Shreyabahen Naik

Developing and Launching a Cybersecurity Course for Business Users

Metropolia University of Applied Sciences

Master's Degree

Degree Programme in Business Informatics

Master's Thesis

18 June 2025

I am sincerely grateful to Metropolia UAS for support and for providing me with the thesis topic. I am also grateful to all the stakeholders, for sharing their insights, valuable ideas, and constructive information about the developing the cybersecurity course for business users.

I would like to express my sincere gratitude to my thesis supervisor, Zinaida Grabovskaia, PhL, Senior Lecturer, for her continuous support, constructive guidance, and encouragement throughout my research. Her valuable insights and suggestions helped me improve my work quality during this thesis.

I would like to extend my thanks to my classmates and cohort members for their help in sharing their experiences.

Lastly, I am also grateful to my parents, whose support and patience have been a source of strength throughout this journey.

Shreyabahen Naik
Helsinki, Finland
June 17, 2025

Abstract

Author:	Shreyabahen Naik
Title:	Developing and Launching a Cybersecurity Course for Business Users
Number of Pages:	72 pages + 3 appendices
Date:	18 June 2025
Degree:	Master of Business Administration
Degree Programme:	Business Informatics
Instructor:	Zinaida Grabovskaia, Senior Lecturer, PhL

The objective of this thesis was to develop a cybersecurity course that would be especially aimed at business students at Metropolia University of Applied Sciences. The goal was to meet the rising need for cybersecurity knowledge among non-technical users who play an important role in the use and protection of organizational data.

The study used a qualitative research approach and included an examination of the literature, the current state analysis, and stakeholder inputs for the proposal development and its validation. Data collection consisted from discussions with subject-matter specialists and comments from management and academic professionals.

The theoretical framework has drawn from the topics related to cybersecurity education, key EU literature like ENISA, and curricular design principles. In the development stage, these initial inputs were extended with actual stakeholder feedback that influenced the process of the course design. Key themes of the proposed course included cybersecurity challenges in business environment, GDPR compliance, cybersecurity awareness, and risk management practices.

The outcome of the thesis is a course developed with modular material, real-life examples, and integrated assessment methods. The course offers a contribution to Metropolia UAS course offerings, that aims at bridging knowledge gaps, enhancing digital resilience, and encouraging a culture of cybersecurity among business users.

Keywords: Cybersecurity course, Business users, ENISA, EU, GDPR

Contents

List of Acronyms

AES	Advanced Encryption Standard
AI	Artificial Intelligence
BYOD	Bring Your Own Devices
CSA	Current State Analysis
CF	Conceptual Framework
CISSP	Certified Information Systems Security Professional
ECSF	European Cybersecurity Skills Framework
ENISA	European Union Agency for Cybersecurity
EU	European Union
GDPR	General Data Protection Regulation
HEI	Higher Education Institutions
ML	Machine Learning
IoT	Internet of Things
SASE	Secure Access Service Edge
SOC	Security Operations Centers
VPN	Virtual Private Networks

List of Tables

List of Figures

1 Introduction

Currently, non-IT professionals require enhanced understanding of cyber dangers and information security. They must cultivate knowledge and practice of data protection. Organizations of all scales encounter escalating risks to their fiscal stability and consumer trust. As digital disruptions persist in reshaping the business landscape, it is imperative for all industry specialists to possess fundamental understanding of cybersecurity. Recent studies indicate that human errors and inadequate cybersecurity training substantially contribute to data breaches (Ponemon, 2017, p. 14). The swift adoption of mobile devices, the Internet of Things (IoT), and the concepts of bring your own device (BYOD) increased the possible vulnerabilities that the organizations must address (Baltuttis, 2024, p. 3). Recently, incidents of cyber-attacks impacted nearly every business sector. Cybercriminals are more adept at exploiting system vulnerabilities, mostly due to the insufficient awareness of cybersecurity among many business users, which hinders the prevention of unauthorized access.

In light of these issues, the imperative to train business personnel in the domain of cybersecurity has never been more pressing. As the East Asia Institute of Management (2024) asserts, "An educated workforce is the primary safeguard against cyber-attacks." This thesis addresses this need by creating and implementing a cybersecurity specifically tailored for business users. This course aims to provide users from non-IT backgrounds with essential knowledge and skills to enhance their capacity to safeguard critical information, hence fostering a more resilient business environment.

This thesis explores available education in the domain of cybersecurity with the focus on the business sector. It highlights the hazards arising from inadequate awareness about cybersecurity. This study creates a cybersecurity course for business users that helps the case organization to improve practical knowledge to mitigate cyber hazards.

1.1 Business Context

This thesis is on the Master’s Degree Programme in Business Informatics at Metropolia University of Applied Sciences. This program has a broad cohort of students, including those with strong IT backgrounds and others who are experts in their respective fields, mostly business. Generally, IT students possess greater familiarity with cybersecurity

concerns. Business students have had adequate exposure to these essential subjects but still have certain skills gap. The goal of the Programme's efforts is to guarantee that all graduates, regardless of their technical or non-technical backgrounds, have the fundamental cybersecurity skills required to safeguard their organization in a more digital and linked corporate environment.

1.2 Business Challenge, Objective and Outcome

The case organization recognizes the necessity to enhance the cybersecurity expertise of business students, who sometimes exhibit gaps in this area. For this end, the case organization endorses the creation of the course particularly designed for this set of users. In the contemporary business landscape, it is essential to possess a foundational understanding of information technology to adequately meet specific requirements. These skills enable business students to enhance their performance in the cybersecurity areas.

The objective of this thesis is *to create a "Cybersecurity Course for Business Users" aimed at creating relevant knowledge of cybersecurity* in this group of users.

The thesis outcome is the development and delivery of *a "Cybersecurity Course for Business Users," aimed at creating relevant knowledge of cybersecurity* in this group of users.

1.3 Thesis Outline

This thesis aims to create a course to provide Business Informatics students with understanding of cybersecurity and its safeguarding within their enterprises. This cybersecurity is designed for business students to acquire understanding of data security and data transfer, as well as to prohibit unauthorized access. This thesis co-creates the course with internal users using interviews to build the course. The course comprises lessons and examples, supplemented by audio and demonstrations implemented on the Moodle platform.

This thesis comprises seven parts. Section 1 delineates the introduction to the thesis, followed by the business problem, objective, and outcome of the thesis. Section 2 delineates the methodology employed for data collection and analysis for the thesis,

encompassing interviews with stakeholders and the research design of the thesis. Section 3 examines the literature and best practice for the development and implementation of a cybersecurity course. Section 4 presents the findings of the initial study, soliciting input from stakeholders on their requirements and expectations. Section 5 delineates the course. Section 6 presents the findings from the validation and a limited trial of the course in Moodle, and, based on the feedback, proposes enhancements to the original course design, informed by the outcomes of the preliminary testing and validation. Finally, Section 7 finishes the thesis.

2 Method and Material

This section reports on qualitative methodology and the data collection and analysis to develop a cybersecurity course for business users.

2.1 Research Approach

Research approaches can be divided according to wider *research paradigms*, including positivism, interpretative and pragmatism etc. that shape the way in which research questions are formed, data are collected and interpreted (Creswell, 2018, p. 389) . Research can also be widely divided into *research families* that differ in purpose and methodology. The aim of the *fundamental* research on while the applied research is focused on solving specific and real problems. In *applied* research, research methods are selected to create practical knowledge and support evidence-based decision making. These techniques ensure that applied research effectively solves real-world challenges (Creswell, 2018, p. 389) . Research can be carried out as *a field study* where data are collected directly in the real environment, or as *a desk study* that includes synthetization of existing literature and secondary data. These differences allow scientists to adapt their approach to the nature and goals of their studies.

Research methodologies are often categorized into qualitative, quantitative, and combined. Each of these methodologies has distinct advantages contingent upon the study objectives. The quantitative approach is grounded on a positivist worldview that posits an objective reality amenable to measurement and quantification. It relies on systematic procedures, including surveys, experiments, and statistical analysis, to test hypotheses and establish formulae or correlations among variables (Bryman, 2016, p. 14). This methodology is extensively employed in scientific and business research, where quantitative data and statistical methods are crucial for validating theoretical investigations. Quantitative research priorities statistical analysis as its technique.

The *qualitative* approach comes in line with interpretivism, focuses on exploring and understanding human experience, behavior and social phenomena in depth. In the study of organizational culture, management and behavior of consumers (Hannes, 2022, p. 5) . Qualitative research focuses on contextual, narrative knowledge for increasing the depth and validity of findings. For example, interviews are used to

capture detailed personal experience and perspectives, while surveys allow the collection of extensive quantitative data from different populations. Observations allow researchers to collect data in the natural environment, provide context specific knowledge and analyze documents facilitating existing records and literature to identify trends and historical formulas. This approach is in line with pragmatic paradigm that recognizes that reality is complex and that different methods can offer additional knowledge (Blank, 2013, p. 325).

Among *the research strategies*, Action research is a cyclical, problem-solving approach often used in applied research contexts, such as organizational development, education and business management (Reason, 2008, p. 246). It usually focuses on the iterative solution of problems with the parties. It includes cooperation between researcher and the other scientific communities to identify problems, implement solutions and evaluate results in the real-world settings.

This thesis employs applied research, using qualitative methodologies and the applied action study strategy to address real-world difficulties. The research methods comprise interviews and study of internal documents. The data is examined using thematic analysis to discern key themes of cybersecurity knowledge for business students. Interviews with stakeholders will be conducted to get information on these difficulties. The learnt expertise facilitates the creation of this course for business students. Business users may have difficulties in comprehending cybersecurity principles; thus, the educational approach must be tailored to their needs. Upon completion of development, the course undergoes evaluation by designated users. The course is enhanced based on comments, resulting in the final version being released.

2.2 Research Design

Figure 1 below illustrates the research design, detailing the procedures involved in producing and releasing a cybersecurity training for business users in this thesis.

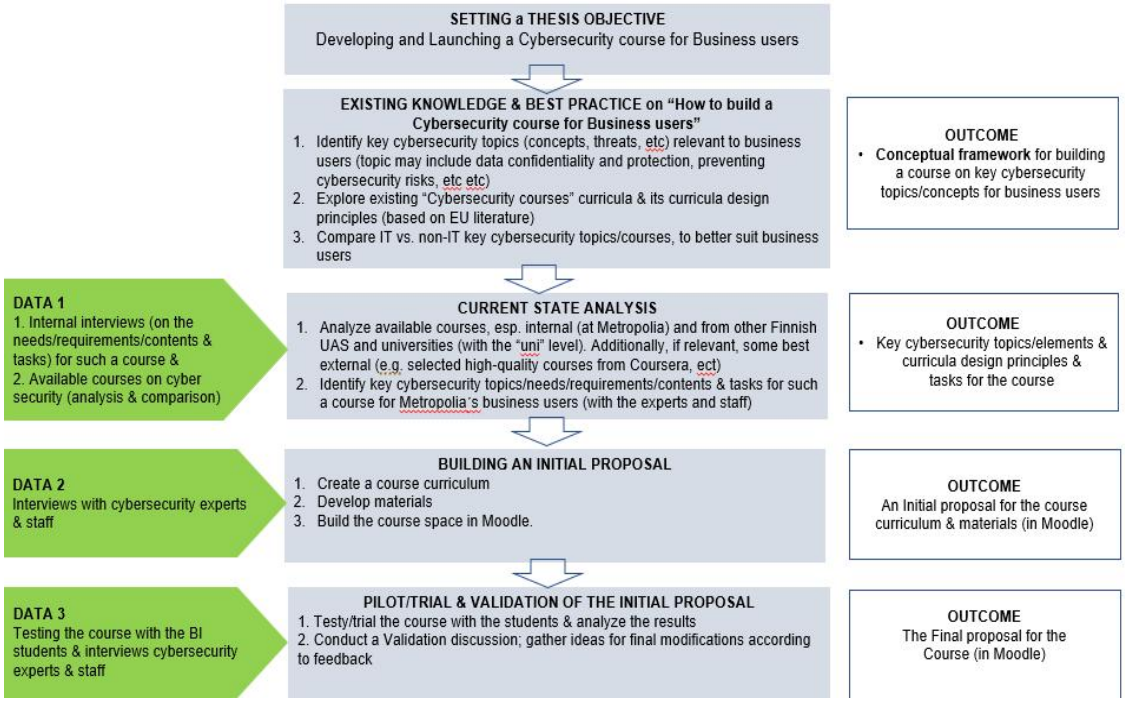


Figure 1. Research design for the thesis.

Figure 1 provides the research design for this thesis project. It starts with the setting of a thesis objective namely the development and the launching of a course. The following step, the available literature and best practice review, identifies the cybersecurity topics and research of the existent curricula, and makes the comparison between the IT and non-IT approaches to cybersecurity. The result of this is a conceptual framework.

Next, the application of the Data 1 (interviews and existing course analysis) in the context of current state analysis provides the cybersecurity themes and the evaluation of offered courses at Metropolia business school. Next, building an initial proposal is based on the Data 2 (interviews of experts) for the development of a course materials, curriculum, and creation of a Moodle space, which lead to the development of an initial proposal. Lastly, the validation uses Data 3 (expert interviews) to perfect the proposal, with the result of the final course.

2.3 Data Collection and Analysis

Education in cybersecurity for business users. Data collection methods included documents analysis, interviews with participating parties and verification based on discussion. Table 1 shows an overview of the data collected in this study.

Table 1. Details of Data collections 1-3 used in this study

	Participants / role	**Data type**	**Topic, description**	**Date, length**	**Documented as**
	Data 1, for the Current state analysis (Section 3)				
1	Stakeholder 1	Online interview	Interview about key cybersecurity concepts, training, risks, course designing, learning methods, critical topics, technical depths for business users.	May, 2025	Recordings & Field notes
2	Stakeholder 2	Online interview	Interview about key cybersecurity concepts, training, risks, course designing, learning methods, critical topics, technical depths for business users.	May, 2025	Recordings & Field notes
3	Stakeholder 3	Online interview	Interview about key cybersecurity concepts, training, risks, course designing, learning methods, critical topics, technical depths for business users.	May, 2025	Recordings & Field notes
4	Stakeholder 4	Online interview	Interview about key cybersecurity concepts, training, risks, course designing, learning methods, critical topics, technical depths for business users.	May, 2025	Field notes
5	Stakeholder 5	Online interview	Interview about key cybersecurity concepts, training, risks, course designing, learning methods, critical topics, technical depths for business users.	May, 2025	Field notes
	Data 2, for Proposal building (Section 5)				
5	Key stakeholders (7) for cybersecurity course	Online interview and discussions	Proposal building	May, 2025	Field notes
	Data 3, from Validation (Section 6)				
8	Key stakeholders (2) for cybersecurity course	Online interview and discussions	Validation, and evaluation of the Proposal	June, 2025	Field notes

As indicated in Table 1, the initial data collection round was conducted for current state analysis (Data 1). This round encompassed interviews with important stakeholders, including cybersecurity specialists, business professionals, and students, to evaluate the existing knowledge of cybersecurity and identify training requirements.

Data 2 included the interviews with key stakeholders to comment on their experiences in relation to cybersecurity courses and contributed to the newly developed course (proposal).

The final phase (Data 3) concentrated on validation. The pilot edition of the cybersecurity course was launched, and validation input was gathered through talks with two experts. Their expertise facilitated the elucidation of the trajectory prior to the ultimate execution. The feedback and discussion sessions conducted in Data 2 and Data 3 offered qualitative insights into the efficacy of the course layout.

The interviews were recorded, and field notes documented for qualitative analysis. All data was analyzed using thematic analysis to uncover reoccurring themes pertaining to education in cybersecurity for business users.

Next, the literature review is presented. The objective of this thesis informed the choice for the topics to explore in available knowledge and best practice. The results of this exploration are addressed in Section 3 below.

3 Available Knowledge and Best Practice on Building Cybersecurity Courses, Especially for Business Users

This section delves into the available knowledge on how to create cybersecurity courses, with an emphasis on those aimed at business users. Information security as a discipline is critical for business users.

3.1.1 Cybersecurity (Concept and Definition)

Cybersecurity is the term used to describe "the operations that are required to defend networks and information systems, as well as the users of such systems and any individuals who are impacted by cyber risks" (ENISA, 2020).

Cybersecurity refers to the practice of protecting information networks, systems, and information from intrusion, misuse, and other forms of cybercrime. "The practice of safeguarding networks, programs, and systems against digital assaults" is how Kabanda (2021) defines cybersecurity. Cybersecurity is "a set of procedures and techniques intended to secure information systems by avoiding, identifying, and reacting to unauthorized access," as stated by David (2016, 15). Proactively creating and carrying out safeguards to protect critical information is what cybersecurity is all about (Awais, 2021). Cybersecurity issues in today's digital world are evolving, with supplementary perspectives highlighting their trans-disciplinary nature and the fact that they are very dynamic (Ambika, 2020).

Due to the exponential growth of digital technologies and their impact on business processes and interactions with stakeholders, cybersecurity has assumed paramount importance in the modern day. Numerous cyber threats pose a growing threat to businesses' financial, operational, and reputational security as they depend more and more on networked systems. According to Verizon (2023), the majority of breaches consist of human mistake, stolen credentials, or social engineering, which accounts for 74% of all breaches. The use of cloud computing, the IoT, and mobile technologies has been accelerated by digital transformation. These innovations increase output, but they also leave a larger digital imprint on a company. Therefore, it might make things more vulnerable to sophisticated cyberattacks. Proactive security measures are required since traditional reactive ones are inadequate when faced with contemporary approaches like AI and ML (Stallings, 2019).

Cybersecurity risks are further intensified by the shift to remote work when employees view sensitive data via personal devices. This weakens security paradigms that have traditionally focused on the perimeter. Because of this, cybersecurity education, especially for non-technical staff, has become more important. Threats like social engineering and phishing can be lessened with its help (Haney & Lutters, 2023).

3.1.2 Core Elements of Cybersecurity as a Field of Knowledge

Various esteemed sources provide comprehensive categorization for fundamental cybersecurity aspects. Stallings (2019) provides a comprehensive analysis of cybersecurity principles in his publication on network security. David (2016) provides a systematic classification that includes supplementary domains such as system safety and handling incidents. The ISC's Common Bank of Knowledge (CBK) (2018) offers a standardized framework addressing cybersecurity across asset security, communication, and security compliance. These three sources constitute the foundation for the classification of cybersecurity aspects in the subsequent section.

