Developing Cybersecurity Awareness: A case study on Enhancing Employee Training in a Marine Manufacturing SME

Niroj Chaulagain

2025 Laurea

Laurea University of Applied Sciences

Developing Cybersecurity Awareness: A case study on Enhancing Employee Training in a Marine Manufacturing SME

Niroj Chaulagain
BIT, Cybersecurity
Thesis
May, 2025

Laurea University of Applied Sciences **Abstract**

Degree Programme in BIT, Cybersecurity

Bachelor's Degree

Niroj Chaulagain

Developing Cybersecurity Awareness: A case study on Enhancing Employee Training in a Marine Manufacturing SME

Year 2025 Number of pages 39

The objective of this thesis project was to develop and implement a cybersecurity awareness training programme tailored to employees at Oceanvolt, a marine manufacturing SME. Commissioned by Oceanvolt, the project aimed to identify existing knowledge gaps and develop a comprehensive training solution designed to enhance cybersecurity awareness in employees.

The development task involved designing a practical, evidence-based training session obtained from the internal survey. The theoretical framework was based on NIST Cybersecurity Framework (CSF) 2.0 and the ADDIE instructional design model, which provided structured guidance for analysing needs, designing content and evaluating impact.

The research utilized mixed-methods approach, first by baselining cybersecurity awareness through the survey and then, through the design and delivery of a one-session live training including interactive demonstrations. A post training survey and qualitative feedback were then used to evaluate effectiveness.

Key findings showed that employees demonstrated strong individual cybersecurity behaviours in some respects. However, awareness of governance roles, recovery procedure, and formal security policy were limited. The training session significantly improved confidence and perceived relevance, as shown by the post training survey. Open feedback revealed strong employee engagement, calls for more company-specific context and support for monthly refreshers. The executive leadership requested the development of formal cybersecurity policy immediately following the session.

The thesis concludes that even a short, practical targeted training initiative supported by leadership and based on real-world context can enhance cybersecurity culture and procedural change within an SME.

Keywords: cybersecurity awareness, NIST CSF, ADDIE Model, marine manufacturing, SME cybersecurity

Contents

1 Introduction

With digital transformation, organizations and consumers entrust sensitive information to digital systems making the need for cybersecurity greater than ever. Cybersecurity means protecting data, networks and connected systems from attacks using tools, processes or behaviour. Despite technology being the backbone, the effectiveness of cybersecurity relies on people. It is often negligence, human error or lack of knowledge in the field that create vulnerabilities which cybercriminals use for exploitation. (Fortinet n.d.)

The technology has advanced rapidly, and businesses are increasingly using new technologies to stay competitive in the market. Advanced cyber threats, integration of Artificial Intelligence (AI) and Machine Learning (ML), concerns in cloud security, vulnerabilities in Internet of Things (IoT) and smart devices and shortage of skilled cybersecurity professionals pose a significant challenge in the cybersecurity space. The threats are also evolving making it difficult to adhere to regulatory framework leading gaps in compliance requirements. (Admass, Munaye & Diro 2024)

Cyber criminals target enterprises of all sizes, including micro, small and medium enterprises (SMEs). SMEs are enterprises that employ less than 250 people and the annual turnover not exceeding EUR 50 million, and/or annual balance sheet total not exceeding EUR 43 million (EUROPA n.d.).

According to ENISA (2021), SMEs represent 99% of all businesses in the EU employing millions of people and accounting half of Europe’s GDP. In a survey carried out by ENISA (2024), 90% of respondents stated that the cybersecurity issues would have adverse effect on their business within a week where 57% respondents stated that their company would be bankrupt or out of business. Cybersecurity has become a primary focus for organizations of all sizes whether large or small with 35% of small organizations reporting insufficient preparedness. (World Economic Forum 2025). With the rise of technology, AI driven social engineering attacks are also increasing, posing significant threat to both individual and organizations (Yu et al. 2024).

Marine manufacturing SMEs use operational technology (OT) together with Information technology (IT) systems. It facilitates complex attack surface. Businesses rely heavily on technology, and with evolving threats, organizations are exposed to increased number of cyber threats and security breaches (Tolossa 2023).

1.1 Problem Statement

With the increasing use of digital tools such as cloud storage, and different machinery connected to the internet, companies are facing cybersecurity threats that can disrupt operations or harm the sensitive information (ENISA 2021). Unlike larger enterprises, SMEs don't usually have a dedicated IT or security staff to protect systems and data (Rombaldo, Becker and Johnson 2023). The employees may not know the risks involved in their everyday actions such as sharing passwords, opening an attachment from email, using public Wi-Fi, or accessing customer information.

The lack of formal training in cybersecurity, missing cybersecurity policies and guidance create gaps in the cybersecurity practices. These gaps may be exploited by the cybercriminals resulting to the exposure of proprietary designs, customer data and other critical information. Without determining the current level of cybersecurity awareness, it is difficult to design a training program to address the critical cybersecurity parts. (Rombaldo et al. 2023)

1.2 Research Goal and Objectives

The primary goal of this thesis is to enhance cybersecurity awareness among employees in a marine manufacturing SME by baselining, developing, delivering and evaluating a structured cybersecurity training program. To achieve this, different objectives are set. The first objective is to determine current levels of cybersecurity awareness within the company through questionnaires. The second objective is to identify key gaps using the data collected from the questionnaire. The third objective is to develop tailored training materials suitable for the employees to bridge the identified gaps and the last objective is to implement the training and measure short-term results.

To achieve the objectives and ultimately the research goal, following research questions are formulated.

- What is the current level of awareness in cybersecurity among the employees in the SME?
- How does the tailored training program help employees understand the cybersecurity threats?
- To what extent does the training program help to impact employee behaviour in short term?

1.3 Significance, Scope and Limitations of the Study

This thesis uses real experiences from the employees to address the issue of employee cybersecurity awareness within a marine manufacturing company through a case study. It helps in creating a simple and repeatable model. It helps SMEs increase awareness and strengthen security without much need of technical resources where budget and time are limited.

The thesis focuses on employees at single marine manufacturing SME with 20 employees. It uses questionnaire mapped to NIST Cybersecurity Framework (CSF) 2.0 for baselining and measuring awareness. Additionally, the thesis also develops simple training materials based on the identified gaps.

Since the thesis is based on a particular marine manufacturing SME, the results may not apply to larger companies or other industries. Additionally, the case company does not have a dedicated security team, and hence, the thesis focuses more on basic awareness and not the advanced practices. The data is also self-reported and can include inaccuracies or bias.

2 Overview of Cybersecurity- Challenges, Risks and Human Factor

This chapter introduces the fundamentals of cybersecurity and the hurdles that SMEs face in achieving confidentiality, integrity, and availability. It then charts sector specific risks in marine and manufacturing operations. Finally, it shows how human factor can widen the cybersecurity gap.

2.1 Cybersecurity and Cybersecurity Challenges in SMEs

Cybersecurity refers to the practice of protecting mobile devices, computers, servers, and data from unauthorized access or digital attacks. Cybersecurity is a continuously evolving discipline, where nature of threats changes with the technological advancement. Every business operation and personal pursuit leaves digital footprint and no matter what profession one is in, cybersecurity plays crucial role. (Cybellium 2023)

Most of the cybersecurity goals of companies are based on 3 pillars - Confidentiality, Integrity and Availability- the CIA Triad. Confidentiality aims at protecting information leaking to unauthorized recipients. Integrity aims at protecting the integrity of data from corruption or unauthorized changes. Availability aims at making information available to the authorized recipients. Adding authentication and non-repudiation to the CIA Triad makes the pillar stronger. Authentication is a mechanism for the verification of identity of a human or system

before access is granted. Non-repudiation makes sure that there is no denial of involvement of the both ends. (Raggad 2010)

To understand cybersecurity, it is essential to understand different types of cyber threats which includes and is not limited to malware, phishing, Man in the Middle (MitM) attack, Denial of Service (DoS), Distributed Denial of Service (DDoS), SQL injection, zero-day attack and AI-powered attacks. Malware includes malicious software comprising of spyware, viruses, worms and ransomware. Malware is installed through attachments or dangerous link or unsecured websites. (Cybellium 2023)

Phishing involves sending fraudulent communications through emails that appear to be from a credible source. The goal of phishing is to get sensitive information or installing malware to the victim's device. DoS occur when a legitimate user cannot use the resource when needed by disrupting the services. SQL Injection or Cross site scripting (XSS) occur when commands are sent to the system by exploiting the vulnerability of the program. Legitimate command is used to get unauthorized access to the database or system. Similarly, zero day attack occurs when there is vulnerability, and no known patch is available to fix the vulnerability. (Cybellium 2023)

AI powered cyberattacks are also evolving where attackers carry out high-impact assaults using the AI tools. Automated phishing, ransomware and different campaigns on misinformation are carried out using the AI tools and technologies such as deep fake.(Arif, Khan and Khan 2024)

The financial impact of cyber incidents on companies extends well beyond the immediate costs associated with data breaches or ransom payments. In long term, these incidents can lead to a significant loss of customer trust which is often difficult to regain. The organizations may face legal penalties and regulatory fines and damage to the reputation affecting customer loyalty and brand perceptions. The resources needed for recovery and incident response can also be substantial. (Edwards 2024)

Due to the financial limitations, lack of internal expertise or time constraints, lack of suitable guidance, online transition and low support from the management, SMEs are uniquely vulnerable to cyber threats (ENISA 2021). According to Rombaldo et al. (2023), SMEs' maturity is often low compared to the larger organizations because they are "unaware, unfunded and uneducated." The authors mentioned that SME owners do not prioritize cybersecurity as they often think they are not the likely targets of the cyberattacks. This reactive mindset instead of initiative-taking mindset make SMEs prime targets for phishing, ransomware or supply chain attacks topped with untrained staff and poor incident response capabilities.

