Devising a Cyber Security Management Module through Integrated Course Design

by JORDAN ALLISON, *University of Gloucestershire*

ARTICLE HISTORY

Compiled October 18, 2023

ABSTRACT

Cyber security is a growing area of international importance, with shortages present for cyber security skills. While many universities have introduced degree programmes for cyber security, the major focus of these programmes is on the development of technical skills with some reports indicating how graduates of these courses lack in softer skills and business acumen. However, cyber security management is a topic area where students can develop such skills. This paper presents the pedagogical and assessment approaches used for cyber security management education, and presents a case study of developing a 'Cyber Security Management' module of study through utilising Finks' Integrated Course Design. This paper presents the findings that active learning approaches are effective methods for teaching this subject area, which include the use of decision-making scenario tasks, group projects, and tasking students with conducting a management report for a real company, where they should conduct interviews with the organisation.

KEYWORDS

Cyber Security Management; Integrated Course Design; Cyber Security Education; Curriculum Design; Cyber Security

---

CONTACT: Dr Jordan Allison
Email: jallison1@glos.ac.uk
ORCID ID: 0000-0001-8513-4646
LinkedIn: https://www.linkedin.com/in/jordanrallison/

1. Introduction

The rate of development of cyber security attacks has led to a critical need for addressing the talent shortage of individuals with appropriate cyber security skills (Hoag 2013; Ricci et al. 2021). One survey revealed that 85% of organisations struggle with recruitment problems for identifying individuals with the right cyber security skills, with the top three in-demand skills being information security architecture, risk management and compliance, and intelligence/threat analysis (Caldwell 2013). This has led to an increased emphasis of the inclusion of cyber security within education (Rashid et al. 2018; Hajny et al. 2021). For instance, the Joint Task Force (ACM and IEEE) on Computing Curricula in 2013 added Information Assurance and Security as a key knowledge area in response to the increased importance of computer and network security (Joint Task Force on Computing Curricula: Association for Computing Machinery (ACM) and IEEE Computer Society 2013). While this document referred to various aspects of cyber security being important in university education, it was not until 2017 where the importance of cyber security in education was made more explicit with the publication of the 'Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cyber security' (Joint Task Force on Cybersecurity Education 2017), where cyber security is defined as an 'interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries' (Joint Task Force on Cybersecurity Education 2017). Cyber security crises have forced institutions to take note of the importance of cyber security and develop courses and guidelines for the creation of a supply of suitably educated cyber security professionals (Crick et al. 2019), with cyber security becoming more embedded into computing specifications. For instance, in March 2022, the United Kingdoms' Quality Assurance Agency (QAA) for Higher Education published their subject benchmark statement for computing where they outline cyber security as a key aspect of computing degrees (The Quality Assurance Agency 2022).

Other guidelines of what cyber security is have also been published such as the American National Institute of Standards and Technology (NIST) workforce framework for cyber security (NICE Framework) (Petersen et al. 2020), the British Cyber

Security Body of Knowledge (CyBOK) (Martin et al. 2021), and certifications such as the Certified Information Systems Security Professional and the Institute of Information Security Professionals Skills Framework. However, despite different guidelines being published, there is a lack of European coordination towards a common cyber security framework for education (Ricci et al. 2021), with some authors contending that there is no globally established cyber security curriculum currently followed by universities (Asghar and Luxton-Reilly 2020). Nevertheless, some authors have tried to mitigate this issue with literature beginning to emerge regarding how institutions could adapt and develop cyber security curricula (for example, see Hoag (2013); Hajny et al. (2021)). However, given the vast nature of topics which cyber security includes, it could be argued that there needs to be a greater account of the lived experiences of the teaching and learning activities used for the breadth of topics cyber security education entails.

Cyber security includes both highly technical and non-technical (soft) skills, and a cyber security graduate needs a combination of technical skills and business acumen to be successful in employment (Joint Task Force on Cybersecurity Education 2017; Department for Digital Culture Media and Sport 2019). However, despite the importance of the development of soft skills (Taylor-Smith et al. 2019), some graduates of computer science related courses feel that university had not prepared them regarding the development of their soft skills (Department for Business Innovation and Skills 2016). Hence, it is no surprise that the QAA reiterates how graduates should be able to link subject knowledge to business use cases (The Quality Assurance Agency 2022). While the development of soft skills may be more difficult in technical modules of study such as networking, cryptography, or securing operating systems, courses that focus on cyber security management provide an opportunity for students to develop these soft skills due to the non-technical and business focused nature of the subject matter. However, good practice examples of teaching cyber security is missing in many countries with no universal guidelines (Hajny et al. 2021), while it has been recommended that there should be further work exploring and evaluating different pedagogical and assessment approaches for cyber security education (Crick et al. 2019), with higher education being deemed as a neccesary partner for the implementation of cyber security

management education (Trilling 2018; Parrish et al. 2018). Therefore, this paper will present a critical and diligent account of the design and implementation of a 'Cyber Security Management' module of study through the theoretical framework of Finks' Integrated Course Design (Fink 2003). In line with this, this paper will aim to answer the following research question.

How can the theoretical framework of Finks' Integrated Course Design be used to aid the design and implementation of a 'Cyber Security Management' module of study?

In order to answer this research question, this paper will be structured as follows: This paper will first present some related work on the pedagogical and assessment approaches which are used for cyber security management education. We conclude that some efforts in this area have been made but it is still largely unexplored. Following this, Finks' Integrated Course Design (Fink 2003) is introduced, and the twelve steps of the framework are utilised to explain the design of the 'Cyber Security Management' module of study. This section reflects on the related work and how existing good practices can be used in this module setting. Finally, this paper presents an evaluation of the module in terms of the effectiveness of the framework in its design and implementation, drawing on personal reflection of module delivery, student results, and student feedback.

