information

MDPI

Article

Cyber Insurance Adoption and Digitalisation in Small and Medium-Sized Enterprises

Nazim Taskin [1], Aslı Özkeleş Yıldırım [1], Handan Derya Ercan [2], Martin Wynn [3,*] and Bilgin Metin [1]

[1] Department of Management Information Systems, Bogazici University, Istanbul 34342, Turkey; nazim.taskin@bogazici.edu.tr (N.T.); asli.ozkeles@gmail.com (A.Ö.Y.); bilgin.metin@bogazici.edu.tr (B.M.)
[2] Department of Management, Bogazici University, Istanbul 33342, Turkey; handan.ercan@std.bogazici.edu.tr
[3] School of Business, Computing and Social Sciences, University of Gloucestershire, Cheltenham GL502RH, UK
* Correspondence: mwynn@glos.ac.uk

Abstract: Digitalisation has significantly increased cybersecurity risks in organisations, notably for small to medium-sized enterprises (SMEs), in which IT departments often have relatively small teams and limited resources. Cyber insurance enables SMEs to navigate cybersecurity risks more economically, providing an essential risk transfer alternative to costly reduction strategies. This article examines the antecedents, emergence, and application of cyber insurance as a solution to cybersecurity concerns against the backdrop of increasing digitalisation. The research adopts a quantitative deductive approach, with an analysis of relevant literature providing the basis for the development of 12 hypotheses, which are then tested via a survey of 168 SMEs in Turkey. Using the Technology–Organisation–Environment–Individual (TOE-I) model as a top-line conceptual framework, the article finds that cyber insurance policy adoption has facilitated a more rapid and secure digitalisation process and that the mitigation of financial risk associated with cyberattacks has allowed companies to invest more widely in information technologies and systems. The article clearly has its limitations, in that it is based on primary research in one European country, but the authors believe that it nevertheless provides some new insights into the potential benefits of cyber insurance, and the key issues SMEs must consider when considering adopting a cyber insurance policy. The findings will be of practical relevance to SMEs and other organisations reviewing their cybersecurity strategy and are also of relevance to the wider debate around the costs and benefits of digitalisation.

Keywords: cybersecurity; digitalisation; risk management; cyber insurance; TOE; Technology–Organisation–Environment–Individual model; TOE-I

Academic Editor: Rúben Pereira

Received: 2 December 2024
Revised: 14 January 2025
Accepted: 15 January 2025
Published: 18 January 2025

Citation: Taskin, N.; Özkeleş Yıldırım, A.; Ercan, H.D.; Wynn, M.; Metin, B. Cyber Insurance Adoption and Digitalisation in Small and Medium-Sized Enterprises. *Information* **2025**, *16*, 66. https://doi.org/10.3390/info16010066

1. Introduction

Digitalisation is the process of integrating digital technologies into business and society for further efficiency and accessibility. Eling and Lehmann [1] defined digitalisation as "the integration of the analogue and digital worlds with new technologies that enhance customer interaction, data availability, and business processes" (p. 363). With digitalisation, digital technologies are integrated with existing information systems to provide new data capture, analytics, and functionality benefits across the supply chain. Digital transformation, however, involves the incorporation of digital technologies into new or redesigned products and services [2,3]. When this happens, the change process is at a different level and often results in a new business model.

While both digitalisation and digital transformation can bring significant business benefits, such significant changes in organisational processes and technology deployment

will almost inevitably increase the cybersecurity vulnerabilities of an organisation. For example, shop floor automation and programmable logical control (plc) data capture devices have hitherto been seen as closed to the outside world and, therefore, were not recognised as an information security concern in many organisations. However, with the increased deployment of IoT devices and data residing in cloud and edge computing environments, some of these systems have become prone to cybersecurity vulnerabilities. The cyber attack surface that needs to be dealt with and defended is rapidly expanding, and in-house IT teams are often lacking the required skills and resources to deal with such challenges.

Small to medium-sized enterprises (SMEs) are one of the main targets of cyber attacks on businesses, as they often have only a low level of cybersecurity awareness. A cybersecurity incident is not only an issue for the company's IT department or data centre but may also have significant commercial consequences that affect a wide variety of stakeholders. For example, ransomware attacks encrypt operating systems and stored data on computers and servers and can affect both the integrity and accessibility of corporate data. Hackers demand ransom for the recovery of data. Organisations experience business interruptions until they try to recover the systems themselves or prefer to pay the ransom [4]. If financial data cannot be accessed for a certain period of time, this can put manufacturers in a difficult situation, because, for example, they cannot issue invoices to their customers. Such cyber incidents can be particularly damaging to SMEs, where resources to manage such incidents are usually limited. Globally, the scale and complexity of cyber attacks continue to increase. The global cost of such attacks was estimated to grow to over USD 8 trillion in 2023 and USD 9.5 trillion in 2024 [5].

Organisations are becoming increasingly aware of the potential impact of cybersecurity-related risks on their businesses [4], and IT risk is now often viewed as part of a company's overall risk management [6]. Cybersecurity insurance, or cyber insurance, has emerged in recent years as a viable approach to business risk mitigation. Cyber insurance includes reimbursements for the costs of cybercrime, as well as guidelines and tools for advanced cybersecurity. It remains, however, a relatively new form of insurance in the rapidly evolving cybersecurity environment and has not yet reached maturity, either globally or in the Turkish market [7,8]. According to SNS Insider [9], the cybersecurity insurance market is growing incrementally with a forecast Compound Annual Growth Rate of 16.4% over the period 2024–2032, which is valued at USD 13.3 billion in 2023 and is expected to reach USD 52.1 billion by 2032. However, there is relatively limited literature that focuses on the rationale for adopting cyber insurance, notably for SMEs [10].

In Turkey, SMEs constitute 99.7% of all businesses, providing 70.6% of total employment [11]. As of 2021, more than 92% of SMEs had access to the Internet, with digital technologies being used for digital marketing, e-commerce, business process change programmes, and Industry 4.0 initiatives [12]. According to industry reports, there was a 50% increase in the global number of cyber attacks in 2021, compared to the previous year [13], and in 2023, Turkey was one of the most targeted regions in the world for cybercrime, as companies, government agencies, and organisations have increasingly adopted digital technologies. On average, a cyber attack may lead a company to be out of business for the following 6 weeks [14]. Cyber incidents, such as data breaches, can take up to 200 days to identify and 75 days to contain [15].

Adopting cyber insurance will normally require companies to implement a certain degree of self-protection against cyber attacks. As an indirect benefit, cyber insurance adoption may engender further investment in digitalisation and digital tools deployment, which in turn increases organisational security performance. However, as highlighted by Adriko and Nurse [16] in their systematic literature review, there is a dearth of research

that analyses the benefits of cyber insurance adoption in the digitalisation process. In a similar vein, Hasani et al. [17] emphasised the lack of substantial empirical research on the impact of cybersecurity adoption on organisational performance, despite its importance in improving overall performance. Previous studies have not examined the constructs of the adoption of cybersecurity technologies and their impact on organisational performance. Accordingly, this research aims to fill this critical gap in the literature by exploring the various factors influencing the adoption of cybersecurity insurance of SMEs in Turkiye. Additionally, the study addresses the gap in the literature examining decision-makers' capabilities in adopting cyber insurance in SMEs.

This study thus aims to contribute to addressing this gap in the cybersecurity literature by investigating the key factors influencing cyber insurance adoption intention and the impact of this adoption on digitalisation through ICT adoption and organisational security performance. Using the Technology–Organisation–Environment–Individual (TOE-I) framework to analyse the perspectives of SME practitioners, the research tests 12 related hypotheses, which are assessed using a quantitative analysis of data from survey responses from 168 Turkish SMEs.

The benefits of this research extend across multiple fronts. First, it provides a deeper understanding of cyber insurance as a cybersecurity risk management tool that not only transfers financial risk but also encourages a proactive cybersecurity culture within SME management, fostering further investment in IT and security. By serving as a flexible risk transfer tool, cyber insurance supports SMEs in balancing cybersecurity costs, particularly when risk reduction methods can be prohibitively expensive. Second, the findings offer valuable insights for policymakers focused on SME support by identifying drivers of cyber insurance adoption, which could inform initiatives aimed at enhancing SME cybersecurity readiness. Third, by using the TOE-I model in the context of cyber insurance, this study demonstrates a further application of the model, providing the basis for future research to explore the interaction of individual, organisational, and environmental factors in similar contexts.

Following this introductory section, a brief assessment of relevant literature ensues. This is followed in Section 3 by the formulation and explanation of 12 hypotheses related to dimensions of the TOE-I framework, which are subsequently tested via survey-based data analysis. The research methodology and design are then discussed in Section 4, and the main results that address the research aim and the postulated hypotheses are set out in Section 5. In Section 6, some of the key themes emerging from the research results are discussed, and in the final conclusion, Section 7 highlights the main issues covered in the article, reflects on its limitations, and points out areas for further research.

2. Literature Review

Cyber risk can be assessed through risk identification, risk analysis, impact evaluation, and risk management (or treatment) [18,19]. In the risk identification step, potential threats and vulnerabilities are recognised. Risk analysis evaluates the likelihood and business impact of each risk. Then, in the risk evaluation stage, risks are prioritised based on their potential consequences. Considering the risk assessment results, appropriate senior management instigates the development and implementation of strategies to manage risks.

Risk management is the act of identifying, analysing, and preventing potential risks to the achievement of an intended goal. In risk management, attempting to prevent risks before they occur is a strategy for maximising resource utilisation and achieving the best possible outcomes. Risk reduction is a way of attempting to mitigate the impact of risks by reducing the complexity of the problem. The risk is tolerable in some cases. In this situation, the potential risk outcomes are accepted, and plans are developed to manage them

successfully as and when they may occur. Another key risk management strategy is risk avoidance. It requires completely avoiding activities that could lead to potential problems. This can be accomplished by either modifying the approach or altogether avoiding the activity. Finally, risk transfer is a means of transferring potential risks to another party, such as an intermediary—for example, an insurance company—to protect against the financial consequences of a risk. It is this last strategy option for risk management that is the focus of this article.

Cyber insurance entails transferring risk that cannot be eliminated to a financial tool or mechanism [20,21]. For instance, many cyber insurance policies cover financial losses from cyberattacks, ensuring partial compensation for business downtime, which can disrupt normal operations and result in lost revenue [22]. Even if companies already have advanced cybersecurity measures in place, the rapidly evolving cybersecurity environment means that many companies remain vulnerable to new types of cyber risk. In these circumstances, it may be adjudged to be less cost-effective to implement more technical cybersecurity solutions, such as additional firewalls or software, than to manage the cyber risk via cyber insurance.

