1977
UNIVERSITY
OF SKÖVDE

Degree Project

Security Awareness Training

Impact of Security Awareness Training on Employee Attitudes, Behaviors, and Organizational Cybersecurity: A Study in Medium-sized Companies

Master Degree Project in Informatics
Second Cycle 30 credits
Spring term 2023
Student: Carl-Adam Spanlang
Supervisor: Ali Padyab
Examiner: Rose-Mharie Åhlfeldt

ABSTRACT

This research study investigates the efficacy of security awareness training programs in managing information security threats. Through a systematic literature review (SLR) and multiple interviews, the research explains the interplay between employees' security knowledge, attitudes, and behaviors in the context of these training programs. It demonstrates that appropriately designed training initiatives can lead to improved threat detection, reporting rates, and overall security-conscious behavior. The study also highlights the role of written policies, standards, and governance documents in guiding and shaping these programs. The interviews bring in practical perspectives, validating and complementing academic findings. Overall, this study highlights the significance of security training programs in creating a work environment that is alert against cyber threats.

Keywords: Information Security, Cybersecurity, Security Awareness Training, Nanolearning

Table of Contents

1. Introduction

The digital world is constantly evolving, and with this evolution, there is an increasing number of cybersecurity threats. To protect against these threats, organizations need to prioritize and promote security practices and security awareness training among employees. These developments have significantly increased the online security risk faced by society, and as a result, many organizations are taking steps to implement their cybersecurity policies effectively (Li et al., 2014). This is especially true considering the quantity, complexity, and accessibility of malicious content and cyberattacks on the internet (Haney, Julie Lutters, 2020).

Information security has become increasingly important for individuals and organizations in recent years. Several high-profile incidents, including data breaches and cyber-attacks on municipalities and other organizations, have highlighted that protecting information assets is no longer optional. It is a necessary responsibility that must be taken seriously.

Despite the availability of advanced security technology, end-users continue to be the weakest link in the information security chain (Furnell et al., 2018). The reason behind this is that employees are often required to use digital technology to complete their work tasks, making them a common target for cybercriminals and cyber threats. Organizations must educate their employees on best practices for maintaining a good IT security level and implement measures to protect against potential threats.

Security awareness training is a type of education that helps employees understand and handle risks in the digital world. The main goal of security awareness training is to change the behaviours of employees, making them more aware of today's threats. This helps to prevent potential security risks that the company may face. The training often includes short lessons that provide more knowledge about specific topics (Al-Daeef et al., 2017).

Al-Daeef, Basir and Saudi, (2017) describes awareness as vital to any information security program. Individuals' lack of awareness can lead to risks such as exposing personal or corporate data to untrustworthy sites, installing harmful applications, and sharing private or corporate information with others. Security awareness programs should be designed to influence users' behaviour and understanding. Security awareness is often defined based on its required characteristics.

Al-Daeef, Basir and Saudi, (2017) also describes security awareness as an ongoing learning process where trainees understand the significance of information security issues, the organization's required security level, and their own security responsibilities. Another definition of security awareness is a state in which organization users are conscious and ideally committed to their security mission.

Prior research has shown that security awareness training can be beneficial in several ways. Li et al., (2014) found that security awareness training can improve employees' knowledge and attitudes toward security practices, leading to more secure behaviour in the workplace. Similarly, a study by Khazaei et al. (2019) found that security awareness training can lead to increased organizational cyber resilience, as employees are more likely to recognize and report potential threats.

Through security awareness training, employees can learn more about the value of cybersecurity and how to defend themselves and their company against potential threats.

This study aims to determine if medium-sized companies that have integrated security awareness training into their work practice have noticed any positive trends in how their employees behave at work and whether any statistics have shown that security awareness training has a beneficial impact on IT security. It also aims to see if security awareness training can potentially decrease the number of security incidents and vulnerabilities.

1.1 Problem Description

Security awareness training is vital for employees because it helps to protect both the individual and the organization against potential cyberthreats. In today's digital world, employees are frequently required to use digital technology to complete their work tasks, making them a common target for cybercriminals. Without proper training, employees may not be aware of best practices for maintaining online security and may inadvertently expose the organization to potential threats through their actions.

Security awareness training can help employees to understand better the importance of cybersecurity and how to protect themselves and their organization from potential threats. By educating employees on how to recognize and report potential threats, organizations can work to reduce their online security risk and protect against cyber-attacks.

Additionally, security awareness training can improve employee knowledge and attitudes toward security practices, leading to more secure behavior in the workplace (Li et al., 2014). This can be particularly important in organizations that handle sensitive or confidential information, as a single security breach could have serious consequences.

1.2 Research aims and research question.

The research questions for this work will be formulated as follows:

Research question 1: How does security awareness training impact employees' attitudes, behaviours, and knowledge related to cyber risk in medium-sized companies?

Research question 2: How can security awareness training impact an organization's IT security and potentially decrease the number of security incidents and vulnerabilities in medium-sized companies?

The research aims to investigate the effects of security awareness training on employees' attitudes and behaviour's related to cyber risk in the workplace, as well as the impact on the organization's IT security. The objective is to determine if the training is successful in fostering a culture of cybersecurity within the organization and decreasing security incidents or vulnerabilities.

2. Background

Both the world and technology are always changing. As new technologies are constantly being developed, businesses and organizations must adapt to the increasingly digitized world by streamlining work and managing routine tasks in the workplace using new methods. Not too long ago, the workspace consisted of a desk and a desktop computer. Working elsewhere was difficult because the office contained all the necessary equipment and information. Today's situation is different. The ever-evolving technology has given the workplace a fresh perspective. Employees can now bring their work with them and complete tasks from home, a café, or anywhere else (Matli & Wamba, 2023). Although it allows for greater flexibility in the workplace, it also gives cybercriminals new attack vectors to exploit (Lang & Connolly, 2022).

The coronavirus was identified at the end of 2019. The virus had many other effects besides the terrible disease. The workplace had to be managed differently by many organizations, and remote work became very popular. According to reports, the number of phishing emails had increased by 600% at the start of 2020 (Lallie et al., 2020). The fraudsters were knowledgeable of this, and COVID-19-related information was frequently included in the phishing emails. According to Chapman, (2021) all businesses must have some level of IT security in place to guard against cyberattacks, regardless of their size or industry. It's crucial to teach employees how to use computers and think safely; security awareness training is a key tool in this process.