First, an essential part of cybersecurity, *network security* seeks to protect data while it travels across networks. Secure network design follows the principle of defence in depth, which is to use several layers of protection to lessen the likelihood of a breach. Secure access service edge (SASE) designs, virtual private networks (VPNs), and segmentation are some of the methods used to create strong defenses. these protections are crucial for preventing attackers from moving laterally after a perimeter compromise (Verizon, 2023).

Second, the security and privacy of information are guaranteed by cryptography. Because of this, only those in possession of the necessary decryption keys will be able to access it. To keep private data safe, cryptographic techniques are necessary. These include hashing, digital signatures, symmetric and asymmetric encryption, and other similar approaches. To protect data transmissions and computer networks, many businesses and organizations use Advance and Robust Algorithm like RSA and AES. In order to build trust in unprotected networks, cryptography is essential for ensuring the authenticity and integrity of data. According to David (2016), it plays a vital role in online banking, e-commerce, and secure communication networks.

Third, the term "cybersecurity risk management" refers to a process that is used to systematically find, assess, and avoid cyber dangers that might compromise data security. To priorities security actions based on probable consequences and danger levels, a solid risk management system is required (Ahmed, 2023). Included in this part are regular checks for security holes, reviews of the system, and the creation of plans to close them. Plans may include accepting, minimizing, transferring, or avoiding risks. Organizations may improve their IT security on a continual basis and better anticipate new dangers with a proactive approach to risk management (Ahmed, 2023).

Fourth, *incident response and recovery* handle the fallout from security disasters like hacks and data breaches, with the goals of repairing damage, getting things back to normal, and stopping such incidents from happening again. Incident response is a crucial part of cybersecurity since no security system is completely safe from cyber-attacks, no matter how careful you are. Policies and processes for identifying, assessing, and recovering from security events are all part of incident response. The steps of being ready, identifying the problem, analyzing it, containing it, eliminating it, and recovering from it are all necessary for an effective incident response plan (Awais, 2021). The goal is to lessen the impact, speed up the recovery process, and learn from previous disasters so they don't happen again. In order to ensure readiness, this component involves forming a specialist crisis response team, implementing ongoing monitoring systems, and conducting routine simulations. In the event of a security breach, incident recovery and business continuity planning work hand in hand to provide for the quick and painless return to normal operations (Awais, 2021).

Fifth, in cybersecurity business policies, procedures, and operations are guided by its *security governance*. Establishing security standards, determining who is responsible for what, and making sure security actions are in line with organizational goals are all part of it. One part of government is making sure everyone follows the rules. As a result, businesses are sure to follow all applicable laws, regulations, and specifications. Effective governance and compliance defend against legal consequences and inspire trust among stakeholders, including users and partners.

3.1.3 Cybersecurity Topics Relevant to Business Users

In the context of cybersecurity for non-technical business users, numerous reputable sources describe specific set of topics that can address operational risks and strategic

management. For example, Haney & Lutters (2023) emphasized the need for inclusive cybersecurity awareness, which should cover topics such as *phishing prevention*, *human errors* leading to cyber risk, and *risk management* practices specifically designed for non-technical environments. Similarly, the European Commission's GDPR emphasizes the importance of *data privacy and protection* (European Commission, 2020). It requires that business users understand legal compliance, regulatory requirements and the practical aspects of protection of personal data. Izzah (2024) provides a standard framework for business leaders which highlights *cybersecurity governance, incident response planning, strategic risk management* and *regulatory compliance.* Table 2 summarizes the key topics pointed out in these sources that are essential for equipping business users to effectively manage cybersecurity risks.

Table 2. Summary of key topics in cybersecurity.

1. Network Security (Stallings, 2019)
    - Firewall Implementation
    - Prevention System Like IDS
    - Secure architectures for Network
2. Cryptography (David, 2016)
    - Confidentiality and integrity of data
3. Risk management (Ahmed, 2023)
    - Cyber Risks Systematic (identification, assessment and mitigation)
4. Incident Response and Recovery (Awais, 2021)
    - Processes and protocols for identifying security incidents
5. Security Governance (EU, 2024)
    - Formation of security standards
    - Incident response planning
    - Strategic risk management
6. Data Confidentiality and Protection (European Commission, 2020).
    - Encryption
    - Multifactor authentication
    - Access policies
7. Cybersecurity Risk Awareness and Human Factors (Haney & Lutters, 2023)
    - Educational programmes
    - Continuous targeted training
8. Regulatory and Compliance Issues (Morgan, 2019)
    - Legal implications of data breaches

- Compliance obligations

9. Incident Management and Business Continuity (Rashid, 2021)

- Resolution of Beches
- Incident response planning

10. Strategic Integration of Cybersecurity into Business Processes (Morgan, 2019)

- Effective cybersecurity strategies

11. Cybersecurity Awareness and Training Programs (Haney & Lutters, 2023)

- cybersecurity training and awareness
- Educating employees

12. Emerging Technologies and Their Implications (Stallings, 2019)

- Understanding of new technologies

Table 2 shows that protecting sensitive corporate and consumer information is an important concern for business users (Verizon, 2023).

Sixth, Stringent access control restrictions are perennially stressed in cybersecurity literature as essential measures for protecting sensitive information. Secure data storage systems and encryption algorithms ensure that data integrity and confidentiality are maintained, even if unauthorized access occurs. Companies with strong data protection policies are less likely to suffer major consequences in the event of a data breach, both financially and in terms of their reputation (Stallings, 2019).

Seventh point is that business users must enhance their cybersecurity risk awareness since human factors and cybersecurity risk awareness are frequently cited as the main causes of security incidents (Haney & Lutters, 2023). Phishing, social engineering, and insider threats are common cyber dangers that non-technical staff members are taught about in educational programs. One common kind of hacking is phishing, in which criminals use deceptive email and social media tactics to steal sensitive data. The effectiveness of such attacks can be significantly reduced via continuous, targeted training (Haney & Lutters, 2023).

Eighth critical topic is the making sense of compliance frameworks and regulatory requirements. Organizational cybersecurity strategies now require these. Scholarly publications frequently use the EU's General Data Protection Regulation (GDPR) as a benchmark for data protection requirements (EU, 2024). Data breaches may have serious legal and regulatory repercussions, such as heavy fines and permanent

damage to a company's reputation, and business users should be aware of these risks. By learning their compliance responsibilities, businesses may avoid legal trouble and encourage honesty and accountability among employees (Morgan, 2019). The provision of an all-encompassing cybersecurity course to business users is, hence, crucial for ensuring regulatory compliance; this course must contain training modules on data privacy regulations and legal frameworks.

Nineth, another important domain for business clients is incident management and business continuity, which are crucial for responding appropriately to cybersecurity problems. While technical teams handle the initial response to security breaches, it is crucial for business executives to understand how these events might impact the overall operations of the company. Business continuity management, crisis communication, and incident response planning are common topics in courses designed for working professionals (Rashid, 2021). Even non-technical staff may help with an effective response that minimizes disruption and allows for quick recovery by learning the basics of event management. Discussions on how to incorporate past disaster lessons into current risk management strategies fall under this umbrella. Organizational resilience will be continually enhanced by this.

Tenth, modern cybersecurity goes beyond technical defences to encompass alignment with complete corporate operations. (Aslaner, (2024)

The eleventh point in order to hone their cybersecurity knowledge and skills. According to Haney and Lutters (2023) and other research, well-planned awareness programs may educate staff about common cyber threats and security practices, which can significantly reduce the incidence of assaults. Programs like this strive to prioritize security in business operations through the use of interactive seminars. It’s is necessary to grasp Emerging Technologies and Their Implications. Therefore, new challenges brought forth by these improvements must also be addressed in cybersecurity education. Even though these technologies can increase operational efficiency, they also pose new hazards, and non-technical business users need to be aware of this. Scalability is a benefit of cloud services, but strict security standards are required to prevent data breaches (Stallings, 2019).

Twelfth is the fast development of the IT industry allows for a more nuanced segmentation to be used, and additional themes to emerge. So, this is only a working

list and new topics will need to be added to it. Studies consistently stress the need for a comprehensive strategy for cybersecurity education among business users. It highlights the importance of data security, being aware of risks, complying with regulations, managing incidents effectively, making strategic decisions, and dealing with the problems caused by new technology.

Finally, along with these well-established factors, *innovations* in cybersecurity are constantly changing the field. When applied to security operations, AI and ML are reshaping the way traditional threat identification and response systems work. The predictive analytics and superior pattern recognition made possible by these technologies are second to none. Because of this, businesses can immediately identify any suspicious activity in their systems. More decentralized IT environments must be protected, and cloud-based security solutions and designs indicate this. These changes highlight how cybersecurity is changing and how important it is to continuously improve administrative and technical measures (Morgan, 2019).

3.2 Curricula Design Principles (in EU) and Existing Cybersecurity Courses

There are several different approaches that the European Union (EU) takes to the issue of cybersecurity. These include legislative measures such as the NIS2 Directive and the Cyber Resilience Act, as well as the EU Cybersecurity Strategy (ENISA, 2020).

According to ENISA (2020), EU cybersecurity regulations aim to: (a) Offer reliable and safe digital surroundings, (b) Avoid every possible cyberattack from networks and information systems, (c) Get ready to resist cyberattacks, (d) Urge member states to cooperate and coordinate inside the union, (e) Improve the degree of cybersecurity found in goods and services offered for sale, (f) Guaranteeing the privacy of personal data. (ENISA, 2020.) The goal is to create a security-aware culture, enabling staff to identify risks, understand compliance obligations, and support organizational cyber resilience (Digital Europe Programme, 2023).

The growing frequency and complexity of cyber threats have made cybersecurity education at Higher Education Institutions (HEIs) quite important recently. HEIs want to provide students with theoretical knowledge and useful abilities to safeguard digital infrastructures in several sectors. Usually taught as a component of computer science,

information technology, or specialized cybersecurity degree is cybersecurity (Clarke & Furnell, 2023). They usually start with basic ideas such threat categories, security principles, legal and ethical considerations, courses then move to more sophisticated topics including penetration testing, security operations centers (SOC), and cyber threat intelligence.

With laboratories and simulations letting students solve real-world problems using technologies like Wireshark, Metasploit, and Kali Linux, practical learning is very vital. To raise employability, several organizations additionally include certifications as CompTIA Security+, Certified Ethical Hacker (CEH), and CISSP preparation into their courses (Karen et al., 2020). To handle the complex nature of cybersecurity, interdisciplinary approaches which combine law, policy, and management points of view with technological content are also urged.

HEIs also stress research and creativity, typically pushing students towards corporate initiatives, hackathons, and cybersecurity contests. Virtual laboratories, cyber ranges, and cloud-based platforms have improved the practical experience in cybersecurity training (Samant et al., 2017). HEIs always changing their courses to match industry requirements and changing threat environments as cybersecurity is becoming a major focus of national security and corporate continuity.

Aiming to standardize and raise the quality of cybersecurity training throughout member states, the European Union (EU) offers thorough direction for cybersecurity education at Higher Education Institutions (HEIs). Working with governments, businesses, and educational institutions to drive cybersecurity education and skill development, the European Union Agency for Cybersecurity (ENISA) is a significant reference point.

3.2.1 Competence based approach to cybersecurity education

To protect its digital infrastructure, the European Union (EU) understands the vital need of creating a trained cybersecurity workforce. The EU has responded by implementing a competence-based cybersecurity strategy stressing uniform skills and role definitions throughout Member States. Designed by the European Union Agency for Cybersecurity (ENISA), the European Cybersecurity Skills Framework (ECSF) is key to this effort.

In the European Union (EU), the European Cybersecurity Framework (ECSF) is a useful instrument that helps to define and express the activities, competencies, skills, and knowledge that are connected with cybersecurity jobs. Its purpose is to establish a shared comprehension among individuals, companies, and educational institutions, with the end goal of bridging the gap between the professional workplace of cybersecurity and the learning settings of the field (ENISA, 2022).

The framework provides an outline of twelve common position profiles for cybersecurity professionals, each of which details unique missions, duties, abilities, and knowledge needs for each profile. The recognition of cybersecurity talents is made easier with the help of these profiles, which also provide assistance for the development of specialized training programs.

The European Cybersecurity Framework (ECSF) is an essential component of the European Union's (EU) larger efforts to improve cybersecurity competences. A Communication on a Cybersecurity Skills Academy was adopted by the European Commission in April 2023 (EU, 2024). The purpose of this communication was to better coordination and integrate the many cyber skills programs that were already in place. The European Competency and Skills Framework (ECSF) serves as the underlying structure for this Academy, making it possible to define and evaluate important skills while also monitoring the development of skill shortfalls. As an additional point of interest, the European Cybersecurity Framework (ECSF) is in accordance with the European Skills, Competences, Qualifications, and Occupations (ESCO) categorization, which guarantees consistency between cybersecurity positions and the wider EU labour market. Other than facilitating job mobility, this alignment also contributes to the establishment of standardized credentials across all Member States (ESCO, 2024).

Despite the steps that have been taken, the European Union is experiencing a serious lack of cybersecurity capabilities. 76% of individuals working in cybersecurity-related professions do not possess formal credentials or accredited training, according to a poll conducted by Eurobarometer. Many businesses are having trouble finding skilled cybersecurity specialists. 74% of businesses have not given their staff with any program or training that is related to cybersecurity (EU, 2024). The European Competency and Skills Framework (ECSF) fills this void by offering a transparent framework for determining the essential skill sets that are necessary from the point of view of the workforce. Policymakers are able to fund efforts that aim to minimize

recognized skill shortages, and it enables providers of learning programs to offer training that is specifically targeted.

ENISA continues to monitor the implementation and development of the European Community Security Framework (ECSF) with the assistance of a specialized *ad hoc* Working Group. Due to the versatility of the framework, it is able to provide assistance for workforce planning that is matched with developing technologies such as artificial intelligence as well as regulatory developments like as the NIS2 Directive.

The European cybersecurity Fund (ECSF) makes a contribution to the achievement of increased security against cyberattacks and to the guarantee of safe information technology systems in society. It provides a standard framework as well as recommendations on how to undertake capacity development within the workforce of the European cybersecurity industry (ECSF, 2022).

A systematic attempt to standardize and improve cybersecurity capabilities across member states is represented by the European Union's (EU) competence-based approach to cybersecurity, which is exemplified by the European Cybersecurity Framework (ECSF). It is possible for the European Commission Support Fund (ECSF) to support focused training, workforce development, and policy-making by establishing precise role profiles and linking with wider EU activities. For the purpose of addressing the skills gap in cybersecurity and strengthening the European Union's resilience against cyber attacks, it is vital to continue investing in such frameworks.

3.2.2 European Cybersecurity Skills Framework (ECSF)

As for *the EU guidelines and principles*, they include the following guiding documents. Based on industrial demands, developing dangers, and digital change, ENISA and the European Commission support the creation of harmonized curriculum. The Cybersecurity Skills Academy project and the Digital Education Action Plan (2021–2027) of the EU help HEIs to enhance their educational initiatives. Introduced by ENISA in 2022, the European Cybersecurity Skills Framework (ECSF) describes roles and competencies needed in the cybersecurity workforce, therefore enabling universities to match courses with professional needs. Table 3 shows principles of curriculum design.

Table 3. Principles for Curriculum Design (ECSF 2022, p. 26-28)

Principle	Description
1. Modular and Flexible Structure	Allowing adaptability to new threats and technologies
2. Skill-based and Competency-driven	Focused on hands-on skills mapped to job roles.
3. Multidisciplinary Approach	Combining IT with law, ethics, and policy
4. Continuous Update	Aligning with evolving cyber threats and best practices
5. Industry and Certification Alignment	Incorporating recognized certifications (e.g., CISSP, CEH, ISO/IEC 27001).

As seen from Table 3, the ability of courses to readily adapt to new threats and developing technology is one of the benefits of having a framework that is both modular and adaptable. A focus that is skill-based and competency-driven places an emphasis on practical, hands-on abilities that are targeted to specific employment functions of the individual. The interdisciplinary approach incorporates knowledge from the fields of information technology, law, ethics, and policy, which helps to promote a more comprehensive understanding of cybersecurity. Keeping the curriculum up to speed with the continuously changing world of cyber risks and industry best practices requires continuous upgrades, which are vital. Elevating the program's legitimacy and relevance by linking it with industry-recognized credentials Certified Information Hardware (CEH).

According to ENISA in 2022, the European Cybersecurity Skills Framework (ECSF) recommended core topics in EU Cybersecurity Curricula, listed in Table 4.

Table 4. cybersecurity core topics (ENISA, 2022).

1. Cybersecurity Fundamentals
2. Network Security
3. Cryptography and PKI
4. Ethical Hacking and Penetration Testing
5. Security Governance and Risk Management
6. Security Operations and Incident Response
7. Digital Forensics
8. Secure Software Development
9. Cyber Law, Ethics, and Privacy (GDPR)

10. Emerging Technologies Security (IoT, Cloud, AI)
11. Cyber Threat Intelligence
12. Critical Infrastructure Protection (ENISA, 2022)

As seen from Table 4, above are 12 key topics for cybersecurity a business users must be aware of such as cybersecurity fundamentals, Network security, Ethical hacking, security governance, digital forensics, cyber law, emerging technologies and critical infrastructure protection.

Tables 5 and 6 offer an overview of selected examples of cybersecurity courses that are available online. They briefly point to the course backgrounds, the material that they cover, the principles that guide the creation of their curriculum, and their locations. as well as the expected user level, either IT or business users (such as foundational, hands-on, or business-focused, depending on whether the user is looking for technical expertise, business understanding, or general awareness). It also includes a short explanation of the topics that are covered in the curriculum, and a direct link to enroll in the course. The table gives but a few examples of the courses that are current available for users to select a course.

Table 5. Examples of cybersecurity courses available online.