Cyber insurance options generally include coverage for downtime in case of a cyber breach, regulatory fines, and legal fees, as well as offering some level of cybersecurity protection to their customers. Some policies also cover ransomware and industry-specified regulation fines. Most cyber insurance also provides anti-virus software and vulnerability screening. More specifically, cyber insurance coverage provided by Turkish insurance companies may include some of the following: data coverage damage, business downtime cost, legal charges against law for protection of personal data, ransom demanded from the hackers, blackmail cost, customers' demands from the insurer due to data security negligence costs, investigation of the cybercrime, public relations support, identity theft, reconstruction cost, network and hardware defection costs, costs of non-compliance with payment card industry data security standard (PCI-DSS), online media responsibility costs, and legal support charges.

There are both benefits and potential problems for any company adopting a cyber insurance strategy. Meeting the requirements for eligibility may be cumbersome for an SME, considering the lack of awareness amongst staff in general and, specifically, the relative dearth of qualified IT/ICT personnel, which is often the norm. Requirements from the insurers may include evidence of weekly backups of critical data, installing anti-virus software, regularly changing passwords, software patches, firewalls, and system upgrades, accessing digital assets only through authorised personnel and security logins, accessing cloud computing through VPN, and training employees about cybersecurity [23]. Lack of data and know-how to support reliable and accurate risk calculation and premium pricing are additional concerns [7]. Dambra et al. [21] report that risk assessment for cyber insurance and applicability to real-world cases are mainly carried out through qualitative analysis based on expert opinions. Quantitative approaches remain relatively undeveloped [21,24].

There are a number of frameworks and models that focus on the adoption of technology solutions that are of relevance to this study, including the Technology Acceptance Model (TAM) [25], the Technology–Organisation–Environment (TOE) framework [26], and the Unified Theory of Acceptance and Use of Technology (UTAUT) model [27], all of which have been used in a range of research studies in the past two decades [28–31]. The TOE framework bases technology adoption on three main contexts: technology, organisation, and environment [32]. In the broadest definition, the technological context includes existing technology in a firm, available technologies outside of the firm, and the characteristics

of technological innovation to be adopted. Firms need to evaluate both their existing technology and new technology to be adopted to determine the size of the change required.

Cybersecurity technology adoption has been studied within the TOE framework [33,34]. Wallace et al. [35] discussed the constructs of the TOE framework, with a specific focus on cybersecurity. The authors added two dimensions, cyber catalysts and practice standards, to the basic TOE model. Herath et al. [33] created an integrative model by combining TOE with elements of Diffusion of Innovation Theory [36] to study the constructs that affect the adoption of information security systems. The authors examined concepts like complexity, compatibility, and perceived gain to offer an integrative model. In the current study, the technology dimension of the model involves testing the influence of complexity, perceived gain, and perceived observability constructs adapted from Albar and Hoque [37], Herath et al. [33] and Hasan et al. [34].

The organisational context of the TOE framework includes the inner workings of a firm, such as decision-making structure, organisational strategy, size of the organisation, communication process, and employee relations [32]. In this study, organisational culture and top management support, which are vital for technology adoption, are tested to understand organisational effects on cyber insurance adoption.

The environmental context considers external elements of technology adoption. This definition includes industrial aspects, such as the state of technological advancements in the industry and in competition companies, as well as regulatory inputs including governmental safety measures [32]. Constructs related to the competitive environment and external pressures are tested to understand environmental effects.

The decision-maker's perspectives and concerns when deciding to adopt and use technology were disregarded in the original TOE framework. For this reason, the TOE framework is often extended by adding individual context with factors from other models [38]. Models extending TOE with the individual context (known as TOE-I) state that the decision-maker's intention to use the technology affects the firm's intention to use the technology; thus, they combine individual intention and the firm's intention within the TOE-I framework [39]. Another perspective of individual context focuses on the familiarity of the CEO with technology. The CEO's support in innovation adoption and general knowledge of ICT can positively affect technological innovation adoption [37]. The CEO/owners' innovativeness and knowledgeability are tested in the current study.

The effects of the adoption of cybersecurity technology on businesses are often studied post-adoption. This is in line with other studies of technology deployment that examine pre- and post-implementation issues [40]. Cyber insurance policies offer lower premiums to businesses that follow effective cybersecurity policies. The net positive effects of the adoption of cyber insurance are thus most relevant and evident after the purchase. SMEs' ICT implementation and organisational security performance are affected by cyber insurance post-adoption. This study, therefore, examines both pre and post-cyber insurance adoption within the digitalisation of SMEs.

3. Hypotheses Development

This section uses a modified TOE framework and key themes emerging from the literature to develop hypotheses that will be assessed via a survey of Turkish SMEs. The hypotheses are related to technology (3), organisation (2), and environment (2), as in the original TOE model, but also to the individual (owner–manager) (2), plus additional post-adoption hypotheses (3), making 12 hypotheses in all. These are briefly discussed below.

3.1. Technology-Related Hypotheses

The potential role of cyber insurance in enhancing an organisation's overall cybersecurity posture has become increasingly relevant in today's digital environment. Herath et al. [33] put forward that implementing security measures will probably result in a reduced likelihood of cybersecurity incidents, which in turn will reduce cyber costs and increase corporate profitability. Herath et al. [33] also argued that the perceived gain coming from adopting information security measures positively affects the speed and scale of the adoption of digital technologies. Once cyber insurance is adopted, it can cover direct and third-party costs associated with cyber incidents. Furthermore, although cybersecurity tools can help reduce the likelihood of attacks, they cannot completely eliminate risk. Cyber insurance offers a financial safety net by covering losses in the event of breaches. This enables companies to confidently invest in new technologies while being protected from major financial setbacks [41]. Since cyber insurance is a tool that helps manage cyber risks, it is reasonable to hypothesise that it can also enhance the information security gains achieved through the implementation of cybersecurity tools.

In addition to cybersecurity measures, businesses are obligated by the Turkish Data Protection Authority to safeguard their customers' data and provide their customers with information regarding data usage and protection policies. In the event of a dispute with the Turkish Data Protection Authority or an attack aimed at compromising the confidentiality of IT systems, the company's reputation may be negatively affected, especially if the company is unable to pay any resulting fines. Cyber insurance can resolve such disputes and cover some charges proportional to the insurance policy, so the insured business is at least partially protected financially. In this context, Grigoriadis [42] observed that cyber insurance can serve as an effective risk mitigation tool, especially in light of recent judgements in US cyber insurance cases.

The significance of the awareness of these potential gains underpins the following hypothesis:

H1. *Perceived gains from cyber insurance will have a direct positive effect on the adoption intention of cyber insurance among Turkish SMEs.*

Perceived complexity is also a key issue affecting cyber insurance adoption intention. If SMEs consider the adoption of cyber insurance as unacceptably complex, they may be less likely to pursue it. This relationship has been examined before, where the degree of ease in adopting technology, understanding the technology, and using the technology, all contribute to overall complexity, a key construct in technology adoption [27]. In this context, Albar and Hoque [37] and Herath et al. [33] suggest SMEs are more likely to adopt technologies that are easy to understand and implement. However, cyber insurance is often perceived as complex due to pricing policies and coverage that can be misunderstood by customers [21,24]. This might be a barrier to SMEs considering cyber insurance. In addition, insurance companies may add prerequisites for an SME to their standard policies in order to reduce their own risk. These prerequisites vary from adopting cybersecurity tools to implementing company-wide policies and regularly training staff to increase awareness [43–45]. Adopting cyber insurance will also require access to IT skills and capabilities—available either in-house or through outsourcing—to understand and manage necessary cybersecurity tools and related issues. Such capabilities are generally lacking in SMEs in Turkey [14]. It can, therefore, be hypothesised that:

H2. *Cyber insurance complexity will have a direct and negative effect on the adoption intention of cyber insurance within Turkish SMEs.*

"Observability" is another relevant concept in cyber insurance adoption intention. Badi et al. [46] noted that positive perceptions of the value of new technology increase the chances of its adoption. In this context, Rogers [36] pointed out that preventative innovations, for which the benefits are less observable than implemented innovative solutions, are adopted more slowly due to their low observability. Disaster management policies are a good example of the effects of observability of insurance in adoption decision-making: people purchase more insurance policies after the disaster occurs, and likewise, they give up the insurance after years of not experiencing a disaster [47]. Considering that the cyber insurance market is not currently mature, cyber insurance adoption may benefit from observability. Hence, the third hypothesis is postulated as follows:

H3. *Perceived observability will have a direct and positive effect on the adoption intention of cyber insurance within Turkish SMEs.*

3.2. Organisation-Related Hypotheses

Organisational culture, and notably open communication, has been seen to have a positive impact on technology adoption [37]. Cyber insurance is not just a cyber risk management tool but also a financial tool that requires a multidisciplinary approach when weighing up the costs and benefits of adoption. As such, it is important to maintain open communication between all parties involved to ensure effective implementation and management of the policy [34]. Bandyopadhyay [48] suggests that businesses with a central risk management system and multiple managers who make decisions on risk-related issues, such as the adequacy of cyber insurance as a risk mitigation tool, are more inclined to adopt cyber insurance. Tang et al. [49] conducted an in-depth case study in a large-scale organisation and found that the organisation's corporate culture influenced information security culture. Security culture is predicted to impact the need for cyber insurance adoption. Accordingly, the following hypothesis is put forward:

H4. *An encouraging organisational culture will have a direct and positive effect on the adoption intention of cyber insurance within Turkish SMEs.*

Support from top management is generally considered to have a strong and positive influence on new technology adoption in numerous studies, notably in major systems projects [50]. The key decision-maker for technology adoption, especially in SMEs, is very likely to be in a senior management position [37]. Hasan et al. [34] point out that the profile and significance of cybersecurity in an SME are enhanced by the support of top management, which in turn positively influences the security behaviour of employees. This will engender the successful adoption of cybersecurity policies and tools and, thus, make organisations readier to deal with cyber attacks. Thus, it can be hypothesised that:

H5. *Top management support will have a direct and positive effect on the adoption intention of cyber insurance within Turkish SMEs.*

3.3. Environment-Related Hypotheses

Competitive pressure and the quest for competitive advantage have been considered important factors affecting technology adoption in business for several decades [35]. This can be traced back to Earl's [51] classic model of IT strategy development, in which the "inside–out" approach involved a review of competitor activities as a driver of strategy development and new investment, including in SMEs [52]. The linkage between technology investment and intense competition has been further developed as digitalisation impacts and changes the processes, products, and services of companies, big and small. Cyberse-

curity is an increasingly significant aspect of such technology investment in an era when, for example, a breach of customer data may cause serious harm to a company, notably in industry sectors where customer reviews are critical [48]. Based on this, the following hypothesis is developed:

H6. *A competitive environment will have a direct and positive effect on the adoption intention of cyber insurance within Turkish SMEs.*

Herath and Herath [53] affirm that both horizontal and vertical business partners consider safety measures taken by a business when entering into a commercial partnership. Cyber attacks and virus infections, for example, can not only affect a company's internal systems but also very likely impact third parties and business partners. In a digitalised technology and business environment, where companies are interconnected through digital systems, an information security strategy and established track record can have a significant impact.