In today's digital landscape, organizations face numerous security challenges. Data is a crucial aspect of digital transformation, and protecting it is vital. Companies should invest in strong data management and security solutions to ensure the safety of private data belonging to stakeholders like customers and employees (Shahi & Sinha, 2021). Cyber threats, such as phishing, social engineering, malware, and data breaches, are constantly evolving and becoming more sophisticated and persistent. Attackers exploit vulnerabilities in systems and networks, leading to financial losses, damage to reputation, and compromised sensitive information (Shahi & Sinha, 2021). Understanding and addressing these security challenges is crucial for organizations to safeguard their assets and maintain trust with stakeholders. Therefore, security awareness training plays a crucial role in equipping employees with the knowledge and skills to recognize and effectively mitigate these threats. By educating individuals about the ever-changing threat landscape, organizations can promote a culture of attentiveness and empower their workforce to actively contribute to maintaining a secure environment.

Security Awareness Training serves as a tool to empower employees to navigate potential cyber threats, such as phishing attacks. Based on own previous research in the field, it has been noted that the number of reports sent to the IT department increased, indicating the success of this strategy. This is the rationale behind the selection of this topic for study - to determine whether more businesses are adopting security awareness training and observing a beneficial impact on their strategy.

2.1 Clarification of the Term “Security”

In this work, the term "security" is used specifically to refer to cybersecurity and information security. It is crucial to note that this usage does not include broader aspects of security such as physical security, personal security, national security, or other areas that may be included under the general term of security. This focused approach has been adopted to allow for an in-depth exploration of the specific challenges and considerations within the domains of cybersecurity and information security.

2.2 Phishing

Phishing is a type of cyber-attack where malicious actors lure individuals into giving up their private information. This might be anything from usernames and passwords to sensitive details like credit cards or social security numbers (Medvet et al., 2008). These malicious actors often use deceptive emails that seemingly originate from a well-known and trusted brand or organization (Jain & Gupta, 2017). This approach makes the deceit all the more convincing, hence the term "phishing mail”.

A typical phishing email appears to be from a trusted source, such as a bank, a social networking site, an online payment processor, or a corporate IT department. The email might contain a seemingly harmless link that directs the recipient to a fraudulent website. On this website, the victim is usually asked to enter their credentials or other sensitive information. The attacker then captures this data.

Phishing emails often play on the victim's emotions, creating a sense of urgency or fear to motivate immediate action. They might warn of an unauthorized login attempt, an impending account closure, or a failed transaction. These scare tactics are surprisingly effective: in fact, 65% of all successful phishing attacks occur because individuals click on the hyperlinks attached in these emails. This compels the recipient to visit the fraudulent website and unfortunately leads them to disclose their personal information (Jain & Gupta, 2017).

In other cases, a phishing email might contain an attachment that, when opened, installs malicious software on the user's device(Akinyelu & Adewumi, 2014). This software can steal information, damage systems, or give the attacker remote control over the device.

Phishing is a significant cybersecurity threat. It relies on human error, rather than technological vulnerabilities, and is thus very effective against even the most secure systems. In 2022 alone, the FBI’s Internet Crime Complaint Center reported that losses caused by phishing scams exceeded $52 million (FBI, 2022).

2.3 Role of security awareness training

A well-functioning security awareness training is crucial for aligning an entire organization with security practices in today's rapidly evolving threat landscape. In an article by Haney and Lutters, (2020), the importance of going beyond mere compliance with training requirements is emphasized to create an effective security culture. To achieve this, several strategies are proposed. Firstly, the security awareness team should be seen as advocates, promoting understanding of security considerations and the adoption of best practices. This requires competencies in communication, creativity, and an understanding of the organization's goals and culture. Secondly, training should make security relatable by communicating its business value and connecting it to various roles within the organization. Additionally, multiple communication channels and techniques should be employed to engage employees and reinforce training concepts. Lastly, training should not only focus on awareness of threats but also provide practical tools and advice to address those threats and promote desired behaviours. By implementing these changes and measuring their effectiveness, organizations can elevate security awareness training to a new level and foster a robust security culture.

3. Research Method

This section outlines the methodology and procedures that will be employed in the study. Research involves gathering, analyzing, and interpreting data to gain knowledge about a specific subject or phenomenon (Leal Filho & Kovaleva, 2015). This study was conducted using a qualitative research approach, which is well-suited for exploring and understanding social phenomena in-depth. The primary data collection method used in this study was interviews, which were conducted with individuals from the selected medium-sized companies in Sweden. In addition to conducting the interviews, a structured literature review was conducted to gather information on the subject of security awareness training.

The purpose of the interviews in this study is to gather rich, first-hand information and insights from the participants. Semi-structured interview questions will be used to guide the interviews and ensure that all relevant topics are covered. Prior to conducting the interviews, a thorough review of existing literature on the topic of security awareness training was conducted to provide a solid foundation for the study. The literature review will help to inform the design of the interview questions, and also serve to contextualize the responses received during the interviews.

This chapter will provide a detailed description of the research design, how the structured literature review was conducted, sample population, data collection methods, data coding, limitations and data analysis techniques that will be used in the study, along with any ethical considerations that will be considered during the research process.