2. Related Work

Cyber security management as a domain has seldom been documented regarding examples of teaching approaches used, but this section will reflect on some of the literature which exists in this area. Early research documents this teaching in the context of 'information security management' as opposed to cyber security management. For instance, Grimaila (2004) details the use of a scenario-based group project as an information security management exercise, where students had to develop a comprehensive security program for an organisation including defining and documenting policies, procedures, and practices for the company. This project involved setting up, securing, and managing the operation of a secure (SSL) web server which accepts orders via the pub-

lic internet, documenting all details about the project, including proposing a five-year budget and risk analysis (Grimaila 2004). Although extensive as a project, and leading to some stress by students, overall, the students enjoyed the experience, and the author explains how companies hiring these students indicated how the project experience has given the students valuable skills relating to security management (Grimaila 2004). While this group task scenario is very detailed, other authors use a lighter approach. One example is where the different pedagogical approaches used in an information security management course are documented, and the author discusses how using case studies as part of a group task resulted in active participation by students and achieved the benefits of active learning (Hazari 2005). They further indicate the importance of decision-making being part of the learning experience due to the nature of the subject (Hazari 2005). What is key in this paper is the reference to active learning, which can be described as where students learn more and retain learning for a longer period of time if they acquire it in an active rather than passive manner (Fink 2003). For instance, through case studies and scenarios as opposed to traditional lecture delivery only.

Later studies also emphasise the importance of active learning for cyber security management education, albeit in different ways. A New Zealand based study reported on the design and implementation of a cyber security master's programme, and although the authors do not explicitly focus on cyber security management, they refer to how graduates of the programme develop expertise in governance, information assurance, and risk analysis, amongst other areas (Asghar and Luxton-Reilly 2020). The paper further explains how although the pedagogical approaches used on the course are diverse, they all generally involve active learning approaches and include group work projects (Asghar and Luxton-Reilly 2020). Similarly, Maguire, English, and Draper (2019) considers the design of a learning activity delivered as part of a master's level cyber security management course with the aim of understanding data protection and privacy laws internationally. The authors emphasised the importance of active learning designs, with student tasks including self-organising into teams, conducting research as a group regarding data protection and privacy laws, and finally, producing a presentation that they present to their peers (Maguire, English, and Draper 2019).

Other authors have incorporated different types of activity other than group tasks, such as one study regarding security management in the context of mobile devices (Yuan et al. 2016). The authors indicate how they incorporated the analysis of implementing BYOD policies, and writing a BYOD policy as part of an assignment task for students (Yuan et al. 2016). Student feedback indicated how they found the course informative, with 81% of students agreeing that the assignment case study helped them understand security policy (Yuan et al. 2016). Meanwhile, Omiya and Kadobayashi (2019) outline the proposal of a cyber security exercise tool, Secu-One, for improving security management skill. The authors highlight how active learning experiences such as the game exercises allow multiple people to participate, helps learners gain knowledge, but also allows the ability to quantitatively comprehend participant capability (Omiya and Kadobayashi 2019). Overall, a variety of methods have been used in the teaching of cyber security management, with the key implication being that methods that promote active learning should be utilised in addition to traditional lecture delivery. These methods can include using case studies and scenarios, group tasks, presentations, and games.

3. Materials and Methods

3.1. *Course Design Methodology: Finks' Integrated Course Design*

A comprehensive level of planning is required to ensure that teaching, learning activities, and assessment methods lead to students having a valuable learning experience (Fink 2003). This involves a systematic process, and one way of doing this is through following Finks' twelve steps of integrated course design (ICD) (Fink 2003), which has been drawn upon in prior evaluations of computing courses. For example, in the mapping and comparison of learning outcomes and assessment between a Computer Information Systems course and a Management Information Systems course (Brooks and Zaidman 2012). More recent research by Ramnath and Hoover (2016) explored the development of a framework for computing courses and explains how in comparison to other course design methods, Finks' ICD incorporates a wide variety of aspects not explicitly included in other processes. Therefore, Finks' twelve steps of ICD will be

used to outline the design of the 'Cyber Security Management' module.

3.2. *Initial Design Phase: Build Strong Primary Components*

3.2.1. Step 1: Identify Situational Factors

This step involves outlining the course context. The module was for forty learners as part of their third year of their undergraduate degree in cyber and computer security (BSc Hons). Taking place in the second semester of the academic year, the module was timetabled for a face-to-face two-hour class once a week in a computing lab for twelve classes in total. Additionally, the module tutor offered four 'drop in sessions' each lasting an hour, resulting in students' having twenty eight hours of total contact time with the module tutor.

The module built upon a module students would have studied in the prior year, 'Managing the Security of Information'. Further, this module addresses a key part of cyber security related to both CYBOK knowledge area 1: 'Risk Management and Governance' (Martin et al. 2021), and the 2017 Cyber security Curricula guidelines knowledge area of 'organizational security', which includes risk management, governance and policy, laws, ethics and compliance, and strategy and planning (Joint Task Force on Cybersecurity Education 2017). All of the students on the module would have already studied modules relating to operating systems, network design and configuration, ethical hacking, and programming fundamentals. Hence, the 'Cyber Security Management' module would be a very different type of module for these students as it was much less technical in nature.

3.2.2. Step 2: Identify Learning Goals

Learning goals should include things such as critical thinking, solving real-world problems, and changing how students think about themselves (Fink 2003). When this is combined with the notion that cyber security management as a discipline combines aspects from both business and technology (Trilling 2018), should be focused on decision-making (Grimaila 2004), and should include aspects such as information and risk management, systems research, and professional skills (Parrish et al. 2018), this

only emphasises the importance of having clear learning goals that address these needs. Furthermore, there should be a focus on the development on students 'soft skills' as this is sometimes lacking in computer science graduates (Department for Business Innovation and Skills 2016). Hence, the following learning outcomes were created where a student passing this module should be able to:

- Critically evaluate and synthesise cyber security management components to understand and develop a cyber intelligence framework for organisations.
- Analyse and evaluate the legal, ethical and privacy concerns and frameworks of cyber security management.
- Critically evaluate cyber security policies, standards, processes, guidelines, and baselines.
- Evaluate and synthesise the components of risk management, operational security, auditing, assurance, and review.
- Effectively communicate the various areas and topics of cyber security management, present arguments, and analysis in a clear and concise manner to stakeholders and management.