	Title of the course	(institution / individual)	Key Content Focus & level (for whom?)	Curricula Design Principles	Content (Elements/Topics)	Reference
1	*Cyber Security [Sec-4]*	MICA	Technical analysis of cybersecurity threats, its defence mechanisms and protective technologies. For Bachelor's Academic level.	Informs technical modules on network security, potential cyber threats and its categorization. Uses modular structure, and shows technical depth and practical focus	• Defining Cyberspace and Overview of Computer and Web-technology • Architecture of cyberspace • Communication and web technology, Internet, World wide web • Advent of internet, Internet infrastructure for data transfer and governance • Internet society, Regulation of cyberspace • Concept of cyber security, Issues and challenges of cyber security	(Ambika, 2020) https://kimsbengaluru.edu.in/assets/pdfs/criterias/criteria-1/criteria-1.1.1/Cyber%20security.pdf
2	*Cyber Security [R18A0521]*	MRCET	Overview of current cybersecurity trends and emerging threats. For Bachelor's Academic level.	Provides insight into up-to-date industry practices and emerging methods to ensure that the course content remains updated.	• Types of cyber-attacks and cyber-crimes • Industry trends, • Emerging threats, • Cyber laws & concepts of cyber forensics • Applied learning • Defensive techniques against these attacks	(MRC, 2021) https://mrcet.com/pdf/Lab%20Manuals/IT/Cyber%20Security.pdf

3	*Introduction to Cybersecurity*	DHET	Fundamental cybersecurity concepts, definitions and historical evolution. For Bachelor's Academic level.	Serves as a base for course introductions, ensuring that students acquire core conceptual knowledge.	• Basics of being safe online. • Different types of malware and attacks, and how organizations are protecting themselves against these attacks. • Different career options in cybersecurity.	(DHET, 2020) https://www.dhet.gov.za/Technical%20and%20Vocational%20Education%20and%20Training%20Co/CISCO%20Lecturer%20Support%20Materials/Lecturer%20Cisco%20Resources/Life%20Orientation/Cisco%20Learning%20Materials/Intro%20to%20Cybersecurity/Introduction%20to%20Cybersecurity.pdf
4	*Introduction to cyber-security*	Jeetendra Pande	Practical examples and case studies illustrating cybersecurity fundamentals. For Bachelor's Academic level.	Provides real-world examples to support applied learning in cybersecurity courses.	• Introduction to cyber crime • Malware and its types • Kind of cyber crime • Authentication • Encryption • Antirvirus, Firewall • Safe browsing	(Pande, 2017) https://uou.ac.in/sites/default/files/slm/Introduction-cyber-security.pdf
	Cyber Security – SITA1602	SIST	Fundamental Concepts and security implementations in organizational settings. For Organizational level users.	Offers examples of best practices and applied learning strategies for cybersecurity training.	• Basic Concepts – Security Architecture, • Attacks, Services, Mechanisms • Model - Cryptography Basics - Symmetric Ciphers – • Transposition, Substitution, Rotor Machines – Block Cipher • Data Encryption Standard – Confidentiality using Symmetric Encryption	(SITA, 2019) https://sist.sathyabama.ac.in/sist_coursematerial/uploads/SITA1602.pdf

6	European Union General Data Protection Regulation (GDPR)	European Commission	Sets stringent data protection and privacy standards for organizations. EU Industry Standard.	Guides the inclusion of legal compliance, data protection and privacy modules in cybersecurity courses.	• Compliance focus, • Data protection, • Legal standardization	(COMMISSION, 2024) https://commission.europa.eu/law/law-topic/data-protection_en
7	ENISA Cybersecurity Skills Framework User Manual	ENISA	Provides design principles for cybersecurity education and professional training, including modularity, competency-based frameworks and flexible learning outcomes. EU Industry Standard.	Serves as a template for designing cybersecurity curricula aligned with EU standards; emphasizes practical competencies and continuous updates.	• Understanding ECSF • ECSF design principles • Applications of ECSF	(ENISA, 2022) https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf

Table 6. Examples of Coursera courses on cybersecurity available online.

	Title of the Course	Level & users	Content (Elements/Topics)	Curricula Design (Principles)	Reference & URL link
1	Google Cybersecurity Professional Certificate	For Any user (No degree or experience required)	• The significance of cybersecurity measures and the effects they have on businesses. • solutions may help you keep your networks, devices, data, and people safe from hackers and other cybercriminals. • Recognise typical dangers, threats, and weaknesses; develop strategies to counteract them	Hands-on, career-focused, Technical depth, Industry-aligned	Developed by Google and Coursera, 2021 https://www.coursera.org/professional-certificates/google-cybersecurity
2	Cybersecurity for Everyone	For any user (No prior experience required)	• Basic cybersecurity concepts, • Evolution of Internet • Telecommunication Architecture • Threats and their motivations • The Hacking process • Direct and indirect consequences	Accessible, Introductory, Broad overview, Interactive	Developed by University of Maryland, Coursera, 2021 https://www.coursera.org/learn/cybersecurity-for-everyone
3	Foundations of Cybersecurity	For IT users (Basic knowledge of IT required)	• A crash course on cybersecurity basics, including database vulnerability management for OS administrators and security specialists • methods and tools for cybersecurity tasks such as penetration testing, incident response, and forensics • Making use of generative AI to enhance your efficiency and output as a cybersecurity analyst	Foundational, Conceptual, Risk Management, Technical	Developed by IBM, Coursera, 2021 https://www.coursera.org/professional-certificates/ibm-cybersecurity-analyst
4	Cybersecurity for Business Specialization	For business users (Business-oriented)	• Cybersecurity for business • Cyber threats and attack vectors • Detecting cyber threats • Proactive computer security	Business-centric, Strategic, Compliance-driven, Applied Knowledge	Developed by University of Colorado Boulder, Coursera, 2020 https://www.coursera.org/specializations/cyber-security-business

5	Introduction to Cybersecurity for Business	For business users	• CIA triad • Daily security • Assess daily risk • Attack surfaces	Business-context, Non-technical, Regulatory, Practical Cases	Developed by University of Colorado, Coursera, 2021 https://www.coursera.org/learn/intro-cyber-security-business

3.3 Comparing IT vs. non-IT Cybersecurity courses

Businesses that rely heavily on information technology place are interested in teaching students specific technical skills, such as how to protect networks, decrypt data, and respond to incidents. Experiential laboratories, technical projects, and practical assessments are the main methods of instruction for these (Kubal, 2025, pp. 24, 48). Risk assessment, regulatory conformity, and strategic decision-making are the main foci of cybersecurity courses designed for business users who do not possess IT expertise. The courses in question include scenario-based learning, interactive conferences, and case studies to convert technological risks into information that is useful for businesses (Giboney, 2021, p.1). Here we will see how the two types of classes compare to one another.

Table 7. Comparison of cybersecurity courses for IT and Non-IT users based on ENISA, SME guide, ECSF, NIS 2 Directive, Digital Europe Programme

	Criteria	**IT Users**	**Non-IT Users**
1	Target Users	IT personnel, network admins, security analysts	Managers, finance, HR, operations, SME owners
2	Program content and structure	• Network and system security • Cryptography • Incident detection • Secure coding • Penetration testing	• Cyber hygiene • GDPR and data privacy • Social engineering threats • Business continuity • Secure remote work
3	Teaching Methods	• Labs • Simulations • Hands-on coding	• Interactive videos • Role-based scenarios • Info graphics • Checklists
4	Assessment Measures	• Lab tests • Certifications (CEH, CompTIA) • Case project reports	• Quizzes • Maturity checklists • Scenario-based knowledge evaluation
5	Learning Outcome	Possession of the ability to protect systems and react to threats	Awareness of threats, legal responsibilities, safe practices
6	Certification	CISSP, CEH, OSCP, CompTIA Security+	Completion certificates, ENISA self-assessment badges
7	EU Framework Reference	ECSF, NIS 2 Directive, ENISA Threat Landscape	ENISA SME Cybersecurity Guide, GDPR, ECSF, Digital Europe Programme

In essence, IT cybersecurity courses offer comprehensive technical training for specialized positions. However, by centering on the regulatory and strategic aspects of

cybersecurity, non-IT courses better serve business clients. When all of these factors are considered, the resulting model for business user education is the most effective. As a result, the resulting curriculum is flexible, interesting, and in line with EU standards, pertinent to addressing the management and operational issues encountered by contemporary corporate organizations.

Table 8. Free courses for business users (ENISA, EU SME).

Course Name	Provider	Course Outline	Teaching Methods
Cybersecurity Toolkit for SMEs	ENISA	• Threat awareness for SMEs. • GDPR & compliance • Password management • Cyber risk scenarios • Remote work policies	• Awareness videos • Role-based guides • Interactive checklists
Cybersecurity4 SMEs Toolbox	European Digital SME Alliance	• Cybersecurity strategy for business • NIS2 Directive basics • Third-party risk • Securing cloud & devices • Staff awareness guides	• eLearning modules • Scenario simulations • Business templates
Introduction to Cybersecurity (EU Version)	Cisco Networking Academy – EU Region	• EU cybersecurity laws overview • Social engineering • Data protection & DLP • Business impact of cyber incidents • Basic cyber hygiene practices	• Self-paced modules • Case studies • Visual learning activities

3.4 Conceptual Framework of This Thesis

This section discussed cybersecurity education by outlining its definitions and core elements. It used academic and industry sources to provide understanding of cybersecurity, setting the base for developing a course for non-technical professionals, more specifically business users.

The chosen literature and best practice are combined into the theoretical framework, to guide the approach in the subsequent stages of this thesis. Table 9 shows the conceptual framework of business user required cybersecurity. This conceptual framework identifies the major points of cybersecurity business users should know.

Table 9. Conceptual framework on the areas important for building a cybersecurity course for business users.

Key Cybersecurity Topics for Business users	1. Network Security (Stallings, 2019) • Implementation of firewalls • Intrusion detection and prevention systems • Secure network architectures 2. Cryptography (Kim, 2016) • Confidentiality and integrity of data 3. Risk management (Disterer, 2013) • Systematic identification, assessment and mitigation of cyber risks 4. Incident Response and Recovery (Rashid, 2021) • Processes and protocols for identifying security incidents 5. Security Governance (EU, 2024) • Formation of security standards • Incident response planning • Strategic risk management 6. Data Confidentiality and Protection (European Commission, 2020). • Encryption • Multifactor authentication • Access policies 7. Cybersecurity Risk Awareness and Human Factors (Bada, 2015) • Educational programmes • Continuous targeted training 8. Regulatory and Compliance Issues (Morgan, 2019) • Legal implications of data breaches • Compliance obligations 9. Incident Management and Business Continuity (Rashid, 2021) • Immediate control and resolution of breaches • Incident response planning 10. Strategic Integration of Cybersecurity into Business Processes (Morgan, 2019) • Effective cyber security strategies 11. Cybersecurity Awareness and Training Programs (Maria Bada, 2015) • Cyber security training and awareness • Educating employees

Curricula design principles (SME cybersecurity guide)	• Modular and Flexible Structure (allowing adaptability to new threats and technologies) • Skill-based and Competency-driven (focused on hands-on skills mapped to job roles) • Multidisciplinary Approach (combining IT with law, ethics, and policy etc) • Continuous Update (aligning with evolving cyber threats and best practices) • Industry and Certification Alignment incorporating recognized certifications (e.g., CISSP, CEH, ISO/IEC 27001).
IT vs. non-IT topics in cybersecurity courses (ENISA 2022)	• IT-oriented courses focus on technical skills for cybersecurity professionals, while non-IT courses build awareness and safe practices for business users. • Non-IT cybersecurity courses are specifically designed for business users such as managers, HR, and SME owners, etc. (ENISA 2022). • Non-technical users can earn awareness-level certifications, such as ENISA's self-assessment badges, promoting ongoing education and accountability.

The conceptual framework categorizes pertinent information into three primary aspects and their sub-elements regarding the instruction of cybersecurity to business users.

First, cybersecurity topics can be categorized into IT-focused and non-IT-focused, depending on the target audience and learning objectives. IT vs. non-IT topics in cybersecurity courses differ in content in depth. IT-oriented courses are highly technical and designed for professionals such as network administrators, penetration testers, and security analysts. These courses typically cover topics like network security, cryptography, secure coding, incident detection, and penetration testing. Learners engage in labs, simulations, and practical coding exercises, often aiming for certifications like CISSP, CEH, or CompTIA Security+ (ENISA, 2023; ECSF Framework, 2022).

Second, curricula design principles focus on modular and flexible structure, Skill-based and competency-driven, Multidisciplinary approach, Continuous update and industry and Certification alignment incorporating recognized certifications.

Third, non-IT cybersecurity courses are tailored for business users including managers, HR personnel, finance teams, and SME owners. These courses focus on non-technical, high-impact areas such as cyber hygiene, GDPR and data privacy, social engineering

threats, business continuity, and secure remote work (ENISA SME Cybersecurity Guide, 2022). Teaching methods include interactive videos, role-based scenarios, info graphics, and checklists.

Next, the identified key cybersecurity topics for business users will provide the content backbone to investigate the current state of instructing these topics to business users in the case organization (in Section 4), and then build a proposal for the cybersecurity course for Business Users (in Section 5).

4 Current State Analysis of cybersecurity Learning at the Case Organization

This section discusses the results from the current state analysis of cybersecurity courses in Finnish universities and Metropolia UAS.

4.1 Overview of the Current State Analysis

The goal of this current state analysis (CSA) is to evaluate the available cybersecurity courses at the case organization, and identify pertinent cybersecurity subjects in them, and review the existing cybersecurity curriculum to identify knowledge gaps. This analysis was conducted in three phases.

Phase 1 was to gather and analyze internal data to determine the cybersecurity needs and existing courses for Metropolia's business users. It included conducting interviews within the organization with both experts and staff members. It helped to identify the needs for topics related to for user verification, issues regarding data confidentiality, identification of cybersecurity threats, preventative methods, and compliance requirements. Current cybersecurity courses were evaluated for the purpose of internal benchmarking.

During Phase 2, a comparison of a few selected cybersecurity courses was conducted, with a special focus on Metropolia and other HEIs in Finland. A focus was placed on the characteristics related to curriculum design, learning techniques, and the degree to which these approaches are able to satisfy the cybersecurity requirements that are particular to businesses.

During the third phase, the analysis compared the requirements for cybersecurity education that are posed for non-IT users and IT users. The purpose of this was to identify particular topics and characteristics of the courses meant for the users with technical background, and more clearly identify the differences between the courses for to the business and IT users. For the purpose of efficiently tailoring the future courses, distinctions between the requirements of IT professionals and those of non-IT staff were made obvious.

4.2 Description of Cybersecurity Courses at Metropolia UAS

The cybersecurity courses offered by Metropolia University of Applied Sciences target both IT and non-IT users, such as including administrative staff, students, and general employees. Currently (spring 2025), there are 15 courses in some way related to digital security and available in Moodle platform of Metropolia.

To start in autumn 2025:	
5 Digital Security Starter (available  **Opettaja:** Natasa Anttila **Opettaja:** Tuija Buure **Opettaja:** Roope Rannikko **Opettaja:** Suvi Väänänen	10 Cyber Security M **Opettaja:** Erik Pätynen **Kategoria:** ICT ja tuotantotalous
	11 Cybersecurity Operations **Opettaja:** Erik Pätynen **Kategoria:** ICT ja tuotantotalous
	12 Endpoint Security (nonstop, 2 ects) **Opettaja:** Kari Järvi **Opettaja:** Virve Prami **Opettaja:** Janne Salonen **Opettaja:** Marko Uusitalo **Opettaja:** Tapio Wikström **Kategoria:** ICT ja tuotantotalous
	13 Information Security with HelmetJS This course is an IT Security course. In order to complete this course it is highly advisable to first complete JavaScript and Node.js courses. This course be completed in straight line with FreeCodeCamp course called Information Security with Helmet. In order to complete this course, you will do the labs on freecodecamp wel site and then a final exam here in Moodle **Opettaja:** Sami Paananen **Opettaja:** Virve Prami **Opettaja:** Janne Salonen **Kategoria:** ICT ja tuotantotalous
	14 Software Supply Chain Security  **Opettaja:** Jukka Paasonen **Kategoria:** ICT ja tuotantotalous

Courses 1-4 designed for general use, emphasize safe practices, and practical security habits. Topics include password management, phishing awareness, data protection, device security, and incident response. Curricula are structured around interactive, scenario-based, and modular formats with self-paced and visual learning elements. These courses aim to bridge the knowledge gap for non-technical users and reinforce institutional cyber hygiene. Regular participation is encouraged to ensure up-to-date understanding of cybersecurity threats and defenses. They are better suitable for a non- IT audience including business professionals and SMEs owners.

Courses 6-14 concern advanced material in cybersecurity defence, protecting software, and specialized information security concepts. They are better suitable for professional IT audience including operations experts.

The subsequent analysis will focus on Courses 1-4 shown in Table 10 below. These basic to intermediate cybersecurity courses centre on fundamental information like cyber threat detection, data security, and online safety measures, these courses. Emphasizing the growing relevance of cybersecurity literacy across many corporate jobs, they are especially helpful for non-IT stakeholders including managers, financial workers, and administrative professionals. They are particularly suitable for non-technical users that increasingly oversee digital tools and sensitive data.

Courses 1-4 in the Metropolia offerings reflect a strong foundation in user-centric cybersecurity education that aligns well with business needs. The “Metropolia Personnel Basic Security Course” and the “Student’s Basic Information Security Training” highlight the critical need for foundational digital hygiene practices among individuals who may not have technical backgrounds but handle sensitive data and systems regularly.

Courses 1-4 aim to equip the students with competencies for integrating cybersecurity into business environments where digital operations are widespread but technical expertise may be limited. These courses prioritize practicality, and accessibility through self-paced formats, simple language, visual aids, and scenario-based content. Such an approach ensures engagement and focus on “security-first” mindset. The introduction of gamified learning, interactive quizzes, and mobile-focused elements, as suggested in course descriptions, could enhance participation and learning outcomes even further.

Table 10. Cybersecurity Courses at Metropolia UAS.