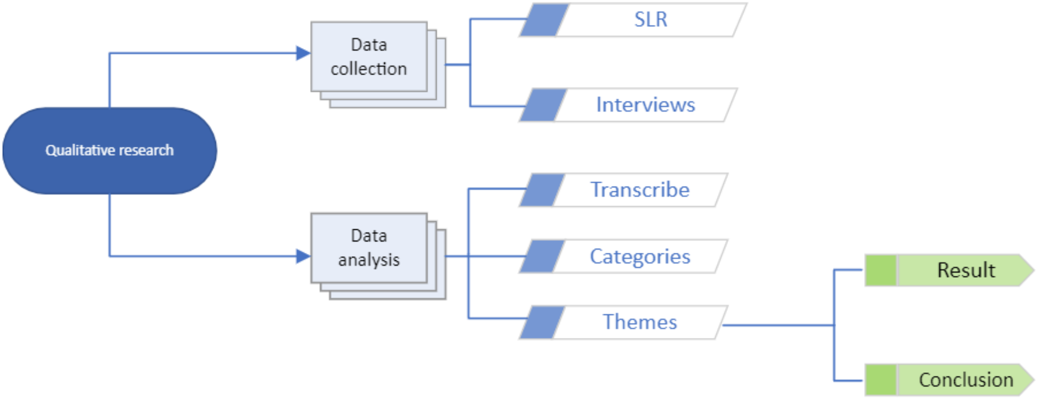

Figure 1. Overview of research methods

3.1 Systematic Literature Review

Research literature reviews can serve multiple purposes, such as establishing a theoretical foundation for further studies, gaining an understanding of the scope of research on a specific topic, or addressing practical questions by examining existing research (Okoli & Schabram, 2010).

The first step in conducting a systematic literature review is the selection of databases. The choice of databases will determine the scope and breadth of the literature search. It is also important to choose peer-reviewed databases, as it will save time and make the selection of articles as smooth as possible.

The next step is the use of search terms. The selection of appropriate search terms is crucial for identifying relevant articles to the study. The use of broad terms will result in a large number of articles, while using more specific terms will result in a smaller number of articles but may miss relevant studies. The use of Boolean operators can help to increase the precision of the search.

The final step is the use of exclusion and inclusion criteria. These criteria will filter the articles and include only those relevant to the research.

The systematic literature review will also be conducted using the eight-step method described by Okoli, (2015). This method will thoroughly go through the existing literature on security awareness training.

1. Defining the purpose of the review and establishing clear goals. This step is crucial as it guides the entire review process and helps to ensure that the findings of the review align with the research question. It is also important for the reviewers to be explicit about the purpose of the review so that readers understand the scope and limitations of the study.
2. Draft protocol and train the team*:* This step will not be utilized since there is only one reviewer.
3. Applying practical screening criteria to determine which studies should be included or excluded from the review. This step is also known as screening for inclusion, and it requires the reviewers to be explicit about what studies they considered for review and which ones they eliminated without further examination. For excluded studies, the reviewers must state their practical reasons for not considering them and justify how the resulting review can still be comprehensive given the practical exclusion criteria.
4. Conducting a comprehensive search for literature and providing details of the search process. The reviewers need to be explicit in describing the details of the literature search and need to explain and justify how they assured the search's comprehensiveness. This is important as it helps to ensure that the review is based on a thorough and up-to-date literature.
5. Extracting relevant data from the selected studies. After reviewers have identified all the studies that should be included in the review, they need to systematically extract the applicable information from each study. This step helps to ensure that the data is consistent and comparable across the studies.
6. Evaluating the quality of the studies and determining which ones will be excluded for insufficient quality. Also called screening for exclusion, the reviewers need to explicitly spell out the criteria they use to judge which papers they will exclude for insufficient quality. Researchers need to score all included papers, depending on the research methodologies they employ, for their quality.

7. Synthesizing the studies also known as analysis, this step involves combining the facts extracted from the studies by using appropriate techniques, whether quantitative, qualitative, or both. This step helps to identify patterns, trends, and inconsistencies in the data and to draw meaningful conclusions from the studies.
8. Writing the review: in addition to the standard principles to be followed in writing research papers, the process of a systematic literature review needs to be reported in sufficient detail such that other researchers can independently reproduce the review's results. This step is important to ensure the transparency and reproducibility of the review.

   Following the eight-steps provided by (Okoli, 2015), a systematic literature review can be carried out, which will provide a comprehensive and thorough analysis of the research that is already available on security awareness training and will assist in the study's further work.

3.2 Database

To find relevant articles for this assignment, ScienceDirect, ACM Digital Library, Emerald Insight and IEEE Xplore were chosen as the main databases. ScienceDirect is a database of scientific and technical literature that includes articles from thousands of scientific journals and conference proceedings. All literature on ScienceDirect is peer-reviewed (Lancet, 2023). This ensures that the articles included in the database are of high quality and can be trusted as reliable sources of information. ACM Digital Library is a database that contains articles, conference proceedings, and other research materials from the Association for Computing Machinery (ACM), a professional organization for computer scientists and IT professionals (About the ACM Digital Library, 2023). Like ScienceDirect, all materials included in the ACM Digital Library are also peer-reviewed. IEEE Xplore is a digital library that contains a wide range of research materials related to electrical engineering, computer science, and other technical fields. It is published by the Institute of Electrical and Electronics Engineers (IEEE), a professional organization for electrical engineers and other professionals in related fields. IEEE Xplore includes articles from IEEE journals, magazines, and conference proceedings, as well as a number of other types of research materials, all of which are peer-reviewed to ensure their quality and reliability (About IEEE Xplore,2023). By using these three databases, it was possible to find high-quality, peer-reviewed articles for this assignment, saving time and effort in the research process.

3.3 Search Terms, Exclusion, and Inclusion Criteria

There are many articles and studies made on the topic of "Security awareness training". To locate the most relevant and helpful articles for this study, search terms were used to narrow down the results and concentrate on specific areas that were related to the study. Logical terms and operators, such as AND, were employed to create intricate but accurate searches that assisted in finding the most relevant articles. These search strategies helped to uncover a number of high-quality articles that were useful for the research (Jesson & Lacey, 2006).

Once the search terms had been established, the process of identifying and eliminating articles that were not relevant to the research began. The first step was to exclude any articles that were published prior to 2017. This helped to ensure that only current and relevant articles were being considered. The second requirement was that all of the articles included in the research must be peer-reviewed. This means that they had been evaluated by a group of experts in the field, who had checked the quality and accuracy of the research. The third step is to exclude any articles that are not written in English. This will help to ensure that all of the articles included in the research are easily understood. Additionally, it will also help to eliminate any potential language barriers that may hinder the understanding and analysis of the research. By following these inclusion and exclusion criteria, the search could be focused on high-quality, relevant articles that would be useful for the research. Any articles that did not meet these criteria were eliminated from the final search results. Once the initial search had been conducted and the search terms refined, the process of reviewing the articles began.