3.2.3. Step 3: Formulate Feedback and Assessment Procedures

The formulation of appropriate assessment and feedback mechanisms can be difficult for many university educators, while most academic literature focuses more on the learner experience of assessment as opposed to the role of designing an assessment (Bearman et al. 2016). Based on this, Bearman et al. (2016) created the Assessment Design Decisions Framework which comprises six categories of assessment considerations. This framework was used to develop the following end-of-module assessment:

Based on a real mid-size SME in UK, provide a full Cyber Security management report (3000 words) which analyses the current stage of the company and provides policies and guidelines to address and manage security risks in the company. You can lay-down assumptions, if some information is not available about the company. The report should be in detail rather than a general discussion about cyber security management. I encourage you to have some interviews with the company to make

your report as real as possible. However, this is not compulsory for the assignment.

The first category of assessment considerations was 'purposes of assessment' (Bearman et al. 2016). The purpose of the above assessment was to provide students with the opportunity to work on a real case study for their assignment that they could interact with, with the aim of students developing a wide range of skills (interviewing, evaluation of a case, report writing, communication etc).

The second category of assessment considerations is 'contexts of assessment' (Bearman et al. 2016). The devised assessment was carefully chosen due to the context of both the students on the course, and the availability of potential SMEs students could connect with in the local area. The university is based in an area with a high proportion of technical and cyber security companies, in addition to many of a non-technical nature too. Hence, students could reach out to whatever type of organisation they prefer. Furthermore, many of the students on the course would be undertaking very technical modules relating to advanced networking and security, penetration testing, and malware analysis. Therefore, the opportunity to develop 'soft skills' was somewhat lacking in their overall course, so this module was the one which needed to provide sufficient opportunities for skill development in this area.

The third consideration is 'learner outcomes' (Bearman et al. 2016), and so the assessment was devised with the aforementioned learning outcomes in mind. The fourth and fifth considerations are 'tasks' (which refers to what the students need to do for the assessment), and 'feedback processes' (Bearman et al. 2016). Based on the learning goals and assessment purpose, the inclusion of conducting interviews was included to help students develop skills beyond the traditional scope of a cyber security course, with some authors highlighting the importance of experiential learning for understanding the issues of information security management (Hazari 2005). However, Fink (2003) explains how feedback and assessment procedures should go beyond backward looking assessments designed to allocate students a grade (as illustrated in the assessment description). Furthermore, it has been described how dialogue between teachers and students is essential for enhanced learning, and that it can help overcome issues where students do not understand assignment briefs (Nicol 2010). Hence, formative assessment methods were used where it was planned for the teaching activities to in-

clude tasks related to the assignment, where students could obtain feedback from the module tutor, their peers, and to undertake self-assessment, a key aspect of learning (Fink 2003).

The final assessment consideration was 'interactions' (Bearman et al. 2016), which refers to the types of interactions which will optimise good assessment design. Hence, the use of interviews as part of the assessment, active learning experiences within class relating to the assessment (discussed in the next session), and various opportunities for students to gain feedback on their assessment progress were all important considerations for the created assessment. Furthermore, it was recognised how what may be beneficial for some students may be detrimental to others (Scager et al. 2017), and so creating an assessment that was accessible to all students was extremely important. Hence, conducting interviews was made a non-compulsory element of the assessment.

3.2.4. Step 4: Select Effective Teaching and Learning Activities

Research on the higher education sector has indicated the importance of challenging students to prevent boredom and stimulate learning (Scager et al. 2017), and so the teaching and learning activities should be chosen carefully on what has been identified as good practice. It has been discussed how active learning experiences enhance the teaching of cyber security management topic areas, such as by Grimaila (2004), and so this was adopted for the 'Cyber Security Management' module. As part of an ICD, Fink suggests three components of active learning: information and ideas, experience, and reflective dialogue (Fink 2003). Similarly, Hazari (2005) reports on the instructional strategies used in a graduate level information security management course, and advocates using traditional lectures combined with active learning techniques such as discussions, case studies and practical experience. Therefore, some of these features were included in the module design where a wide variety of potential activities were deemed beneficial for learning. This included traditional lecture delivery, group discussions and tasks such as analysing texts available on the virtual learning environment or role playing exercises (e.g. a case study where decisions need to be made with someone acting as a CISO, someone else as a finance director etc), simulation games available online where users have a budget of what to spend and have to make cyber security

management decisions based on the information provided, and applied tasks based on lecture content that relate to the given assignment.

3.2.5. Step 5: Ensure Primary Components are Integrated

This steps involves ensuring that the four previous steps are in alignment and appropriate (Fink 2003), with the author deeming that this is the case as it was considered throughout.

3.3. *Intermediate Design Phase: Assemble Components into a Coherent Whole*

3.3.1. Step 6: Create Thematic Structure of Course

Creating a course structure involves dividing the semester into segments that focus on key concepts or topics (Fink 2003). Fink advocates for four to seven segments, but for this module, the course was divided into two major areas; understanding the organisation (understanding business overview, assets, threats, and associated risks), and measures to implement a cyber security management plan (policies and controls).

3.3.2. Step 7: Select/Create Instructional Strategy

Fink states how an instructional strategy is "a set of learning activities, arranged in a particular sequence so that the energy for learning increases and accumulates as students go through the sequence" (Fink 2003). Therefore, it was important to firstly contextualise topics such as the main components of risk analysis and assessment before going into further topics such as misconceptions of risk, and applying risk frameworks to their chosen organisation. Logically, once areas like this have been studied and worked upon, students could then formulate controls to mitigate what the key identified risks for their organisation may be.