	Title of the course	Level & users	Content (topics)	Curricula Design (principles)	Comments
1	"Metropolia Personnel Basic Security Course" Metropolia UAS	Beginner Level (Non-IT personnel, administrative staff, general employees needing basic security awareness)	1. Fundamentals of cybersecurity awareness 2. Password management and safe practices 3. Identifying phishing emails and scams 4. Physical security measures 5. Incident reporting procedures 6. Protecting personal and organizational data 7. Safe use of IT equipment and networks	Awareness-Focused, Practical Orientation, Simple Language and Visuals, Interactive Learning, Modular Approach Brief evaluations at the conclusion of each module	This is a practical course that is aimed at regular users. It describes fundamental security practices that are performed on a daily basis that, if broadly implemented, would improve the security of an organization. Each employee is required to participate in this training on a yearly basis.
2	"Student's Basic Information Security Training" Metropolia UAS	Beginner Level (Students of all academic backgrounds, primarily non-IT students needing basic cybersecurity awareness.)	1. Introduction to information security principles 2. Managing passwords securely 3. Safe online behavior (e.g., browsing, email use) 4. Understanding and avoiding phishing attacks 5. Handling personal and university data responsibly 6. Device security and software updates 7. Responding to security incidents	Awareness-Based, Use of Visual Aids, Scenario-Based Examples, Self-Paced Learning, Actionable Focus	An essential course for students who are frequently the victim of phishing and social engineering attempts. This course covers the basic topics that a student who is not technically orientated has to be aware of. • There is the potential for improvement by providing brief interactive quizzes or gamified tasks at the conclusion of each segment. • Given the extent to which students rely on mobile devices, it would be even more effective if it placed an emphasis on ensuring their safety.
3	"Introduction to Cybersecurity" Metropolia University of Applied	Beginner to Intermediate Level	1. Basic concepts of cybersecurity 2. Common threats and vulnerabilities 3. Introduction to cryptography basics 4. Network security fundamentals 5. Cyber ethics and responsible online behavior	Self-Paced Learning, Video-Based Instruction, Practical Focus, Inclusive Design, Continuous Access	The course offers a comprehensive overview appropriate for a wide range of students. It is especially helpful for increasing general understanding rather than delving deeply into the technical implementations of the solutions. The

	Sciences)		6. Understanding security policies and frameworks 7. Best practices for protecting devices and personal data		course has videos. • It would be beneficial to include brief quizzes or interactive components to guarantee user involvement at all times. • It would be beneficial to add checklists or summaries to videos that could be downloaded electronically.
4	"Basics of Information Security" Metropolia University of Applied Sciences	Beginner Level	1. Core principles of information security (Confidentiality, Integrity, Availability) 2. Password management and multi-factor authentication (MFA) 3. Data protection principles and regulations (e.g., GDPR basics) 4. Email security and phishing awareness 5. Safe browsing practices 6. Protecting devices (laptops, mobile phones) 7. How to act during a security incident	Fundamental Focus, Compliance-Oriented, Scenario-Based Learning, Self-Learning Structure	This course is aimed at users of all levels, with the stress on cyber dangers. This course explains why security procedures are important to non-IT users. • An additional improvement could be to incorporate more frequent assessments to strengthen retention. • This course is suitable as a "must-do" course for both students and workers of the institution as a required introduction activity.

Course 1 is intended especially for non-IT staff members including general and administrative staff members requiring basic cybersecurity knowledge. Reflecting main behavioral goals discussed in stakeholder interviews, the material is quite relevant to daily company operations including phishing identification, password management, and secure device usage (Stakeholder 1, Stakeholder 4). The curriculum design favors modularity, simplicity, and practical application, therefore enabling even users with little digital confidence. As the comments point out, annual course repetition helps to build positive habits and represents best practices in awareness continuity. Though it may be improved with customizable learning pathways for various departments or positions, the major strength of the course is its connection with organizational risk reducing.

Course 2 covers subjects related to phishing and social engineering. Its addition of incident response and device security captures stakeholder focus on ethics, accountability, and digital behaviour (Stakeholder 5). For non-technical students, the self-paced, visual, and scenario-based design of the course offers several learning modes. As the comments points out, though, including interactive quizzes or mobile-oriented materials might better fit students' device usage patterns and help to reinforce recall. Though the lack of gamification or progress tracking may lower long-term engagement, the simplicity of material fits very well with CF aspects like usability and relevance (Haney & Lutters, 2023).

Course 3 introduces cryptography, network security, and policy frameworks, therefore extending the field beyond fundamental understanding between beginning and intermediate levels. Students and staff looking for a conceptual link between user-level activities and technical knowledge would find it most appropriate. While using video-based, self-paced courses fits inclusive design, if students passively ingest the materials it might lower interaction. As advised, adding interactive checkpoints, downloadable summaries, or reflective assignments will greatly increase involvement. Although this course may surpass the comfort level of certain non-IT users without extra scaffolding, it lies at the junction of awareness and technical introduction essential for dedicated students.

Course 4 is for general institutional usage as it effectively combines regulatory subjects (e.g., GDPR) with useful behaviours like secure surfing and MFA. Emphasizing compliance and basic knowledge of cybersecurity concepts like confidentiality, integrity, and availability (CIA triad), and using self-guided modules and scenario-based learning,

the curriculum fits stakeholders' need for realistic, low-barrier training approaches (Stakeholder 1, Stakeholder 2). Although this is a basic orientation or introduction course for all users, it might benefit from more regular tests or role-based variants to support learning. Its thorough yet approachable quality makes it perfect for institutional onboarding, where awareness and compliance meet.

4.3 A Glance at Cybersecurity courses at Finnish Universities (selected examples)

The conceptual framework outlined in Table 10 identifies the essential cybersecurity competencies that business users should possess, categorized across areas such as network security, risk management, governance, data protection, compliance, and user education. These domains reflect the evolving threat landscape where both technical defenses and human awareness are critical. The selected courses AI & Cybersecurity (Turku University), cybersecurity Base 2025 (University of Helsinki), and Introduction to Information Security Management (Aalto University) were chosen to illustrate different user profiles, from beginners to experts.

4.3.1 Content Relevance

Each course addresses core topics listed in the conceptual framework. For example, Aalto's course introduces risk management, incident response, and governance (aligning with Ahmed, 2023 and EU, 2024). The Helsinki course integrates advanced topics like cryptography and network security (Stallings, 2019; Awais, 2021), while the Turku course uniquely focuses on AI-driven threat detection, aligning with strategic cybersecurity integration (Morgan, 2019) and emerging future competencies.

4.3.2 User-Level Appropriateness

The three courses are strategically structured for different levels: Aalto's course supports non-technical business users by covering foundational principles without complex jargon. Helsinki's course is for technically inclined learners, fostering advanced skills through hands-on projects and CTF challenges. Turku's offering targets specialized professionals or students dealing with AI in cybersecurity a growing domain of strategic importance.

4.3.3 Curricula Design Principles

Design across all three emphasizes accessibility, modular structure, and active learning. Aalto employs real-life examples to enhance comprehension for business users. Helsinki uses escalating challenge levels to build confidence and practical fluency. Turku integrates problem-based learning and research-oriented discussions, ideal for cultivating interdisciplinary expertise.

Together, these courses offer a comprehensive training pathway mapped precisely to business cybersecurity needs as detailed in Table 11, ensuring both technical proficiency and organizational cyber hygiene.

Table 11. Cybersecurity courses at Finnish universities (selected examples).

	Title of the course	Level & users	Content (topics)	Curricula Design (principles)	Comments
1	AI & CYBERSECURITY (Source: Turku University Course)	Advanced Level (Targeted at Master's students or professionals in cybersecurity, AI, or related technical fields.)	• AI in cyber defense and offense • Anomaly detection and fraud prevention Systems that use machine learning to identify potential dangers. • Future developments in the combination of artificial intelligence and cybersecurity • Moral issues surrounding cybersecurity that relies on AI	• Research-Driven Approach • Interdisciplinary Learning • Problem-Based Learning • Skill Development	• Given the increasing significance of artificial intelligence in the field of cybersecurity, the course is extremely pertinent. • Theoretical considerations (such as research and ethics) and practical applications (such as threat identification and anomaly analysis) are efficiently balanced by it. • A further enhancement of skill development would be achieved with the addition of additional lab sessions or hands-on AI projects relevant to cybersecurity.
2	cybersecurity Base 2025 (Source: University of Helsinki)	Intermediate to Advanced Level (Designed for IT professionals, computer science students, and individuals with programming experience)	• Introduction to cybersecurity • Securing Software • Project I (Identifying and Fixing Security Flaws) • Advanced Topics (Network Security, Cryptography, Log Mining) • Project II (System Hardening and Penetration Testing) • Capture The Flag (CTF)	• Structured modularly, integrating theoretical background with hands-on practice. • Place a focus on practical exercises to strengthen comprehension • Using practical situations to improve problem-solving abilities. • Increasing difficulty to suit players of diverse skill levels.	• A completely comprehensive course that covers both fundamental and advanced issues related to cybersecurity. • An invaluable opportunity to get hands-on experience is provided by the incorporation of actual projects and a CTF competition. • Learners are able to advance at their own speed because to the adaptable nature of the online format. • Ideally suited for those who are interested in expanding their knowledge about cybersecurity.

			Competition		
3	Introduction to Information Security Management (Source: Aalto University)	Beginner Level (Suitable for non-IT professionals, business managers, and anyone interested in understanding information security principles)	• Key Concepts and Objectives of Information Security • Information Security Policies and Culture • Risk Management and Threat Assessment • Incident Response and Business Continuity • Case Studies and Practical Exercises	• Learn at your own speed with interactive video lessons, quizzes, and real-world examples. • Learning may be better contextualized by focusing on real-life circumstances and applications. • Created with the goal of being easily understood by those without a technical background. • Focus on learning all aspects of information security management.	• This course is an excellent option for anyone who are interested in gaining a foundational understanding of information security without getting into the technical complexity involved. • Through the use of real-world examples and a practical approach, the information is made more approachable and interesting. • Structures that are flexible are able to support a variety of learning schedules. • Lays a strong groundwork for ongoing investigation into many aspects of cybersecurity

4.4 Analysis of Current Cybersecurity Education at the Case Organization

The interview insights emphasized the importance of foundational and role-relevant cybersecurity knowledge tailored to business users, especially non-IT personnel. Participants highlighted three main elements consistent with the Conceptual Framework (CF): topic relevance, user-level appropriateness, and curricula design.

4.4.1 Cybersecurity Topics for Business Users in Current Education at the Case Organization

The stakeholders emphasized the differences across the following three directions.

A. Content Relevance vs. Technical Depth

Business users must get training anchored on realistic risk scenarios, not theoretical detail, said stakeholders. According to Stakeholder 1, "business users are often overwhelmed by technical detail," and she underlined the need of material including phishing awareness, password hygiene, and incident reporting. Stakeholder 4 underlined this by stating, "beyond the basics, we risk losing learners."

By contrast, courses with an IT concentration such as Cybersecurity Base 2025 from University of Helsinki give complicated topics like anomaly detection and cryptography top priority. The discrepancy in course complexity helps to justify the conclusion that, particularly for administrative and HR staff, business-oriented material has to give simplicity and relevance top priority.

B. User-Level Appropriateness

Every one of the five interviewers set the demands of technical students apart from non-technical users. Stakeholder 3 contended that rather than a one-time technological need, cybersecurity ought to be a daily thought process. Adding, "we need to remove the 'black box' perception by making cybersecurity accessible," Stakeholder 2 and Stakeholder 5 similarly cautioned against creating one-size-fits-all courses: "Most staff don't need deep cryptographic knowledge, but must know how to avoid social engineering." These revelations complement Haney & Lutters (2023) focus on non-technical awareness training as a strategic organizational strategy.

C. Curriculum Design Must Reflect Context and Role

Business users' cybersecurity education has to be developed to interact, inform, and empower non-specialists. Modular and scenario-based learning was much welcomed by stakeholders. Stakeholder 4 advised visual storytelling and practical examples: "Short simulations or gamified micro-modules can make a big difference in retention." Stakeholder 2 pointed out that the security starting course for Metropolia uses this approach, guaranteeing great involvement among administrative and academic personnel. These choices perfectly line up with Haney & Lutters (2023), who advises awareness training using scenario-based, behavior-based learning models.

Finnish university courses mirror this variation. Although Aalto's Introduction to Information Security Management covers risk and governance issues relevant to everyone, more technical courses like Turku's AI and Cybersecurity target advanced students. Tables 10 and 11 clearly illustrate that Metropolia's fundamental courses focus on behaviour modification and legal awareness, therefore emphasizing the need of curriculum design reflecting the learner's function, background, and cognitive load.

Table 12. Significant topics for the development of cybersecurity course for business users

• Fundamentals of Cybersecurity Awareness (Stakeholder 2) • Password Management and Multi-Factor Authentication (MFA) (Stakeholder 4) • Identification and Prevention of Phishing Attacks (Stakeholder 3, Stakeholder 4) • Safe Online Behavior (browsing, email usage, social media caution) (Stakeholder 1, Stakeholder 2) • Incident Reporting Procedures (Stakeholder 3) • Protection of Personal and Organizational Data (Stakeholder 1) • Physical Security Measures (securing devices, office spaces) (Stakeholder 4) • Basic Concepts of Data Protection and GDPR Compliance (Stakeholder 1)	• Device Security (laptops, smartphones, workstations) (Stakeholder 4) • Understanding Cyber Threats and Common Vulnerabilities (Stakeholder 1, Stakeholder 2) • Cyber Ethics and Responsible Digital Behavior (Stakeholder 5) • Introduction to Security Policies, Standards, and Frameworks (Stakeholder 2) • Business Continuity and Risk Management Awareness (Stakeholder 3, Stakeholder 5) • Safe Use of IT Equipment and Secure Network Practices (Stakeholder 4) • Handling and Securing Confidential Business Information (Stakeholder 1, Stakeholder 5) • Awareness of Emerging Threat Trends (basic level) (Stakeholder 2)

4.4.2 Curricula Design Principles

The findings from interviews (Stakeholders 1–5, May 2025) confirm ENISA's (2022) distinction between IT and non-IT cybersecurity training. Business-focused cybersecurity education must be tailored to the non-technical user in terms of target audience, content, and recognition, as outlined below.

First, as for *the Target Audience*, the interviewed stakeholders emphasized the importance of customizing training for non-IT staff—especially administrative workers, HR, and SME owners. Stakeholder 2 stated: "Courses must avoid technical jargon if we want managers or finance staff to benefit from them." This supports ENISA's view that non-IT cybersecurity courses must target users beyond IT departments (Stakeholder 2).

Second, as for *the Content,* the interviews revealed a shared concern about information overload. Stakeholder 4 explained: "Phishing, password safety, and incident reporting are the three must-haves. Beyond that, we risk losing learners" (Stakeholder 4). Stakeholder 1 and Stakeholder 3 also stressed the importance of real-life applicability and organizational relevance in selecting topics (Stakeholder 1, Stakeholder 3). This matches ENISA's principle that non-IT courses prioritize awareness and safe practices, unlike IT-oriented content which emphasizes coding or system hardening.

Third, in relation to *Recognition*, the joint option was that non-IT users could benefit from simpler, motivational recognition. Stakeholder 3 suggested using "badges or digital certificates after completing short modules, which help make learning tangible" (Stakeholder 3). Stakeholder 5 also supported this with emphasis on self-paced micro-credentials for user motivation (Stakeholder 5). This aligns with ENISA's support of awareness-level certifications like self-assessment badges, which reinforce accountability without demanding technical mastery.

By analyzing Tables 11 and 12, the curricula design principles are listed below (Turku University, University of Helsinki, Aalto University, Metropolia UAS).

Table 13. Curricula design principles of cybersecurity course for business users

• Focus on simple, practical, and action-	• Ensure compliance focus (basic GDPR,

oriented content. (Stakeholder 3) • Include scenario-based learning and real-life examples. (Stakeholder 3) • Emphasize self-paced, interactive formats (videos, quizzes, cases). (Stakeholder 1)	organizational security policies). (Stakeholder 1) • Incorporate hands-on practices for password setting, phishing simulations, and device protection tips. (Stakeholder 2)

Finnish universities reflect the ENISA (2022) framework by clearly distinguishing between IT and non-IT user needs. Metropolia's basic courses target non-technical staff and students, focusing on awareness, phishing, and password safety—topics emphasized by interviewees. Aalto's course for business managers further aligns with non-IT audiences by offering practical, scenario-based training. In contrast, the University of Helsinki's and Turku's courses cater to IT professionals, integrating advanced content like penetration testing and AI-based threat detection. This tiered approach ensures both accessibility for general users and depth for technical learners, aligning well with ENISA's model.

4.4.3 Difference with IT courses in Cybersecurity

Interviews with key stakeholders (May 2025) revealed significant differences between cybersecurity courses designed for IT and non-IT users, aligning with ENISA's framework across three elements: (1) target audience, (2) content, and (3) recognition. Table 14 summarizes key differences between IT and Non-IT cybersecurity courses based on interviews and course analysis.

Table 14. Key Differences Between IT and Non-IT Cybersecurity Courses (based on interviews and course analysis, May 2025)

Element	IT-Focused Courses	Non-IT (Business User) Courses
Target Audience	IT professionals, system administrators, CS students, engineers (e.g., Graduate, Post graduate level)	Managers, HR personnel, admin staff, SME owners, general non-technical users
Learning Background	Prior technical knowledge assumed	Little to no technical knowledge assumed
Content Focus	Cryptography, secure architectures, penetration testing, anomaly detection, system hardening	Phishing awareness, password hygiene, device safety, incident reporting
Learning Objectives	Technical proficiency, system-level understanding, problem-solving in complex environments	Awareness, secure behavior, risk mitigation, fostering security culture

Methodology	Hands-on labs, coding tasks, simulations, problem-solving projects	Visuals, real-life scenarios, modular micro-learning, self-paced formats
Certification	Multi-tiered, formal certifications (e.g., CISSP, CEH, Uni degrees)	Awareness-level badges, digital certificates (low-barrier recognition)
Institutional Examples	University of Helsinki, Aalto, Turku University	Metropolia UAS, internal corporate training programs
Design Challenge	Depth of content, keeping up with threat evolution	Avoiding overload, ensuring engagement and practical understanding
Quote Examples	“Courses require considerable technical knowledge…” (Stakeholder 1)	“Phishing, password safety, and incident reporting are the must-haves…” (Stakeholder 4), “Use-case-driven training…” (Stakeholder 3)

IT courses target technically skilled professionals such as system administrators and developers, whereas non-IT courses are developed for managers, HR staff, and SME owners who often lack technical expertise. Stakeholder 1 emphasized that non-technical users need context-relevant training rather than in-depth technical explanations.

