS** How do you estimate the relationship between insurance costs and CRI-covered claims costs? **01:02:14 Respondent** The current policy now covers losses up to and including the liquidation of the company. In order to get such a policy, we had to fulfil certain security requirements and

Sicherheitsanforderungen und Obliegenheiten erfüllen. Natürlich konnten wir einen Plan für unsere IT-Sicherheit vorlegen, weil wir uns ja gerade ausführlich damit auseinandergesetzt hatten. Aber die Versicherungsprämie halte ich nach wie vor als zu hoch angesetzt. Das mag wohl an der schlechten Kalkulationsbasis bei den Versicherern liegen als auch vermutlich an den hohen Sicherheitszuschlägen.	obligations within the company. Of course, we were able to present a plan for our IT security because we had just dealt with it in detail. But I still think the insurance premium was set too high. This may well be due to the insurers' poor calculation basis and probably also due to the high security surcharges.
01:03:01 HS Wie schätzt der Interviewpartner ein akzeptables Verhältnis zwischen Kosten für Cyber-Risikomanagement und -Mitigation und Cyber-Risikoversicherung ein? **01:03:12 Befragter** Wir erachten Informationen und ihren Schutz als einen wichtigen Teil unseres Geschäftserfolgs, insbesondere bei Forschungs- und Entwicklungsdaten oder sensiblen Kundeninformationen. Unsere Investitionen in die Aktualisierung und dem Ausbau von IT verstehen wir auch indirekt als Investitionen in die Cybersicherheit. Damit sollte unsere Technologie, Vermögenswerte und kritische Informationen geschützt werden. Letztendlich geht es auch darum unseren Ruf zu wahren und Schäden oder finanzielle Verluste durch unbefugten Zugriff auf unsere Systeme und Daten zu verhindern.	**01:03:01 HS** How does the Respondent assess an acceptable ratio between cyber-risk management and mitigation costs and cyber-risk insurance? **01:03:12 Respondent** We consider information and its protection to be an important part of our business success, especially in the case of research and development data or sensitive customer information. We also see our investments in updating and expanding IT indirectly as investments in cyber security. This should protect our technology, assets, and critical information. Ultimately, it is also about protecting our reputation and preventing damage or financial losses due to unauthorised access to our systems and data.
01:03:49 HS Wie, glauben Sie, stabilisiert oder verbessert der Cyber-Versicherungsschutz Ihren Geschäftserfolg?	**01:03:49 HS** How do you think cyber-risk insurance coverage stabilizes or improves your business performance?

01:03:58 Befragter Wir hatten damals bereits ein Angebot vorliegen und dann kam der Angriff. Heute muss man sagen: Die Police hätte uns ohnehin nicht viel geholfen, weil dort Schäden bis maximal 50.000 Euro abgedeckt gewesen wären. Mit dem Wissen von heute ist das natürlich viel zu wenig. Nach der Erfahrung, die wir damals mit der Ransomware-Attacke machen mussten, kann ich Unternehmen nur dringend empfehlen, sich mit einer solchen Police zu beschäftigen. Das ist wie eine Elementarschadenversicherung fürs Haus – aus meiner Sicht unbedingt notwendig. Das Thema Cyberversicherung sind wir angegangen, sobald wir nach dem Angriff wieder einen klaren Kopf hatten. Inzwischen haben wir eine passende Versicherung gefunden und abgeschlossen. Die aktuelle Police deckt Schäden bis hin zur Abwicklung des Unternehmens ab. Um eine solche Police zu bekommen, müssen Unternehmen ja bestimmten Sicherheitsanforderungen genügen. Natürlich konnten wir einen Plan für unsere IT-Sicherheit vorlegen, weil wir uns ja gerade ausführlich damit auseinandergesetzt hatten. Unternehmen, die noch nicht so weit sind, bekommen von den Versicherern Hilfe angeboten, um die Kriterien zu erfüllen.	**01:03:58 Respondent** At that time, we already had an offer, and then the attack came. Today, we have to say: The policy wouldn't have helped us much anyway because it would have covered damage up to a maximum of 50,000 euros. With today's knowledge, this is, of course, far too little. After the experience we had with the ransomware attack back then, I can only strongly recommend that companies take up such a policy. It's like natural hazard insurance for the house, which is absolutely necessary in my opinion. We addressed the topic of cyber-risk insurance as soon as we had a clear head after the attack. We have now found and taken out suitable insurance. The current policy covers damages up to and including the liquidation of the business. In order to obtain such a policy, companies must meet certain security requirements. Of course, we were able to present a plan for our IT security because we had already dealt with it in detail. Companies that are not yet ready are offered help by insurers to meet the criteria.
01:05:39 HS Welche Risiken hält der Interviewpartner für beherrschbar durch die CRM-Strategie und -Maßnahmen eines Unternehmens und welche Restrisiken sollten durch CRI abgedeckt werden? **01:05:49 Befragter**	**01:05:39 HS** Which risks does the Respondent consider to be manageable by a company's CRM strategy and measures and which residual risks should be covered by CRI? **01:05:49 Respondent**