In addition to consideration of potential business partners, organisations must also comply with regulatory requirements, such as, in the case of Turkey, the Turkish Personal Data Protection Law, or, in a wider European context, the EU General Data Protection Regulation (GDPR). By imposing fines for data breaches and violations, this regulatory environment plays a significant role in shaping the readiness of organisations to respond to cyber incidents. Hasan et al. [34] suggest that these regulations serve to protect customer data, and non-compliance may lead to customers seeking assistance from authorities if needed.

Ramdani et al. [54] used the TOE framework to explore factors that influence SMEs' adoption of enterprise applications. Their findings highlighted the significance of environmental factors in new technology adoption by SMEs, notably competitive pressure, customer pressure, industry pressure, and the availability of governmental support. Hasani et al. [17] similarly studied the effects of environmental factors, but here more specifically on cybersecurity adoption, and found competitive pressure had a positive relationship with both cybersecurity technology adoption and with the organisational performance of SMEs: business partners and customers requested the use of specific security technologies and practices. In this context, the following hypothesis is thus put forward:

H7. *External pressures for security will have a direct and positive effect on the adoption intention of cyber insurance in Turkish SMEs.*

3.4. Individual (Owner–Manager)-Related Hypotheses

Company owners are often the key individuals in SMEs who exert a major influence on strategy, policy, and investment decisions. These individuals have founded and/or invested in the company and usually retain a significant ownership stake in the company. Key decisions often reflect the owner's individual beliefs, knowledge, and behaviour [55,56]. Recent research has used the TOE framework, in its original or extended form, in the investigation of e-commerce technology adoption by SMEs [57,58]. Similarly, insurance purchase and adoption decisions are also heavily influenced by the decision-maker's approach to risk [59]. Thus, when looking at the adoption of cyber insurance for SMEs, firm-level context alone is not sufficient, as the individual profiling of the company owner is also of direct relevance [60]. Purchasing proposals may come from line management functions, but the final decision- maker for any significant investment is often the owner–manager or CEO [37]. This is as valid for information and cybersecurity purchasing decisions as for any other procurement or investment decision [61]. Owners of SMEs play a significant role in decision-making, and their individual context and approach to risk must

be considered for the adoption of cyber insurance and the implementation of cybersecurity measures. The following hypothesis is thus added to those above:

H8. *Owners'/managers' innovativeness will have a direct and positive effect on the adoption intention of cyber insurance in Turkish SMEs.*

In addition, owners/managers with more experience in IT may be more likely to adopt cyber insurance, reducing the uncertainties and risks of investment [55]. According to the empirical study by Nair et al. [62], SME owners' attitudes towards, and knowledge of, IT resources determine technology preparedness and infrastructure adoption. In a similar vein, it can be postulated that owners'/managers' knowledge and experience play a critical role in cyber insurance adoption intention:

H9. *Owners'/managers' knowledge and experience will have a direct and positive effect on the adoption intention of cyber insurance in Turkish SMEs.*

3.5. Post-Adoption Hypotheses: Information Communications Technology Adoption Intention (ICT) and Organisational Security Performance (OSP)

When a company seeks cyber insurance, it must have IT and cybersecurity infrastructure in place. Cyber insurance coverage is also important [63]. Insurance companies may impose certain prerequisites on SME customers within their policies to improve organisational cybersecurity. These requirements can range from adopting cybersecurity tools and implementing organisation-wide policies to regularly training staff to increase awareness. If a company already has cyber insurance, it means it already has a cybersecurity solution in place and is prepared to protect itself in the event of a cyber incident [22,23]. If a company does not currently have cyber insurance but intends to obtain it, it must show a commitment to implementing the necessary IT infrastructure [64]. The intention to adopt cyber insurance can drive the intention to invest in and adopt other ICT tools. Therefore, the hypothesis is as follows:

H10. *Cyber insurance adoption intention affects ICT adoption intention in a positive way for Turkish SMEs.*

Organisational security performance (OSP) is a concept that combines system protection and combat capabilities but also includes other variables such as availability. It can be seen as a measure of an organisation's security in the event of a cyber attack [34]. Even if IT infrastructure and cybersecurity tools cannot prevent cyberattacks all the time, they can still reduce the impact of an attack on the company's systems and databases. Adopting cyber insurance can create a sense of security which may encourage increased investment in ICT tools. This, in turn, can enhance organisational security performance.

H11. *Cyber insurance adoption intention affects organisational security performance through ICT adoption for Turkish SMEs.*

Finally, the positive and direct effect of cyber insurance adoption regarding ICT adoption may demonstrate the opportunity and benefits of digitalisation for Turkish SMEs with cyber insurance. Cybersecurity investments may come to an upper limit in terms of effectiveness. At a certain level, it would not be beneficial to invest in cybersecurity systems for risks that may never be eliminated. Investing in cyber insurance and other ICT tools can be more effective overall. In case of a cyberattack, the direct financial effects—such as ransom payments—can be too difficult to recover from [23]. As cyber insurance adoption mitigates the financial risk, companies can use their financial resources to invest in other

digitalisation tools and technologies. In this manner, cyber insurance adoption intention can affect organisational security performance directly and positively. The reasoning above suggests the following hypothesis:

H12. *ICT adoption intention affects organisational security performance in a positive way for Turkish SMEs.*

The 12 hypotheses are represented diagrammatically in Figure 1.

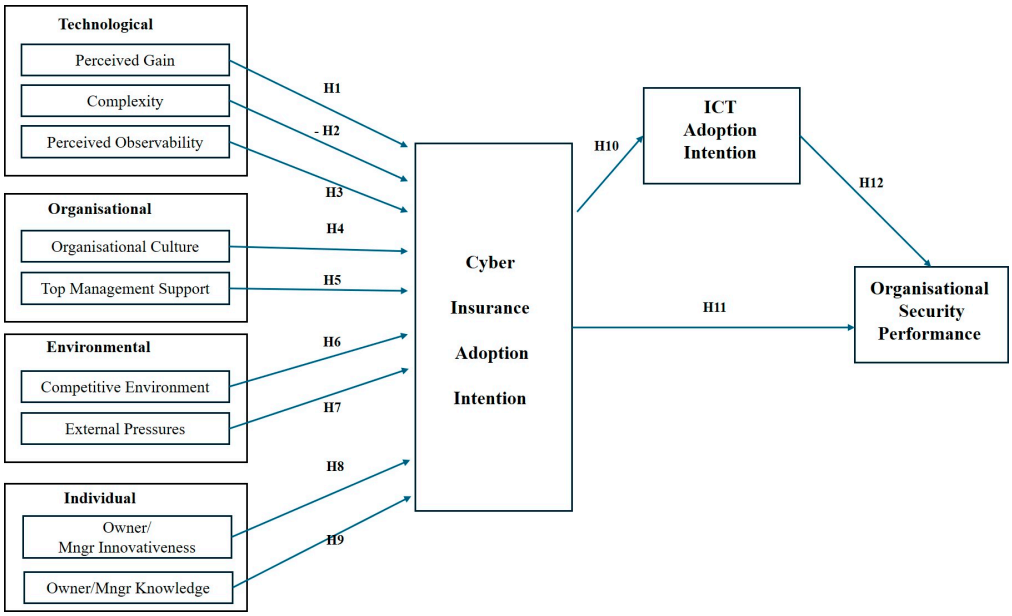

Figure 1. Cyber insurance adoption model and related hypotheses.

4. Research Method

The study used a quantitative survey that was developed from the literature review. Initially, the respondents were asked demographic questions about themselves to ascertain descriptive statistics, followed by the two main sections of the survey. The first section aimed to gain insight into the respondents' knowledge and experience on ICT systems and tools, cybersecurity, and cybersecurity insurance. The second section was designed to test the study model and related hypotheses. The questions were based upon those used in previous studies reviewed in Section 2 above. The indicators of the model with source studies are detailed in Table A1 in Appendix A. The scales were all five-point Likert scales with the exception of "perceived gain" and "external pressures", where a seven-point Likert scale was used, as in the source upon which this question was based [33].

The questions were originally in English and were translated into Turkish for the survey, which targeted Turkish respondents. The questions were then back-translated into English to confirm the correct translation [65]. The survey questions were shared with cybersecurity and insurance sales experts for pre-testing their clarity and content validity [66,67]. In addition, an initial pilot study was conducted with 20 respondents. Grammatical errors were corrected, and questions that were less clear were rephrased.

For measuring the reliability and internal consistency of the initial study, Cronbach's alpha and composite reliability scores were calculated and considered for the study if the scores were above 0.7 for each group of items that were used to measure each construct (Table 1) [68]. Following the pilot study, data regarding potential survey respondents were collected through links shared on social media platforms. The target audience of the

survey was the owners or managers of SMEs, who were deemed appropriately qualified to participate in cyber insurance adoption decision-making for their companies.

Table 1. Definition of constructs used in the research.

Context	Construct	Definition	Field of Referenced Study	Referenced Study
Technology	Perceived gain	The expected financial and non-financial gain from adopting the cyber insurance.	Information systems security	Herath et al. [33]
	Complexity	The difficulty of adopting cyber insurance due to the prerequisites of the policy.	ICT	Albar and Hoque [37]
	Perceived observability	The ability to realise the benefits of adopting cyber insurance from others.	Smart contracts	Badi et al. [46]
Organisational	Top management support	The emphasis and support of top management to adopt cyber insurance and associated prerequisites.	Cyber insurance ICT Cybersecurity	Bandyopadhyay [48] Albar and Hoque [37] Hasan et al. [34]
	Organisational culture	The collaboration, communication, and centralisation of risk management in the organisation.		
Environmental	Competitive environment	The nature of the industry in which the company operates.	Cyber insurance ICT	Bandyopadhyay [48] Albar and Hoque [37]
	External pressures	The regulatory obligations, supplier requirements, and customer demands that the company must follow.	ISS Cyber insurance Cybersecurity	Herath et al. [33] Mbatha [10] Hasan et al. [34]
Individual	Owner/ manager innovativeness	The characteristic of the owner/manager is to embrace innovative technologies.	IS	Thong [69] Albar and Hoque [37]
	Owner/ manager knowledge	The level of knowledge of the owner/manager regarding cyber insurance and cybersecurity.	IS ICT	Thong [69] Albar and Hoque [37]
Cyber insurance adoption	Cyber insurance adoption intention	Company intention to buy or renew cybersecurity insurance.		Albar and Hoque [37]
Cyber insurance post-adoption	ICT adoption intention	Firm's willingness and intention to adopt ICT.	ICT	Albar and Hoque [37]
Cyber insurance post-adoption	Organisational security performance	Benefits of keeping a secure system against a cyber attack.	Cybersecurity	Hasan et al. [34]

For determining the minimum sample size, three different techniques were followed. The "rule of thumb" used for structural equation modelling–based partial least squares (PLS-SEM) models was first applied, based on a multiple of 10 times the number of hypotheses [70]. This gives a sample size of 120 (12 hypotheses times 10). The second and third techniques, which are more conservative, were developed by Kock and Hadaya [71]. Gamma-exponential and inverse square root methods consider the minimum absolute path

coefficients, significance levels, and statistical power required. Applying these methods, the minimum sample size calculated for the gamma-exponential method was 146, and for the inverse square root method, the minimum sample size was calculated as 160. Data cleaning was performed to eliminate non-SME respondents, responses with missing data, and respondents providing repetitive answers to all questions, i.e., the same answer for all multiple-choice questions [72]. The survey yielded 168 responses, exceeding the quantity required by all three methods of minimum sample size calculation.