> “The courses (for IT users) are designed for B.Sc and M.Sc level engineering students and require considerable technical knowledge. Understandably the competences in the field of engineering and business administration are considerably different and using engineering courses for the starting point could lead into less optimal outcomes.” (Stakeholder 1)

Regarding content, Stakeholder 4 noted that business users should focus on practical topics like phishing awareness, password hygiene, and incident reporting, while IT-focused courses delve into complex subjects like cryptography, secure architectures, and penetration testing. (Stakeholder 4)

Stakeholder 3 added that use-case-driven and scenario-based approaches make cybersecurity more relatable for non-IT staff. Recognition mechanisms also differ significantly (Stakeholder 3).

Stakeholder 5 suggested awareness-level certifications or badges to motivate and acknowledge learning progress among business users, contrasting with the multi-tiered certifications available for IT professionals. (Stakeholder 5)

These findings reinforce the importance of clearly differentiating course design to match user profiles and learning objectives, ensuring that cybersecurity education

remains both relevant and effective for the intended audience, whether they are technical specialists or general staff in business environments.

A comparison of Tables 11 and 12 demonstrates that there are significant distinctions between the cybersecurity courses that are specifically developed for IT users and those that are intended for those who are not IT users. Table 11 has a number of courses that are highly technical and specialized. Some examples of these courses are cybersecurity base 2025 (University of Helsinki), artificial intelligence and cybersecurity (Turku University), and introduction to information security management (Aalto University). Machine learning for threat detection, network security, cryptography, anomaly detection, penetration testing, and system hardening are some of the advanced subjects that are covered in these seminars. The goal of these courses is to acquire research-driven, problem-solving, and hands-on skills such as those necessary to handle complex cybersecurity situations. The courses are aimed at persons with prior technical experience, as well as IT professionals and students of computer science.

The courses that are included in Table 12 from Metropolia UAS are primarily intended for users who are not working with information technology. These users include administrative workers, general employees, and students who come from a variety of academic backgrounds. The classes have an emphasis on essential cybersecurity awareness subjects such as the administration of secure passwords, the identification of phishing attacks, the safe use of devices. Using self-paced learning, visual aids, real-world scenarios, and fundamental actionable principles, the curricula have been condensed to concentrate on everyday cybersecurity activities. This simplicity promotes easy comprehension. In contrast to the in-depth technical training that is provided to IT users, these courses place a greater emphasis on developing a robust security culture among non-technical staff members. They do this by focusing on the reasons why cybersecurity measures are extremely essential, rather than on the technical implementation of these measures.

Business user courses prioritize simplicity, awareness, and everyday security practices to secure organizations at the user level. In conclusion, information technology courses emphasize technical depth, practical laboratories, and hands-on projects to equip students to become experts in cybersecurity. In the field of cybersecurity, both types of

courses are necessary, but they serve to quite distinct learning demands and degrees of proficiency.

4.4.4 Other Considerations

The core content and audience distinctions, the interviews (May 2025) highlighted several critical factors that influence the design and delivery of cybersecurity training for business users. One prominent theme was the importance of competence-based learning. They emphasized that

> *"…Courses should not only deliver information but ensure that learners demonstrate understanding through practical, task-oriented outcomes."* (Stakeholder 5)

This aligns with the idea of integrating competence-based projects, where users complete real-world tasks such as identifying phishing emails or drafting basic incident response plans.

There was also mentioned the need for ongoing support and adaptability:

> *"…cybersecurity training cannot be one-off; it must be refreshed regularly as threats evolve."* (Stakeholder 2)

Another issue raised was organizational culture and leadership involvement:

> *"…Senior managers need to set an example; otherwise, training becomes a checkbox exercise."* (Stakeholder 3)

Furthermore, Stakeholder 5 suggested embedding cybersecurity topics into daily workflows, using microlearning or brief interactive reminders (Stakeholder 5).

The interviewees also supported inter-institutional collaboration, where universities and companies co-develop content based on shared needs. These additional considerations show that effective cybersecurity training goes beyond static content—it requires practical assessment, leadership endorsement, and adaptive, embedded learning formats to build lasting competence and engagement among business users. (Stakeholder 1, Stakeholder 5)

It is essential to take into consideration not only the content of the cybersecurity courses that are designed for business users, but also the methods of delivery and the tactics for user engagement. It is vital to avoid using jargon when communicating with business users because they typically come from non-technical backgrounds. This means that the language used should be straightforward and basic (Stakeholder 1, Stakeholder 2).

It was stressed in the interviews and the analyzed courses that, for non-IT users, phishing emails, secure password generation, data handling, and the safe use of digital technologies should be the primary topics of discussion during the course. The course should place a significant emphasis on real-world scenarios that business users confront on a regular basis (Stakeholder 3, Stakeholder 4).

Importantly, engaging and retaining information may be considerably improved with the use of interactive features such as brief quizzes, gamified activities, and decision-making based on hypothetical settings. A further point to consider is that the training should be tailored to individual roles, addressing the distinct cybersecurity threats that are faced by various departments, such as sales, human resources, or finance. Maintaining awareness over time is something that may be accomplished through the use of frequent brief refresher modules rather than a single lengthy session.

It is also necessary to incorporate compliance criteria, such as the General Data Protection Regulation (GDPR) or business rules, to guarantee that users comprehend the significance of cybersecurity from both a legal and organizational standpoint (Stakeholder 1, Stakeholder 2).

In conclusion, the incorporation of quantifiable learning outcomes, frequent evaluations, and feedback systems enables one to continuously enhance the content of the course and assures that the training continues to be successful despite the evolution of cyber threats (Turku University, University of Helsinki, Aalto University, Metropolia UAS).

4.5 Key Findings: Summary of the Current State Analysis Results

Based on the analysis of the topics mentioned in the current state section, this part presents the key findings according to the 3 key areas of research.

The interviews with stakeholders (May 2025) provided detailed insights into the essential elements of cybersecurity awareness and education for business users. Key findings indicate that cybersecurity is no longer just a technical concern but a strategic business issue intertwined with legal, ethical, and operational responsibilities. Stakeholders consistently emphasized the importance of core concepts such as GDPR compliance, lawful data handling, password hygiene, phishing awareness, identity management, and risk perception. Key findings also focused on data classification and legal bases for processing and also highlighted national competence frameworks and human factors, noting that many users perceive cybersecurity as a “black box”. Findings stressed the need for cultural and strategic alignment, arguing that users must understand how cybersecurity supports business value. Course design should be short, scenario-based, role-specific, and free of jargon. Real-world examples and microlearning formats were recommended to increase relevance and retention. Engagement remains a challenge; users often underestimate risks or deprioritize training. Therefore, courses should be mandatory, regularly updated, and tied to risk management rather than compliance alone. Methods like storytelling, quizzes, gamified elements, and domain-specific case studies were widely supported. Ultimately, cybersecurity training must be practical, relatable, and integrated into the organizational culture to be truly effective. Table 15 summarizes results from current state analysis.

Table 15. Results from the current state analysis.

Key Area	**Findings**
1. Topics Identified from courses and interviews (relevant for Business Users)	1.Awareness of cybersecurity and phishing attacks, 2.Protection management, 3.Data protection and compliance with the GDPR, 4.Safe browsing and email usage, 5.Incident reporting and escalation procedures, 6.Principles of cyber ethics, 7.Business continuity and risk awareness 8. Recognition of common cyber threats and trends
2. Curricula Design Principles for cybersecurity courses (identified in courses and interviews)	1. Content that is straightforward, operational, and action-oriented, 2. Learning based on scenarios, case study, quiz. 3. Interactive modules that can be completed at the user's own speed, 4. Learning based on simulation 5. Hands-on practice with security tools.
3. Making difference between IT and	- The courses for IT users are technical, research-driven, and skills-based (for example, cryptography and penetration testing), - Courses for non-IT users that are not related to

non-IT courses	information technology are streamlined, awareness-focused, and practice-oriented.
4. Other Considerations	- Maintain an emphasis on real-world scenarios, - steer clear of technical jargon, - employ interactive learning methods (such as quizzes and gamified assignments), - adapt information to user jobs (such as human resources, finance, and sales). - include evaluation of the results of learning and verification of compliance integration.

The study of internal and external cybersecurity courses pointed to the topics, design principles, and differentiation of the existing courses.

Based on the learning from the existing examples, this study will move to create a cybersecurity course for business users in the next section.

5 Building the Cybersecurity Course for Business Users

This section reports on the development of a cybersecurity course that is especially targeted at business users (students) for the case organization.

5.1 Overview of the Proposal Building Stage

The cybersecurity course for business users was developed based on three main sources. First, as discussed in Section 4 of the (CSA), there is a gap in the availability of cybersecurity course for business users those who are not IT experts. This course emphasizes the content tailored to the needs of business users. Second, literature and best practice review indicated the critical subjects that should be incorporated into such course in cybersecurity. These topics include network security, risk management, incident response, and regulatory compliance. Third, the inputs obtained from key stakeholders during Data 2 collection provided recommendations about the structure of the course, the methods of delivery, and the relevancy of the material expected from the case organization for such a course. Together, these sources provided the foundation for the development of a cybersecurity course that is not only adaptable and business-relevant, but also realistic and practical, with the goal of bridging the knowledge gap for non-technical learners. The third phase made an emphasis on co-creation, during which stakeholders, including students, lecturers, and development managers, submitted input and ideas for the course.

5.2 Findings from Data 2 (pulling together CSA, CF and Data 2)

A summary of the most important inputs from stakeholders (Data 2) that were used in the construction of the plan is provided in this part. The emphasis areas from CSA (Data 1) and the related literature (Conceptual Framework) were taken into consideration to triangulate these elements.

The insights that were supplied by stakeholders verified numerous major goals for the proposed cybersecurity course, as can be shown in Table 15. First, there was a significant focus placed on addressing subjects that are not technically related but are strategically essential in terms of cybersecurity and are useful for business users. Stakeholders brought attention to the requirement for a learning style that is both modular and interactive. This would enable learners to go at their own speed while

simultaneously engaging with information that is scenario-based and practical. It was deemed necessary that the content of the course continue to be closely connected with the demands of the real-world industry, and that it incorporate actual case studies to improve both the extent of application and the level of comprehension. Finally, stakeholders emphasized the significance of clearly distinguishing between curriculum components that are focused on information technology and those that are not focused on IT to guarantee that the course continues to be accessible and beneficial to the audience that it is meant for, which is non-technical.

Table 16. Key stakeholder suggestions (Data 2) aligned with the findings from the CSA and the Conceptual framework.

	Areas of focus of CSA (from Data 1)	*Inputs from literature (**CF**)*	*Suggestions by stakeholders (from Data 2)*	*Descriptions of their suggestions (in more detail)*
1	Understanding the cybersecurity topics needed for business users	Cybersecurity awareness, GDPR, risk management, secure practices (Haney & Lutters, 2023; EU, 2024)	Create a course with a business-user concentration	Stakeholders underlined that case-based examples such as "How a phishing scam affected HR" should be applied, therefore making more relevant.
2	Creating a course suitable for non-IT users	Modular, competency-based curriculum (ENISA, 2022; ECSF)	The course can be organized for advanced, intermediate, and beginning levels.	According to stakeholders, the course should begin with awareness and then go towards more in-depth risk evaluation assignments.
		Use simplified terminology, focus on human factors (Haney & Lutters, 2023)	Include visual aids, analogies, and gamified quizzes	"Cyber jargon" should be substituted with common business terms.
3	Interest in certifications that can relate to such a course	Integration with ENISA badges, CISSP/ISO frameworks (SME guide)	Include completion badges or a completion certification	Ideally, a certificate or badge be issued following successful completion of the course to boost motivation and visibility on student profiles.

It is clear from Table 16 that the feedback from stakeholders immediately addressed the focal areas that were highlighted in the CSA and fit well with the aspects of the coalition. It is abundantly obvious that stakeholders favoured a course structure that is adaptable, non-technical, and scenario-driven to guarantee comprehension and preservation of information.

5.3 Initial Proposal

A cybersecurity course that is specifically geared towards business users is presented in this part: first, the content and structure of the course, second, the teaching techniques, and third, the evaluation and certification processes. Each component is developed so that the course is applicable, and accessible to individuals who are not from the IT field.

The course URL link in Moodle: https://moodle.metropolia.fi/course/view.php?id=7006

5.3.1 Element 1: Course Structure and Content

The course has a modular structure and consists of 9 chapters, and each of them aims at assisting users in the process of creating a foundation in the cybersecurity basics for business users. Each chapter contains an informative PowerPoint elaborating important ideas and useful metadata such as an overview of the topic and any required prerequisites. At the end of every chapter, there is a quiz that can tell how much a student learned. The course includes additional materials in the form of curated YouTube videos that provides real-life examples and expert information, as well as detailed supporting documents in case different people would like to learn more.

The 9 chapters include the following topics:

1. Overview of Computer and Web-technology
2. Introduction of Cyber Security
3. Cyber Attacks & Malware
4. Cybercrime and Cyber law
5. Cyber Security Techniques
6. Social Media Overview and Security
7. E- Commerce & Security
8. End Point device and Mobile phone security
9. Conventional and Symmetric Cryptography

The main views of the course on Moodle are shown below, in Figures 2 and 3.

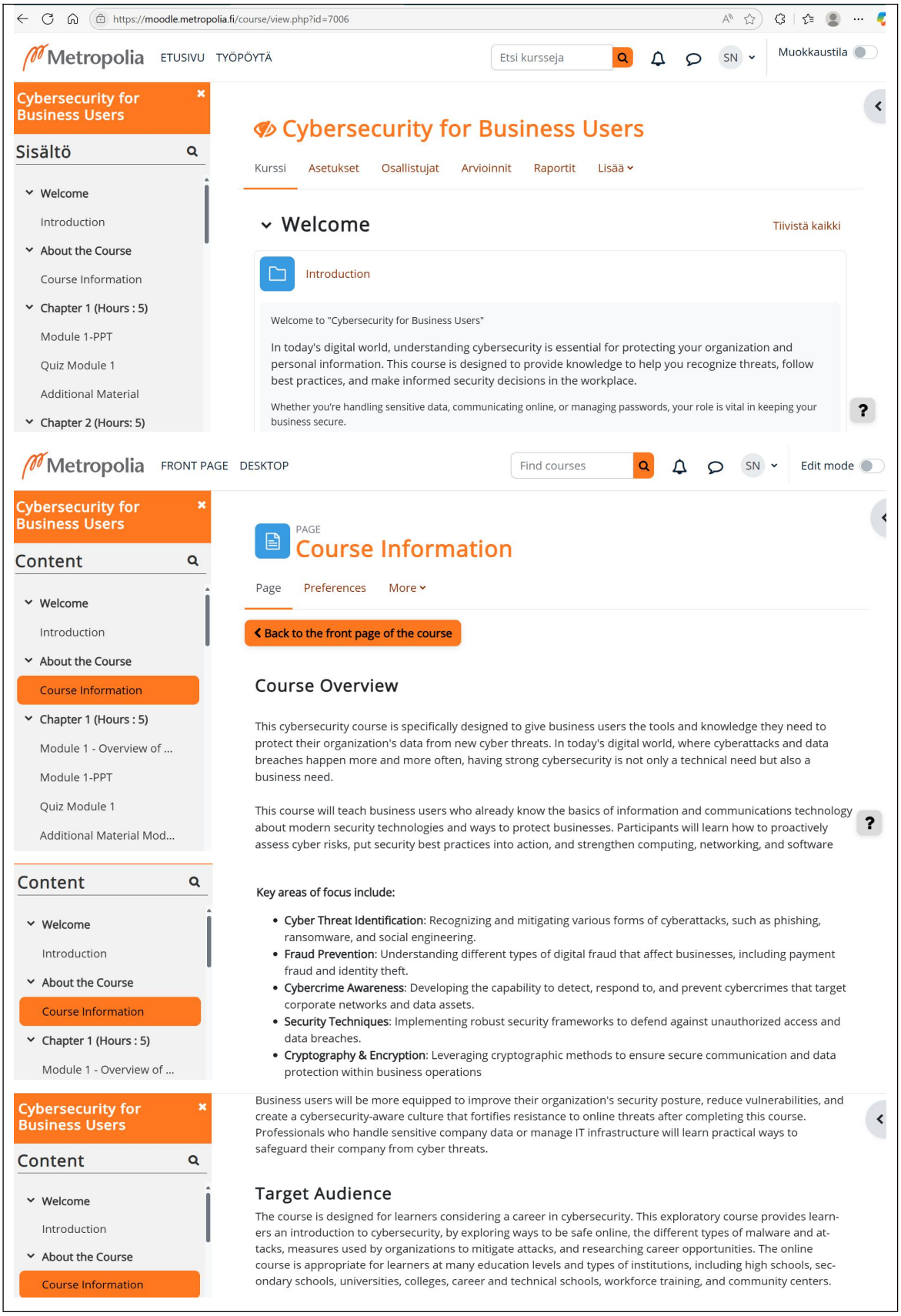


Figure 2: Course Overview

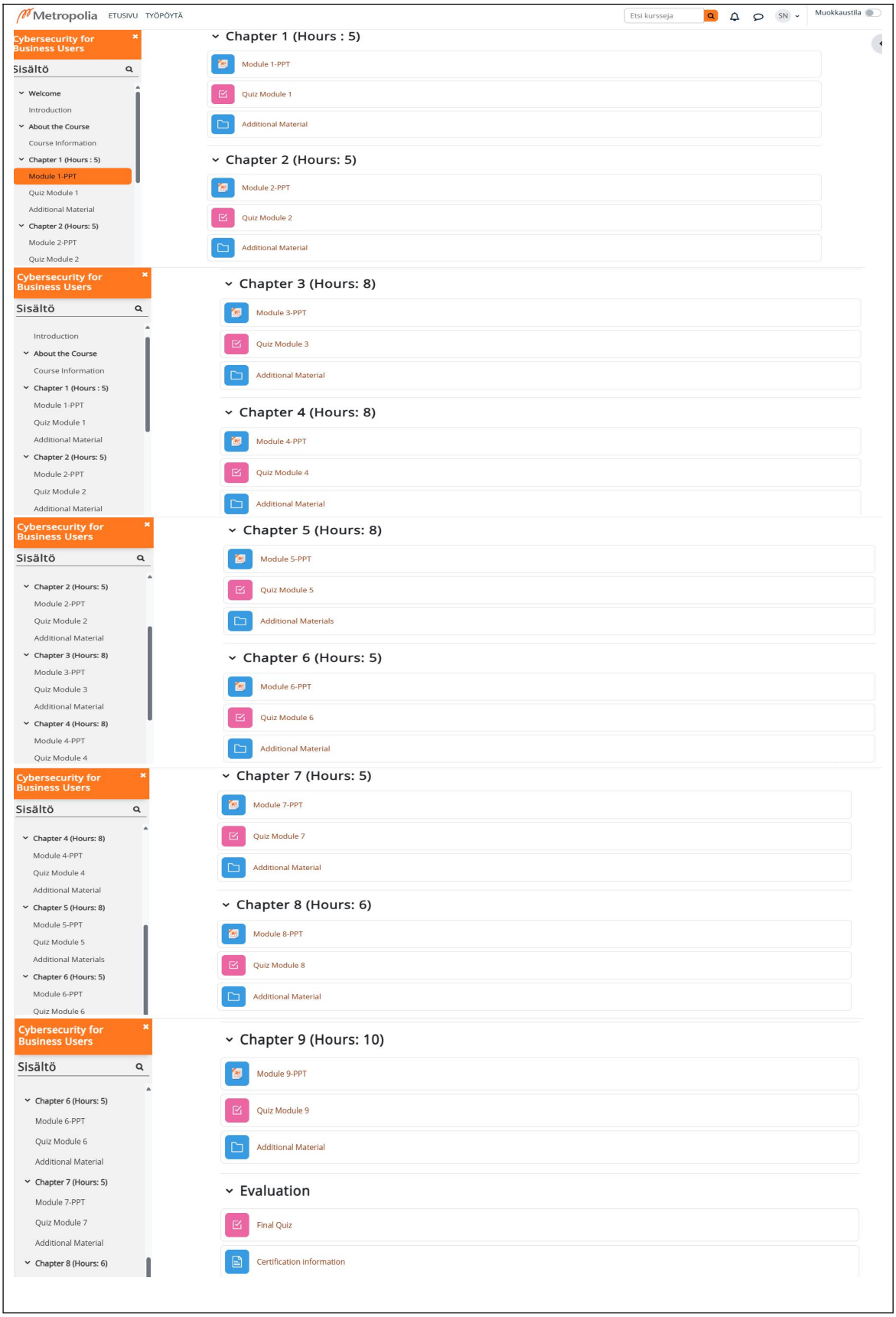


Figure 3: Chapter Structure.