In total, the search resulted in a large number of articles that were relevant to the research. However, by following the established inclusion and exclusion criteria, the number of articles was narrowed down to a manageable number that could be thoroughly reviewed and analysed for the literature review. Additionally, one article was identified through the use of backward search, which involved examining the reference lists of relevant articles. The final search strings, databases used, and the number of articles included in the literature review can be seen in the figure below.

Table 1: Overview of research strings, database, results and how many articles that were included.

Search strings	Database	Result	Included
"Security awareness training" AND "users"	ACM Digital Library	27	2
Security awareness training AND “users”	IEEE Xplore	45	2
"Security awareness training" AND "users"	ScienceDirect	60	5
"Security awareness training" AND "users"	Emerald insight	160	7

This table presents the search strings used in different databases, the number of results obtained, and the number of results that were included in the research.

3.4 Data Collection

The data collection in this study includes two types of methods: a systematic literature review (SLR) followed by semi-structured interviews.

Starting with a SLR, this method is essential for providing an extensive understanding of the existing literature on security awareness training. It will help in establishing the current knowledge base, identifying gaps, and framing the context for the interviews.

Following the SLR, semi-structured interviews was employed as the second method of data collection. Semi-structured interviews are a popular method for collecting data in qualitative research studies because they allow for a level of flexibility and exploration while still maintaining a structured approach. During a semi-structured interview, the interviewer has a set of prepared questions to guide the conversation, but the exact order and form of the questions may be modified based on the interviewee's responses and the direction of the conversation (Denscombe, 2014) This approach allows the interviewer to probe deeper into topics that the interviewee brings up, while also giving the interviewee the freedom to elaborate on their thoughts and experiences. It also allows the interviewer to clarify any points and ask follow-up questions as needed.

3.4.1 Interviews

One of the key benefits of using semi-structured interviews is that it encourages the interviewee to provide detailed and in-depth information about the subject at hand. The questions are open-ended and focus on exploring the interviewee's thoughts, feelings, and experiences, rather than simply gathering factual information. Additionally, the use of semi-structured interviews in this study allows for the discovery of new themes and perspectives that may not have been anticipated in the initial question list. This is a key advantage of using semi-structured interviews as a data collection method, as it allows for a more open-ended and exploratory approach to data collection. The semi-structured format allows for the flexibility to follow up on unexpected or intriguing responses, which can lead to the discovery of new insights and information that would not have been uncovered through the use of a strictly structured interview format (Young et al., 2018). This approach will enable a more comprehensive understanding of the research topic and to explore the perspectives and experiences of the participants in greater depth. Furthermore, in order to ensure the accuracy of the collected data, the interviews will be transcribed verbatim. This means that every word spoken during the interview will be transcribed in written form, including any pauses, repetitions, or filler words. The transcribed interviews will be used as the primary source of data for the analysis. This will allow for an in-depth examination of the participants' responses and will provide a detailed account of their perspectives and experiences.

Overall, semi-structured interviews offer a balance between structure and flexibility, allowing for a rich and nuanced understanding of the subject being studied. This makes it a valuable method for collecting data in qualitative research studies and can lead to a more complete understanding of the research topic.

3.5 Data Analysis

After the data collection process is done, the next step is to analyse the data to extract insights and draw conclusions from the study.

3.5.1 Data Coding

The initial phase of the analysis involves transcribing recorded interviews into a textual form, setting the stage for the subsequent examination. Following this, a methodological approach known as 'deductive category coding' is employed. This strategy, grounded in deductive content analysis, is generally applied when the analytical structure is informed by pre-existing knowledge and the research objective is focused on validating or testing a theory (Elo & Kyngäs, 2008).

Deductive content analysis proves useful when there is a comprehensive understanding of the phenomenon under research. This approach permits the application of established theoretical constructs to the data, leading to a structured examination. Predefined categories, in this context, guide the exploration of existing data within a new framework.

The data is thoroughly observed during the deductive coding process, with suitable categories systematically assigned to each segment. These predefined categories serve as a structured framework, simplifying the organization and interpretation of the data. Utilizing these categories helps identify and classify emerging patterns or themes from the data, thus ensuring uniformity in the analysis.

This is an example of how the themes and codes were chosen, based on previous knowledge and the research question 1. The first theme identified was 'Shift in employees' attitudes towards cyber risk', with the codes 'Awareness' and 'Improved understanding'. These codes helped in exploring how employees' attitudes towards cyber risk changed after undergoing security awareness training.

The second theme was 'Structure and delivery of nanolearning'. This theme focused on how the training was delivered to the employees and how the structure of the program contributed to their learning. The codes under this theme included 'Program delivery', 'Time', 'Topics', and 'Adaption'. These allowed for the detailed analysis of how the training was received and how well it was adapted to fit the needs and constraints of the employees.

Finally, the third theme was 'Challenges'. This theme aimed to identify any obstacles encountered during the training and how they were addressed. The codes used to capture this theme were 'Maintain interest', 'Adapting to changes', and 'Talk about it'. These codes helped in understanding the hurdles faced by employees and the organization in maintaining engagement and adapting to the rapidly changing cyber risk landscape.

Through the systematic assignment of these codes to each piece of data, the analysis could capture the experiences, perceptions, and shifts in employees' attitudes towards cyber risks. The study also highlighted the challenges faced and how they were tackled, providing insights into the efficacy and adaptability of the nanolearning method in cybersecurity awareness training.

3.6 Selection

Denscombe (2014) discusses that the selection of individuals for interviews is a crucial aspect of any research study. Two commonly used approaches for selecting interviewees are random selection and non-random selection.

Random selection is a process where participants are selected at random without any specific qualifications or requirements. This approach is often used when the research question is broad, and the study aims to obtain a representative sample of the population. However, this approach may not always be the most appropriate, particularly when the research question is specific and requires participants with specific knowledge or expertise (Denscombe, 2014).

Non-random selection, on the other hand, is an approach where individuals are specifically chosen for their relevant knowledge or expertise. This approach is often used when the research question is specific, and the study aims to obtain in-depth insights from individuals who possess unique experiences or perspectives (Denscombe, 2014).