Rombaldo et al (2023) also highlighted the root cause for cybersecurity failures in SME is due to literacy gap which affects decision making and daily operations. With limited budget and other technical constraints within the SMEs, resilience could drastically improve from cybersecurity awareness training that are tailored to specific industry and specific enterprise based on popular framework such as NIST CSF 2.0.

2.2 Cybersecurity Risks in Manufacturing Sector

A study conducted by Kannus and Ilvonen (2018) using Delphi approach pointed out the top priorities in the manufacturing industry in terms of cybersecurity. This includes IoT and security where the use of IoT create new attack surface. It also includes digitization and industrial automation where legacy systems are integrated to modern IT stacks leaving legacy devices vulnerable. Besides this, the other priorities included human-factor gaps and workforce cybersecurity strengthening. (Kannus and Ilvonen 2018)

Johansson, Paulsson, Bergström and Seigerroth (2022) explored cybersecurity awareness among SMEs in the manufacturing industry and how cybersecurity training could be implemented. The recommendations to manufacturing sector included the use of contextualized information, delivery of training materials in modules that are small, focused and contained. They also suggested repeating critical topics through various approach to avoid low motivation in learning cybersecurity.

2.3 Cyber Threat Landscape in Marine Industry

Ships, yachts, and boats are increasingly getting interconnected embracing the digitization. This brings in new cyber risk vectors. Bolbot, Kulkarni, Brunou, Banda and Musharraf (2022) highlighted several key challenges in the marine industry. Device and system heterogeneity is one of it. With the use of decade old operational technology equipment connected with modern IoT devices, the lack of standardization makes it extremely difficult for secure integration and patch management. Human factor and training gaps are other challenges. Crew members lack cyber security training or even if they do, it is minimal. Lack of standardized risk assessment and benchmarking is another challenge. Risk levels comparison is difficult with no standardized risk assessment or when benchmarking is not available. Other challenges include security monitoring and detection gaps and cyber-physical resilience (Bolbot et al. 2022).

According to the 2023 Cyber Trends and Insights in Marine Environment report published by U.S. Coast Guard Cyber Command (no date) ransomware, advanced persistent threats (APTs), OT vulnerabilities, phishing and spoofing, Denial-of-Service (DoS) and persistent basic hygiene gaps are the cyber threats in marine environment. On top of that, supply chain, third-party risks and internet facing system exploits are also leading cyber threats. Phishing or spoofing

accounted for 22 percent of reported incident leading to credentials harvesting or executing malicious payloads. The report mentioned increase of ransomware incidents by 80 percent form 2022 and disrupting operations for longer period by using partial encryption. The report also highlighted the supply chain risks where cybercriminals target technology service providers and exploit vendor managed systems to gain access to critical networks.

2.4 Human Factors in Cybersecurity

Human factor constitutes a significant role in cybersecurity. According to Cano and Jeimy (2019) security executive and leaders do not fully understand how people think and act. Even with security procedures and technical efforts, people remain on front line in exposing organizations to vulnerabilities. To understand the human side of data security, following rules and professional standards are not enough. It is more about diving deeper to understand how people think and work. Cano and Jeimy (2019) also mentioned that cybersecurity awareness approach often leads to frustration if carried out without recognising where people are vulnerable and without understanding how they work. Instead of considering people as the “weak link”, they should be valuable part of the solution (Cano and Jeimy 2019).

A study conducted by Pollini et al. (2022) found that security procedures are too complex and don’t help employees’ daily tasks. Even if people know the rules, the organization’s security culture can expose organization to human vulnerabilities. The study emphasized on considering what user are trying to accomplish and how security can help achieve those goals.

Przymus, Malagocka and Przybyszewski (2024) identified individual behaviour to be the key to improve cybersecurity especially in remote work settings. The authors also developed a diagnostic tool for identification of different cyber risk profiles. They mentioned that only rules are not enough since behaviours are shaped attitudes, habits and working environment. Instead of following generic protocol, threats should be managed such that it fits their actual work (Przymus et al. 2024).

3 Training Methods and Frameworks for Cybersecurity Awareness

The focus on this chapter will be on training methods utilized in cybersecurity awareness programs, their effectiveness, and challenges. Additionally, NIST CSF 2.0 and ADDIE model, which provide structured approaches to developing and delivering comprehensive training initiative will be discussed.

3.1 Overview of Current Cybersecurity Training Methods

Prümmer, Vaan Steen and Van Den Berg (2024) conducted a comprehensive systemic review of 142 articles on training methods and identified several common approaches for training. It included traditional methods, gamified training, simulation-based training, and training using emerging technologies. Traditional methods of training include lectures, web-based modules and briefings. Gamified training approach incorporates gaming elements for higher engagement with technique like capture the flag (CTF) to gain practical skills. The simulation-based training encompasses realistic scenarios such as phishing simulations and incident response drills. With the advancement of technology, new and emerging technologies such as virtual reality (VR) and augmented Reality (AR) are used for immersive training that offers hands on training but in a controlled environment (Prümmer et al. Den 2024).

Different themes were identified from the study regarding the cybersecurity topics covered by in the training materials. The most common theme was social engineering followed by password safety, workplace safety, malware and WIFI safety. (Prümmer et al. 2024)

3.2 Challenges in Implementing Cyber Training in SME

Challenges in implementing training and awareness programs are present across multiple sectors, not limited to cybersecurity. There are several factors affecting training implementation and awareness program. It includes business environment, social dynamics, legal and ethical issues, organizational issues, economic issues and personal issues. (Aldawood and Skinner 2019)

In a fast paced and competitive business environment where time and resources are limited, awareness training on cybersecurity are often deprioritized against profits and things that have immediate value to productivity. The lack of security-oriented culture within the organization and behaviour from colleagues create challenge on implementing proper cybersecurity training. Employees can neglect training or dismiss threats as unlikely. Similarly, designing a training and making it effective require considering the local privacy laws especially when monitoring or simulating cyberattacks. Inconsistent policies or lack of leadership support create organizational challenges. Moreover, limited financial resources and personal challenges such as motivation or attitude towards security also cause hindrance to the effective implementation of cybersecurity training in an organization. (Aldawood & Skinner 2019)

3.3 NIST Cyber Security Framework 2.0

NIST CSF is one of the important frameworks to reduce and manage risks within the organization irrespective of size and sectors. The framework provides as a reference to all

organizations such as nonprofit, government, industry, and academia. The implementation might vary depending upon the organization, risk appetites and tolerances, and organizational goals and missions.(NIST 2024)

With evolving threats, NIST updated its CSF to version 2.0 from 1.0 in 2023, providing a through guideline for organizations including maritime industry. It is a voluntary framework that includes standards, guidelines and best practices for systematic management and reduction of cyber risk. The core functions include Identify, Protect, Detect, Respond and Recover along with newly integrated Govern function as shown in figure 1. The outcomes from the functions - identify, protect, detect and govern help in prevention and preparation for the incidents. Respond and recover together with govern help in discovery and management of incidents. (Edwards 2024)

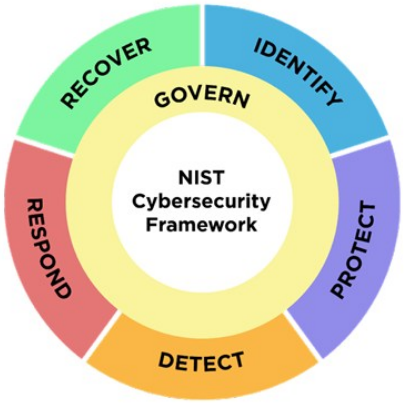


Figure 1 NIST CSF Functions (NIST 2024)

Govern: This function focuses on clear cybersecurity roles and responsibilities, procedures and policies while complying with applicable laws and regulations (NIST 2024). For marine manufacturers, defining roles and responsibilities clearly from executives to the engineers to production workers help attain robust governance while ensuring compliance with marine specific cybersecurity standards and regulations. With governance, risks across production processes, product lifecycle management and supply chains are addressed proactively.