Table 1. Scheme of Learning Activities

Week	Topic	Practical Sessions
1	Introduction to Cyber Security Management	Group Task - Assuming a breach mindset
2	Risk Analysis	Applied Task - Understanding assets and associated threats
3	Risk Assessment	Applied Task - Complete risk register / Applying FMEA
4	Reading Week (no teaching)	
5	Misperception of Risk	Group Task - Identifying priority decisions for a case study
6	Understanding your Organisation / Assignment Workshop	Applied Task - Stakeholder analysis / Risk appetite framework
7	Reading Week (no teaching)	
8	Approaching Organisations / Interview Guidance	Applied Task - Create interview guide / Draft email template
9	Policy	Group Task - Policy analysis
10	Managing Risks with Controls	Group Task - Identifying priority controls for a case study
11	Network Controls	Applied Task - Identifying network related issues
12	Physical Security Controls	Applied Task - Characterising controls
13-15	Spring Break (no teaching)	
16	People and Culture / Assignment Workshop	Group Task - Creating an effective cyber security culture
17	Module Review and Plan Critique	Applied Task - Student Presentations
18	Assignment Due	

3.3.3. Step 8: Integrate Course Structure and Strategy to Create Overall Scheme of Learning Activities

Step 8 refers to creating an overall scheme of learning activities, which can be seen in Table 1. Table 1 outlines two types of practical sessions; group tasks, and applied tasks. Group tasks are the learning activities where students were tasked with analysing documents together, or to make security decisions for a case study, with the aim to help develop communication and decision making skills (i.e. 'soft skills'). Meanwhile, applied tasks were individual tasks directly linking to their assignment, such as conducting a stakeholder analysis, or a risk appetite framework.

3.4. *Final Design Phase: Finish Important Remaining Tasks*

3.4.1. Step 9: Develop Grading System

The next step was to devise an appropriate grading system for the assessment. However, previous research has found that if different academics are to mark students work there can be inconsistencies, with many approaches to grading being based on a judgement as opposed to a precise measurement which can lead to marking being unreliable (Henderson et al. 2019; Mcconlogue 2020). However, various technologies exist to help develop appropriate grading systems. For example, Moodle, a type of student learning environment, is used by many academic institutions where students can submit work for marking and assessment (Lopes 2011). Moodle is the system used by the authors' home institution and so this was used to help with the marking process. More specifically, the in-built feature of creating a marking rubric was utilised,

as this is increasingly being used as a popular assessment grading technique in education settings due to their ability to provide feedback and improve course design (Ragupathi and Lee 2020). Ragupathi and Lee (2020) define a rubric as 'an assessment tool that explicitly lists the criteria for student work and articulates the levels of quality for each criterion. It is a visual narrative that breaks down the assignment into component parts and provides clear descriptions of the characteristics of the work associated with each component.' This section will present how the rubric appeared for the assessment and how it links to this definition.

The Moodle marking rubric was created for the assessment, where the assessment components and weightings of marks were as follows (total marks equals 100):

- [4 points] Introduction to the report
- [5 points] Organisation Analysis: Company overview and strategy
- [7 points] Organisation Analysis: Assets (linking to threats)
- [7 points] Organisation Analysis: Stakeholders
- [7 points] Organisation Analysis: Current policies and procedures
- [12 points] Organisation Analysis: Risk Analysis and Assessment
- [14 points] Cyber Security Management Plan: Provides relevant solution that links to the organisational profile
- [30 points] Cyber Security Management Plan: Relevant discussion provided on different aspects of cyber security
- [4 points] Conclusion
- [5 points] Overall Standard of Submission
- [5 points] Referencing and Citation

These components were added to a Moodle marking rubric, where each component was divided into brackets, with each bracket allocating a different amount of marks and feedback for each component (see Figure 1 for an example of how this was designed). Once the rubric was designed, it can then be allocated for grading purposes, with Figure 1 also showing how the rubric appears to a marker. It is here where the marker can scroll and select which bracket they would like for each component of the assignment (then highlighted in green). Markers can also add additional

comments in the right hand text box. Once grading is finished, the rubric would automatically calculate how many marks the student achieved, while the marker could also add supplementary overall comments too. Hence, this rubric allowed markers to score reliability, and make more valid judgments based on each assessed criterion, which allow for clarification of teacher expectations in a visual format that is easy to follow (Ragupathi and Lee 2020).

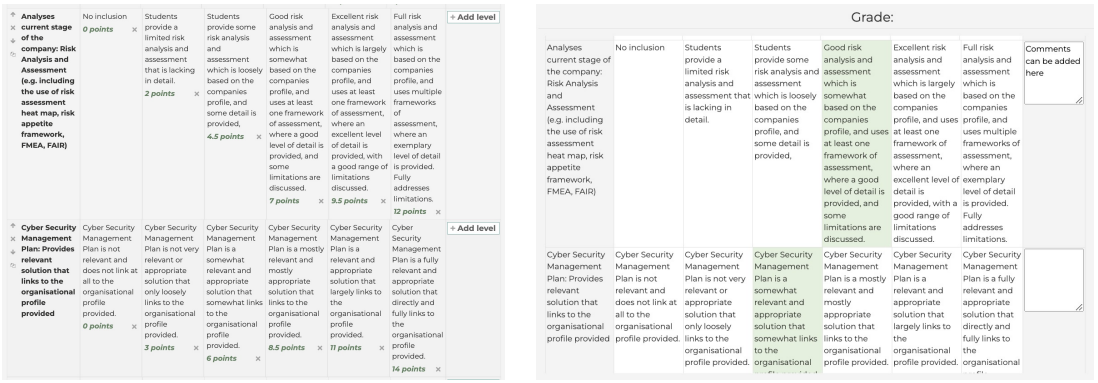

Figure 1. Marking Rubric. Left: Design View. Right: Grading View

3.4.2. Step 10: De-Bug Possible Problems

This steps primarily refers to thinking about potential issues that could arise (Fink 2003). The most notable issue was that students may not be able to find someone to interview as part of their assessment, and so this is another reason why this was made a non-compulsory element. No other major issues were identified.