Ich denke, alle identifizierten IT-Sicherheitsrisiken, die wir nach erfolgter Risikomitigation als niedrig einstufen. Alle anderen Risiken, die ein substantielleres Schadenpotential haben und deren Ausmaß für das Unternehmend finanziell gefährdend wären, sollten durch eine Cyberversicherung gedeckt und vom Schaden her entlastet werden.	I think all identified IT security risks that we classify as low after risk mitigation. All other risks that have a more substantial damage potential and whose extent would be financially dangerous for the company should be covered by cyber-risk insurance and relieved of the damage.
01:06:23 HS Zum Abschluss des Interviews würde ich von Ihnen noch gerne wissen, inwieweit potenzielle Cyber-Risiken und nachfolgende Cybersicherheitsinvestitionen eine Rolle bei der Entscheidung über zukünftige Geschäftsprioritäten oder Investitionen spielen? **01:06:45 Befragter** In den kommenden zwei bis drei Jahren werden wir weitere Investitionen in die IT tätigen. Durch die Aktualisierung der Software und der Applikationen sollten dabei auch weitere Schutzmaßnahmen gegen Cyberkriminalität in der IT erledigt sein. Also, natürlich zeigen wir im Maschinenbau grundsätzlich eine Investitionsbereitschaft in IT-Sicherheit aber speziell ein Budget, dass Investitionen exklusiv in die Cybersicherheit zuordnet, haben wir nicht. Wie gesagt, fließen die Ausgaben in die Erneuerung und/oder dem Ausbau der IT im Unternehmen zu. Das sollte meines Erachtens ausreichen, dass die am häufigsten von Kriminellen verwendete Angriffsmethode, nämlich über unser Mailsystem Zugang zu unseren Servern und Netzwerken zu finden und letztendlich Schadsoftware in unser Netzwerk einzuschleusen und dabei die Kontrolle über die infizierten Rechner zu übernehmen, weitestgehend abgewendet wird. Wir wissen natürlich, dass man finanziell und auch personell merklich mehr in Cyberschutz investieren könnte und vor allem gegen Phishing-Angriffe besser gewappnet zu	**01:06:23 HS** To conclude the interview, I would like to hear from you to what extent potential cyber-risks and subsequent cybersecurity investments play a role in deciding future business priorities or investments? **01:06:45 Respondent** We will make further investments in IT in the next two to three years. By updating the software and applications, further protective measures against cybercrime in IT should also be taken. So, of course, in mechanical engineering, we generally show a willingness to invest in IT security, but we don't have a specific budget that allocates investments exclusively to cybersecurity. As I said, the expenses go towards renewing and/or expanding the company's IT. In my opinion, this should be enough to largely avert the attack method most commonly used by criminals, namely using our mail system to gain access to our servers and networks, ultimately injecting malware into our network and thereby taking control of the infected computers. Of course, we know that we could invest noticeably more in cyber protection, both financially and in terms of personnel, and, above all, to be better prepared against