For the analysis of the survey data, PLS-SEM was used. PLS-SEM is suitable for theory development with complex models as well as smaller sample sizes and non-normalised data [67]. PLS-SEM is often employed when the researchers formulate a theory based on existing literature and expertise [70,73]). The statistical power of PLS-SEM makes it more suitable for research in the development phase of theory [74]. For this study, WarpPLS 8.0 [72,73] was used for the reflective measurement model and structural model analysis.

In the reflective measurement model, indicator reliability, internal consistency reliability, convergent validity, and discriminant validity values were measured for evaluation [74]. Indicator reliability for the model was measured with indicator loadings. Each of the indicator loadings was above the threshold of 0.7 [67,74]. *p*-values of the indicators were below 0.001, thus indicating good reliability [75,76]. For internal consistency, both composite reliability and Cronbach's alpha were calculated. All measures were above the threshold values of 0.70 [67,74]. As the data were collected through an online survey, common method bias (CMB) was measured using both Harman's single factor test and full collinearity variance inflation factors (FVIF) [77,78]. These tests indicated that common method bias was not considered an issue for the model. For composite reliability, Cronbach's alpha, AVE and construct correlations were used (see Table A4 in Appendix A).

For the evaluation of the structural model, collinearity, significance of path coefficients, the magnitude and explanatory power of path coefficients, and predictive power were calculated [74]. The model does not have a problem of collinearity as the average VIF values are below the threshold of 3.3. *p*-value calculation was done using Stable3, jackknifing, and bootstrapping techniques with a one-tailed test, which is the default and recommended setting in WarpPLS [67,77]. Discriminant validity was assessed using the heterotrait–monotrait (HTMT) ratio of correlations [79], which demonstrated that the measurement items are valid and reliable and can, therefore, be used to test the developed hypotheses. The explanatory values can be seen in Table A5 in Appendix A.

5. Results

5.1. Demographic Profile of Respondents

Out of 168 respondents, 91 were men and 77 were women. A total of 121 respondents were between the ages of 21 and 40 years old. The majority of respondents had at least an undergraduate degree. A total of 63 respondents were company owners, and 29 identified themselves as the CEOs, who were fully authorised to make cyber insurance adoption decisions. The rest of the respondents were in managerial positions with authority and relevance to consider cyber insurance as a risk management tool and make suggestions, accordingly, to the owner or CEO. Table 2 summarises the demographics of the respondents.

The respondents were asked about their knowledge and experience with using IT systems and tools such as enterprise resource planning (ERP) software and cybersecurity. A total of 110 respondents (65%) stated that they have been using IT tools for up to 10 years, while 27 respondents (16%) have been using IT tools for more than 10 years. 54 respondents (32%) stated that they had been victims of a cybersecurity incident in their career. In terms of the company profile, 70 (42%) of the 168 businesses belonged to the micro segment (less than 10 employees with 10 million TL), 58 (35%) of respondents were owners or

managers of small business enterprises (employing between 10–50 staff and with annual turnover between 10–100 million TL), and 40 (24%) respondents worked for or managed by mid-size enterprises (employing between 50–250 staff and with an annual turnover between 100–500 million TL), according to the latest official gazette regulation of Ministry of Industry and Technology, dated 25 May 2023. The majority of companies belong to one of three main industry sectors: service industries (51, 30%), production (30, 18%) and wholesale/retail commerce (25, 15%).

Table 2. Respondents' demographics.

Category		Freq.	Category		Freq.
Age	21–30	66	*Company size*	Micro segment or self-employed	70
	31–40	55		Small enterprises	58
	41–50	28		Medium enterprises	40
	Above 50	19	*Role in the company*	Owner of the company	63
Gender	Female	77		Procurement manager	31
	Male	91		CEO	29
Education Level	Middle school	2		IT manager	27
	High school	22		Accounting manager	10
	Preliminary	30		Project/production manager	5
	Undergraduate	90		Finance manager	3
	Graduate	22	*Use of IT*	Did not specify	4
	Doctorate	2		Less than a year	25
Industry	Service	51		Between 1–10 years	110
	Production	30		More than 10 years	27
	Wholesale and retail commerce	25	*Experienced a cybersecurity incident in their career*	I prefer not to specify	10
	Accommodation	14		Do not know	7
	E-commerce	12		Yes	54
	Construction	9		No	97
	Managerial services	6	*Result of cybersecurity incident*	Disruption of work due to an incident	24
	Content creator	5		Loss of internal data	18
	Health	5		Customer complaints	16
	Education	2		Legal process fees	13
	IT	2		Compliance penalty	9
	Logistics and storage	2		Ransom payment to cyber criminals	6
	Insurance	2		Stolen customer data	6
	Biotechnology	1		Stolen trade secrets	5
	Other	1		No mention	71

Regarding the cybersecurity tools used to protect their systems, only 16 (10%) respondents claimed that they were not using cybersecurity tools while 133 (79%) respondents stated that they use more than one cybersecurity tool (see Table A2 in Appendix A). A total of 125 (74%) respondents used anti-virus software, this being the most commonly used cybersecurity tool.

In addition to using cybersecurity tools, 145 (86%) respondents also claimed that they perform standard cybersecurity measures, such as data backups, compliance controls, and employee training. Among the most frequently pursued cybersecurity measures

were critical data backups and compliance controls for the Personal Data Protection Law. More complex measures, such as vulnerability testing and system logs, were seen among respondents who already took other measures as well (Table A3 in Appendix A). Out of 168 respondents, 39 (23%) claimed to have adopted cyber insurance, 95 (57%) claimed they have not adopted cyber insurance, and 34 (20%) stated that they do not know whether they have adopted it or not.

5.2. Model Development and Hypotheses Testing Overview

Figure 2 depicts the conceptual model of the study with results from the PLS-SEM analysis. Based on the model, top management support, external pressures, and owner/manager innovativeness have direct effects on cyber insurance adoption intention, as indicated by the cyber insurance adoption intention (Insadpin) relationships in Figure 2 and Table 3.

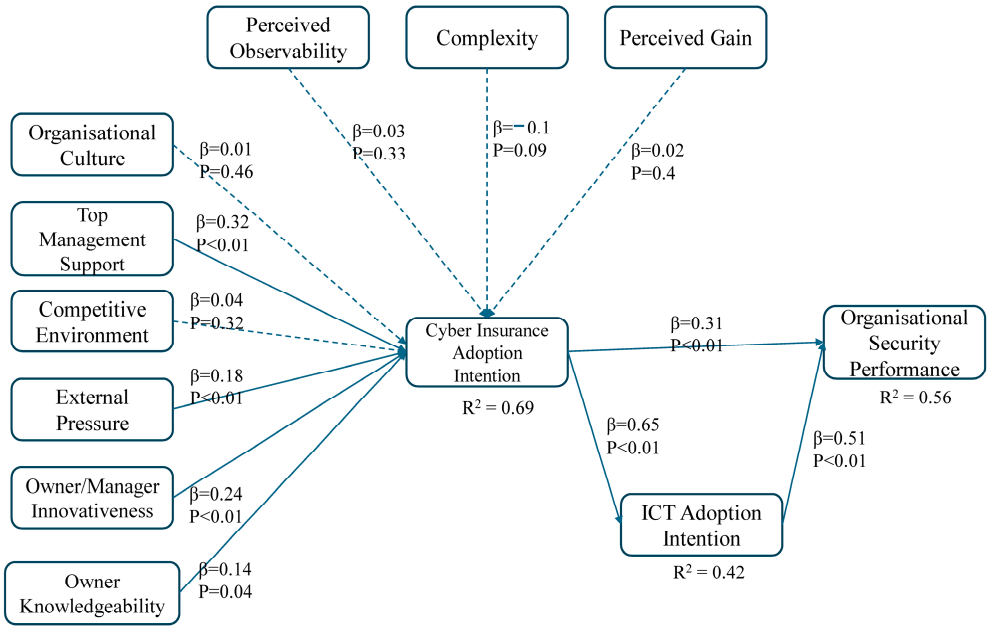

Figure 2. Final model: PLS-SEM results.

Table 3. Hypotheses testing results.

Hypothesis	Relationships	*p*-Value	Path Coefficient (β)	Results
H1	prcvdga-Insadpin	0.403	0.019	Not supported
H2	complxt-Insadpin	0.087	−0.103	Not supported
H3	prcvobs-Insadpin	0.327	0.034	Not supported
H4	orgcult-Insadpin	0.461	0.008	Not supported
H5	tpmngsu-Insadpin	<0.001	0.324	Supported
H6	cmptven-Insadpin	0.318	0.036	Not supported
H7	extrnpr-Insadpin	0.007	0.184	Supported
H8	ow/mgin-Insadpin	<0.001	0.239	Supported
H9	ownknow-Insadpin	0.036	0.135	Not supported
H10	Insadpin-ictadop	<0.001	0.647	Supported
H11	ictadop-orgscrp	<0.001	0.512	Supported
H12	Insadpin-orgscrp	<0.001	0.31	Supported

Key to abbreviations: Insadpin = cyber insurance adoption intention; prcvdga = perceived gain; complxt = complexity; prcvobs = perceived observability; orgcult = organisational culture; tpmngsu = top management support; cmptven = competitive environment; extrnpr = external pressures; ow/mgin = owner/manager innovativeness; ownknow = owner/manager knowledge; ictadop = ICT adoption intention; orgscrp = organisational security performance.

Additionally, cyber insurance adoption directly and positively affects post-activities related to digital transformation. ICT adoption intention mediates organisational security performance, while cyber insurance adoption intention directly and positively affects ICT adoption intention and organisational security performance. The nine hypotheses concerning antecedents, and three hypotheses for consequences, of cyber insurance adoption intention are discussed in more detail below.

The coefficient of determination (R^2) of the exogenous latent variables was measured to ensure model validity. As seen from Table A6 in Appendix A, R2 of cyber insurance adoption intention was 0.689, which is considered close to substantial, 0.538 for organisational security performance and 0.562 for ICT adoption intention, which are all above the 0.333 average threshold [67].

6. Discussion

6.1. Technological Factors

Drawing upon an analysis of the relevant literature, a number of technology-related factors were included in the study, for which no significant relationship with the intention to adopt cyber insurance was found. These factors included complexity, perceived gain and perceived observability.