Identify: This function helps organizations fully understand their cybersecurity risks. It is necessary for effective cybersecurity management. At this stage the organizational assets whether hardware, software, or people are identified including vulnerabilities in embedded systems, communication interfaces or third-party components. A thorough asset inventories and potential threat vectors mapped to the assets help assess the current situation and prioritize resources effectively. (Edwards 2024)

Protect: Protect function focuses on implementing safeguards such as and not limited to secure coding practices, access controls and encrypted communications for minimal impact during cyber incidents. It covers wide range of activities from Identity and Access Management (IAM) to data encryption and maintaining security technologies. Employee training and awareness also falls under protect as human factors are critical in maintaining secure environment. (Edwards 2024)

Detect: The detect function is important to promptly identify cyber security events. Since no defence is full proof, continuous monitoring and detection processes are crucial for identification and mitigation of threats. A real time monitoring of network and systems for vulnerabilities, anomalies, or incidents help organizations to detect and address cyber threats. (Edwards 2024)

Respond: A response process requires structured and planned approach. It helps containing and mitigating the impact in the event of cybersecurity incident. The respond function in the CSF includes incident management planning, root cause analysis, communication strategies, and coordination procedure with related bodies and experts on the field. It also includes preservation of evidence and implementing improvements from the lessons learned. (Edwards 2024)

Recover: The last core function on the NIST CSF is recover. It focuses on restoring functionalities and services affected by the cybersecurity incident. This encompasses recovery planning along with proper communications with the internal and external stakeholders, building resilience and proactively prepare for future incidents. (Edwards 2024)

The thesis uses NIST CSF 2.0 as a reference to employ a questionnaire based on its core functions which provides structured method to assess cybersecurity awareness among the employees of a marine SME. This helps in identifying awareness gaps as well as providing clear analysis and comparison supporting marine manufacturing SME to improve cybersecurity resilience and reduce operational risks.

3.4 ADDIE Model for Developing Cybersecurity Training

The ADDIE Model comprises of five different phases – Analyse, Design, Develop, Implement, and Evaluate as shown in Figure 2. Each phase is linked with evaluate phase as evaluation is done in each phase. It is one of the widely used frameworks in organizations for instructional design. According to Branch (2009), the ADDIE framework provides a systematic approach to developing effective training programs by aligning instructional strategies, learning needs, content delivery and assessment. The flexibility of this framework allows it to be used for every industry for concrete results. This includes healthcare sector, aviation as well as cybersecurity in marine industry.

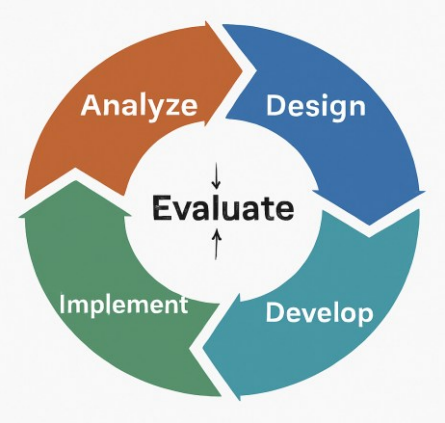


Figure 2: ADDIE Model

Analyse: The first phase is analysing phase where identification of problem begins by defining learning environments and assessing current knowledge levels (Branch 2009). In the marine environment, it involves understanding current level of cybersecurity understanding and identifying cyber risks from executive level to production worker. This aligns well with Identify and Govern functions of the NIST CSF 2.0.

Design and Development The design phase focuses on learning experiences and structuring it. At this phase learning objectives are defined, and instructional contents are sequenced. The delivery methods are selected together with the strategies for assessment. In terms of cybersecurity awareness training, the design decisions may include contents aligned with NIST CSF modules and selecting whether to conduct in-person workshops or incorporating adult learning principles. It is also important to consider learners' motivation and practical applications as mentioned by Branch (2009). During the development phase, assets and materials described in design phase are brought to life by creating learning materials. The materials developed should be relevant. Branch (2009) suggests using visual cues and real-world scenarios for higher effectivity.

Implementation and Evaluation: Once the learning materials are developed, the delivery of training program is implemented. At this phase, instructor must ensure that learners understand the contents and achieve the learning objectives. The revised version of ADDIE framework presents evaluation as a continuous process taking place at each phase. This helps in continuous improvement in quality by evaluating each phase against the requirements (Branch 2009). At this phase effectiveness of training is evaluated in both formative and summative ways.

A detailed study conducted by Pears and Konstantinidis (2021), ADDIE model was effectively applied in healthcare sector for cybersecurity awareness. The study focused on the human element in cybersecurity. It revealed the increased confidence and awareness against cyber

threats tailored to frontline staff based on ADDIE model. It made the use of both analytical decision-making models and rule-based model for the participants to detect and respond to cyber threats. Despite moderate increase in knowledge, the authors noted that confidence grew significantly even with short-format and well-structured workshops.

4 Research Methodology

This study adopts a mix of quantitative case study approach followed by applied research to investigate and enhance cybersecurity awareness in a marine manufacturing SME. The use of this mixed approach not only gives a deeper understanding of the cybersecurity culture within the case organization but also contributes a practical training solution aimed at improving employees' awareness level against digital threats.

4.1 Case Study Research

The first part of this thesis adopts case study methodology to explore the development and impact of cybersecurity awareness in a marine manufacturing SME. As described by Yin (2017), case study is a research methodology used in exploring specific, contemporary issue in detail. This is particularly conducted when the issue is interconnected to the setting in which it takes place. Case study is most appropriate when understanding complex interactions in real-life situations is the prime goal.

The study investigates the level of cybersecurity awareness among employees within a single marine SME. It focuses on the interconnected aspects of organizational culture and operational structure. The research is limited to the timeframe of the security awareness training project. Individual employees are the unit of analysis, and their knowledge and skills were assessed using structured questionnaire before and after the training. This makes case study approach particularly suitable for this research.

4.2 Applied Research

The latter part of the study followed an applied research approach aiming to develop a practical solution for a marine manufacturing SME – improving cybersecurity awareness in employees. According to Creswell (2014), applied research is problem driven and solution oriented with practical application bridging academic understanding with the real world impact.

For this study, the research did not only observe current practices but actively intervened by designing, implementing, and evaluating a cybersecurity training program tailored to the SME. The training program was designed to address the issues identified using the cybersecurity

assessment mapped to the NIST CSF 2.0 where the research aligned with the organization's internal goals of reducing risk and strengthening digital resilience in every department. The training was developed using ADDIE instructional model.

4.3 Theoretical Framework

This study included two major frameworks: NIST CSF 2.0 and ADDIE instructional design model. These frameworks provided the structural and pedagogical basis for both identification of cybersecurity awareness needs and design of effective training within the marine SME context.

The NIST CSF 2.0 was used to baseline cybersecurity posture of the SME through questionnaire based on the core functions of the framework including Govern, identify, protect, detect, respond, and recover. This allowed to assess the key areas of organizational risks to be systematically addressed. In parallel, the training was developed using ADDIE model for effective instructional materials. The training considered the non-technical audience in the SME.

4.4 Participant Profile

The participants in this study included employees from Oceanvolt Oy, a marine manufacturing SME. All the departments were included, consisting of production, sales and marketing, logistics and operations, product development, accounting, and executive leadership. This ensured comprehensive exposure to cybersecurity awareness across multiple domains.

Production employees included those working in hands-on manufacturing and assembly. Sales and marketing employees manage external communications and client data; logistics and operations employees are responsible for handling supply chain. The product development team included employees working with software integration, design, and electronics.

A total number of 14 employees answered the baseline survey and 16 employees attended the training. 13 employees answered the post survey. The questionnaire and feedback form were anonymized, and no personally identifiable information were registered, keeping privacy in mind.

4.5 Data Collection Methods and Timeline

This study utilized two primary instruments for data collection. The first one was cybersecurity awareness questionnaire, and the second one was post-training feedback form. Both were administered at different stages of the training process. Figure 3 represents the

timeline of key steps performed during the thesis project.