sein und auch die Mitarbeiter stärker zu schulen und für das Thema zu sensibilisieren. Angesichts unserer Betriebsgröße und Gewinnerwartungen können wir uns aber zusätzliche Ausgaben schwerlich leisten. Das käme auch einen Kulturwandel gleich, derweil wir bisher das Geld in den Geschäftsausbau gesteckt haben.	phishing attacks and also to train employees more and raise their awareness of the topic. However, given our size and profit expectations, we can hardly afford additional expenses. That would also amount to a cultural change, whereas we have previously invested the money in expanding our business.
01:08:36 HS Welche weiteren Themen im Zusammenhang mit Cyber-Risiko halten Sie für wichtig bei mittelständischen Unternehmen? **01:08:45 Befragter** Ja, damals haben wir als Geschäftsführung gelernt, mehr mit unseren Mitarbeitern zu reden. Kommunikation mit jeder Mitarbeiterin, mit jedem Mitarbeiter ist gerade in Krisenzeiten ein wichtiges Element. Nur so kann ich dafür sorgen, dass sie das Vertrauen in die Firma und in die Geschäftsführung behalten. Das heißt, ich erkläre meine Entscheidungen heute ausführlicher als früher. Wir im Unternehmen sind uns bewusst, dass die Chancen durch Industrie 4.0 klar die Risiken, ich meine hier speziell die Risiken durch Cyberkriminalität, überwiegen. Doch Industrie 4.0, soweit verstehe ich das auch, wird langfristig nur funktionieren, wenn die Cyber-Security in Entwicklung und Betrieb angemessen berücksichtigt wird. Wir werden uns darauf einstellen müssen, mehr Gelder in die IT-Ausstattung und IT-Sicherheit zu investieren, denn Industrie 4.0 und die digitalen Geschäftsmodelle werden dadurch erst ermöglicht.	**01:08:36 HS** What other topics related to cyber-risk do you consider important for medium-sized enterprises? **01:08:45 Respondent** Yes, back then, we as management, learned to talk more to our employees. Communication with every employee is an important element, especially in times of crisis. This is the only way I can ensure that they retain trust in the company and the management. This means that I explain my decisions in more detail today than before. We in the company are aware that the opportunities presented by Industry 4.0 clearly outweigh the risks, and I mean here specifically the risks of cybercrime. But Industry 4.0, as far as I understand it, will only work in the long term if cyber security is adequately taken into account in development and operation. We will have to prepare ourselves to invest more money in IT equipment and IT security, because this will make Industry 4.0 and digital business models possible.

Aber wie gesagt, Security kostet Geld und da die Mittel auch bei uns aus dem IT-Budget kommen und wir kein separates Budget für Cybersecurity haben müssen wir leider zugeben, dass wir der wachsenden Bedeutung von Vernetzung im Maschinen- und Anlagenbau nicht ausreichend Rechnung tragen. Das wird zukünftig mit wachsender Betriebsgröße eine Herausforderung für uns und auch die organisatorische Umsetzung. Das heißt, selbst wenn wir ein zusätzliches Cybersecurity Budget einrichten würden, müssten wir erst die Fachkräfte, die IT-Sicherheitsexperten finden. Maschinenbau, hier sprechen wir nicht nur über die Office-IT sondern auch über Arbeit draußen in der Produktionsumgebung, ist für IT-ler auf den ersten Blick weder sexy noch zahlen wir überdurchschnittlich hohe Gehälter. Dabei gibt es gerade hier die Themen der Zukunft, deren Absicherung die Unternehmen stark zunehmend im Fokus haben. Bei produzierenden Unternehmen liegen Risiken nicht nur in der Office-IT, sondern auch in den Produktionsumgebungen.	But as I said, security costs money, and since the funds come from our IT budget and we don't have a separate budget for cybersecurity, we unfortunately have to admit that we are not taking sufficient account of the growing importance of networking in mechanical and plant engineering. As the size of the company grows, this will be a challenge for us in the future, as will the organisational implementation. This means that even if we were to set up an additional cybersecurity budget, we would first have to find the skilled workers, the IT security experts. In mechanical engineering, here we are not just talking about office IT but also about work outside in the production environment, which is at first glance neither sexy for IT people nor do we pay above-average salaries. Here, in particular, there are the issues of the future that companies are increasingly focusing on securing. For manufacturing companies, risks lie not only in the office IT but also in the production environments.
01:11:05 HS Herr xxxx haben Sie herzlichen Dank für Ihre Zeit und das ausführliche Interview.	**01:11:05 HS** Mr. xxxx, thank you very much for your time and the detailed interview.