In this study, non-random selection was utilized to ensure that the interviewees possessed valuable insights into the IT departments and knowledge of Security awareness training in medium-sized companies. This approach enhances the quality and validity of the study, as the interviewees are well-suited to provide relevant and meaningful responses to the research question.

Each interview is expected to last approximately 20 minutes, depending on the depth of the answers and the discussion. Careful consideration of the selection process and the specific qualifications and experiences of the interviewees is crucial for ensuring the quality and validity of the study's results.

3.7 Sampling strategy

To gain a comprehensive understanding of the general operations and practices of medium-sized companies in Sweden, a representative sample of 6 companies will be strategically selected for in-depth interviews. Choosing a study sample is crucial for this research project as it is often not feasible, cost-effective, or ethical to study entire populations. The goal of this sampling method is to select a representative sample of medium-sized companies so that the findings from the sample can be extrapolated to the entire population. This allows for inferences and conclusions about the larger population of medium-sized companies in Sweden based on a smaller, more manageable subset (Marshall, 1996).

By carefully selecting a diverse sample of medium-sized companies of varying industries, regions, and demographics, the perspective on the current state of medium-sized companies in Sweden will be broadened and any common challenges or best practices that can be shared across companies will be identified. Furthermore, this sample size is considered sufficient to provide a well-rounded and accurate picture of the current state of medium-sized companies in the country. It's worth noting that larger samples may not always provide more accurate results and there is usually little to be gained from studying very large samples as the error in the selection of the sample gets smaller as the sample size increases (Marshall, 1996).

3.8 Participants

Table 2: Participant Details

Interview Respondent	Role in organization	Platform	Alias
1	Security Manager/ Information Security Coordinator	Teams	IR1
2	Product owner IT, Security and Cloud	Zoom	IR2
3	Security Manager	Teams	IR3
4	Information Security Coordinator	Teams	IR4
5	IT-Application Owner	Email/Phone	IR5
6	Information security officer	Teams	IR6

Table 2 provides information about the interview respondents, including their roles in the organization, the platform used for the interview, and the alias or pseudonym assigned to each respondent.

3.9 Implementation

According to Denscombe's (2014), the predominant form of interview utilized in research is the one-on-one interview, wherein the researcher engages in a face-to-face interaction with the respondent. One-on-one interviews are considered the most straightforward to arrange, as they necessitate communication solely between two parties. The individualized nature of this interview format allows for a more manageable and controlled interaction between the researcher and the participant. Moreover, during the subsequent transcription phase, the task is simplified as the transcriber only needs to transcribe a single voice, minimizing potential complexities.

3.10 Interview Questions

In this section, the design of the interview questions is explicated in relation to addressing the research questions. The interview questions are strategically formulated to encompass the influence of security awareness training on various aspects of employees' attitudes, behaviours, and knowledge related to cyber risk in medium-sized companies. Additionally, the questions aim to investigate the potential effects of such training on an organization's IT security posture, including the potential reduction of security incidents and vulnerabilities. The questions are designed to elicit open-ended responses from participants, in accordance with the recommendation posited by (Wohlin et al., 2012) with the objective of obtaining comprehensive insights into the research questions.

In conducting the interviews, an initial set of general questions were asked to establish and understand the participant's background. These questions served as an icebreaker, helping to create an open and relaxed atmosphere conducive to a natural conversation.

Following the introductory questions, the interview transitioned into a more focused discussion of the research questions. The first set of questions was targeted at understanding the impact of security awareness training on the participants' attitudes, behaviors, and knowledge related to cyber risk, aligning with Research Question 1. This in-depth exploration aimed to capture any shifts in employees' attitudes and the ways their behaviors and understanding of cyber risk might have changed as a result of the training.

The interview then proceeded to questions relating to Research Question 2, examining how security awareness training could influence an organization's IT security and potentially decrease the number of security incidents and vulnerabilities. This section of the interview sought to gather insights into how the training could affect broader organizational IT security parameters and incident rates.

Throughout the interview, the goal was to maintain an interactive conversation by asking follow-up questions based on the participants' responses. This approach helped to promote a natural dialogue, which was instrumental in gaining deeper insights and understanding.

3.11 Metrics

One of the study's aims is to investigate the use of security awareness training in medium-sized companies and the impact it has on improving security, but also whether it has a measurable positive impact. As mentioned before, the primary method for collecting data will be through interviews with relevant personnel within the companies. Through these interviews, one of the points will be to determine whether medium-sized companies are using security awareness training or not, and if so, whether they have implemented any methods for measuring the positive impact of the training. The method used could include measuring the number of phishing attacks reported by the employees or other security incidents reported within the companies. The measurement of the impact can be done in different ways, and it will be through the interviews that the answers to these questions will be gathered.

3.12 Expected Results

The research aims to understand the impact of security awareness training on employees' attitudes, behaviours, and knowledge related to cyber risk in the workplace. To gain a comprehensive understanding of this topic, a representative sample of 6 medium-sized companies in Sweden will be strategically selected for in-depth interviews. This sample size is considered sufficient to provide a well-rounded and accurate picture of the current state of medium-sized companies in the country regarding their approach to security awareness training.

The companies selected for the interviews will be diverse in nature, including those of varying sizes, regions, and demographics. This will enable a broad perspective on the current state of medium-sized companies in Sweden and identify any common challenges or best practices that can be shared across companies. The study will take a two-pronged approach, beginning with a systematic literature review and followed by gathering information through interviews. The systematic literature review will involve searching various databases and scientific journals and reviewing various studies on the topic.

This step will provide a strong foundation of knowledge by providing an overview of the current state of knowledge on the topic and how security awareness training affects employees' attitudes and knowledge of cyber risks. Additionally, this literature review will serve as material for the later conducted interviews, as it will provide a good understanding of the topic and the possible questions that can be asked. In addition, the study will also include an examination of how medium-sized companies carry out security awareness training and if there are any measurable results.