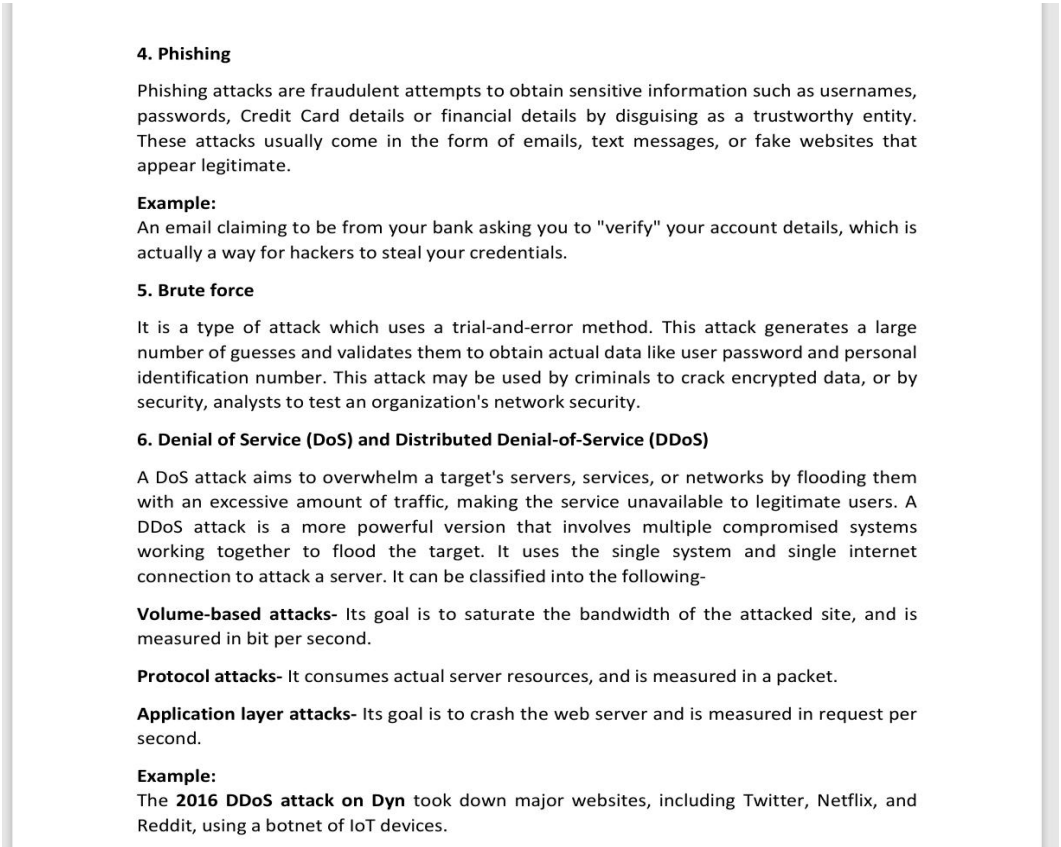
Figure 3 depicts chapter structure in the course. Every chapter comes with an informative PPT and a short quiz.Also,extra materials—YouTube videos links, along with detailed supporting documents for those who want to explore further.

5.3.2 Element 2: Teaching techniques

This course uses a teaching approach designed for all learning styles:

- Each chapter starts with a PowerPoint that explains key concepts, along with helpful information and any basics you might be needed.
- A short quiz follows to check understanding.
- Added YouTube videos with real-world examples and expert tips related to topics.
- Curious to dive deep, detailed documents offer extra insights.
- It’s a flexible, self-paced format that makes cybersecurity feel approachable and useful for any business users.

Figure 4 shows the example of the description that is available as part of additional material for the business users to gain knowledge on the topic.



4. Phishing

Phishing attacks are fraudulent attempts to obtain sensitive information such as usernames, passwords, Credit Card details or financial details by disguising as a trustworthy entity. These attacks usually come in the form of emails, text messages, or fake websites that appear legitimate.

Example:
An email claiming to be from your bank asking you to "verify" your account details, which is actually a way for hackers to steal your credentials.

5. Brute force

It is a type of attack which uses a trial-and-error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

6. Denial of Service (DoS) and Distributed Denial-of-Service (DDoS)

A DoS attack aims to overwhelm a target's servers, services, or networks by flooding them with an excessive amount of traffic, making the service unavailable to legitimate users. A DDoS attack is a more powerful version that involves multiple compromised systems working together to flood the target. It uses the single system and single internet connection to attack a server. It can be classified into the following-

Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.

Protocol attacks- It consumes actual server resources, and is measured in a packet.

Application layer attacks- Its goal is to crash the web server and is measured in request per second.

Example:
The **2016 DDoS attack on Dyn** took down major websites, including Twitter, Netflix, and Reddit, using a botnet of IoT devices.

Figure 4: Additional materials.

5.3.3 Element 3: Assessment and Certification

The below assessment process depicts how the business users will be evaluated while undergoing the course.

1. Tests to check the obtained knowledge throughout the course (via quizzes).
2. Evaluation using a Pass/Fail system (with a final quiz).
3. Additionally, students are encouraged to earn self-assessment badges offered by ENISA and the GDPR awareness certificates (https://www.tuvsud.com/en-in/store/academy-in/sectors/information-technology/0063-Data-Privacy-EU-GDPR-Practitioner-Training-Certification)

Each module ends with a quiz (e.g., phishing simulation, case discussion).

As the Business user will undergo a quiz, as per the instruction mentioned on the question, the business user has to select the correct answer. On giving the correct answer, scores are allocated to the to the users, the users will have to score more than 60% to successfully complete the quiz.

An example of a quiz in shown in Figure 5 below.

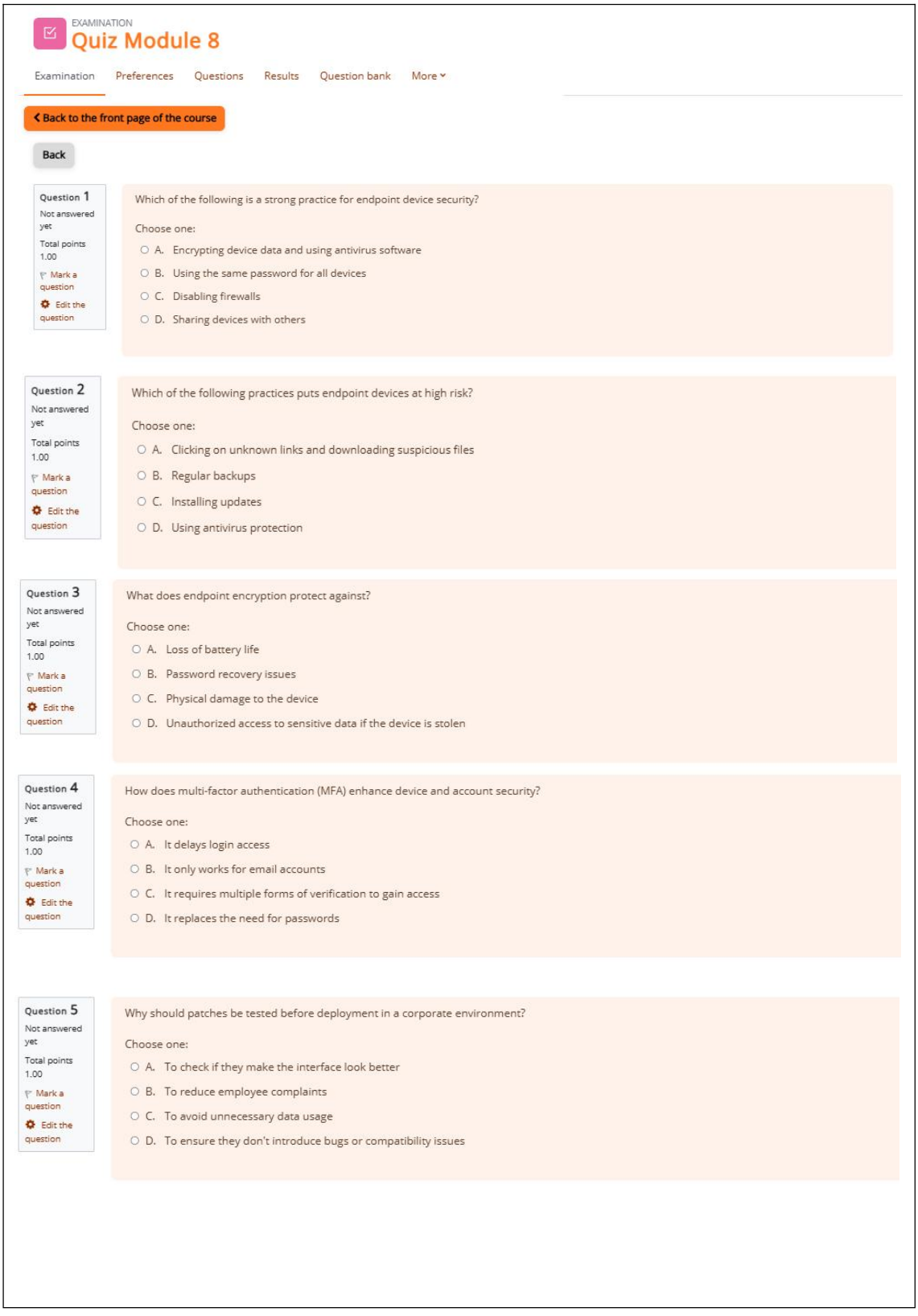


Figure 5: An example of a quiz, screenshot.

Once the business users are confident enough, they can enroll for the Practitioner Certification Training Program on Data Privacy and EU GDPR course. Once they successfully pass the course, they will be granted a Certificated as shown in Figure 6.

Figure 6: ENISA and the GDPR awareness certificates.

Figure 7 depicts the number of approximate hours a business user has to devote to understand a specified chapter and to undertake a quiz and go through the additional materials and links related to the chapter.

Module	Module Name	Learning Hrs
1	Overview of Computer and Web-technology	5
2	Introduction of Cyber Security	5
3	Cyber Attacks & Malware	8
4	Cybercrime and Cyber law	8
5	Cyber Security Techniques	8
6	Social Media Overview and Security	5
7	E- Commerce & Security	5
8	End Point device and Mobile phone security	6
9	Conventional and Symmetric Cryptography	10
	Total Learning Hrs	**60**

Figure 7: Student workload in the course (calculation).

Finally, the following logic for assigning the ECTS credits for a course based on student workload.

ECTS Calculation Basics:

- 1 ECTS credit = appx. 27 hours of total student workload.

Course ECTS Credit Calculation:

- 60 hrs of student workload = appx. 2 ECTS

5.4 Summary of the Initial Proposal

The outline of the course elements is given in Table 17 below together with information on desired results, content, and delivery techniques.

Table 17. Summary of the course elements.

	Element	**Description**	**Format**	**Outcome**
1	Course Content	Balanced content which includes topic like GDPR, risk, phishing, incident response	Modular, flexible	Understanding of core topics
2	Teaching Methods	Self Learning	Moodle	Engagement, practical relevance
3	Assessment & Certification	Quizzes, ENISA badge, final test	Formative and summative	Badge/certificate of completion

The course elements outline the cybersecurity topics that need to be known by business users. The next step is validation and final improvements in the following section.

6 Validation of the Proposal

The aim of this step was to evaluate the relevance and improve the proposed course through expert judgement.

6.1 Overview of the Validation Stage

The validation gathered two expert inputs to the proposed cybersecurity course. The course was presented to two internal experts for evaluation and suggestions to the course structure, materials, and selected teaching methodology.

The proposal that was produced in Section 5 and discussed in this validation phase, which made it possible for each component of the course to be evaluated, collect recommendations, and make practical adjustments.

6.2 Developments to the Proposal (based on Data Collection 3)

The feedback that was gathered during the validation stage (Data 3) resulted in a number of adjustments that were quite beneficial to the initial plan. A summary table below reflects the ideas expressed by experts and the improvements that resulted from them.

Table 18. Expert suggestions (findings of Data 3) for the Initial proposal.

	Element 1 of the Initial proposal	*Parts commented in Validation*	*Expert commentary (in detail) on the comment/feedback*	*Evolution from the First Application*
1	Course Content & Topics	Risk Management & GDPR module	Experts underlined the need of clarifying for business users the useful use of GDPR and encryption. She advised using relevant concepts such digital signatures, encryption, and message security in regular corporate tools.	Added were real-world instances (such as digital signature and email encryption use). Content in Module 9 was streamlined and rendered more commercially relevant.
2	Teaching Methodology	Interactive Elements	Experts underlined the absence of logical flow between subjects and meta-text. They advised	Every module had meta-text, transitions, and well stated learning objectives.

			include signposts and using more deliberate, accessible graphics (such as understandable fonts, picture relevancy).	Visuals were changed with regard for accessibility, intent and fonts.
3	Assessment & Certification	Final Quiz and Badge	Experts underlined the significance of teaching students about outside certification choices fit for non-technical users. She also advised including video links straight after every module to improve engagement and stacking of materials for different students.	Added post-quiz were recommended certificates (ENISA, ISC2 CC). Every lesson included integrated YouTube links and video tutorials as additional resources.

Table 18 summarizes expert recommendations emphasizing contextual relevance, teaching methods and assessment. Their validation supported further improvements for the course.

6.2.1 Developments to Element 1: Course Content

Particularly in the courses on cryptography and risk management, experts' comments enhanced the course material with useful applications and real-life scenarios. Rather than concentrating just on technical concepts, these courses now explain how encryption is applied in common business tools such digital signatures, messaging applications, and client communications. For Business users, this helped make abstract subjects more relevant. Module 9 was changed to incorporate easier explanations and visual breakdowns of cryptographic methods, and projected time durations for every module were checked to guarantee they were reasonable and fitting for the learner level.

6.2.2 Developments to Elements 2: Teaching Methodology

Experts underlined the requirement of logical flow and clear navigation via the need for the title for each course element. Every module now starts with a quick meta-text introduction that outlines what students will learn and the reasons behind the importance. To provide reasonable transitions between subjects, signposts such as "Next, we will explore...” were included. Revised images and visual aids guaranteed accessibility and relevancy. Larger fonts, better formatting, and more inclusive design

helped PowerPoint slides to be rebuilt for every user. Links and other resource files were arranged for easier user access.

6.2.3 Developments to Elements 3: Assessment and Certification

The comments of experts underlined for students the need of acknowledgement and outside validation. Though a formal certification was not originally included, the course was changed to suggest beginner-friendly external qualifications such ENISA Cyber Hygiene, ISC2 Certified in Cybersecurity (CC), and CompTIA Security+ basic topics. The last quiz also provides clarifying comments for every question, therefore enabling students to learn from their errors. After every module, supplementary video links were included to satisfy various student interests and offer rapid, graphic reinforcement of important ideas.

6.3 Final Proposal

The last draft of the cybersecurity course shows significant improvements resulting from expert evaluation. It is currently set up around nine modules, each meant to give Businessusers basic cybersecurity understanding by combining: first, practical materials with real-world examples; second, interactive and easily available instructional strategies (including tests, images, signposts, and videos); and third, evaluation instruments with instantaneous feedback and direction on future actions. The final proposal is shown in Figure 8 below.

Business users will be able to continue their adventure in cybersecurity beyond the scope of this beginning course because the course also offers references to external certifications for beginners. As a micro-credential or elective module, it has the potential to be adopted by other faculties as well. It is planned to be included into the business curriculum at Metropolia University of the Arts and Sciences. The course's usability, instructional value, and practical effect have all been improved significantly as a result of the modifications that were led by the input from experts.