Regarding the complexity factor (H2), respondents did not consider cyber insurance to be too complicated an initiative or that the required skills to use and integrate cyber insurance into work practices were overly complex. This contrasted with the findings in some of the extant literature, which suggested that the general perception of insurance policies as complicated had dissuaded some SMEs from adopting cyber insurance [21,24]. This may be explained by differing perceptions of what cyber insurance is, with some organisations not considering it to be a technological aspect but rather related to wider financial and risk management functions.

Nevertheless, a comprehensive understanding of the nature and scale of cyber risk in a company is essential for evaluating insurance policy options, and this may be problematic for some SMEs. Indeed, several insurance companies make such an understanding a prerequisite for cyber insurance policies. Additionally, the lack of IT employees with a detailed knowledge of cyber risk issues in SMEs may result in increased perceived complexity concerning cyber insurance. This perception may be compounded by the technical prerequisites of entering into a cyber insurance policy agreement: log management, database management, and a documented and practised recovery plan, which are not simple tasks to achieve without qualified IT employees.

However, as noted above, complexity was not perceived as a critical issue or barrier to entry by the Turkish SMEs studied here. This may also be explained by Turkish SMEs' relatively high level of digitalisation (as evidenced in Tables A2 and A3 in Appendix A, for example) and the fact that some SMEs in the sample set are already utilising cyber insurance. Having some experience with cyber insurance may mitigate the barriers to cyber insurance adoption intention.

Study results suggest that perceived gain (H1) and perceived observability (H3) do not significantly influence cyber insurance adoption behaviour, with neither H1 nor H3 indicating a positive effect on cyber insurance adoption. Some of the literature puts forward a different perspective, with Herath et al. [33], for example, contending that the perceived benefits of implementing information security measures positively influence the adoption of digital technologies. This supports the view that the observability of cyber insurance is probably low, in part because companies will normally not publicise cyberattack incidents because of potential reputational damage. Organisations may also avoid publicising the benefits they gain from cyber insurance and thus not experience the

knock-on observability that emerges from such benefits. In this context, Sangari et al. [80] show that companies often underreport cyber incidents because of reputational risk and its possible financial impact, and this under-reporting is especially common when incidents involve a breach of protected data. Sangari et al. [80] note that only 3% of all cyber incidents are accounted for in databases of publicly reported events. Insufficient publicity about the positive effects of cyber insurance may hinder a clear understanding of the positive effects of cyber insurance adoption by others. In addition, the lack of awareness about the consequences of cybersecurity breaches may lead to an underestimation of the financial risk from unmanaged cybersecurity threats [81], and perceived gains are also thereby underestimated. Accordingly, perceived observability does not significantly affect the intention to adopt.

To this same point, it is of relevance that there are only a handful of insurance companies that offer cyber insurance in Turkey, and the immaturity of this market has led to non-standardised policies, coverages, and pricing. Biener et al. [7] claimed that changing pricing policies, non-standardised calculation methods, and non-sufficient coverages have negatively affected the perceived gain from adopting insurance. The immaturity of the cyber insurance market has meant that products and their potential benefits are not well known or observed within the SME sector.

6.2. Environmental Factors

It is widely accepted that competitive pressure and the pursuit of a competitive edge are significant drivers of technology adoption in business [37]. In line with the perceived observability and perceived gain criteria, which are mainly related to the firm's perception influenced by others, the findings here suggest the competitive environment (H6) is not a significant factor for Turkish SMEs. This is in contrast to Bandyopadhyay [48], who concluded that a highly competitive environment was effective in cyber insurance adoption. Even though—to gain competitive advantage—digitalisation is becoming more common among SMEs, the cybersecurity requirements, and implications for technology integration and data sharing, are often not adequately recognised or acknowledged. Kshetri [82] sees this situation as resulting from a lack of awareness of cyber risk exposure, and thus, an underestimation of the competitive value of cyber insurance.

Awareness of the vulnerabilities that come with digitalisation is necessary for both the safety of SMEs and the growth of the cyber insurance market. In terms of the competitive environment, the reputational damage that companies may face in case of cyber incidents was also regarded as a part of the competitive environment effect. While this concern was not shown in the developed model for SMEs, it might be a valid concern for larger enterprises, for whom the financial consequences and the reputational damage can be more severe. Thus, a competitive environment may show a positive and significant effect on a model fit for large enterprises. However, the results here suggest that SMEs do not significantly believe they will lose their customers to competition and their market share if they do not plan to invest in cyber insurance. Additionally, they do not feel cyber insurance is a strategic necessity to compete in the marketplace either. Nevertheless, as Kshetri [82] observes, the competitive advantage of cyber insurance is highlighted and better appreciated after the negative experience of a cyber incident.

On the other hand, external pressures (H7) have a significant positive impact on Turkish SMEs' adoption of cyber insurance. Of relevance here is that cyber insurance policies commonly cover legal fees incurred due to violations of personal data protection laws, such as the GDPR in the EU and the Personal Data Protection Law in Turkey. Even though, as previously mentioned, perceived gain does not have a positive relationship with adoption, external pressure that comes from the mandatory rules regarding privacy laws

does. Privacy law requirements are considered a crucial legal practice for safeguarding customer data, with significant financial repercussions for non-compliance. The risk of a financial burden of non-compliance pushes businesses to adopt cyber insurance. The significant effect of environmental pressure on cyber insurance adoption emphasises the success of the regulatory controls of cyber protection for businesses. Our findings align with those of Hasan et al. [34], who suggest that these regulations serve to protect customer data, and non-compliance may lead to customers seeking assistance from authorities if needed.

6.3. Organisational Factors

Top management support and an encouraging culture are seen as two of the key organisational factors in the extant literature. Top management support (H5) has a direct and positive effect on the adoption intention of cyber insurance within Turkish SMEs. Senior management has a responsibility to decide and implement cyber insurance policies so that their support can significantly impact adoption intention. In a similar manner, the results of the study by Hasan et al. [34] have shown a significant positive correlation between top management support and readiness to combat cyber attacks.

While top management support affects cyber insurance adoption in a positive way, organisational culture (H4) does not have a significant effect on the adoption intention of cyber insurance. Cyber insurance is a specialised risk management tool that may not be fully understood or prioritised across all levels of an organisation, so general cultural values may not significantly influence the decision to adopt it. Furthermore, organisational culture might influence general behaviours but may not directly impact specific strategic decisions like purchasing insurance, which is often handled by upper management. This result is aligned with the findings of Albar and Hoque's [37] study, which did not find a significant relationship between organisational culture and technology adoption intention.

This finding can be viewed in combination with the individual context (H8) in the developed model, discussed below: owner/manager innovativeness and cybersecurity knowledge affect the adoption of cyber insurance for SMEs. This may influence the marketing strategy of cyber insurance companies: to reach more customers, insurance companies can create awareness of cybersecurity topics, educate their customers on cybersecurity, and then offer cyber insurance as a complementary risk mitigation tool.

6.4. Individual Factors

Individual factors cover owners'/managers' innovativeness and experience. Owners'/managers' innovativeness (H8) has a direct and positive effect on the adoption intention of cyber insurance in Turkish SMEs. This aligns with the findings of Omri et al. [83], who found that innovative behaviour positively influences business performance through its impact on innovation output. The owners/managers in SMEs that are innovative look for new ways to go digital and are aware of cyber risks, which influences top management to push for utilising the coverage and benefits that come with cyber insurance adoption.

Similarly, our findings align with the study of Laury et al. [59], who emphasises that insurance purchase and adoption decisions are also heavily influenced by the decision-maker's approach to risk and their innovativeness. Thus, when looking at the adoption of cyber insurance for SMEs, firm-level context alone is not sufficient, as the individual profiling of the company owner is also of direct relevance [63].

If top management, including the owner/manager, has significant knowledge and understanding of cyber insurance or cybersecurity issues, this may mitigate concerns derived from the perceived complexity of cyber insurance adoption. However, results also suggest that owners'/managers' knowledge (H9) is not believed to have a significant effect on cyber insurance adoption intention. This contrasts with the findings of Thong [69], but

the author was looking more generally at the impact of owner knowledge on information systems investment, rather than just cyber insurance.

6.5. ICT Adoption Intention and Organisational Security Performance (H10, H11, H12)

Post-cyber insurance adoption hypotheses H10, H11, and H12 are all supported. Cyber insurance adoption intention affects ICT adoption intention in a positive way, as stated in H10. Also, it affects organisational security performance through ICT adoption, as stated in H11. Therefore, ICT adoption intention affects organisational security performance in a positive way, as stated in H12

The positive relationship between cyber insurance adoption and ICT adoption in H10 results from many factors acting in combination. Cyber insurance is a risk transfer tool for cyber risks. The coverage provided by cyber insurance can create a sense of security for businesses, potentially leading to increased investment in ICT infrastructure. There are various additional risks involved in digitalisation for SMEs. Each year, the number and financial impact of cyber attacks targeting SMEs have increased. Failure to comply with privacy laws can lead to high financial penalties, and cyber tools may be complex and costly. In case of a cyberattack, the direct financial effects—such as ransom payments—can be too difficult to recover from [23]. This may discourage some SMEs from progressing digitalisation initiatives. Adopting cyber insurance can provide a correct sense of security and encourage digitalisation through the adoption of ICT, supporting H10. Also, if a company does not currently have cyber insurance but intends to obtain it, it must commit to implementing the necessary IT infrastructure [64].

As noted above in relation to H11, cyber insurance adoption intention affects organisational security performance through ICT adoption. The findings from this study parallel those from Watson et al. [22] and Kesan and Hayes [23], who state that companies with cyber insurance will often have cybersecurity solutions in place as prerequisites for cyber insurance, resulting in an increase in organisational security performance. Furthermore, cyber insurance provides financial protection by compensating for losses in the event of security breaches, allowing companies to invest in new technologies with insurance against significant financial risks [43].

Regarding H12, results align with the study by Chang et al. [84], which demonstrated a positive relationship between IT capabilities and the implementation of information security management in enterprises, as IT systems and resources can support security controls and measures.

6.6. Summary Issues

The hypotheses testing results discussed in the above sections raise some issues of a more general nature that merit further discussion. First, the results highlight the significance of senior management's understanding of cybersecurity issues and the potential role of insurance companies in simplifying the perceived complexity of cyber insurance adoption. Cyber insurance companies have a role to play, albeit not necessarily a fully objective one, in educating their customers on cybersecurity, and cyber insurance could be offered as a complementary risk mitigation tool to SMEs that may already be customers regarding other risk or security issues. To increase SME cyber insurance adoption in Turkey, cyber insurance companies need to be more open and explain the requirements and the adoption process with more clarity to enhance the likelihood of cyber insurance adoption.