3.4.3. Step 11: Write Course Syllabus

Once the course was designed, and the timetable was declared by the institution, this information was conveyed to students via their virtual learning environment. Other details regarding the module were discussed in the first face-to-face session with students, where they had the opportunity to ask any questions.

3.4.4. Step 12: Plan Evaluation of Course and Teaching

Students were asked to complete a mid-module evaluation which consisted of ten four-point likert-scale questions (strongly agree (SA), agree (A), disagree (D), and strongly

disagree (SD)) (See Table 3), and two open questions where students could provide free text responses; 'What I liked most about this module is', and 'My suggestions for improving the module'. Students also completed an overall final module evaluation when they had completed the module as standard practice of the university. Here, they were asked likert-scale questions about module quality and satisfaction. General student feedback would also be sought throughout the module, while overall assessment results and practitioner reflection would serve as other evaluation methods. It should be noted that this research did not require formal approval by the University's Research Ethics Committee due to the research adhering to the ethical consequences of researching with human subjects, and by following the home institutions Research Ethics guidelines.

4. Results and Discussion

4.1. *Overall Evaluation of the Cyber Security Management Module*

This paper set out to answer *'How can the theoretical framework of Finks' Integrated Course Design be used to aid the design and implementation of a 'Cyber Security Management' module of study?'* From an anecdotal perspective, the organisation and structure of the module worked very well, with the teaching and learning activities suitably building upon one another, with each session helping the students construct their organisational profile and cyber security management plan. Furthermore, with the inclusion of group tasks and discussion, case studies, presentations and conducting interviews with real businesses, the module design provided plenty of opportunities to develop the 'soft skills' that are so often lacking in cyber security students (Department for Business Innovation and Skills 2016). Nevertheless, to provide a more detailed analysis on how Finks' ICD aided the design and implementation of the module, final module survey results have been compiled.

Table 2 provides the results of the final module evaluation survey that was completed by students and is a standard survey delivered across the authors' home institution. For this survey, students were asked to rate each statement according to the following scale:

Table 2. Final Module Evaluation Survey Scores

Question	Score 2020/2021	Score 2021/2022
1) Overall, I am satisfied with the quality of the module	2.80	4.56
2) I have found the delivery of this module stimulating	2.20	4.56
3) I am satisfied with the teaching on this module	3.00	4.67
4) The module has a range of teaching styles which helped me learn	N/A	4.44
5) The assessment brief was clear	2.80	4.56
6) I received appropriate support and guidance for assessment	2.60	4.78
7) The module was well organised	2.80	4.78

- Definitely agree (5)
- Mostly agree (4)
- Neither agree or disagree (3)
- Mostly disagree (2)
- Definitely disagree (1)

An average score is then calculated for each statement, with the minimum response rate for reporting across the institution being at least 5 students. Table 2 shows the scores for both the academic year 2020/2021 prior to implementing the changes, and the academic year 2021/2022 where the changes were implemented to focus on active learning approaches.

Most notably, overall module quality and teaching satisfaction (questions 1 and 3) increased from a score indicating neither agree or disagree to a score of 4.56 and 4.67 respectively, indicating that students were more satisfied with the module approach, and hence, that the module design and implementation worked well.

Other key improvements can be linked more closely with Finks' ICD such as the questions about organisation and assessment (questions 5,6 and 7). Formulating feedback and assessment procedures is a key step in Finks' ICD (step 3), and much consideration was given to ensure the module was organised and designed so that students are supported in developing their assessment and also in their overall learning (e.g. see steps 7 and 8 of the module design). Hence, key improvements in these final module survey scores is very encouraging, particularly as module organisation and appropriate assessment support and guidance improved from scores of 2.80 and 2.60, to 4.78 and 4.78 respectively.

The final key improvements were regarding the questions that indirectly relate to the emphasis placed on ensuring active learning activities were embedded throughout

the module. For example, the scheme of learning activities in Table 1 identifies the active learning approaches used throughout the module such as case scenarios, group tasks, and presentations. These techniques have previously been used in other security management related modules (e.g. see Hazari (2005); Asghar and Luxton-Reilly (2020)), and all of these active learning activities are where learning is done in an active, rather than passive manner (Fink 2003), which was a key design feature for this iteration of the module. The final module survey scores indicated this approach likely worked well, as question 2 regarding finding the module stimulating improved from a score of 2.20 (disagree) in 2020/2021 to a 4.56 (definitely agree) in 2021/2022. Furthermore, a new question (question 4) asked in 2021/2022 was whether the module had a range of teaching styles to help students learn, and this resulted in a score of 4.44 (definitely agree). Although there is no comparison of this question to the previous year, these results indicate how the focus on different active learning approaches resonated well with the student cohort overall.

Given the experience of teaching the module, and in combination with the aforementioned module survey results, the module tutor considers that using Finks' ICD (Fink 2003) is beneficial in designing and implementing a 'Cyber Security Management' module of study, and therefore this paper adds to the body of literature of its use for designing computing related courses (e.g. Brooks and Zaidman (2012); Ramnath and Hoover (2016)). While there was a clear plan which helped for module delivery, what did not work so well was student engagement for all activities. For the traditional lecture delivery, there was little student engagement in terms of answering and asking questions. However, when students were set with discussion activities in groups or the applied tasks, students seemed more keen to engage in discussion and debate. In each session, the module tutor always took time to speak to each student in the class to gauge progress and while students seemed to appreciate this, it did take a sufficient proportion of the overall lecture time. However, with students simultaneously working on other structured activities, this did not seem too much of an issue.