Annex 5: Ethical Considerations

Ethical principles are fundamental to the conduct of every stage of the research study and are vital for the protection of both researchers and participants. Ethical standards safeguard the rights and wellbeing of participants and are designed to reduce the risk of mental and physical harm, danger, or discomfort that may arise from research processes (Shaw, 2023). From the researcher perspective, adherence to ethical guidelines protects the right to conduct legitimate studies in addition to preserving the reputation of academic institutions or sponsoring bodies and avoiding claims of negligence or unethical practices (Goodwin, 2020). The main ethical principles involve the fidelity, justice, and veracity of the researcher, the autonomy, confidentiality, and non-harm of interviewees, and the wider benefit of the research.

This research was undertaken following in-depth consideration of how this research may advantage participants and construct wider societal benefit with regard to cyber security. In promoting increased understanding of CRM, this research provides an important contribution towards knowledge for the cyber security awareness and cyber-risk mitigation of German Manufacturing medium-sized enterprises, particularly in the under-researched context of how CRMi relates to the business success of such organisations.

The conduct of this entire research has conformed to the key principles underlying ethical research, of which one of the most prominent is to ensure that the risk of harm to either participant or researcher is minimised (Saunders et al., 2020). Accordingly, substantial prior consideration has been given to research design and processes to reduce any inherent risk of harm and to safeguard the rights of participants in the conducted semi-structured interviews. One significant risk that has been recognised and scrutinised links to the principle of autonomy for interviewees. This requires that the right of individuals to make their own decisions is acknowledged and respected and forms the foundation upon which the entitlement to free and informed consent is based (Klykken, 2022).

Adhering to the three major elements of informed consent, this study provided accurate, truthful, and sufficient information to allow comprehension of the nature of the research, its purpose, and the processes and procedures followed, in addition to detailing any potential risks or benefits. The interviewee´s volition was fully supported by the voluntary nature of

the study, in which participants were informed of their right to withdraw at any point in the research (Goodwin, 2020).

The research was conducted in accordance with the ethical research policies and procedures of "The University of Gloucestershire's Handbook of Research Ethics (2008)". A copy of these guidelines was offered to all participants on request.

Further, during the course of this research, steps were also taken to avoid harm to participants through the negligent exposure of information, which compromises their entitlement to privacy and confidentiality (Cohen et al., 2013). The principle of the protection of privacy and confidentiality is essential to ensuring that freely given information does not impact the welfare of participants (Goodwin, 2020) and was safeguarded in this study through the protection of access, control, and dissemination of personal identifying details.

This research further acknowledged that ethically, it was important to build a trusting relationship with participants, without which the fidelity and quality of the data could be compromised (Saunders et al., 2020). Besides ensuring that participants were fully informed of their rights trust-building extended to engaging with any concerns or issues the participants may have had. Further, the wellbeing of participants was continually monitored during the participant elements of the research process, and considerable reflection was focused on ensuring justice and fairness, including making certain that all participants were fairly and equally treated.

The researcher is an Executive Director in the reinsurance industry. His position in the (re)insurance industry may be a cause for concern among some participants since part of the research refers to CRMi and cyber-risk insurance. However, a strict code of conduct was formulated for collecting data from the participants. It was understood that all data arising from the interview and protocol as well as any other data would be stored safely on the researcher's personal computer and destroyed after approval of the thesis by the University of Gloucestershire. Also, full compliance with the rules of ethics underlines the fact that the thesis reports data, information and results honestly while avoiding bias in the interpretation of data analysis.

To resolve ethical issues involved in the research, all participants were volunteers and were provided with a clause of confidentiality. This ensured that the identity of the participants

was kept confidential. In this regard, a consent agreement to this effect was provided for the participants. They were also informed about how the information provided by them would be used in the study. Only relevant information would be collected and used for the purpose of the research.