Through the interviews with individuals who are responsible for implementing and overseeing the training within the companies, the study will gather information about the strategies used for training, the resources allocated to it, and any measurable results or outcomes that have been observed. The combination of both parts will not only provide a comprehensive understanding of the impact of security awareness training on employees' attitudes and knowledge related to cyber risk in the workplace but also on the approach of different medium-sized companies in handling security awareness training. Furthermore, it will enable a comparison of the best strategies with the best result from the companies to the previous research on the topic and their findings.

4. Systematic Literature Review

4.1 Phishing attacks and Training Programs

Phishing attacks are a common cyber-attack that employees may be subjected to and therefore require training. According to Kwak et al., (2020) spear phishing, the practice of sending emails with malware that appear to come from legitimate sources, is a common method used by hackers to target individuals or departments within organizations. It has been responsible for many high-profile breaches and has also been linked to attacks on industrial control systems, espionage, and terrorism. Most training programs for increasing security awareness focus on encouraging individuals to report suspected spear phishing emails to incident response teams. A study by Tschakert and Ngamsuriyaroj, (2019) found that these training programs can effectively reduce the number of individuals who fall victim to these types of attacks (also known as the false-negative rate) and increase the confidence of participants in detecting and avoiding them. However, the effectiveness of these programs is limited by individuals' failure or ignorance in following recommended policies and by relapse into habitual patterns of email use. Research has also identified message cues, such as authority and urgency, and individual differences, such as personality traits and cognitive information processing, as contributing to individuals' vulnerability to phishing attacks. In addition, evidence suggests that individuals do not often report suspicious emails, and there is a lack of research on the effectiveness of different reporting mechanisms. To be most effective, the authors suggest that information security awareness programs utilize various learning methods to cater to the target audience's preferences. In order to tailor the training program to the needs of the group, administrators need to assess the preferences of their target audience. Doing so can make the training more effective and produce better results in helping employees recognize and avoid phishing attacks.

4.2 The Link Between Knowledge, Attitudes, and Behavior

The importance of understanding the effectiveness and impact of security awareness initiatives in the workplace cannot be overstated. Most companies want their employees to exhibit security-compliant behavior, so it is crucial to clearly understand how to promote this behavior effectively. To gain more insight into this topic, Sas et al., (2021) conducted a study with two aims: to examine the relationship between employees' security knowledge, attitudes, and self-reported behavior (Study 1) and to measure the impact of a security training session on employees' level of security awareness (Study 2).

The results of the first study showed that there was a significant relationship between employees' knowledge and their attitudes toward security issues. In other words, those with more security knowledge tended to have a better attitude toward security. Additionally, the study found that employees who reported having more security knowledge and a better attitude towards security also indicated that they would behave in a more secure way. However, no significant relationship was found between employees' attitudes toward security and their self-reported behavior. The study also looked at the influence of socio-demographic characteristics on security knowledge and found that age, length of career, and percentage of full-time effort were all positively associated with security knowledge. Older employees also reported behaving in a more secure way.

The second study conducted by Sas et al. (2021) aimed to measure the impact of a security training session on employees' level of security awareness. The researchers found that the training had a positive effect on both employees' security knowledge and attitudes toward security issues. However, the impact on self-reported behavior was less strong compared to the impact on knowledge and attitude. Despite this, the training was still found to be effective in increasing employees' overall security awareness.

Several studies have examined the effectiveness of different approaches to improving security awareness in the workplace. Alshaikh, Maynard and Ahmad, (2021) conducted a study to investigate the relationship between security knowledge, attitude, and behavior. They found that employees with a higher level of security knowledge and a more positive attitude towards security were more likely to engage in self-reported security-compliant behavior. They also concluded that security training sessions could effectively increase employees' security knowledge and attitudes.

In addition to traditional training methods, the use of a social marketing approach may be a promising method for changing employees' behavior related to information security. According to Alshaikh, Maynard, and Ahmad (2021), this approach involves using marketing techniques to influence the attitudes and behaviors of a target audience and could potentially be applied to the development of security awareness initiatives in the workplace.

Fagade et al. (2017) discuss the theory of planned behavior, which provides insights into why it is difficult to change the behavior of malevolent insiders when it comes to following security protocols. According to the theory, a person's intention, perceived behavior towards crime, subjective norms, and attitude are key factors in predicting behavior.

The authors point out that security managers may provide training, policies, and guidelines, but users may not comply even when mandated. The authors further suggest that pre-employment background checks and other mechanisms can help identify agents that pose behavioral risk. Some of these risks may be unrelated to employment, such as anxiety, depression, and medical conditions. Nevertheless, they may help address psychological factors required to form group homogeneity.

Fagade et al. (2017) concludes that behavior and external environmental influences can indicate early signs of cybersecurity risks. They suggest that human resource staff are particularly well trained to apply observation techniques and recognize high-scoring risk indicators as predictors of anomalous behavior. By doing so, organizations can take necessary actions to mitigate insider threats and enhance their cybersecurity posture.

4.3 Non-traditional methods for improving security awareness in the workplace.

Another study conducted by Abu-Amara and Tamimi, (2021) found that interactive video games may be an effective method for promoting security awareness in the workplace. The findings discovered by Abu-Amara and Tamimi (2021), are supported by the research of (Alkhazi et al., 2022) and (Tonkin and Kosasih, 2022), which also found that non-trivial methods can be effective in improving security awareness. Tonkin and Kosasih's (2022) study present “Aurelius,” a cybersecurity simulation game designed to train executives to understand the relationship between cybersecurity policies and business outcomes. The game simulates the effects of different cybersecurity policies on an organization's profits and reputation and is intended to be a novel approach to cybersecurity awareness training, using a serious simulation game to engage players in making cybersecurity investment decisions and experiencing the real-time consequences of those decisions. This finding supports the idea that non-traditional methods can be effective in improving security awareness and suggests that organizations may want to consider using a variety of approaches in their security awareness training programs. Many organizations today provide security awareness training or send out warnings and advise employees on how to behave securely (Hielscher et al., 2021). However, old advice is rarely explicitly retired, and the language and cues associated with old behaviors are often left in place. This can be overwhelming for employees whose main job is not security, as they must navigate the complexity and contradictions of the different instructions; implementing non-traditional methods can be proven effective in such cases.