Figure 3: Key steps during the project

The thesis project commenced with a background study during the first week, followed by the administration of a baseline survey in the second week. In the third week, the collected data were analysed, and training materials were developed in the fourth week. Finally, in the fifth week, training was delivered, and a post survey was conducted. The results of the post-survey were subsequently analysed.

4.5.1 Cybersecurity Awareness Questionnaire

A 43-item questionnaire was developed based on the core functions of NIST Cybersecurity Framework 2.0. It included yes/No questions, Likert-scale question (1 = Strongly Disagree to 6 = Strongly Agree) and open-ended questions. A scale of 1-6 was intentionally implemented for Likert-scale question to eliminate the possibility of neutral responses. It helped in receiving definitive answers and assessing the awareness level effectively.

The analysis of the 43 questions revealed a specific distribution across various functions. The “govern” function included 3 questions, the “identify” function had 8 questions, the “protect” function had 9 questions, the “detect” function featured 7 questions, the “respond” function contained 5 questions and the “recover” function included 4 questions. Additionally, there were 5 questions on company culture and training along with 3 open ended questions.

4.5.2 Post-training survey form

For the evaluation of cybersecurity awareness training, a post-training survey was administered at the end of the session. The goal was to measure changes in participants’ understanding and perceptions of key topics addressed during the training. The contents were social engineering, password practices, identifying secure websites, and personal responsibility for cybersecurity.

Topics such as governance, incident recovery procedures, were intentionally excluded as these require long-term structural interventions. They were not addressed directly in the

training content. However, importance of these were repeated multiple times during the session. The survey included a combination of open and closed ended questions. The intention was not to measure comprehensive organisational change but to assess immediate knowledge strengthening and clarity of training content. There were 10 questions on the post training survey with 7 closed ended and 3 open ended.

4.6 Data Analysis

The closed-ended survey responses were analysed using descriptive statistics. Likert-scale questions (rated from 1 = Strongly Disagree to 6 = Strongly Agree) were averaged to produce a mean score per question mapped to each domain of the NIST CSF 2.0. For consistent interpretation across all items, percentage-of-ideal score was calculated. The maximum value being 6, the scores were normalized into percentage for uniform comparison. The percentage of ideal score was calculated as follows:

$$\% \text{ of Ideal} = (\text{Mean Score} \div 6) \times 100$$

Binary (Yes/No) questions were excluded from the calculation of percentage of ideal to obtain consistent scale. Those items were analysed separately using frequency counts and the percentage of respondents answering ‘Yes.’ A selection of key questions was visualised using response distribution graphs to demonstrate how responses were spread across the scale.

4.7 Training Development Process

The development of the cybersecurity awareness training programme followed the ADDIE instructional design model. This model was chosen because of its suitability for both structured institutional training and rapid development cycles. The analysis phase used the survey results to identify critical knowledge gaps, which helped in designing the training content. Key topics were selected based on both quantitative and qualitative findings, including and not limited to governance, credential management and social engineering risks.

During the development phase, Google Slide was used for the creation of training materials supported by real-time hands-on demonstrations built in a controlled test environment. Demonstrations were chosen to increase engagement and show practical impact. Some of the demonstrations included credential harvesting via phishing using Social Engineering Toolkit, session hijacking, website spoofing and identification of secure and insecure websites. The demonstration was built using openly available tools and ensured no real systems or data were compromised.

4.8 Training Implementation

Due to the time constraints of the thesis project, the training was implemented as a single instructor led session with hands on demonstration and discussion. The session was conducted in person and lasted approximately one and a half hour.

The session included brief introduction, instructional slides covering core concepts, live demonstrations, discussions, and Q&A at the end. Attendance was voluntary, but it was supported by the management to encourage full participation. A follow-up survey was administered immediately after the session to measure changes in cybersecurity awareness and gather feedback on training content and delivery.

4.9 Ethical Considerations

The research was conducted adhering to the established ethical principles. It included implied consent, data confidentiality and risk minimization. A research permission was obtained from the workplace instructor.

Implied Consent: The employees were informed about the purpose of the study, nature of their involvement and data to be collected. The consent was obtained at the point of data collection through the first page of the questionnaire. It included a clear explanation of the study's purpose, and how data would be used. The participants were explicitly informed that no personally identifiable information was collected. They could proceed to the research only if they consented to it. Since, the use case was low risk and the questionnaire was anonymous, implied consent was used.

Anonymity and Confidentiality: The only data collected were through google forms and all were anonymous as it did not include any personal information such as names, job titles or contact information, or email addresses. The completed forms were stored securely in company's google drive.

Use of results and data retention: The results of the study will be used solely for academic purposes as a part of bachelor's thesis and for internal awareness on cybersecurity. All data will be retained securely 1 month following the thesis submission after which it will be deleted permanently. The exception is for the training material, policy drafts, and internal wiki which will be handed to the case company for further use.

4.10 Limitations of the Methodology

The study was conducted considering time and organizational constraints. The research was limited to a single marine manufacturing SME which restricts the generalizability of the findings. Although the case study approach allowed contextual insight, it did not represent

the broader industry. The results may, hence useful for similar SMEs but not for all marine-based businesses.

Due to the time constraints, the study mostly relied on quantitative and qualitative data. The data was collected through structured open and closed ended questionnaires. It did not consider data such as interviews or focus groups. The pre-training data showed low awareness in certain areas, but the study did not gather deeper insights or how employees perceive cybersecurity in practice. The post-training data measured immediate learning rather than long term behavioural change.

5 Pre-Findings

This chapter presents the analysis of the responses to the cyber security awareness survey. The instruments and its structure were described earlier in Methodology section. To briefly reiterate, the survey was designed aligning with the NIST CSF 2.0 that included 43 questions out of which 40 were closed-ended (using Likert-scale 1-6 and Yes/No format) and three were open-ended. These questions were distributed across key CSF domains including govern, identify, protect, detect, respond, and recover. It also included questions on workplace culture and training.

The data presented here builds on the existing framework. It highlights areas of high awareness and identifies critical gaps. Normalized scores are used to facilitate comparisons across different domains and response types to understand the overall landscape.

5.1 Overall Awareness Levels

Domain-Level Scores: Mean scores for each NIST core functions along with Culture and Training are summarized in table 1 and visualized in figure 4. Only Likert-scale items from the questionnaire are selected and Yes/No format are excluded from mean calculations. These excluded questions are separately analysed in following section.

Table 1 Mean scores and percentage of ideal for different domain

Domain	**Mean (/6)**	**% of Ideal**	**Interpretation**
Govern	1.96	32.7%	Critically Weak
Identify	4.63	77.2%	Moderate

Detect	4.67	77.8%	Moderate-Strong
Protect	4.79	79.8%	Moderate-Strong
Respond	4.11	68.5%	Weak-Moderate
Recover	2.86	47.7%	Very Weak
Culture & Training	3.40	56.7%	Weak

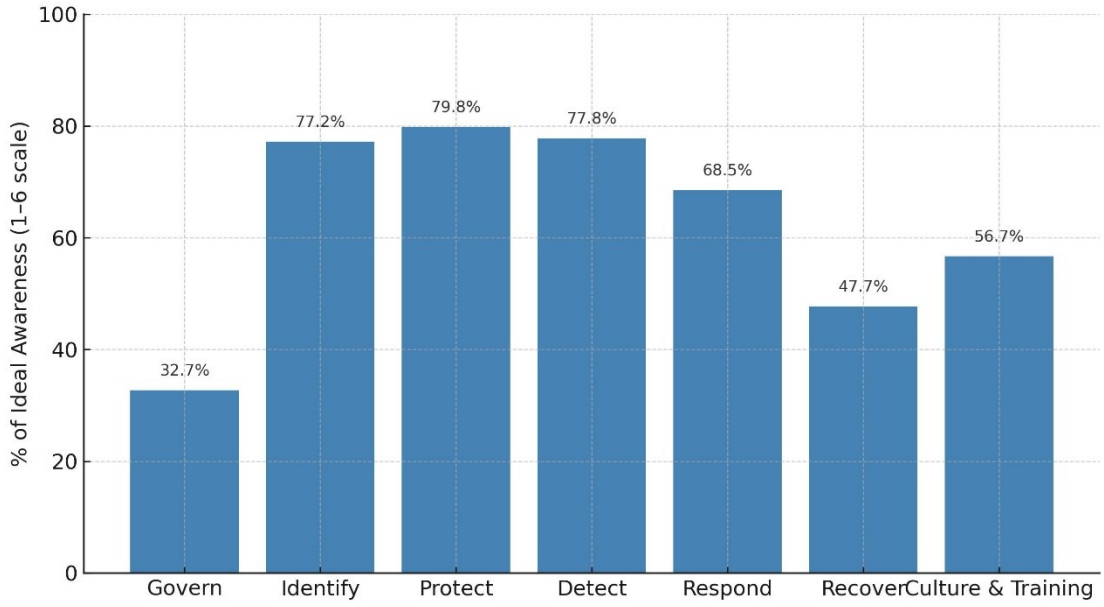


Figure 4: Cybersecurity Awareness by Domain

Figure 4 shows the comparative maturity across domains. The employees demonstrated strongest behaviour in Protect and Detect functions while Govern and Recover showed the lowest levels of awareness and preparation.