4.2. *Effectiveness of Assessment and Module Results*

Prior to the implementation of Finks' ICD (Fink 2003) and the focus on active learning approaches, in the academic year 2020-2021, the average module grade was 48.13 with a standard deviation of 14.61. In this academic year there were 25 students registered on the module and there were 22 students who submitted an assessment, with five students failing the module (achieved less than 40%). However, for the academic year 2021-2022 where Finks' ICD (Fink 2003) was implemented, the overall module results improved by over 5%. More specifically, the module results followed a normal distribution with an average grade of 53.2 and a standard deviation of 15.4, where 37/40 students submitted an assessment, and four students failed the module (achieved less than 40%). Based on this improvement in module results, it could be argued that the focus on ICD and active learning approaches led to the improvement in module results. However, there are also other factors which could have influenced the overall module results such as the change in module tutor, and that student survey data highlighted how their appeared to be a significant improvement in assessment support and guidance from one year to the next (see Table 2). That said, appropriate assessment support and guidance was a key factor of the module design where there were many applied tasks throughout the scheme of work (see Table 1) so that students could link module content to their assessment effectively and recieve formative feedback.

For the academic year 2021-2022, for those students that failed the assessment (n=4), neither of these students conducted an interview, and had poor attendance throughout with submissions reflecting a lack of understanding of the assessment requirements. Almost all of those who passed had engaged in the process of conducting an interview, with many of those who had not conducted an interview instead contacting companies and acquiring further information via email.

University students differ in ability and this presents the dilemma of creating an optimal assessment that caters to all levels almost impossible (Scager et al. 2017). However, despite this difficulty, it was found that overall, the students provided a good evaluation of their chosen organisation, with many providing relevant cyber security management plans that were contextualised to their chosen organisation. Where many students lost marks was not referring to sufficient standards and academic literature, or

by providing too much of a generic discussion as opposed to specific detail. Nevertheless, through marking the assessments, it was clear that most students had engaged in the process well, with many demonstrating sufficient understanding of the cyber security management concepts taught within the module. However, while the assessment results are encouraging, there is no clear evidence that the student results were improved due to using Finks' ICD and the designed assessment as opposed to other course design methods and assessment techniques. Nevertheless, this paper presents an approach to engage with the problem of developing a teaching and assessment strategy for a module which focuses on developing soft skills in a group of students that are typically faced with skills development of a technical nature.

4.3. *Effectiveness of Marking Rubric*

Regarding the marking rubric, it took approximately three hours to create, largely due to assigning appropriate weightings and criteria for each assignment component. However, using the rubric helped significantly with marking the assignment, with each assignment taking approximately 15-20 minutes to download, read and mark, but this time also included providing annotated feedback on their submission. Due to the ease of using the rubric, and automatically calculating an overall grade, it is recommended that other practitioners consider adopting a similar approach in designing and implementing a detailed marking rubric. This work therefore supports the suggestions of using a marking rubric which were made by Ragupathi and Lee (2020), and places the feedback process as an integral part of course design where students should be aware of how they will be assessed, and how criteria link to different levels of grading. A detailed marking rubric allows for this, and alleviates the typical issues of feedback mechanisms within higher education as discussed by Winstone and Boud (2022) where feedback is highlighted as being subordinate to other aspects of course design.

Table 3. Results of Mid-Module Feedback (Likert Scale Questions, n=20)

Question	SD	D	A	SA
1) The module tutor makes it clear what I am expected to do	0%	0%	10%	90%
2) The module is well organised	0%	0%	10%	90%
3) The module is challenging me to achieve my best work	0%	5%	65%	30%
4) The module provides me with opportunities to explore ideas or concepts in depth	0%	5%	50%	45%
5) Resources available on Moodle for this module are helpful to my learning	0%	0%	25%	75%
6) The specialist resources, hardware and software provided support my learning on this module	5%	0%	80%	15%
7) The library resources (e.g. books, online services, learning spaces) support my learning	0%	5%	85%	10%
8) I have the opportunity to get useful formative feedback on my progress with the assessments	0%	5%	50%	45%
9) The module provides me opportunities to bring information/ideas from different topics	0%	0%	60%	40%
10) I would recommend this module to other students	0%	0%	40%	60%

4.4. *Other Student Feedback*

4.4.1. Quantitative Feedback

Table 3 indicates how 20/40 students in the cohort completed the mid-module evaluation, with 90% of students strongly agreeing that the module was well organised and it was clear what they need to do, a testament to the effectiveness of using Finks' ICD in this setting. All students who completed the questionnaire also agreed that they would recommend the module to others, the resources on Moodle were helpful to their learning, and that the module provided them opportunities to bring ideas from other topics. The latter is particularly encouraging as it was intended for the active learning activities such as group tasks to facilitate wider discussion between students while the case studies were utilised to provide students with varying scenarios across business sectors.

Similarly, a key aspect of the teaching and learning activities (step 4) and the overall scheme of learning activities (step 8) was the inclusion of applied tasks. Applied tasks were designed to directly link to the students assessment as a means of formative assessment. Therefore, with 95% of students agreeing that they had opportunities for useful formative feedback, this indicates that this desired design consideration was implemented successfully.

4.4.2. Qualitative Feedback

Table 4 details the responses to the open-ended questions which added greater context to the quantitative responses. Here, students indicated how they liked the relevancy of the module content and skills to the real world. For instance, in regards to what they like about the module, students commented:

- *'Seems like a very useful skillset and experience for the real world'*
- *'Business led lectures allow us a broader perspective on the subject'*
- *'Its relevance and applicability towards future experiences in industry'*

These comments highlight how students acknowledged the skills that were being developed throughout the module. Therefore, it is suggested that the inclusion of active learning approaches throughout the module (as discussed in step 4) to help develop student 'soft skills' appears to have been successful, as students mention skill sets and applicability to future employment despite not being asked explicitly about these aspects.

Positive comments were also made regarding the teaching style such as:

- *'Explains the concepts with real life examples which makes it easy to understand'*
- *'Taught well, interactive - really nice PowerPoints. Enjoy the real-world examples'*
- *'The teaching style, its way more engaging than any of the other modules'*

These positive comments regarding teaching style are particularly encouraging as one of the reasons for using Finks' ICD was to create an effective and engaging teaching and learning environment for mostly technical students where the subject matter is non-technical.