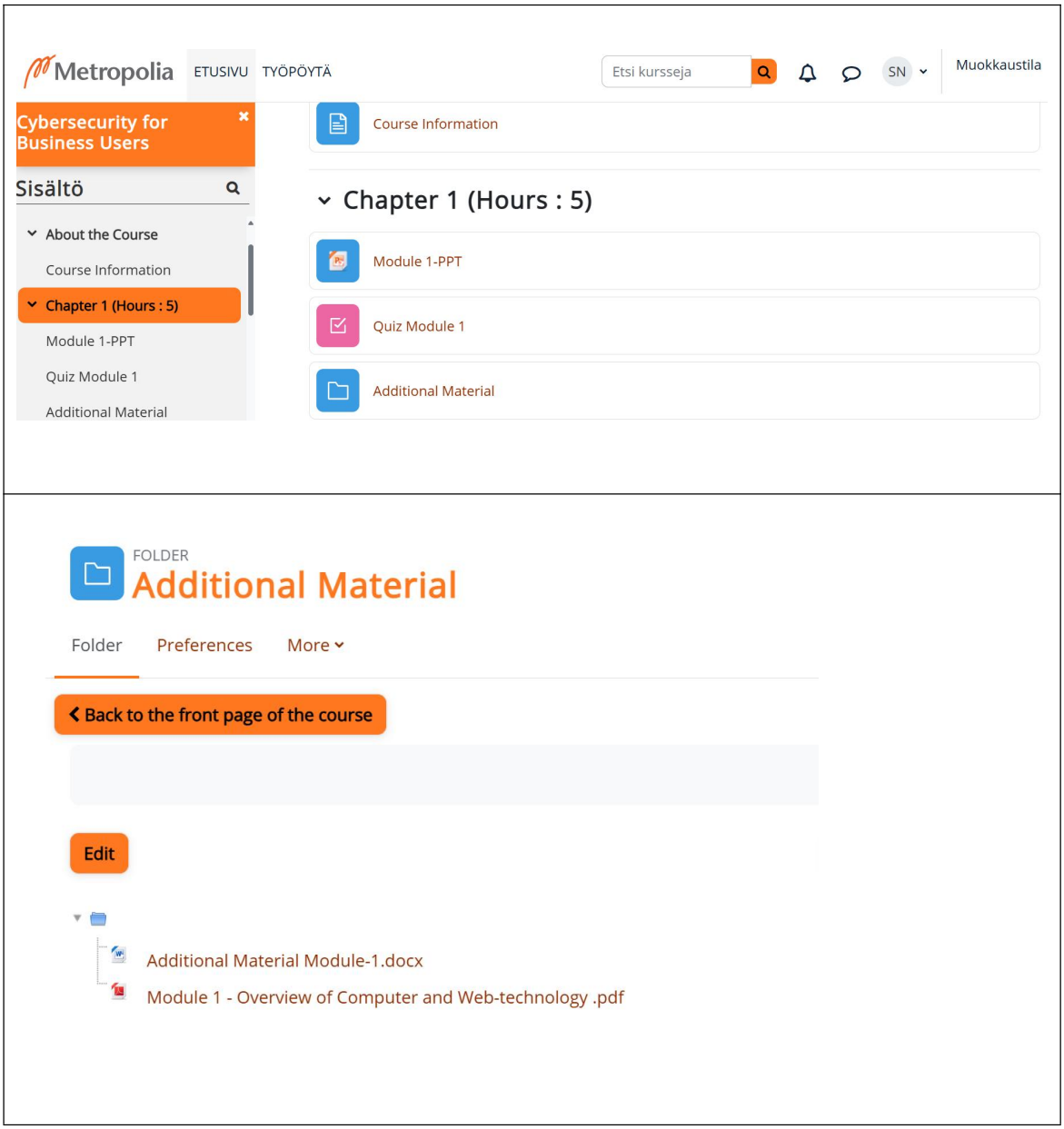


Figure 8: Suggested improvements-1.

As suggested the detailed documentation for every chapter is added under “Additional Material”.

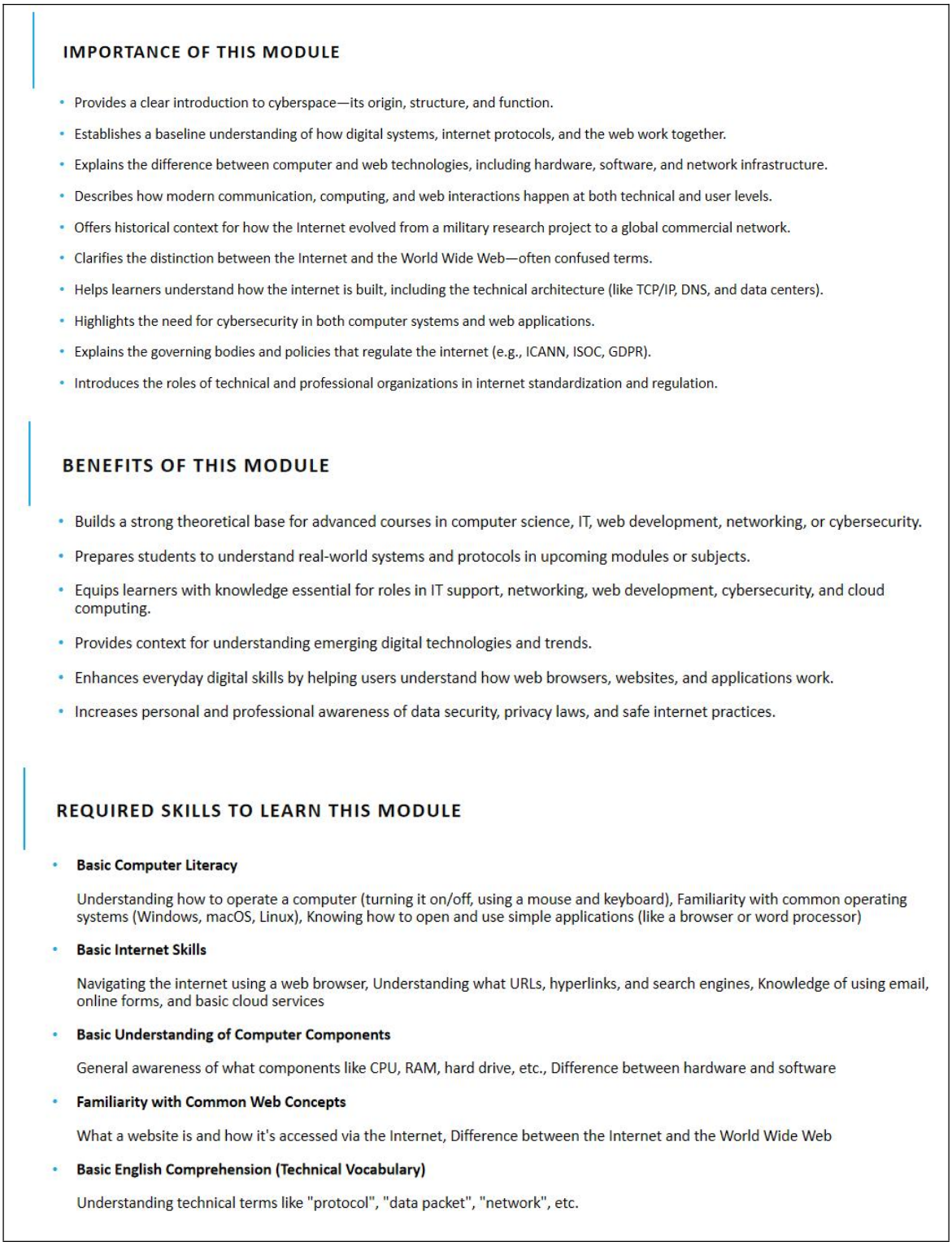


Figure 9: Suggested improvements-2.

As suggested the metadata is added to the Presentation of each chapter which showcase the benefits and prerequisites of the specified chapter.

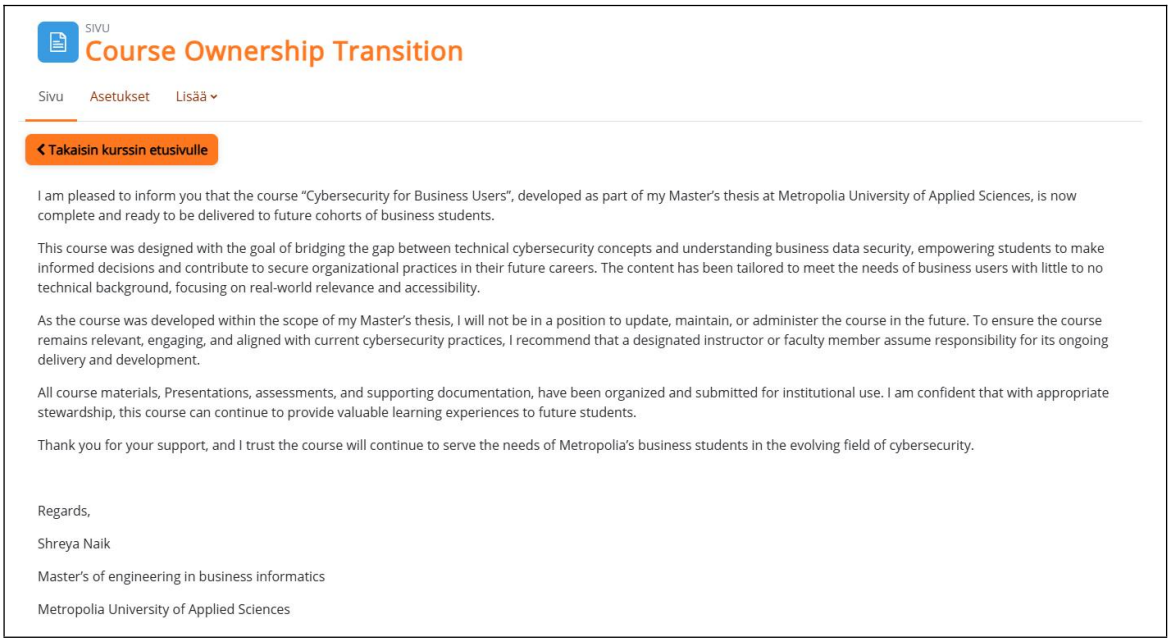


Figure 10: Suggested improvements-3.

As suggested, added the notice sharing about the course been developed and added as part of Master thesis and it can be handled and upgraded by responsible instructor of Metropolia UAS in the future.

7 Conclusion

This concluding section provides a summary of the most important results, presenting the executive summary, next steps, and last thoughts. Specifically, it offers evaluation of the findings and the practical implications those findings for the case organization.

7.1 Executive Summary

This thesis sought to build and suggest a cybersecurity training especially fit for Metropolia UAS non-IT business users. Business users are a high-risk category as they are often exposed to digital hazards without the knowledge necessary to recognize or handle those hazards. This work filled up this need by creating an instructional solution based on scholarly theory, pragmatic wisdom, and professional validation.

The objective of this thesis was to develop a cybersecurity course that would be especially aimed at business students at Metropolia University of Applied Sciences. The goal was to meet the rising need for cybersecurity knowledge among non-technical users who play an important role in the use and protection of organizational data. The study used a qualitative research approach and included an examination of the literature, the current state analysis, and stakeholder inputs for the proposal development and its validation.

Data collection consisted from discussions with subject-matter specialists and comments from management and academic professionals. Three-phase data collecting was used for the study. The examination of the literature found the topics that need to be used to boost cybersecurity understanding among business users. The theoretical approach has drawn from the topics related to cybersecurity education, key EU literature like ENISA, and curricular design principles. A conceptual framework based on EU guidance — e.g., ENISA, ECSF — and best practices was developed. The current state analysis by means of interviews, followed by the proposal development and validation with academic professionals.

In the development stage, the theoretical inputs were extended with actual stakeholder feedback that influenced the process of the course design. Key themes of the proposed

course included cybersecurity challenges in business environment, GDPR compliance, cybersecurity awareness, and risk management practices.

The outcome of the thesis is a course developed with modular material, real-life examples, and integrated assessment methods. Comprising twelve major cybersecurity issues, the suggested course is set out using modular components, and ongoing evaluation. Material simplification for non-technical users and recommendation of accessible certifications were among the various enhancements resulting from expert validation phase comments. These improvements raised the usefulness and relevancy of the course. The course offers a contribution to Metropolia UAS course offerings, that aims at bridging knowledge gaps, enhancing digital resilience, and encouraging a culture of cybersecurity among business users.

7.2 Next Steps and Recommendations toward Implementation

Several actions are advised to guarantee the effective introduction of the proposed “Cybersecurity course for business users”.

First, the final course design should still be implemented, after which it can be included into institutional curricula. This will entail matching degree formats (business informatics, international business), credit rules, and institutional quality criteria.

Second, it is imperative to continue improving the course by appointed owners with pedagogical knowledge as well as cybersecurity experience. To provide a complete educational experience, a multidisciplinary teaching team ideally should still revise the course (also periodically) incorporating expertise from law, business, and information security.

Third, a system of performance evaluations still has to be developed. It should record indicators such learner comments, quiz results, completion rates, and degrees of involvement. Improving quality and proving the long-term instructional influence of the course depend on these metrics.

Fourth, it is advised to improve the course with actual case studies and guest lectures by means of cooperation with outside cybersecurity experts and trainers. This

guarantees congruence with present business trends and enhances professional exposure for students.

At last, the course need to be taken into consideration for development as a micro-credential or elective available across other departments including design, engineering, or healthcare. This would extend its influence and raise awareness of cybersecurity among institutions all around.

7.3 Thesis Evaluation

The goal of this thesis was to develop a cybersecurity course for business users, which are often overlooked by cybersecurity training and education projects. The objective was pursued by employing a structured research design that comprised analysis of the current state, exploration of literature and best practice for conceptual framework, and using co-creation with stakeholders and validation through expert feedback. The development of a course concept that is both pertinent and rooted in the requirements of the real world was made possible by the combination of academic rigour and the participation of practical stakeholders. Through the production of a course that addresses gaps in business user knowledge and cybersecurity threats, the thesis was able to meet its primary purpose. By conducting interviews with stakeholders, doing a literature study, and validating the findings, the triangulation of data sources helped to increase the trustworthiness of the results and guaranteed that the plan was not constructed only on the basis of assumptions.

It is important to understand that there are certain limitations in this study. In the validation phase, only a small number of stakeholders were involved. If the pilot had been conducted, it would have yielded more in-depth insights and feedback that would be more representative. The evaluation of learning outcomes relied on qualitative feedback rather than pre- and post-course knowledge assessments, which may be a useful addition in further rounds.

This work continues to create practical value despite the limits that have been discussed above. There was a methodical approach to the technique at each level, well-documented and based on both theory and input from stakeholders. The expansion of the data collection, which should include quantitative performance

measurements, and the monitoring of long-term behavioural change among learners, would be beneficial to future attempts.

7.4 Closing Words

Nowadays, cybersecurity is a strategic business problem that impacts organizations across all levels, rather than just a specialist technological worry. On a regular basis, business users engage with sensitive data and digital systems, but they are typically neglected when it comes to training and education in this area compared to IT specialists. To address this knowledge gap, this thesis suggested that Metropolia UAS provide a cybersecurity course tailored to non-technical business executives that is both targeted and grounded in fact. A thorough course proposal was created and approved through a mix of academic research, stakeholder participation, and institutional analysis. Learners will be empowered by the proposed course because it raises awareness, encourages responsible behaviour, and provides them with the information they need to recognise and respond to cyber dangers. Business users will be better equipped to navigate the modern digital terrain safely thanks to the program's focus on practical learning, modular flexibility, and real-world applicability.

The thesis provides the course and helps become a more cybersecurity-aware society and safer workplaces in the long run. This thesis represents a modest but significant attempt in that regard.

References

Ahmed, H. S. A. (2023). *A guide to the updated ISO/IEC 27002:2022 standard, Part 2*. ISACA.

Ambika, M., (2020). Module-I: Introduction to cybersecurity. Teoksessa: cybersecurity [SEC-4]. s.l.:MICA. https://kimsbengaluru.edu.in/assets/pdfs/criterias/criteria-1/criteria-1.1.1/Cyber%20security.pdf

Aslaner, M. (2024). Cybersecurity Strategies and Best Practices: A comprehensive guide to mastering enterprise cyber defense tactics and techniques. Packt Publishing Ltd.

Awais Rashid, (2021). The cybersecurity Body of Knowledge, s.l.: Crown. https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf

Baltuttis, D., (2024). A typology of cybersecurity behavior among knowledge workers. ELSEVIER, p. 3. https://www.sciencedirect.com/science/article/pii/S0167404824000427

Blank, C. A. L., (2013). Mixed Methods in Social & Behavioral Research. Journal of Music Therapy, Issue Vol 50. https://www.researchgate.net/publication/263859683_Mixed_Methods_in_Social_Behavioral_Research

Bosquet, P. (2022) Higher education institutions to cooperate to develop cybersecurity education – information psychology research also to be boosted. Ministry of Education and Culture. Published in English on 22 December. Available at: https://okm.fi/en/-/higher-education-institutions-to-cooperate-to-develop-cyber-security-education-information-psychology-research-also-to-be-boosted

Bryman, A., (2016). Social Research Methods. Fifth Edition ed. Oxford: OXFORD University Press. https://ktpu.kpi.ua/wp-content/uploads/2014/02/social-research-methods-alan-bryman.pdf

Clarke, N., & Furnell, S. (2023). Editorial: Human aspects of cybersecurity. Information and Computer Security, 31(3), 265–266.

David Kim, M. G. S., (2016). Fundamentals of Information Systems Security, 3rd Edition, s.l.: Jones & Bartlett Learning. https://www.oreilly.com/library/view/fundamentals-of-information/9781284116465/

DHET (2020). Introduction to Cybersecurity, s.l.: Department of Higher Education and Training. Department of Higher Education and Training

East Asia Institute of Management (EAIM), (2024). Why Non-Technology Professionals Should Learn cybersecurity. https://www.linkedin.com/pulse/why-non-technology-professionals-should-s5udc

ECSM (2022). EU Cybersecurity Month. https://cybersecuritymonth.eu

Edwards, J., & Weaver, G. (2024). The cybersecurity guide to governance, risk, and compliance. Wiley.