Individual Likert Question Analysis

Each Likert question was individually analysed for its average score and percentage of the maximum possible value. For better illustration of the key results, sample questions are presented with detailed scores and interpretation.

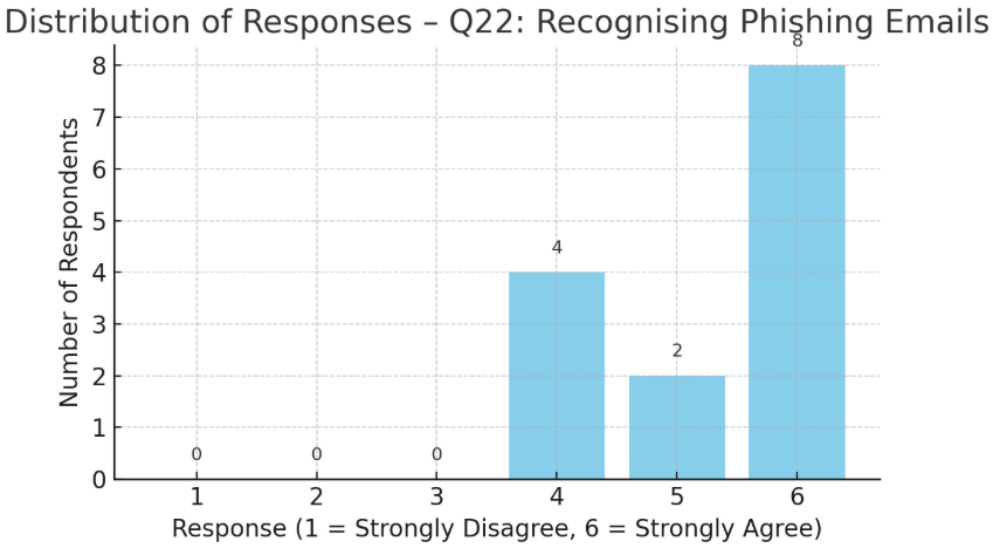


Figure 5: Q22 Distribution of Responses

Question 22, which asked whether employees could identify phishing emails, scored 5.29/6 (88.1% of Ideal). The distribution of responses is shown in figure 5. This indicates very strong awareness of phishing in majority. Similarly, Question 6 which asked the respondents about the understanding of types of information considered sensitive scored 5.5/6 (91.7% of Ideal). This reflects sound data classification knowledge. Question 7 assessed whether employees understood the value of backing up important data. The score was 5.38 out of 6 (89.3%).

On the lower end, question 1- knowledge of who is responsible for cybersecurity in the organization averaged only 1.36/6 (22.7%). Similarly, question 36 asked if employees had received formal training and it scored only 1.14/6 (19%). The response of question 36 is presented in figure 6. This highlights critical areas of weakness particularly on governance, formal training, and familiarity with recovery.

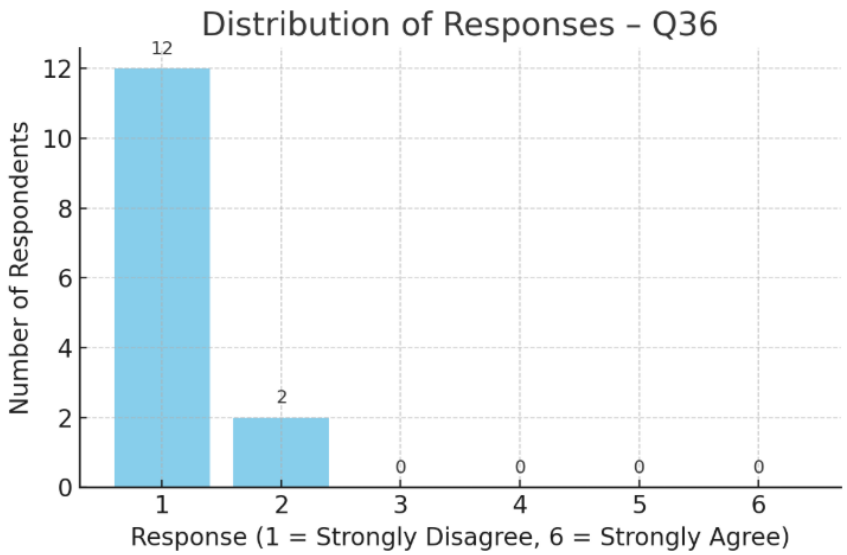


Figure 6: Q36 Distribution of Responses

The result shows that while many employees demonstrate sound personal cybersecurity habits, significant gaps remain in understanding leadership roles and formal training expectations.

Binary (Yes/No) Questions Analysis

Seven yes/no questions were assessed separately and are summarized in Figure 7.

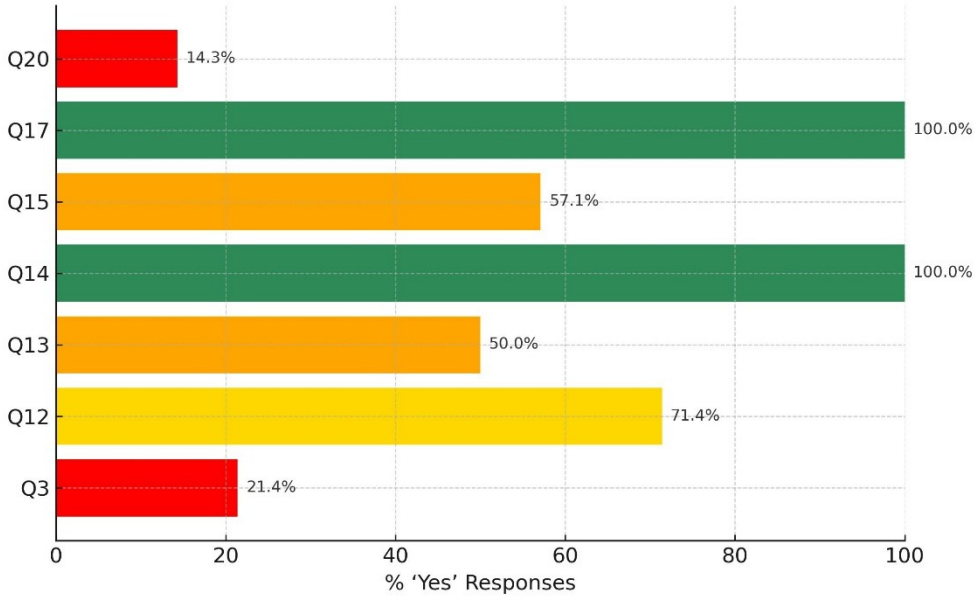


Figure 7: Yes/No Awareness Questions

All respondents indicated they lock their devices when away (Q17). They also understand the risk of sharing passwords (Q14), suggesting strong personal device and credential habits. A majority also reported using strong passwords (Q12). However, only around half (57%) of the respondents use two-factor authentication (Q15) when available. Similarly, 50 percent admitted reusing the same password across different accounts (Q13). Organizational awareness was notably low for policy-related items with just 21.4% of respondents aware of the internal cybersecurity leadership (Q3). Only 14.3% reported awareness of formal procedures for accessing shared devices or cloud services (Q20).

These findings show that while basic habits are good, procedural and governance related knowledge is critically lacking.

5.2 Open-Ended Responses and Thematic Insights

The analysis of open-ended responses provided more context to the quantitative data. The employees voiced a need for visible cybersecurity policies and named contacts for reporting incidents. Some expressed need for documentation on best practices. Several respondents also felt that expectations were not clearly communicated. This contributed to uncertainty in incidents and responses.

Training needs were frequently mentioned. Respondents were calling for short, mandatory and repetitive training sessions, with one respondent mentioning the Hoxhunt platform for cybersecurity training. There was also concern that current cybersecurity culture felt individualized rather than team based. Some said that they relied on personal judgement rather than organizational guidance to determine how to stay secure.

Finally, there were also practical suggestions such as providing VPN subsidies and access to password managers. Other suggestions include better support for updates and software programs used within the company. These responses clearly show that the staffs are willing to engage with cybersecurity more actively if given the tools, structure, and support from the company.