Overall, it is clear that both traditional and non-traditional methods can be effective in improving security awareness in the workplace. In order to ensure the success of security awareness initiatives, it may be necessary for organizations to use a combination of methods, tailoring their approach to the specific needs and characteristics of their employees.

4.4 Enhancing Information Security Awareness Training Programs (SAT)

The effectiveness of security awareness training programs (SAT) in managing information security and safeguarding organizational assets cannot be overstated. These programs are widely recognized as a crucial component of an organization's comprehensive information security strategy, aiming to increase employee awareness (Alyami et al., 2022). In a study by Dahabiyeh, (2021), important factors for improving Security Awareness Training (SAT) programs are described. The study shows that the technological context had the greatest influence, followed by the environmental context, and then the organizational context. Within each context, several important factors were identified, including usability and implementation, content quality, customization capabilities, integration, top management support, employee engagement, presence of dedicated IT security personnel, vendor support team, and compliance with regulations and guidelines. Emphasizing a proactive approach, SAT programs primarily focus on mitigating unintentional security breaches resulting from employees' lack of awareness. Through active participation in these programs, employees gain comprehensive knowledge of prevalent security threats, available countermeasures, and the potential consequences of violating security policies. Building upon the crucial role of SAT programs in managing information security, Stewart and Jürjens, (2017) highlights the importance of organizational policies in their research. According to Stewart and Jürjens, (2017), these policies act as foundational rule sets, designed to safeguard an organization's network and assets against fraudulent activities and embezzlement. Especially if they are spoken of in the training programs.

Stewart and Jürjens, (2017) argues that these security policies effectively deter unlawful activities, such as unauthorized intrusion into computer systems, viewing of inappropriate websites, and theft of company software. They underscore the crucial role of compliance, asserting that adherence to these policies is central to their effectiveness. Although the study’s analysis of security policies might not be exhaustive, he acknowledges their substantial role in shaping employee behavior and implementing security practices within an organization. Their work emphasizes the interconnectedness of policies, compliance, and the overall effectiveness of information security management in an organization.

Moreover, SAT programs aim to reinforce employees' understanding of their roles and responsibilities in protecting the organization's valuable information assets. The importance of promoting a strong security culture among employees and developing their cybersecurity skills is also emphasized in the literature (Bada & Nurse, 2019) Tailoring programs to SMEs'(Small- and Medium-sized Enterprises) resources and providing practical and relevant advice tailored to the company's operations are key considerations. Governments and local organizations offer support through various initiatives, including security objectives, training, hardware, and software tools. However, engaging SMEs effectively in cybersecurity initiatives can be challenging due to their limited resources and focus on operational activities. Effective communication and engagement strategies are crucial to increase awareness and understanding of cybersecurity among SMEs.

It is clear that security awareness training programs, including those designed for SMEs, play a vital role in mitigating security risks. The effectiveness of such programs can be enhanced by considering the factors highlighted in the literature, such as technological usability, content quality, customization capabilities, top management support, and employee engagement. Furthermore, tailoring programs to SMEs' specific needs and providing practical support and resources from governments and local organizations can significantly contribute to the development of a strong security culture and improved cybersecurity skills among employees.

Bada and Nurse, (2019) also emphasizes the need for further research and development to provide concrete programs and interactive support for SMEs in different locations and cities. By bridging the gap between research and practical implementation, we can ensure that SMEs receive effective cybersecurity training and support tailored to their unique contexts and limitations. This ongoing research will ultimately lead to the continuous enhancement of SAT programs, positively influencing employees' behaviors and beliefs, and strengthening the overall information security posture of organizations, including SMEs.

4.5 Importance of tailored and Context-based Training

Tailored training is emerging as a central element for the effectiveness of Security Education, Training, and Awareness (SETA) and Information Security Awareness (ISA) programs. Alyami et al. (2022) emphasizes the importance of tailoring SETA programs to employees' learning styles and job roles, suggesting that personalized training plans and adaptive learning platforms are key for engaging participants.

Pattinson et al. (2020) reinforce this notion in the context of ISA programs, finding that the alignment of training type with participants' learning preferences and demographics, including age and gender, is more significant than training frequency. They assert that custom-tailored interventions are critical for ISA enhancement.

In contrast, Zhang et al. (2021) bring attention to the negative consequences of inadequate security training initiatives. Their study reveals that employee’s express dissatisfaction and reduced engagement when training fails to address their unique needs and the specific security requirements of their organization. This highlights the risks of not implementing customization in security training.

Together, these studies form a compelling case for the significance of tailored training in security awareness programs. By integrating the insights from Alyami et al. (2023), Pattinson et al. (2020), and Zhang et al. (2021), it becomes evident that customization, which takes into account learning preferences, job roles, and demographic characteristics, is essential in fostering engagement and meeting the unique security needs of both individuals and organizations. Organizations are urged to design and continuously adapt their security training programs with customization at the forefront to achieve effective and impactful outcomes.

In addition to tailoring training based on learning styles, job roles, and demographic traits, an innovative technique called Context-Based Micro-Training (CBMT) is gaining attention in SETA. Kävrestad et al. (2023) shed light on CBMT as a way to offer training right when users come across situations where that training is needed. For instance, teaching users about secure passwords just as they are creating an account or educating them on phishing when they are about to open an email that might be sketchy. By giving the right information at the right time, CBMT raises awareness and makes sure the learning is relevant and can be used immediately. This approach is beneficial because it addresses the challenges of knowledge retention and ensures that the training is timely, directly applicable, and less likely to be viewed as an interruption, hence encouraging user participation and engagement.

4.6 Connecting the dots from the SLR

Security awareness training is important for managing information security and safeguarding an organization's assets. This is also true in medium-sized organizations. However, the effectiveness of these programs hinges on a range of factors that influence employee behavior and the training's overall efficacy.

Phishing attacks remain one of the most prevalent cyber threats that employees face. Training programs that concentrate on educating employees about phishing attacks have been found effective in reducing false negatives and maintaining confidence in identifying malicious emails. Nevertheless, a tendency to revert to habitual email usage patterns and disregard for policies can undermine this effectiveness. Understanding the relationship between knowledge, attitudes, and behavior in security compliance is critical. Employees who possess a higher level of security knowledge are likely to have more positive attitudes towards security. While training can positively impact knowledge and attitudes, it has been found to be less effective in modifying behavior.