Regarding student suggestions for improvement, five students commented how the interview session should have been delivered earlier in the semester, for example:

- *'Do the interview lecture earlier, as it was really good'*

Comments were also made how there should be more practical activities:

- *'More examples and demonstrations'*
- *'Do more interactive stuff'*

As these comments were in response to what could be done to improve, it is not known whether these students thought there were not enough active learning based activities, or that they liked them so wanted there to be even more. A key issue that did exist though was that one student highlighted how *'the luck of getting an interview or not almost caused issues'*, and so perhaps more guidance should be

Table 4. Results of Mid-Module Feedback (Open Questions)

Question	Responses
11) What I liked most about this module is	The opportunity to discuss topics in more depth Explains the concepts with real life examples which makes it easy to understand Seems like a very useful skillset and experience for the real world Taught well, interactive - really nice PowerPoints. Enjoy the real-world examples The teaching style Business led lectures allow us a broader perspective on the subject Its relevance and applicability towards future experiences in industry Good communication between lecturer and students Presented concisely and in an engaging way Happy to pause lecture to answer any areas we aren't sure about. Teaching and presentation style ([Lecturer] is by far one of the most engaging) Teaching approach The teaching style, its way more engaging than any of the other modules Relevancy of module content to assignment
12) My suggestions for improving the module	More opportunities to work though tasks in groups Maybe should have conducting interview section a bit earlier compared to this year The luck of getting an interview or not almost caused issues Have face to face meeting or teams meetings to check on with the progress Do more interactive stuff More examples and demonstrations Do the interview lecture earlier, as it was really good Do the lecture on interviewing earlier in the semester Sometimes unclear how much of what is discussed should go to the assignment Spend less time on risk Have the interviewing lecture earlier in the semester

given on how to approach organisations and individuals for interviews in any future delivery of the module. Nevertheless, following completion of the module, two students informed the module leader how they secured graduate roles which they attribute to partaking in this module and the skills they developed having to complete the assessment. Therefore, it is believed that the module design helped contribute to the development of student 'soft skills', and subsequently graduate employability, although further research would be required to explore this sufficiently.

5. Conclusion

Prior work has suggested that there should be further work exploring the pedagogical and assessment approaches for cyber security education (Crick et al. 2019), and this paper contributes to knowledge by presenting a case study of cyber security management teaching and assessment, and builds upon the works presented by Hoag (2013) and Hajny et al. (2021) regarding cyber security curricula. Furthermore, this paper aimed to address the research question of how the theoretical framework of Finks' ICD (Fink 2003) could be used to aid the design and implementation of a 'Cyber Security

Management' module of study. It was found that ICD could be used to effectively ensure constructive alignment of learning outcomes, assessment and teaching activities within a cyber security module, where the focus was on the non-technical side of cyber security and the development of 'soft skills'. It was also found that using ICD allowed for the effective combination of learning activities that lead to improved student outcomes. Moreover, through using ICD, it ensured effective module organisation and led to an improvement in overall module satisfaction in comparison to previous years (see Table 2).

Due to how Finks' ICD was effectively used for a module such as this, it is expected that the framework could also be used effectively in the design of other generic management courses too. Furthermore, this paper aimed to assess what pedagogical and assessment approaches are used for cyber security management education and found that although work in this area is largely still unexplored, related work predominantly focused on utilising active learning approaches (Hazari 2005; Omiya and Kadobayashi 2019; Asghar and Luxton-Reilly 2020). This paper utilised and supports the use of these methods in cyber security management education such as writing and analysing policies (see Yuan et al. (2016)), and group task case studies with an emphasis on decision-making (see Hazari (2005)). Related work also utilised a range of assessment methods such as group projects and scenario based exercises, and this paper presents a more unique contribution to knowledge and practice through detailing how interviews can be used as part of a cyber security management assessment, which could be used to help students develop their 'soft skills'. Furthermore, it can be argued that one of the purposes of higher education is to impact the local community (Trinidad, Raz, and Magsalin 2021). Therefore, by facilitating the opportunity for cyber security students to work with SMEs that may not have sufficient cyber security knowledge, some of these companies may have increased their own awareness of their cyber security posture. However, this was not formally assessed and so future iterations of the module could incorporate company perspectives to further help evaluate the potential benefits an assessment approach like that described in this paper may provide.

It should be noted that the experience report outlined here is not a singular pro-

cess, as the module should continue to evolve and develop. Hence the reflections of this experience will inform the future design and delivery of the module for the academic year 2022-2023 and beyond, while practitioners can use the details provided in this paper to help inform their own module design and assessment practices. However, as noted by Bearman et al. (2016), educators must consider their own particular circumstances when making strategic choices of what would constitute as an effective course design and assessment strategy.

Word count = 6649 words

Disclosure statement

The authors report there are no competing interests to declare.

References

Asghar, Muhammad Rizwan, and Andrew Luxton-Reilly. 2020. "A Case Study of a Cybersecurity Programme: Curriculum Design, Resource Management, and Reflections." In *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, New York, feb, 16–22. ACM.

Bearman, Margaret, Phillip Dawson, Phillip Dawson, Sue Bennett, Matt Hall, and Elizabeth Molloy. 2016. "Support for assessment practice: developing the Assessment Design Decisions Framework." *Teaching in Higher Education* 21 (5): 545–556.

Brooks, Gail, and Marsha Zaidman. 2012. "A Comparison of the MIS and CIS Foundation Courses at the University of Mary Washington." *Journal of Computing Sciences in Colleges* 27 (3): 131–137.

Caldwell, T. 2013. "Plugging the cyber-security skills gap." *Computer Fraud & Security* 7: 5–10.

Crick, Tom, James H. Davenport, Alastair Irons, and Tom Prickett. 2019. "A UK Case Study on Cybersecurity Education and Accreditation." In *2019 IEEE Frontiers in Education Conference (FIE)*, Covington, 1–9. IEEE.

Department for Business Innovation and Skills. 2016. *Computer Science Graduate Employability: qualitative interviews with graduates.* London: Department for Business, Innovation and Skills.

Department for Digital Culture Media and Sport. 2019. *Initial National Cyber Security Skills Strategy: increasing the UK's cyber security capability - a call for views, Executive Summary*. Technical Report. London: Department for Digital, Culture, Media and Sport.