One respondent said, “I think I missed, or at least I have never heard about company security policies or guidelines here”, and another respondent said, “We need policies and training regarding the use of AI.” This shows that the employees are concerned about security guidelines and the implications of using AI tools at work in terms of security.

5.3 Summary of Key Gaps and Implications

The survey findings identify critical vulnerabilities which is presented in table 2 below.

Table 2: Findings from the Survey

Area	Gap Observed	Implication
Governance	Policy ownership unclear, decision-maker unknown	Noncompliance, inconsistent practices
Training	Few have received formal cybersecurity awareness	Low preparedness against threats
Recovery	Uncertainty around incident response and backups	Longer downtime, higher exposure
Access Management	Limited awareness of role-based access, or least privilege principle	Elevated risk of unauthorised access
Personal Credential Hygiene	Password reuse and inconsistent 2FA adoption	Susceptibility to account breaches
Phishing	Majority can detect phishing but still some cannot	Increased vulnerability and potential for data breach

Several critical gaps affecting the organization's cybersecurity posture were identified. Governance practices were unclear. The policy ownership or decision-maker was unknown which may lead to inconsistent practices. Most employees had never received formal training in cybersecurity. This results in low preparedness against common threats. Limited understanding of access management and the principle of least privilege also raised concerns for unauthorised access. Additionally, password reuse and failure to adapt to 2FA makes account susceptible to breaches. While general phishing awareness was generally strong, a small but significant number of employees were still unsure about it.

These findings form the evidence base for the design phase of the cybersecurity awareness program. Training efforts will focus heavily on closing governance, recovery, culture gaps and reinforcing strong individual cybersecurity habits.

6 Training Program Development

To address the cybersecurity gaps identified in Chapter 5, a targeted training programme was developed using the ADDIE instructional design model. The model comprised different phases including Analyse, Design, Develop, Implement, and Evaluate which provided structured framework for creating educational interventions. In the context of this thesis, the training

session was condensed into a single session due to time constraints. The focus was given more to practical demonstrations and direct engagement.

Analyse: The analyse phase was drawn from the findings of the cybersecurity awareness survey. The key areas of concern included the lack of clarity about cybersecurity responsibilities, insufficient training, credential misuse, weak governance, and recovery. Open ended responses further highlighted a demand for short, practical, and relevant training sessions.

Design: The training was designed to directly address the specific awareness gaps revealed by the survey. The session content was aligned with the NIST Cybersecurity Framework domains and structured to combine knowledge with real world relevance. For enhanced engagement, a practical approach was used to demonstrate the risks and techniques associated with:

- Phishing and Credential harvesting using the Social Engineering Toolkit (SET)
- Session Hijacking through cookie-based access
- Website spoofing

The demonstrations were planned to help participants visualize how attacks work and understand indicators of compromise. Besides this, training also included segment of secure password practices, importance of using unique, complex passwords together with two-factor authentication.

The participants were shown how to check if their credentials had been exposed in known breaches using public tools such as HaveIBeenPwned. The session also addressed importance of internal cybersecurity policies, clearly defined roles, escalation procedures and recovery plans.

Develop: The training materials were developed in PowerPoint format that was supported by live demonstration run in a controlled environment. Each topic included a brief explanatory slide followed by walkthrough of simulated cyberattack scenario. The demonstrations were created using publicly available tools with all sensitive content anonymised. The session was designed to be approximately one hour in length. However, it had to be extended to one hour and a half because of active engagement, discussion, participant questions and demonstrations.

At the end of the session, participants were provided with a link to company's internal cybersecurity wiki. The online resource included best practices for password hygiene, phishing detection, secure browsing, use of company resource and more which could be regularly updated as policies and threats evolve.

Implement: The training was delivered in a single session to the available staff members as part of the thesis implementation. The format included brief instruction followed by live demonstration and facilitated discussion. The support from management encouraged attendance and participation. There were 16 participants in total where 12 were present physically and 4 online. The participants were encouraged to ask questions.

Evaluate: The evaluation phase included a post-training survey based on the original diagnostic tool. This was used to measure changes in awareness and gather feedback on the training material, training clarity, and its effectiveness. While the session was limited to one session, the evaluation provided initial insight into the training impact and areas for future training cycles.

The ADDIE model proved adaptable even within constrained timelines. It enabled to develop focused and practical training experience based on real organisational needs.

7 Post-findings

Following the one and a half hour awareness session, employees completed a post-training survey designed to assess changes in cybersecurity confidence and perceived relevance. Out of 16 participants, only 13 answered the survey. The survey used five questions with 6-point Likert scale (1 = Strongly Disagree, 6 = Strongly Agree), one with multiple choice and three open-ended questions.

Figure 8: Average Scores of Training Effectiveness

Quantitative results show a consistently high level of agreement, with most responses in the 5-6 range across all items. Average scores of training effectiveness are presented in figure 8. The highest average score was observed in the understanding of strong passwords and two factor authentication with average score of 5.92. This suggests that the topic aligned well with the participants and was effectively communicated.

Other areas also received strong ratings, including understanding common cybersecurity threats with average score of 5.69. Similarly, clarity and applicability of the cybersecurity and best practices provided during the session received 5.46. The relevance of the training content to their specific roles was also strong with a rating of 5.46 out of 6. The confidence of recognizing suspicious emails and messages was rated 5.31 showing strong result.

Qualitative feedback reflected strong engagement from participants. Many expressed appreciations for the clarity and practicality of the session. A recurring theme was the desire for more company-specific context. It included regulations such as Cyber Resilience Act (CRA) and following best practices. This showed increased awareness and interest in the company's digital environment and policies.

Participants also suggested improving the pacing of the session by pairing each threat demonstration with actionable advice rather than waiting until the end of the session for actions against the specific threat. Several participants called for deeper simulations and monthly micro-trainings to reinforce behaviour over time.

At the end of the session, senior leadership including the CEO and CFO expressed strong support for improving the organization's cybersecurity posture. They acknowledged the importance of institutionalizing practices discussed during the training. They requested development of a formal cybersecurity policy within two weeks. This demonstrates a strong outcome of the awareness initiative – turning employee level education into leadership-driven policy development. A draft policy was already in preparation and is now being finalised in collaboration with the management team.

The post-training results show a clear improvement in participants' cybersecurity awareness and confidence when compared to the pre-training assessment. High average score of post-training survey suggests the training was highly effective in delivering content that was both practical and well received. The training helped address some gaps obtained from the survey before the training. The participants requested ongoing sessions which further reinforced the impact. The training not only delivered immediate value but also laid the foundation for long-term cultural change within the organization.

8 Conclusion

This thesis aimed to improve cybersecurity awareness in a marine manufacturing SME through a structured training program. Using the NIST CSF and the ADDIE instructional model, the work focused on identifying current gaps in awareness, developing, and delivering a targeted session and evaluating outcomes. The initial survey showed that while most employees understood basic security practices, there were major gaps in areas like governance, recovery, incident response and the use of secure tools.

A training session was designed and delivered. The original planned one-hour session extended to one and half hours due to active participation and engagement. It included demonstrations of phishing, session hijacking, insecure websites, password harvesting, and tools to check the strength of password. Tools like HaveIBeenPwned and BreachDirectory were also presented. The post-training survey showed that the participants felt more confident and found content useful and relevant to their job roles as shown in figure 9. The comparison aligned with post survey questions to have uniformity in result. Participants demonstrated higher post-training scores in areas such as phishing recognition, understanding threats, and perceived relevance of cybersecurity to their roles.

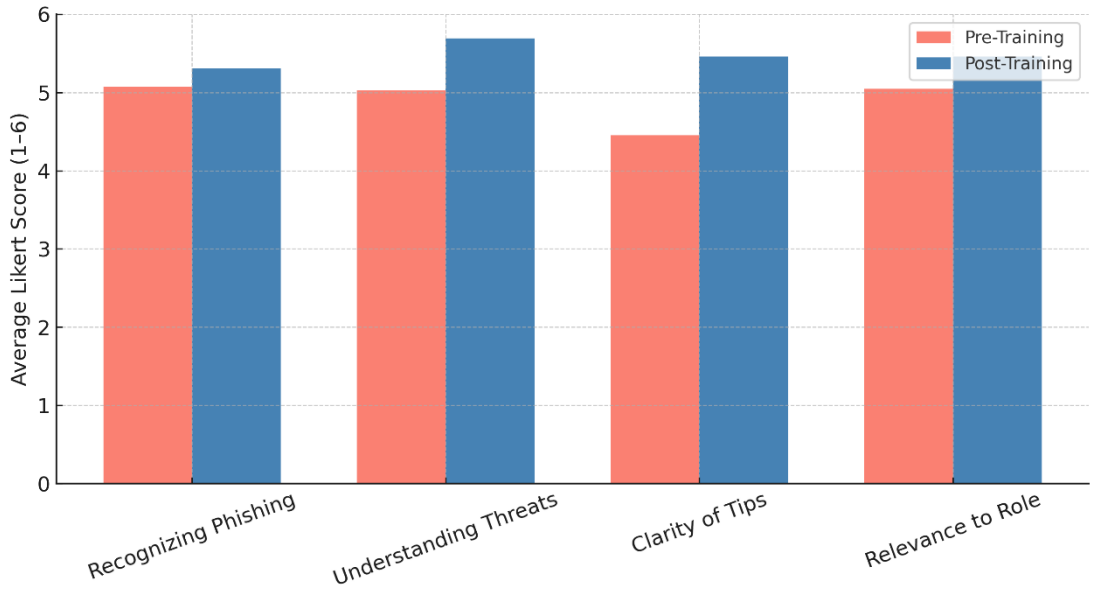


Figure 9: Pre- and Post- Training Comparison

Employees gave feedback asking for more company-specific examples, guidance after each demonstration and continued training in the future. Their suggestions reflected a genuine interest in applying what have been learned. One important outcome was the strong support from the company's leadership, who requested the creation of a formal cybersecurity policy following the session.