Secondly, hypothesis H7 concerning the impact of external pressure was supported, suggesting that regulative measures or incentives are likely to increase cyber insurance adoption. The significant effect of environmental pressure on cyber insurance adoption emphasises the success of the regulatory controls of cyber protection for businesses. Oblig-

atory measures push companies to be more careful, proactively protecting themselves and adopting a risk management perspective. If these rules and regulations were to increase to make cyber insurance mandatory, the collective cyber readiness of Turkish SMEs would also increase. For instance, insurance companies conduct a due diligence process upon insuring a business. Not only would cyber insurance mitigate the financial risk of a cyber attack, but a more mature market might also relax the prerequisites of insurance companies. In addition, mitigating the financial aspect of the cyber risk can reduce the risk of bankruptcy in case of cyber events, which would be beneficial in the context of the wider economy. Even though cyber insurance is not mandatory for businesses yet, the effect of protecting customer data with regulations can be seen as a positive step towards safer digitalisation for SMEs in future.

Thirdly, it is clear that cyber insurance adoption is positively related to owner/manager's innovativeness. The combined effects of the model constructs suggest that owners'/managers' innovativeness has a significant and positive relation to ICT adoption: the innovative nature of the owner/manager is likely to support both cyber insurance and ICT adoption. Having an innovative leader thus emerges as a critical property in this context.

Fourthly, the positive and direct effect of cyber insurance adoption on ICT adoption indicates the support for on-going digitalisation that cyber insurance can provide for Turkish SMEs. Cyber insurance can be viewed as one piece in the jigsaw that represents a successful transition to a digitalised business. Cyber insurance allows companies to invest in digitalisation projects without undue concern regarding the potentially disastrous financial implications of a cyberattack.

7. Conclusions

This article has explored the various aspects of cyber insurance as a cybersecurity strategy for SMEs. Through a review of the current literature and the testing of 12 related hypotheses, qualified conclusions have been drawn regarding the technological, organisational, environmental and individual factors impacting the decision-making process regarding cyber insurance adoption. The survey results and PLS-SEM analysis identified top management support, external pressures, and owner/manager innovativeness as being of particular significance in positively engendering the adoption of cyber insurance, as well as ICT adoption and digitalisation overall. Furthermore, cyber insurance adoption intention affects ICT adoption and organisational security performance. ICT adoption intention also mediates the relationship between cyber insurance adoption intention and organisational security performance.

The emerging concept of cyber insurance provides flexibility in risk management and allows companies to transfer some of the cyber risks as part of their overall risk management strategy. This can put in place the cybersecurity foundation for initiating company-wide digitalisation projects, with IT and cybersecurity risk becoming a part of overall corporate risk management in some companies. The positive and direct effect of cyber insurance adoption regarding ICT adoption in general enhances the opportunities for successful digitalisation in Turkish SMEs with cyber insurance. Cyber insurance adoption mitigates the financial risk of ransomware and other cyber attacks, allowing companies to use their financial resources to invest in other digitalisation tools and organisational security technologies.

This article clearly has its limitations. It is based on a survey of Turkish SMEs, so generalisation across the wider SME sector must be treated with caution. Nevertheless, the authors believe this research provides some new insights into the dynamics of cyber insurance adoption, which is a relatively under-researched area of study. The findings enhance understanding of cyber insurance as a valuable and cost-effective tool for managing

cyber risks, which can be viewed as an alternative to expensive risk mitigation methods. SME leaders can utilise these insights to make informed decisions about integrating cyber insurance into their overall digitalisation strategy, particularly in relation to cybersecurity considerations. For policymakers, the study identifies key factors that influence the adoption of cyber insurance, such as support from top management and external pressures. This information can help inform the development of policies to improve cybersecurity within SMEs. Furthermore, applying the Technology–Organisation–Environment–Individual (TOE-I) model to the adoption of cyber insurance broadens its theoretical relevance, extending beyond traditional technology adoption and laying the groundwork for future research in cyber risk management. Future research could profitably build upon these findings to provide more in-depth case studies on cyber insurance to complement the quantitative survey results presented here. More specifically, considering the impact of cybersecurity and cyber insurance adoption on the customers of SMEs, future studies could focus on customer perception of cybersecurity issues and their perspectives on the risks to customer data. Conceptual development could also examine how cyber insurance relates to broader risk management themes and frameworks.

Author Contributions: Conceptualisation, N.T., A.Ö.Y. and B.M.; methodology, N.T., A.Ö.Y., H.D.E., M.W. and B.M.; software, N.T. and H.D.E.; validation, N.T., A.Ö.Y., H.D.E., M.W. and B.M.; formal analysis, N.T., A.Ö.Y., H.D.E., M.W. and B.M.; investigation, N.T., A.Ö.Y., H.D.E., M.W. and B.M.; resources, N.T., A.Ö.Y., H.D.E., M.W. and B.M.; data curation, N.T., A.Ö.Y., H.D.E., M.W. and B.M.; writing—original draft preparation, N.T., A.Ö.Y., H.D.E., M.W. and B.M.; writing—review and editing, N.T., A.Ö.Y., H.D.E., M.W. and B.M.; visualisation, N.T., A.Ö.Y., H.D.E., M.W. and B.M.; supervision, N.T., M.W. and B.M.; project administration, B.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data upon which this research is based is held in a university environment. All company and individual names have been anonymised. Further details are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

Table A1. Survey constructs, questions and sources used in the research study.

Construct	Adapted Questions	Source	Scale
Perceived gain (prcvdga)	PG1: Cyber insurance decreases potential losses due to security incidents	Herath et al. [33]	Seven-point Likert scale (from strongly disagree to strongly agree)
	PG2: Cyber insurance keeps risks related to security incidents to a minimum		
	PG3: Cyber insurance has contributed to the value of our business.		
	PG4: Cyber insurance has increased our market share (profitability) due to secure transaction practices.		
	PG5: Cyber insurance has increased the competitive advantage for our company		

Table A1. *Cont.*

Construct	Adapted Questions	Source	Scale
Complexity (complxt)	COM1: We believe that cyber insurance is very difficult to use	Albar and Hoque [37]	Five-point Likert scale
	COM2: The skills required to use cyber insurance is too complex for our employees		
	COM3: Integrating cyber insurance our work practices will be very difficult		
Perceived observability (prcvobs)	PO1: There is good publicity about the positive effects of cyber insurance	Badi et al. [46]	Five-point Likert scale
	PO2: Other organisations using cyber insurance liked using them.		
	PO3: I have a clear understanding of the positive effects of cyber insurance		
Top management support (topmngs)	TM1: Top management enthusiastically supports the adoption of cyber insurance	Albar and Hoque [37]	Five-point Likert scale
	TM2: Top management has allocated adequate resources to the adoption of cyber insurance		
Organisational culture (Orgcult)	OC1: Our organisation is very responsive and changes easily	Albar and Hoque [37]	Five-point Likert scale
	OC2: There is a high level of agreement about how we do things in this company		
	OC3: There is a shared vision of what this organisation will be similar to in the future		
Competitive environment (cmptven)	CE1: We believe we will lose our customers to our competitors if we do not adopt cyber insurance	Albar and Hoque [37]	Five-point Likert scale
	CE2: We feel it is a strategic necessity to use cyber insurance to compete in the marketplace		
	CE3: We believe we will lose our market share if we do not adopt cyber insurance		
External pressure (extrnpr)	EP1: Our business partners require that we have strong security program.	Herath et al. [33]	Seven-point Likert scale
	EP2: Our suppliers/business partners require use of specific security technologies and practices from us.		
	EP3: Our consumers are demanding about privacy and security		
Owner/manager innovativeness (ow/mgin)	OMI1: If we heard about a new information technology, we would look for ways to experiment with it	Albar and Hoque [37]	Five-point Likert scale
	OMI2: Among our peers, we are usually the first to try out new information technology		
	OMI3: We do not hesitate to try new information technology		
Owner/manager knowledge (ownknow)	OMK1: We have the necessary skills and knowledge to use cyber insurance	Albar and Hoque [37]	Five-point Likert scale
	OMK2: We are familiar with cyber insurance.		
	OMK3: We have the experience to use cyber insurance.		

Table A1. *Cont.*

Construct	Adapted Questions	Source	Scale
Cyber insurance adoption intention (Insadpi)	IA1: We have the intention to buy or renew cyber insurance.	Albar and Hoque [37]	Five-point Likert scale
	IA2: We want to get more information about buying or renewing cyber insurance.		
	IA3: We plan to buy or renew cyber insurance.		
Organisational security performance (orgscrp)	OSP1: The number of data breaches in our organisation is decreasing over time.	Hasan et al. [34]	Five-point Likert scale
	OSP2: Our organisation has a legitimate security reputation.		
	OSP3: The internal processes of our organisation are becoming more secure.		
	OSP4: Our organisation's databases are available whenever needed.		
	OSP5: Our organisation has a reliable system with adequate capabilities and capacities for information processing.		
ICT adoption intention (ictadop)	ICT1: We have a high intention to use information technologies in our organisation.	Albar and Hoque [37]	Five-point Likert scale
	ICT2: We intend to learn about information technologies.		
	ICT3: We plan to use information technologies to manage our business well.		

Table A2. Number of security tools used by survey respondents.

	Number of cybersecurity tools used per respondent	0	1	2	3	4	5	6	7	8	9	10	#of respondents
	Total # of respondents per # of cybersecurity tools used	16	19	17	22	35	13	16	13	4	3	10	168
Cybersecurity tools used by respondents	Anti-virus software	0	9	11	20	32	9	15	12	4	3	10	125
	Firewalls	0	1	3	8	23	9	11	11	4	3	10	83
	User authorisation	0	1	5	13	16	9	12	10	3	3	10	82
	File encryption	0	1	2	8	18	7	10	11	3	3	10	73
	Content filtering	0	2	3	3	10	6	9	11	4	3	10	61
	Strong password requirement	0	1	3	4	8	3	10	11	3	3	10	56
	Anti-spam software	0	0	1	4	12	4	10	8	3	2	10	54
	Digital identity	0	3	1	3	5	7	7	8	2	3	10	49
	One-time password	0	1	5	1	12	4	2	6	3	2	10	46
	VPN access	0	0	0	2	4	7	10	3	3	2	10	41
	I do not know	11	0	0	0	0	0	0	0	0	0	0	11
	None	5	0	0	0	0	0	0	0	0	0	0	5

Table A3. Number of security measures performed by respondents.

	Number of cybersecurity measures performed by respondent	0	1	2	3	4	5	6	7	# of respondents
	Total # of respondents per total # of measures taken	23	50	39	26	12	9	2	7	168
Cybersecurity measures	Backups of critical and personal data (at least once a week)	0	24	26	20	11	7	2	7	97
	Regular controls for compliance with Personal Data Protection Law	0	14	29	16	9	8	2	7	85
	Regular cybersecurity tests (vulnerability testing, IT auditing, etc.)	0	4	4	12	12	6	2	7	47
	Conducting employee training on cybersecurity	0	5	5	11	5	7	2	7	42
	System logs	0	1	4	11	4	6	0	7	33
	Recovery plan in case of an incident	0	1	6	4	4	8	2	7	32
	Getting internationally recognised certifications, such as PCI-DSS, ISO27001 [85]	0	0	3	4	3	3	2	7	22
	Others	0	1	1	0	0	0	0	0	2

Table A4. Reliability, AVE and construct correlations.