Fink, Dee. 2003. *A Self-Directed Guide to Designing Courses for Significant Learning*. San Francisco: Jossey Bass.

Grimaila, Michael R. 2004. "A novel scenario-based information security management exercise." In *Proceedings of the 1st annual conference on Information security curriculum development - InfoSecCD '04*, New York, 66–70. ACM Press.

Hajny, Jan, Sara Ricci, Edmundas Piesarskas, and Marek Sikora. 2021. "Cybersecurity Curricula Designer." In *The 16th International Conference on Availability, Reliability and Security*, New York, aug, 1–7. ACM.

Hazari, Sunil. 2005. "Instructional strategies for a graduate level Information Security Management course." In *InfoSecCD Conference'04*, 71–75. ACM.

Henderson, Michael, Michael Phillips, Tracii Ryan, David Boud, Phillip Dawson, Elizabeth Molloy, and Paige Mahoney. 2019. "Conditions that enable effective feedback." *Higher Education Research & Development* 38 (7): 1401–1416.

Hoag, Jim. 2013. "Evolution of a Cybersecurity curriculum." In *Proceedings of the 2013 Information Security Curriculum Development Conference - InfoSecCD '13*, New York, 94–99. ACM.

Joint Task Force on Computing Curricula: Association for Computing Machinery (ACM) and IEEE Computer Society. 2013. *Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science*. New York, New York, USA: Association for Computing Machinery.

Joint Task Force on Cybersecurity Education. 2017. *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. New York: Association for Computing Machinery.

Lopes, Ana Paula. 2011. "Teaching with Moodle in Higher Education." .

Maguire, Joseph, Rosanne English, and Steve Draper. 2019. "Data Protection and Privacy Regulations as an Inter-Active-Constructive Practice." In *Proceedings of the 3rd Conference on Computing Education Practice*, New York, jan, 1–4. ACM.

Martin, Andrew, Awais Rashid, Howard Chivers, Steve Schneider, Emil Lupu, and George Danezis. 2021. *Introduction to CyBOK Knowledge Areas*. Technical Report. Bristol: Bristol Cyber Security Group.

Mcconlogue, Teresa. 2020. *Assessment and Feedback in Higher Education: A Guide for Teachers.*

Nicol, David. 2010. "From monologue to dialogue: improving written feedback processes in mass higher education." *Assessment & Evaluation in Higher Education* 35 (5): 501–517.

Omiya, Tan, and Youki Kadobayashi. 2019. "Secu-One: A Proposal of Cyber Security Exercise Tool for Improving Security Management Skill." In *Proceedings of the 2019 7th International Conference on Information and Education Technology - ICIET 2019*, New York, 259–268. ACM.

Parrish, Allen, John Impagliazzo, Rajendra K. Raj, Henrique Santos, Muhammad Rizwan Asghar, Audun Jøsang, Teresa Pereira, and Eliana Stavrou. 2018. "Global perspectives on cybersecurity education for 2030: a case for a meta-discipline." In *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*, New York, jul, 36–54. ACM.

Petersen, R, D Santos, MC Smith, KA Wetzel, and Greg Witte. 2020. *Workforce Framework for Cybersecurity (NICE Framework).* Technical Report. National Institute of Standards and Technology.

Ragupathi, Kiruthika, and Adrian Lee. 2020. *Beyond Fairness and Consistency in Grading: The Role of Rubrics in Higher Education*, 73–95. Singapore: Springer Singapore.

Ramnath, Sarnath, and John H. Hoover. 2016. "Enhancing Engagement by Blending Rigor and Relevance." In *Proceedings of the 47th ACM Technical Symposium on Computing Science Education*, New York, feb, 108–113. ACM.

Rashid, Awais, George Danezis, Howard Chivers, Emil Lupu, Andrew Martin, Makayla Lewis, and Claudia Peersman. 2018. "Scoping the Cyber Security Body of Knowledge." *IEEE Security & Privacy* 16 (3): 96–102.

Ricci, Sara, Vladimir Janout, Simon Parker, Jan Jerabek, Jan Hajny, Argyro Chatzopoulou, and Remi Badonnel. 2021. "PESTLE Analysis of Cybersecurity Education." In *The 16th International Conference on Availability, Reliability and Security*, New York, aug, 1–8. ACM.

Scager, Karin, Sanne F. Akkerman, Albert Pilot, and Theo Wubbels. 2017. "Teacher dilemmas in challenging students in higher education." *Teaching in Higher Education* 22 (3): 318–335. https://doi.org/10.1080/13562517.2016.1248392.

Taylor-Smith, Ella, Sally Smith, Khristin Fabian, Tessa Berg, Debbie Meharg, and Alison Varey. 2019. "Bridging the digital skills gap: Are computing degree apprenticeships the answer?" In *Annual Conference on Innovation and Technology in Computer Science Edu-*

cation, ITiCSE, Aberdeen, 126–132. ACM.

The Quality Assurance Agency. 2022. *Subject benchmark statement: Computing*. Technical Report March. Gloucester: The Quality Assurance Agency for Higher Education.

Trilling, Rick. 2018. "Creating a New Academic Discipline: Cybersecurity Management Education." In *Proceedings of the 19th Annual SIG Conference on Information Technology Education*, New York, 78–83. ACM.

Trinidad, Jose Eos, Maxine Diane Raz, and Iva Melissa Magsalin. 2021. ""More than professional skills:" student perspectives on higher education's purpose." *Teaching in Higher Education* 1–15.

Winstone, Naomi E., and David Boud. 2022. "The need to disentangle assessment and feedback in higher education." *Studies in Higher Education* 47 (3): 656–667.

Yuan, Xiaohong, Wu He, Li Yang, and Lindsay Simpkins. 2016. "Teaching Security Management for Mobile Devices." In *Proceedings of the 17th Annual Conference on Information Technology Education*, New York, sep, 14–19. ACM.