In conclusion, the study shows that even with time constraints, a short training session conducted can make a difference when it is practical, relevant, and well timed. It also highlights the value of employee input and leadership support in making cybersecurity part of organization's culture. This thesis serves as a starting point for building a more secure and aware workplace.

9 Limitations and Future Research

While the thesis has shown that the targeted cybersecurity awareness training session can influence positively, certain limitations must be acknowledged. The most notable constraint was the scope of the training intervention, which was limited to single session. Although the training session was extended beyond the planned duration due to active participation, one-time training cannot be expected to bring long-term behavioural change. A full adoption of policies cannot be expected. Further reinforcement and longitudinal follow-up would help in assessing enduring impact.

The other limitation was that the study was conducted within a single company. While the findings reflect patterns, similar training in other SMEs could produce different result based on leadership, workplace culture, technological maturity, or the industry. Moreover, the evaluation was carried out immediately after the training session where the result showed increased awareness and confidence but the actual change in behaviour was not examined. Similarly, the structural gaps identified such as unclear governance roles and absence of cybersecurity policy remained unsolved. However, leadership were positive and ready to address them.

Based on the limitations and outcomes of this thesis, several research directions can be proposed. One promising area would be to conduct longitudinal study for evaluation of changes in a long run. This would help measure practical effectiveness. Similarly, the research could also be extended to other SMEs in related or unrelated industries to understand how organizational culture and leadership support along with technical environments influence cybersecurity training outcomes. This would help validate the generalisability of findings by comparing results across multiple SMEs.

It would also be valuable to explore how management commitment during the training affects the speed and effectiveness of policy development and adoption. This study observed immediate support from the leadership, but further investigation could provide better insights into sustained organizational change.

References

Admass, W.S., Munaye, Y.Y. & Diro, A.A. 2024. Cyber security: State of the art, challenges and future directions. Cyber Security and Applications. 2:100031. doi: 10.1016/j.csa.2023.100031.

Aldawood, H. & Skinner, G. 2019. Challenges of Implementing Training and Awareness Programs Targeting Cyber Security Social Engineering. In: Cybersecurity and Cyberforensics Conference (CCC). Melbourne, Australia: IEEE. 111–117. doi: 10.1109/CCC.2019.00004.

Allen, W.C. 2006. Overview and Evolution of the ADDIE Training System. Advances in Developing Human Resources. 8(4):430–441. doi: 10.1177/1523422306292942.

Arif, A., Khan, M.I. & Khan, A.R.A. 2024. An Overview of Cyber Threats Generated by AI. International Journal of Multidisciplinary Sciences and Arts. 3(4):67–76. doi: 10.47709/ijmdsa.v3i4.4753.

Bolbot, V., Kulkarni, K., Brunou, P., Banda, O.V. & Musharraf, M. 2022. Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. International Journal of Critical Infrastructure Protection. 39:100571. doi: 10.1016/j.ijcip.2022.100571.

Branch, R.M. 2009. Instructional Design: The ADDIE Approach. Boston, MA: Springer US. doi: 10.1007/978-0-387-09506-6.

Cano, M. & Jeimy, J. 2019. 2019 Volume 5 The Human Factor in Information Security. Accessed 22 April 2025 https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/the-human-factor-in-information-security

Creswell, J.W. 2014. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. SAGE.

Cybellium. 2023. Mastering Cyber Security. Cybellium Ltd.

Edwards, J. 2024. A Comprehensive Guide to the NIST Cybersecurity Framework 2.0: Strategies, Implementation, and Best Practice. John Wiley & Sons.

ENISA. 2024. SMEs Cybersecurity. Accessed 20 April 2025 https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/smes-cybersecurity.

EUROPA. n.d. SME Definition. Accessed 20 April 2025. https://single-market-economy.ec.europa.eu/smes/sme-fundamentals/sme-definition_en.

ENISA. 2021. Cybersecurity for SMEs: challenges and recommendations. LU: Publications Office. doi: 10.2824/770352.

Johansson, K., Paulsson, T., Bergström, M, E. & Seigerroth, U. 2022. Improving Cybersecurity Awareness Among SMEs in the Manufacturing Industry. In: SPS2022. IOS Press. 209–220. doi: 10.3233/ATDE220140.

Kannus, K. & Ilvonen, I. 2018. Future Prospects of Cyber Security in Manufacturing: Findings from a Delphi Study. doi: 10.24251/HICSS.2018.599.

NIST. 2024. The NIST Cybersecurity Framework (CSF) 2.0. (NIST CSWP 29). Gaithersburg, MD: National Institute of Standards and Technology. doi: 10.6028/NIST.CSWP.29.

Pears, M. & Konstantinidis, S.Th. 2021. Cybersecurity Training in the Healthcare Workforce – Utilization of the ADDIE Model. In: 2021 IEEE Global Engineering Education Conference (EDUCON). doi: 10.1109/EDUCON46332.2021.9454062.

Pollini, A., Callari, T.C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F. & Guerri, D. 2022. Leveraging human factors in cybersecurity: an integrated methodological approach. Cognition, Technology & Work. 24(2):371–390. doi: 10.1007/s10111-021-00683-y.

Prümmer, J., Van Steen, T. & Van Den Berg, B. 2024. A systematic review of current cybersecurity training methods. Computers & Security. 136:103585. doi: 10.1016/j.cose.2023.103585.

Przymus, Z., Małagocka, K. & Przybyszewski, K. 2024. The human factor in cybersecurity: from risk profiles to resilience. Procedia Computer Science. 246:1437–1445. doi: 10.1016/j.procs.2024.09.587.

Raggad, B.G. 2010. Information Security Management: Concepts and Practice. CRC Press.

Rombaldo, C., Jr., Becker, I. & Johnson, S. 2023. Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity. doi: 10.48550/arXiv.2309.17186.

Tolossa, D. 2023. IMPORTANCE OF CYBERSECURITY AWARENESS TRAINING FOR EMPLOYEES IN BUSINESS. VIDYA - A JOURNAL OF GUJARAT UNIVERSITY. 2(2):104–107. doi: 10.47413/vidya.v2i2.206.

U.S. Coast Guard Cyber Command. n.d. 2023 Cyber Trends and Insights in Marine Environment. Accessed 30 April 2025 https://www.uscg.mil/Portals/0/Images/cyber/CTIME_2023_FINAL.pdf.

“WEF Global Cybersecurity Outlook 2025”. No date. Accessed 19 April 2025. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.

What is Cybersecurity? No date. Accessed 11 April 2025. https://www.fortinet.com/resources/cyberglossary/what-is-cybersecurity.

Yin, R.K. 2017. Case Study Research and Applications: Design and Methods. SAGE Publications.

Yu, J., Yu, Y., Wang, X., Lin, Y., Yang, M., Qiao, Y. & Wang, F.-Y. 2024. The Shadow of Fraud: The Emerging Danger of AI-powered Social Engineering and its Possible Cure. doi: 10.48550/arXiv.2407.15912.

Figures

Tables

Appendices

Appendix 1: Awareness Survey Questions

1. Our company has a documented cybersecurity policy that I know exists and understand.

2. We have clear guidelines on acceptable use of company assets including computers, networks, and mobile devices.

3. I understand who in our organization is responsible for cybersecurity decisions.

4. I understand what types of data I handle are considered sensitive or confidential.

5. I can identify the cybersecurity risks that affect my job role.

6. I have access to files or systems at work that I don't need for my job.

7. I think access to company information should be based on job needs.

8. I know who to ask if I have questions about keeping company information safe.

9. I know which information should never be shared over email or messaging apps.

10. I understand protecting company systems and data is part of my responsibility.

11. I am aware that handling personal or customer information at work must follow privacy laws like GDPR.

12. I use strong passwords for my work accounts. (length at least 12-16 characters, includes uppercase, lower case, numbers and special characters and not some guessable information such as first name and birthdate.)