Construct	CR	Cronbach's alpha	AVE	Orgcult	prcvdga	prcvobs	cmptven	extrnpr	orgscrp	Insadpin	ow/mgin	complxt	ictadop	ownknow	topmngs
Orgcult	0.91	0.85	0.77	0.88											
prcvdga	0.92	0.89	0.70	0.32	0.84										
prcvobs	0.90	0.84	0.75	0.30	0.57	0.87									
cmptven	0.92	0.87	0.80	0.14	0.50	0.57	0.87								
extrnpr	0.90	0.84	0.75	0.27	0.39	0.64	0.52	0.90							
orgscrp	0.93	0.88	0.81	0.38	0.50	0.62	0.51	0.61	0.80						
Insadpi	0.90	0.86	0.64	0.31	0.34	0.58	0.48	0.69	0.63	0.91					
ow/mgin	0.96	0.94	0.89	0.30	0.31	0.54	0.51	0.63	0.54	0.67	0.84				
complxt	0.88	0.79	0.71	−0.05	0.17	0.12	0.12	−0.06	−0.07	−0.06	−0.01	0.81			
ictadop	0.93	0.89	0.83	0.40	0.28	0.46	0.29	0.50	0.71	0.65	0.45	−0.20	0.94		
ownknow	0.85	0.74	0.66	0.32	0.39	0.67	0.53	0.72	0.62	0.70	0.62	0.04	0.52	0.91	
topmngs	0.97	0.96	0.73	0.43	0.40	0.60	0.46	0.66	0.62	0.73	0.59	−0.04	0.57	0.75	0.90

Table A5. Explanatory values for the model.

Average path coefficient (APC)	0.258, $p < 0.001$
Average R-squared (ARS)	0.571, $p < 0.001$
Average adjusted R-squared (AARS)	0.563, $p < 0.001$
Average block VIF (AVIF)	2.214, acceptable if $\leq$5, ideally $\leq$ 3.3
Average full collinearity VIF (AFVIF)	2.705, acceptable if $\leq$5, ideally $\leq$ 3.3

Table A6. Coefficients of structural model.

	Orgcult	prcvdga	prcvobs	cmptven	extrnpr	orgscrp	Insadpin	ow/mgin	complxt	ictadop	ow/mgkn	tpmngsp
R^2						0.562	0.689			0.418		
Adjusted R^2						0.556	0.672			0.415		
Composite reliability	0.911	0.921	0.901	0.901	0.928	0.899	0.938	0.879	0.852	0.960	0.934	0.89
Cronbach's alpha	0.854	0.892	0.835	0.835	0.883	0.859	0.901	0.792	0.739	0.937	0.894	0.753
AVE	0.774	0.701	0.752	0.753	0.812	0.644	0.835	0.707	0.657	0.889	0.826	0.802
Full collinearity VIFs	1.38	1.80	2.62	1.91	2.77	3.06	3.37	2.18	1.16	2.61	3.30	3.10
Q-squared						0.564	0.678			0.422		

References

1. Eling, M.; Lehmann, M. The impact of digitalisation on the insurance value chain and the insurability of risks. *Geneva Pap. Risk Insur.-Issues Pract.* **2018**, *43*, 359–396. [CrossRef]
2. Wynn, M.; Felser, K. Digitalisation and Change in the Management of IT. *Computers* **2023**, *12*, 251. [CrossRef]
3. Abdallah-Ou-Moussa, S.; Wynn, M.; Kharbouch, O.; Rouaine, Z. Digitalization and Corporate Social Responsibility: A Case Study of the Moroccan Auto Insurance Sector. *Adm. Sci.* **2024**, *14*, 282. [CrossRef]
4. Datta, P.M.; Acton, T. From disruption to ransomware: Lessons From hackers. *J. Inf. Technol. Teach. Cases* **2023**, *13*, 182–192. [CrossRef]
5. Morgan, S. Cybercrime to Cost the World 8 Trillion Annually in 2023. *Cybercrime Magazine*. 17 October 2022. Available online: https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/ (accessed on 12 October 2024).
6. Hopkin, P. *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management*; Kogan Page Publishers: London, UK, 2018.
7. Biener, C.; Eling, M.; Wirfs, J.H. Insurability of cyber risk: An empirical analysis. The International Association for the Study of Insurance Economics 1018-5895/14. *Geneva Pap.* **2014**, 1–28. Available online: https://www.internationalinsurance.org/sites/default/files/2018-03/Insurability%20of%20Cyber%20Risk.pdf (accessed on 23 December 2024).
8. Altuntaş, E.; Kara, E.; Soylu, A.B.; Kırkbeşoğlu, E. Siber Sigortalar: Son Gelişmeler, Uygulamalar ve Sorunlar. *Bankacılık Sigortacılık Araştırmaları Derg.* **2018**, *12*, 8–22.
9. SNS Insider. Cybersecurity Insurance Market. 2024. Available online: https://www.snsinsider.com/reports/cyber-security-insurance-market-2273 (accessed on 19 December 2024).
10. Mbatha, N.S. Factors Influencing Cyber Insurance Adoption in South Africa Industry. Master's Thesis, Management in the Field of Digital Business, University of the Witwatersrand, Johannesburg, South Africa, 2020. Available online: https://wiredspace.wits.ac.za/server/api/core/bitstreams/94ace97c-1910-4bb9-ad05-7e848f16c1d8/content (accessed on 12 October 2024).
11. Turkish Statistical Institute. Small and Medium Enterprise Statistics. 2022. Available online: https://data.tuik.gov.tr/Bulten/Index?p=Small-and-Medium-Sized-Enterprises-Statistics-2022-49438 (accessed on 23 June 2024).
12. Tubisad (Informatics Industry Association). Basın Bültenleri. 2021. Available online: https://www.tubisad.org.tr/tr/tubisad/detay/Verimlilik-ve-katma-deger-artisi-icin-KOBIlerin-teknoloji-vizyonunda-degisim-sart-/19/157/0 (accessed on 30 August 2024).
13. Patterson, C.M.; Nurse, J.R.; Franqueira, V.N. I don't think we're there yet: The practices and challenges of organisational learning from cyber security incidents. *Comput. Secur.* **2024**, *139*, 103699. [CrossRef]
14. Es, A.; Serdar, N. Siber Saldirilara Karşi Kobilerin Farkindalik Düzeylerinin İncelenmesi: Ankara İli Örneği. *Düzce Üniversitesi Sos. Bilim. Enstitüsü Derg.* **2021**, *11*, 133–151.
15. IBM Security. Cost of a Data Breach Report 2021. 2021. Available online: https://info.techdata.com/rs/946-OMQ-360/images/Cost_of_a_Data_Breach_Report_2021.PDF (accessed on 18 October 2024).
16. Adriko, R.; Nurse, J.R. Cybersecurity, cyber insurance, and small-to-medium-sized enterprises: A systematic review. *Inf. Comput. Secur.* **2024**, *32*, 691–710. [CrossRef]
17. Hasani, T.; O'Reilly, N.; Dehghantanha, A.; Rezania, D.; Levallet, N. Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Bus. Econ.* **2023**, *3*, 97. [CrossRef]
18. Refsdal, A.; Solhaug, B.; Stølen, K. Cyber-risk management. In *Cyber-Risk Management*; Springer: Cham, Switzerland, 2015; pp. 33–47.
19. McShane, M.; Eling, M.; Nguyen, T. Cyber risk management: History and future research directions. *Risk Manag. Insur. Rev.* **2021**, *24*, 93–125.

20. Eling, M.; Schnell, W. What do we know about cyber risk and cyber risk insurance? *J. Risk Financ.* **2016**, *17*, 474–491. [CrossRef]
21. Dambra, S.; Bilge, L.; Balzarotti, D. SoK: Cyber insurance—Technical challenges and a system security roadmap. In Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 18–21 May 2020; pp. 1367–1383.
22. Watson, T.; Thakur, K.; Ali, M. The Impact of Purchasing Cyber Insurance on the Enhancement of Operational Cyber Risk Mitigation of U.S. Banks—A Case Study. In Proceedings of the 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 26–29 January 2022; pp. 0709–0715. [CrossRef]
23. Kesan, J.; Hayes, C. Strengthening Cybersecurity with Cyber Insurance Markets and Better Risk Assessment. *Minn. Law Rev.* **2017**, *102*, 191–276. [CrossRef]
24. Uuganbayar, G.; Yautsiukhin, A.; Martinelli, F.; Massacci, F. Optimisation of cyber insurance coverage with selection of cost effective security controls. *Comput. Secur.* **2021**, *101*, 102121. [CrossRef]
25. Davis, F.D. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q.* **1989**, *13*, 319–340. [CrossRef]
26. DePietro, D.; Wiarda, E.; Fleischer, M. *Processes of Technological Innovation*; Lexington Books: Massachusetts, MA, USA, 1990.
27. Venkatesh, V.; Morris, M.G.; Davis, G.B.; Davis, F.D. User Acceptance of Information Technology: Toward a Unified View. *MIS Q.* **2003**, *27*, 425–478. [CrossRef]
28. Awa, H.O.; Ukoha, O.; Emecheta, B.C. Using T-O-E theoretical framework to study the adoption of ERP solution. *Cogent Bus. Manag.* **2016**, *3*, 1196571. [CrossRef]
29. Racherla, P.; Hu, C. eCRM System Adoption by Hospitality Organizations: A Technology-Organization-Environment (TOE) Framework. *J. Hosp. Leis. Mark.* **2008**, *17*, 30–58. [CrossRef]
30. Oliveira, T.; Martins, M.F.O. Understanding the determinant factors of Internet business solutions adoption: The case of Portuguese firms. *Appl. Econ. Lett.* **2011**, *18*, 1769–1775. [CrossRef]
31. Skuridin, A.; Wynn, M. Chatbot Design and Implementation: Towards an Operational Model for Chatbots. *Information* **2024**, *15*, 226. [CrossRef]
32. Baker, J. The technology–organization–environment framework. In *Information Systems Theory: Explaining and Predicting Our Digital Society*; Dwivedi, Y.K., Scott, L.M., Schneberger, L., Systems, I.S., Eds.; University of Hamburg: Hamburg, Germany, 2012. [CrossRef]
33. Herath, T.C.; Herath, H.S.; D'Arcy, J. Organizational adoption of information security solutions: An integrative lens based on innovation adoption and the technology-organization-environment framework. *ACM SIGMIS Database DATABASE Adv. Inf. Syst.* **2020**, *51*, 12–35. [CrossRef]
34. Hasan, S.; Ali, M.; Kurnia, S.; Thurasamy, R. Evaluating the cyber security readiness of organizations and its influence on performance. *J. Inf. Secur. Appl.* **2021**, *58*, 102726. [CrossRef]
35. Wallace, S.; Green, K.; Johnson, C.; Cooper, J.; Gilstrap, C. An extended TOE framework for cybersecurity adoption decisions. *Commun. Assoc. Inf. Syst.* **2021**, *47*, 51. [CrossRef]
36. Rogers, E.M. *Diffusion of Innovations*; Free Press: New York, NY, USA, 1995.
37. Albar, A.M.; Hoque, M.R. Factors affecting the adoption of information and communication technology in small and medium enterprises: A perspective from rural Saudi Arabia. *Inf. Technol. Dev.* **2019**, *25*, 715–738. [CrossRef]
38. Hameed, M.A.; Arachchilage, N.A. A Conceptual Model for the Organizational Adoption of Information System Security Innovations. *arXiv* **2017**, arXiv:1704.03867.
39. Awa, H.O.; Ukoha, O.; Igwe, S.R. Revisiting technology-organization-environment (TOE) theory for enriched applicability. *Bottom Line* **2017**, *30*, 2–22. [CrossRef]
40. Wynn, M.; Rezaeian, M. ERP implementation in manufacturing SMEs: Lessons from the Knowledge Transfer Partnership scheme. *InImpact J. Innov. Impact* **2015**, *8*, 75–92.
41. Shackelford, S. Should Your Firm Invest in Cyber Risk Insurance. *Bus. Horiz.* **2012**, *55*, 349–356. [CrossRef]
42. Grigoriadis, L. Cybersecurity Insurance and New EU Cybersecurity and Data Protection Rules. *Bus. Law Rev.* **2017**, *38*, 210–218. [CrossRef]
43. Ak Sigorta. Cyber Protection Insurance: Frequently Asked Questions, Corporate. Ak Sigorta. Available online: https://www.aksigorta.com.tr/yardim-merkezi/sikca-sorulan-sorular/kurumsal/siber-koruma-sigortasi (accessed on 23 October 2024).
44. StrongDM. Cyber Insurance Requirements; StrongDM Blog. Available online: https://www.strongdm.com/blog/cyber-insurance-requirements (accessed on 12 October 2024).
45. Coalition Inc. 5 Essential Cyber Insurance Requirements. Available online: https://www.coalitioninc.com/topics/5-essential-cyber-insurance-requirements (accessed on 12 October 2024).
46. Badi, S.; Ochieng, E.; Nasaj, M.; Papadaki, M. Technological, organisational and environmental determinants of smart contracts adoption: UK construction sector viewpoint. *Constr. Manag. Econ.* **2021**, *39*, 36–54. [CrossRef]
47. Buzatu, C. The influence of behavioral factors on insurance decision—A Romanian approach. *Procedia Econ. Financ.* **2013**, *6*, 31–40. [CrossRef]