ENISA (2020). Cybersecurity Education and Training Standards. https://www.enisa.europa.eu/publications/cybersecurity-education-training-standards

ENISA (2021). Cybersecurity for SMEs. https://www.enisa.europa.eu/topics/cybersecurity-education/smes

ENISA (2022). Cybersecurity Awareness for SMEs and Entrepreneurs. https://www.enisa.europa.eu/publications/cybersecurity-awareness-for-smes

ENISA (2022). European Cybersecurity Skills Framework (ECSF) - User Manual, s.l.: European Network and Information Security Agency (ENISA). https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf

ENISA (2022). European Cybersecurity Skills Framework (ECSF) | ENISA. Retrieved from https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf

ENISA (2022). European Cybersecurity Skills Framework (ECSF). https://www.enisa.europa.eu

ENISA. (2022). European Cybersecurity Skills Framework Role Profiles. Retrieved from https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

ESCO. (2024). Crosswalk between ESCO and the European Cybersecurity Skills Framework (ECSF). Retrieved from https://esco.ec.europa.eu/en/about-esco/publications/publication/crosswalk-between-esco-and-european-cybersecurity-skills

EUROPEAN COMMISSION (2021). Digital Education Action Plan 2021–2027. https://education.ec.europa.eu

European commission (2022). Digital Skills and Jobs Platform. https://digital-skills-jobs.europa.eu

EUROPEAN COMMISSION (2024). Second Report on the application of the General Data Protection Regulation, s.l.: EUROPEAN COMMISSION. https://ec.europa.eu/info/law/law-topic/data-protection_en

European Commission. (2024). *Data protection in the EU*. https://ec.europa.eu/info/law/law-topic/data-protection_en

European Commission. (2024). EU must reinforce cybersecurity skills. Retrieved from https://digital-strategy.ec.europa.eu/en/news/eu-must-reinforce-cybersecurity-skills

Haney, J. M., & Lutters, W. (2023). *From compliance to impact: Tracing the transformation of an organizational security awareness program*. *arXiv*. https://doi.org/10.48550/arXiv.2309.07724

Hannes, K., Bishop, L. M., & Buchanan, C. D. (Eds.). (2022). *The SAGE handbook of qualitative research design: Being creative with resources in qualitative research* (1st ed.). SAGE Publications Ltd. https://www.researchgate.net/publication/359898621_The_SAGE_Handbook_of_Qualitative_Research_Design_Being_Creative_with_Resources_in_Qualitative_Research

John W. Creswell, J. D. C., (2018). Research Design Qualitative, Quantitative, and Mixed Methods. Fifth Edition ed. s.l.:SAGE. https://spada.uns.ac.id/pluginfile.php/510378/mod_resource/content/1/creswell.pdf

Justin Scott Giboney, (2021). Increasing Cybersecurity Career Interest through Playable Case Studies. Springer Association for Educational Communications & Technology. https://par.nsf.gov/servlets/purl/10257039

Kabanda, G., (2021). Cybersecurity Risk Management Plan for a Blockchain Application Model. Gnoscience Group, Vol 2(Iss 1), p. 1. https://gnoscience.com/uploads/journals/articles/665167939166.pdf

Karen Davis and Jeffrey Miller (2020). Cybersecurity education: curriculum and challenges. ACM SIGCSE Bulletin.

Kubal, S., (2025). Computer Science and Technology. Kolhapur: Shivaji University. https://www.unishivaji.ac.in/uploads/bosnew/engineering/B.Tech%20Computer%20Sci%20&%20Tech%20SY%20Syllabus%202024-25%20DOT%20NEP.pdf

MICA (2020). Module-I: Introduction to cybersecurity. Teoksessa: cybersecurity [SEC-4]. s.l.:MICA. https://kimsbengaluru.edu.in/assets/pdfs/criterias/criteria-1/criteria-1.1.1/Cyber%20security.pdf

Morgan, S., (2019). Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021. cybersecurity Ventures, 10 June. https://cybersecurityventures.com/cybersecurity-market-report/

MRC (2021). cybersecurity [R18A0521]. Secunderabad: MALLA REDDY COLLEGE OF ENGINEERING AND TECHNOLOGY. https://mrcet.com/pdf/Lab%20Manuals/IT/Cyber%20Security.pdf

Pande, J. (2017). Introduction to cybersecurity (FCS). Haldwani: Uttarakhand Open University. https://uou.ac.in/sites/default/files/slm/Introduction-cyber-security.pdf

Peter Reason, H. B. (2008). The SAGE Handbook of Action Research. Sage Publications Ltd, Volume Second Edition. https://www.daneshnamehicsa.ir/userfiles/files/1/9-%20The%20SAGE%20Handbook%20of%20Action%20Research_%20Participative%20Inquiry%20and%20Practice.pdf

Ponemon (2017). Cost of Data Breach Study, Traverse City, Michigan: Ponemon Institute Research Report. https://www.ponemon.org/news-updates/blog/security/2017-cost-of-data-breach-study-united-states.html

Samant K, Lene T.S., Knud E.S. (2017). Cybersecurity education and training: Bridging the gap between academia and industry. IEEE Security & Privacy.

SITA (2019). cybersecurity SITA1602. Chennai: Sathyabama Institute of Science and Technology. https://sist.sathyabama.ac.in/sist_coursematerial/uploads/SITA1602.pdf

Stallings, W. (2019). NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS. FOURTH EDITION toim. s.l.:Pearson Education. Network Security Essentials: Applications and Standards (Fourth edition)

Verizon (2023). DBIR 2023 Data Breach Investigations Report, s.l.: Verizon. https://inquest.net/wp-content/uploads/2023-data-breach-investigations-report-dbir.pdf https://digital-skills-jobs.europa.eu/en/opportunities/training/free-online-cybersecurity-course-small-businesses | https://www.itgovernance.eu/fi-fi/cyber-security-training-courses-fi

Appendix 1. Module of cybersecurity course

Information security training – Module 1
The implementation of the information security and data privacy in Metropolia University

Metropolia

General policy on the use of information systems

Guiding principles for information systems' use:

- All authorized users have the right to reasonable and appropriate use.
- No harm or damage should be caused to other users, organizations, or information systems in the network.
- Privacy must be respected.
- The access rights granted by the university of applied sciences are personal.
- The user is responsible for all use of their credentials.

General Policy on the Use of Information Systems

This document describes the general usage rules for Metropolia's information systems. The rules apply to everyone who uses Metropolia's information systems. They also apply to workstations commonly used at the university of applied sciences and all devices connected to the university's network. A summary of the instructions can be found on the Wiki pages. The official policy can be read from the Policies section of Metropolia's OMA intranet.

A summary of the general policy can be found below, which contains the most important points.

You can read the document from here

Metropolia

Information security training – Module 2
Metropolia's information security practices

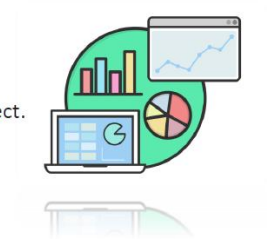
Metropolia

Privacy protection; confidentiality of personal information; data protection	Arrangements aimed at ensuring the proper processing of personal data and safeguard their privacy.
Information security	Preserving the confidentiality, integrity and availability of information.
Cybersecurity; cyber security	A target state in which the cyberspace can be trusted, when information and cybersecurity activities are conducted.
An information security incident	Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
A cyber environment; cyberspace; a cyber domain	an operating environment consisting of one or more digital information systems
Multi-factor authentication (MFA)	A multi-factor authentication means that your identity is confirmed using two or more methods of authentication.
A data backup	A backup copy is a duplicate of data stored separately from the original. In the event of the original file being destroyed, the backup copy can be used to recover the data.
A personal data breach	A personal data breach means an event leading to the destruction, loss, alteration or unauthorised disclosure of, or access to, personal data. A personal data breach can have consequences such as loss of control over personal data, identity theft or fraud, damage to reputation, or the reversal of pseudonymisation or loss of confidentiality of personal data.

Information security training – Module 3
Secure processing of information assets and data

Metropolia

Information risks



"Security" means freedom from concern. Information security ensures reliable processing of information assets. Information risks are uncertainties affecting objectives, like threats to a project.

Important data (the list is not exhaustive):

- Passwords and user IDs
- Project materials
- Private and health data
- Financial information
- Thesis materials

Simple safeguards to store sensitive data:

- Save files in at least two locations.
- Automate data back ups. IT Services backs up network drives like the Z drive. You are responsible for other backups.
- Don't rely solely on cloud services; keep copies on your Z drive.

Metropolia

Information security training – Module 3
Secure processing of information assets and data

Metropolia

Classification of data

- Classifying documents and data based on their confidentiality level is essential for information security throughout the data lifecycle. Once classified, data can be stored or published in appropriate locations, such as network drives, local drives, external storage devices, data systems, or cloud services. This classification adheres to the terms and conditions set by cloud service policies, legislation, or common agreements.
- The data owner or processor is always responsible for classifying the data.
- Metropolia uses the following data classifications:
  - **Public Information**: No restrictions on viewing. Examples include press releases or course information.
  - **Internal or Limited Use Information**: Accessible by Metropolia's staff and students. Examples include internal announcements or teaching materials.
  - **Confidential Information**: Accessible by specific groups, such as project teams.
  - **Classified or Secret Information**: Includes health data or sensitive personal data, which must be handled with special care.

More information can be found in the information classification model.

Metropolia

CYBER SECURITY

Module 4: Cybercrime and Cyber law

4.7 MODUS OPERANDI OF CYBER CRIMINALS

In general, modus operandi is the method acquired by any criminal for the successful commission of a crime. At a minimum, every Modus Operandi will contain three basic elements namely:

1. Ensure success of the crime
2. Protect identity
3. Facilitate effective escape

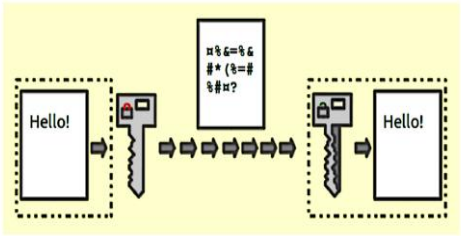
Common forms of modus operandi

1. Sending Annoying Messages

- Annoying, Insulting, Misleading, Defaming messages are often sent using mobile phones in bulk. Hence the actual source could not be fixed.
- Such messages are often a cause of misperception among people of different race, culture and tradition many a times often resulting in fights or riots.
- Unaware and innocent people often fall in traps of cyber criminals for SMS of lottery, Emails of prize money, false promise of jobs, and false mail for admission in reputed colleges.

CYBER SECURITY

Module 5: Cyber Security Techniques



5.0.3 DIGITAL SIGNATURES

It is a technique for validation of data. Validation is a process of certifying the content of a document.

The digital signatures not only validate the data but also used for authentication.

The digital signature is created by encrypting the data with the private key of the sender.

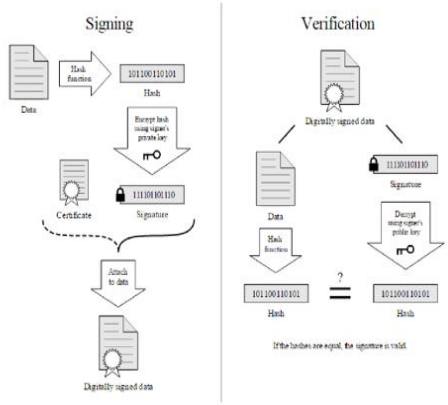
The encrypted data is attached along with the original message and sent over the internet to the destination.

The receiver can decrypt the signature with the public key of the sender.

Now the decrypted message is compared with the original message. If both are same, it signifies that the data is not tempered and also the authenticity of the sender is verified as someone with the private key(which is known to the owner only) can encrypt the data which was then decrypted by his public key.

If the data is tempered while transmission, it is easily detected by the receiver as the data will not be verified.

Moreover, the massage cannot be re-encrypted after tempering as the private key, which is posses only by the original sender, is required for this purpose.



As more and more documents are transmitted over internet, digital signatures are essential part of the legal as well as the financial transition.

It not only provides the authentication of a person and the validation of the document; it also prevents the denial or agreement at a later stage.

Suppose a shareholder instructs the broker via email to sell the share at the current price. After the completion of the transaction, by any chance, the shareholder reclaims the shares by claiming the email to be forge or bogus. To prevent these unpleasant situations, the digital signatures are used.

5.0.5 FIREWALLS

It is a hardware/software which acts as a shield between an organization's network and the internet and protects it from the threats like virus, malware, hackers, etc.

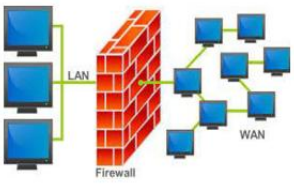
It can be used to limit the persons who can have access to your network and send information to you.

There are two types of traffic in an organization viz. inbound traffic and outbound traffic. Using firewall, it is possible to configure and monitor the traffic of the ports.

Only the packets from trusted source address can enter the organization's network and the sources which are blacklisted and unauthorized address are denied access to the network.

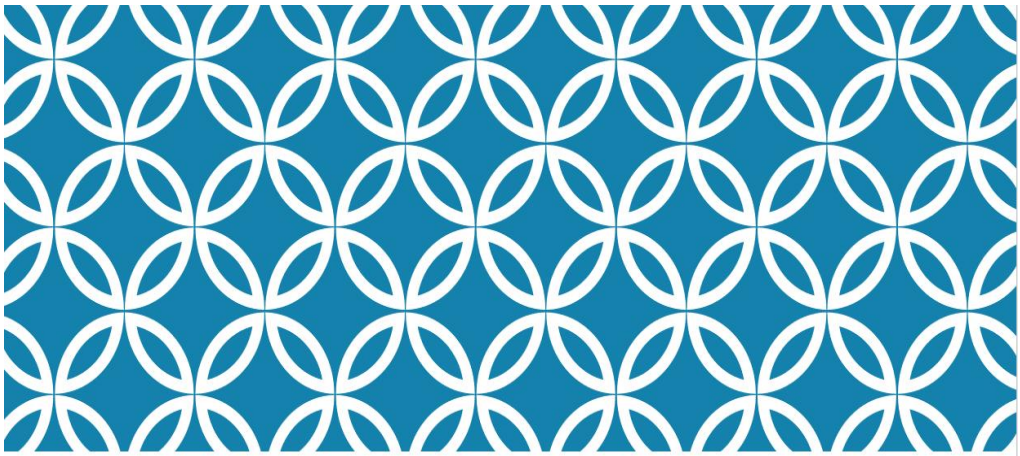
It is important to have firewalls to prevent the network from unauthorized access, but firewall does not guarantee this until and unless it is configured correctly.

A firewall can be implemented using hardware as well as software or the combination of both.



Hardware Firewalls: example of hardware firewalls are routers through which the network is connected to the network outside the organization i.e. Internet.

Software Firewalls: These firewalls are installed and installed on the server and client machines and it acts as a gateway to the organizations‟ network.



CYBER SECURITY

Module 6: Social Media Overview and Security

6.6 SECURITY ISSUES RELATED TO SOCIAL MEDIA

Social media platforms have revolutionized communication, connecting individuals globally. However, they also pose significant security risks. Here are some key issues:

1. **Privacy Concerns:** Social media often requires personal information for account creation. Users may unintentionally disclose sensitive data, leading to identity theft, stalking, or harassment.
2. **Data Breaches:** Cyber attackers target social media platforms to access user data, including login credentials, personal details, and private messages. These breaches can result in widespread identity theft and financial loss.
3. **Phishing Attacks:** Malicious actors use social media to execute phishing attacks, tricking users into revealing personal information or clicking on harmful links that install malware.
4. **Fake Accounts and Impersonation:** Fraudulent profiles impersonating real users or organizations deceive individuals. This can lead to reputational damage or financial scams.
5. **Cyberbullying:** Social media enables anonymous or semi-anonymous communication, fostering cyberbullying, harassment, and hate speech.
6. **Misinformation and Fake News:** False information can spread rapidly on social media platforms, influencing opinions, and causing societal discord.

Appendix 2: Interview Questions

General questions

1. What are the key cybersecurity concepts that business users must absolutely understand?
2. How important is cybersecurity training for non-technical business users in today's digital environment?
3. What common cybersecurity risks do business users typically underestimate?

Questions related to course

4. What factors should be considered when designing a cybersecurity course specifically for business users (versus technical staff)?
5. How should the course be structured to keep business users engaged and motivated to complete it?
6. What methods (e.g., case studies, simulations, gamification) do you recommend to make the learning experience more impactful?
7. What are the free certification courses available for the business users?

Questions related to content

8. What are the critical topics that must be included in the curriculum for business users?
9. How to balance technical depth with accessibility so business users don't feel overwhelmed?
10. Should real-world examples of cybersecurity breaches be part of the course content? Why or why not?

Questions related to user challenges

11. What are the main challenges in getting business users to prioritize cybersecurity learning?
12. How would you recommend handling resistance or lack of interest from users?
13. How often should the course content be updated to stay relevant?
14. What common mistakes should be avoided when designing and launching such a course?

Appendix 3: The Statement on the Use of AI in This Thesis

WRITTEN STATEMENT
on the use of AI-based tools in this thesis

by Shreyabahen Naik, the student of BI Master's Degree Programme

Thesis title : Developing and Launching a Cybersecurity Course for Business Users

According to the "Guidance for addressing the use of AI-based tools in studies at Metropolia Business School (for written submissions)" from August 2023, I make this statement on the use of AI-based tools in my submitted Master's thesis.

1. Which AI-based large language models or other AI-based tools I used
ChatGPT and Grammarly

2. In which parts of the thesis which tools were used, and for which tasks
- ChatGPT for understanding, meaning, definitions and processes.
- Grammarly for checking any grammar and spelling mistakes.

3. What portion of the text was helped with these tools, for each use
- ChatGPT was used to understand processes, vocabularies and certain definitions meanings.
- Grammarly was used to find and correct vocab, spelling and grammar errors.

4. Which prompts were asked, exactly (please indicate the page number in the text where used)
- ChatGPT was used in chapter 3 (pages 14 to 20), chapter 4 (pages 36 to 41, 44 to 47) and chapter 5 (pages 57 to 60).
- Grammarly was used in the whole document to find spelling and grammar mistakes.

5. Here, I describe what continues an ethical and reliable use of AI-based tools that I used
I used the AI for understanding terminology, processes, definitions and as well as to check spelling and grammar mistakes.

6. Here, I describe how ethically and reliably I used the AI-based tools in my thesis submission
AI based tools in my thesis submission was used to understand the terminologies and to improve overall document in accordance with study guidelines.

This written statement makes part of my thesis and is done to help in evaluation an assessment.

17.06.2025

(Date and Place)

Shreyabahen Naik

(Signature)