13. I use the same password for more than one account.

14. I understand why sharing passwords at work can be a security risk.

15. I use two-factor authentication (2FA) whenever it's available to secure my accounts. (2FA includes SMS, Authenticator, physical device etc.)

16. I can recognize secure (HTTPS) vs. non-secure websites.

17. I lock my computer or device when not in use or when I am away.

18. I avoid connecting to public Wi-Fi for work tasks.

19. I understand why regular software updates are important for security.

20. Do you know if there is any procedure or formal instructions to access shared drive or cloud resource such as Dropbox in your company?

21. I can recognize a phishing email or message.

22. I always verify the email address and links before clicking or replying to an email.

23. I know what to look for in a suspicious attachment or message.

24. I know how to recognize unusual behaviour on my work device (e.g., slow performance, pop-ups).

25. I report anything suspicious, even if I'm not sure it's a threat.

26. I know that cybersecurity threats can target anyone, not just IT staff.

27. I know who in the company is responsible for responding to security incidents.

28. I know how to report a cybersecurity incident or suspicious activity.

29. I feel confident I could respond calmly if I clicked on a suspicious link by mistake.

30. I believe it is important to report near-misses, even if no damage was done.

31. I have been informed about how incident response works in our company.

32. I understand the importance of regular data backups.

33. I know who is responsible for restoring data after an incident.

34. I feel confident our company has a plan to recover from cyberattacks.

35. I would know what to do if my files suddenly became unavailable or accidently delete it.

36. I have received cybersecurity awareness training at this company.

37. Cybersecurity is treated as a shared responsibility by all staff.

38. I would like to receive more tips or training in an easy-to-understand way.

39. I believe our leadership cares about protecting digital assets.

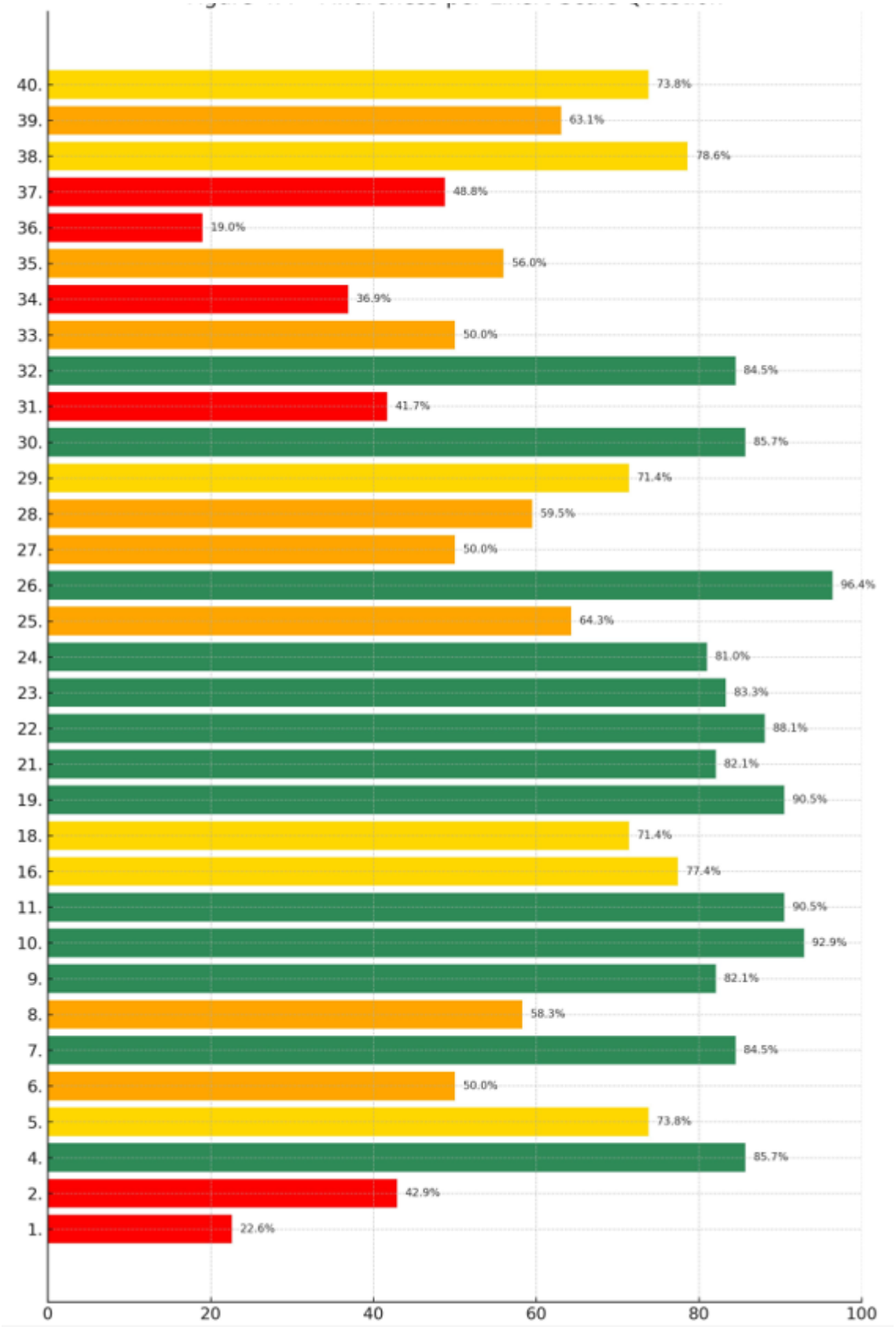
40. I feel confident asking questions if I don't understand something security-related.

41. What's one thing you wish you understood better about cybersecurity at work?

42. What would make cybersecurity training more useful or interesting to you?

43. Any other comments or ideas to improve our cybersecurity awareness?

Appendix 2: Awareness per Likert-scale question



Appendix 3: Post training survey questions

1. The training helped me better understand common cybersecurity threats.
2. I feel more confident recognizing suspicious emails and messages.
3. I now understand the importance of using strong password and two factor authentication.
4. The training provided clear and practical cybersecurity tips I can apply at work.
5. The content felt relevant to my role.
6. After today's session, choose which of the following you would be more careful about.
7. What part of the training did you find interesting or useful?
8. Was there anything unclear or confusing?
9. What topic would you like to learn more about?
10. Any suggestions to improve the training session for the future?

Appendix 4: Google Form for Cybersecurity Awareness Questionnaire

https://forms.gle/GGuu3nUYF4hCfbFK9

Appendix 5: Post Training Questionnaire

https://forms.gle/pUKpCf97QxhtvWKEA

Appendix 6: Training Material Slide

https://docs.google.com/presentation/d/1FLA84PRvnir333jEjCvHq8xDo41j7vaLskYeT0Z-zno/edit?usp=sharing

Appendix 7: Sample Slides for Training

Password Security

Risks

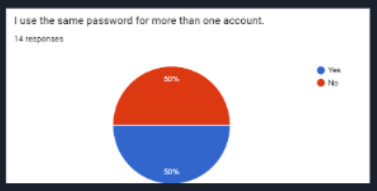
- Credential Stuffing, brute forcing, rainbow table, password spraying

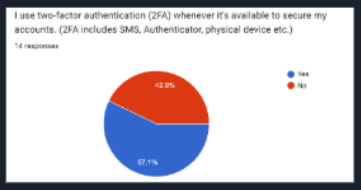
Mitigation

- Strong and Unique Password
- Password Managers
- Multi factor Authentication wherever available

→ Have I Been Pwned

→ Breach Directory





Data protection and Privacy

GDPR (General Data Protection Regulation)

- Includes principles of integrity, confidentiality, purpose limitation, transparency, lawfulness and fairness for data processing
- Gives rights to individual on personal data including right to access, rectify, erase, restrict, or object to data processing
- Accountability and compliance (Larger organizations needs Data Protection Officer (DPO))
- Within 72 hours, data breaches must be reported.
- Non compliance results in upto 20 million in fines.

CRA (Cyber Resilience Act)

- Mandatory cybersecurity requirements for all products with digital elements (software, embedded systems, remote access tools, and smart equipment)
- Starting 2026 and full security deployment in Dec 2027
- Choose CRA-compliant suppliers, keep software/firmware updated
- Report vulnerabilities