48. Bandyopadhyay, T. Organizational Adoption of Cyber Insurance Instruments in IT Security Risk Management: A Modeling Approach. AIS Electronic Library (AISeL). 2012. Available online: https://core.ac.uk/outputs/301355308/?utm_source=pdf&utm_medium=banner&utm_campaign=pdf-decoration-v1 (accessed on 12 August 2024).
49. Tang, M.; Li, M.G.; Zhang, T. The impacts of organizational culture on information security culture: A case study. *Inf. Technol. Manag.* **2016**, *17*, 179–186. [CrossRef]
50. Wynn, M.; Ilyas, J.; Isleyen, O.F.; Brüntrup, H.; Metin, B. Reassessing Critical Success Factors for ERP Implementation in the Digital Era. *Digit. Technol. Res. Appl.* **2024**, *3*, 140–154. [CrossRef]
51. Earl, M.J. *Management Strategies for Information Technology*, 1st ed.; Prentice Hall: Hoboken, NJ, USA, 1989.
52. Wynn, M. Information systems strategy development and implementation in SMEs. *Manag. Res. News* **2009**, *32*, 78–90. [CrossRef]
53. Herath, H.; Herath, T. Copula-based actuarial model for pricing cyber-insurance policies. *Insur. Mark. Co. Anal. Actuar. Comput.* **2011**, *2*, 7–20.
54. Ramdani, B.; Chevers, D.; Williams, D.A. SMEs' adoption of enterprise applications: A technology organization-environment model. *J. Small Bus. Enterp. Dev.* **2013**, *20*, 735–753. [CrossRef]
55. Shiau, W.L.; Hsu, P.Y.; Wang, J.Z. Development of measures to assess the ERP adoption of small and medium enterprises. *J. Enterp. Inf. Manag.* **2009**, *22*, 99–118. [CrossRef]
56. Awa, H.O.; Emecheta, B.C.; Ukoha, O. Location factors as moderators between some critical demographic characteristics and ICT adoption: A study of SMEs. *Sociol. Anthropol.* **2015**, *3*, 493–501. [CrossRef]
57. Olayinka, O.; Wynn, M. Digital Transformation in the Nigerian Small Business Sector. In *Handbook of Research on Digital Transformation, Industry Use Cases, and the Impact of Disruptive Technologies*; Wynn, M., Ed.; IGI-Global: Hershey, PA, USA, 2022; pp. 359–382. [CrossRef]
58. Bening, S.A.; Dachyar, M.; Pratama, N.R.; Park, J.; Chang, Y. E-Commerce technologies adoption strategy selection in Indonesian SMEs using the decision-makers, technological, organizational and environmental (DTOE) framework. *Sustainability* **2023**, *15*, 9361. [CrossRef]
59. Laury, S.; McInnes, M.M.; Swarthout, J.T. Insurance Purchase for Low-Probability Losses; Andrew Young School of Policy Studies Research Paper No. 08-05. 2008. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1090266# (accessed on 3 December 2024).
60. Yilmaz, Y. Transition to the Digital Economy, Its Measurement and the Relationship between Digitalisation and Productivity. *Istanb. J. Econ.* **2021**, *71*, 283–316.
61. Alahmari, A.; Duncan, B. Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In Proceedings of the 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 15–19 June 2020.
62. Nair, J.; Chellasamy, A.; Singh, B.B. Readiness factors for information technology adoption in SMEs: Testing an exploratory model in an Indian context. *J. Asia Bus. Stud.* **2019**, *13*, 694–718. [CrossRef]
63. Bodin, L.; Gordon, L.; Loeb, M.; Wang, A. Cybersecurity insurance and risk-sharing. *J. Account. Public Policy* **2018**, *37*, 527–544. [CrossRef]
64. Lloyd, M. Using cyber insurance to run virtuous circles around cyber risk. *Comput. Fraud Secur.* **2018**, *10*, 6–8. [CrossRef]
65. Brislin, R.W. Back-translation for cross-cultural research. *J. Cross-Cult. Psychol.* **1970**, *1*, 185–216. [CrossRef]
66. Forsyth, B.H.; Kudela, M.S.; Levin, K.; Lawrence, D.; Willis, G.B. Methods for translating an English-language survey questionnaire on tobacco use into Mandarin, Cantonese, Korean, and Vietnamese. *Field Methods* **2007**, *19*, 264–283. [CrossRef]
67. Urbach, N.; Ahlemann, F. Structural equation modeling in information systems research using partial least squares. *J. Inf. Technol. Theory Appl.* **2010**, *11*, 5–40.
68. Gliner, J.A.; Morgan, G.A. *Research Methods in Applied Settings: An Integrated Approach to Design and Analysis*; Lawrence Erlbaum Associates Publishers: Mahwah, NJ, USA, 2000.
69. Thong, J. An integrated model of information systems adoption in small businesses. *J. Manag. Inf. Syst.* **1999**, *15*, 27–31. [CrossRef]
70. Hair, J.F.; Ringle, C.M.; Sarstedt, M. PLS-SEM: Indeed a silver bullet. *J. Mark. Theory Pract.* **2011**, *19*, 139–152. [CrossRef]
71. Kock, N.; Hadaya, P. Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. *Inf. Syst. J.* **2018**, *28*, 227–261. [CrossRef]
72. Acock, A.C. Working with missing values. *J. Marriage Fam.* **2005**, *67*, 1012–1028. [CrossRef]
73. Memon, M.A.; Ting, H.; Ramayah, T.; Chuah, F.; Cheah, J.H. Editorial: A review of the methodological misconceptions and guidelines related to the application of structural equation modelling: A Malaysian scenario. *J. Appl. Struct. Equ. Model.* **2017**, *1*, 1–13.
74. Sarstedt, M.; Ringle, C.M.; Hair, J.F. Partial least squares structural equation modeling. *Handb. Mark. Res.* **2017**, *26*, 1–40.
75. Kock, N. Should bootstrapping be used in pls-sem? Toward stable p- value calculation methods. *J. Appl. Struct. Equ. Model.* **2018**, *2*, 1–12. [CrossRef]

76. Kock, N. Advanced mediating effects tests, multi-group analyses, and measurement model assessments in PLS-based SEM. *Int. J. E-Collab.* **2014**, *10*, 1–13. [CrossRef]
77. Kock, N. One-tailed or two-tailed P values in PLS-SEM? *Int. J. E-Collab. (IJeC)* **2015**, *11*, 1–7. [CrossRef]
78. Podsakoff, P.M.; MacKenzie, S.B.; Lee, J.Y.; Podsakoff, N.P. Common Method Biasesin Behavioral Research: A Critical Review of the Literature and Recommended Remedies. *J. Appl. Psychol.* **2003**, *88*, 879–903. [CrossRef] [PubMed]
79. Henseler, J.; Ringle, C.M.; Sarstedt, M. A new criterion for assessing discriminant validity in variance-based structural equation modeling. *J. Acad. Mark. Sci.* **2015**, *43*, 115–135. [CrossRef]
80. Sangari, S.; Dallal, E.; Whitman, M. Modeling Under-Reporting in Cyber Incidents. *Risks* **2022**, *10*, 200. [CrossRef]
81. Tanriverdi, N.S.; Metin, B. Enterprise Information Security Awareness and Behavior as an Element of Security Culture During Remote Work. In *Remote Work and Sustainable Changes for the Future of Global Business*; IGI Global: Hersey, PA, USA, 2021; pp. 119–138.
82. Kshetri, N. The Economics of Cyber-Insurance. *IT Prof.* **2018**, *20*, 9–14. [CrossRef]
83. Omri, W. Innovative behavior and venture performance of SMEs. *Eur. J. Innov. Manag.* **2015**, *18*, 195–217. [CrossRef]
84. Chang, Y.W.; Chang, P.Y.; Xu, Q.; Ho, K.H.; Halim, W.L. An empirical investigation of switching intention to private cloud computing in large enterprises. In Proceedings of the 22nd Asia-Pacific Conference on Communications (APCC), Yogyakarta, Indonesia, 25–27 August 2016; pp. 323–329. [CrossRef]
85. *ISO/IEC 27001:2022*; Information Security Management—The International Standard for Information Security. ISO: Geneva, Switzerland, 2022.