Diversifying training approaches is significant in catering to the varying preferences and learning styles of employees. Employing a mix of traditional and innovative training methods is instrumental in engaging employees and ensuring the effectiveness of training programs.

Moreover, the effectiveness of Security Awareness Training (SAT) programs is influenced by various contexts, including technological, environmental, and organizational factors. It is imperative to take a proactive approach, emphasizing the quality of content, customization, support from top management, and employee engagement. Additionally, a robust policy framework is vital for guiding employee behavior. Small- and Medium-sized Enterprises (SMEs) face unique challenges due to resource constraints, and targeted support from government and local organizations can be instrumental.

Tailoring training programs to employees' learning styles and job roles has been identified as a critical factor in promoting engagement and improving the efficacy of Security Education, Training, and Awareness (SETA) and Information Security Awareness (ISA) programs.

In conclusion, an effective security awareness training program should be comprehensive and tailored, considering individual differences among employees. It is essential to combine traditional training methods with innovative approaches, incorporate a robust policy framework, engagement from top management, and adapt to the specific security needs and characteristics of the organization. Training has a limited impact on behavior change, so complementary strategies are necessary to strengthen the organization's overall security posture.

5. Results

5.1 Interviews

The result presents the findings and implementation of the interviews conducted. The results are based on the codes and themes derived from a deductive category coding approach, aligned with the research questions.

The first step in analysing the data collected through the interviews is to transcribe it into written form. Once transcribed, a deductive category coding approach will be employed to examine the data. This approach involves applying pre-existing categories or concepts derived from relevant literature and theories to the data.

To ensure a systematic and focused analysis, the coding process will involve carefully applying the predetermined categories to the interview transcripts. Each relevant excerpt of data will be assigned to the corresponding category based on its alignment with the established criteria. This deductive category coding approach allows for a structured analysis that connects the research questions with the identified categories.

By utilizing this deductive coding method, this study aims to provide a comprehensive understanding of the research questions while building upon existing knowledge and theoretical frameworks. The subsequent sections will present the detailed results and insights obtained from the analysis, organized according to the predetermined categories.

5.1.1 Impact of Security Awareness Training on Attitudes, behaviours, and Knowledge

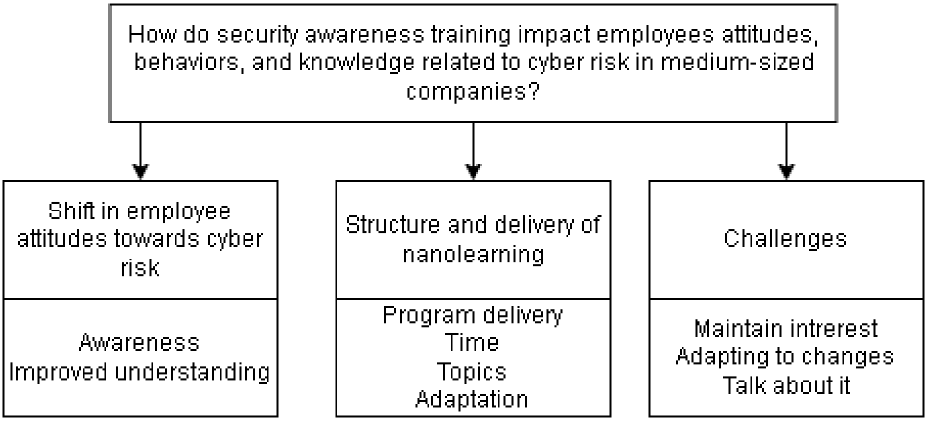
How do security awareness training impact employees attitudes, behaviors, and knowledge related to cyber risk in medium-sized companies?
Shift in employee attitudes towards cyber risk
Awareness
Improved understanding
Structure and delivery of nanolearning
Program delivery
Time
Topics
Adaptation
Challenges
Maintain intrerest
Adapting to changes
Talk about it

Figure 2, Themes and codes related to Research Question 1 (authors own)

Shift in employee attitudes towards cyber risks

In the exploration of how security awareness training changes the way employees in medium-sized companies think and act about cyber risks, some common ideas emerged from the interviews with all respondents.

All of the respondents talked about how important it is to keep the training going. They agreed that one training session isn't enough. IR2 said that continuous training really helps employees understand more about cyber risks. IR1 also noticed that employees started to act differently after they introduced regular security training. This shows that training needs to happen regularly to really make a difference.

Everyone mentioned that having the support of management can make a big difference in how employees see cyber risks. IR3 was clear about this, saying, "you need the bosses on board to build a real security culture in the company." This idea matched what IR2 and IR1 said about their experiences getting people in their companies to understand how important cybersecurity is.

IR4 added that not only is management support crucial, but the active involvement of both employees and managers in raising information security issues has increased. IR4 highlighted that they often reach out for advice or report suspicions, such as emails that could be phishing attempts or other questions related to information security.

Ir5 mentioned that employees even outside the IT-department have developed a better understanding of the importance of IT-security. This shows that the broader organizational awareness and underscores that the training is not just benefiting the IT-department but the company as whole.

IR3, IR1, IR4 and IR6 emphasized that the attitudes of the employees have changed for the better. IR3 mentioned that employees are more engaged and actively participate by asking questions during trainings and conferences. IR3 stated, "They are more cautious now; they don't thoughtlessly click on links, and they don't authenticate without thinking twice." Similarly, IR1 noted that the staff has become more aware of cyber risks and security measures. This indicates that the employees have gained a better understanding of why the trainings are conducted and have become more open to participating and understanding the importance of these programs. IR1 points out one significant change in behaviour since the introduction of nano-learning programs, saying, "Another noticeable change is that we have seen the staff taking better care of their work areas. For example, we have noticed that they now tidy away sensitive papers from their desks when they go home or go for lunch to ensure that no unauthorized person has access to them. This shows an increased awareness of handling sensitive information and greater caution in the work environment." IR6 mentions, "What I can say is that when we send out phishing tests, the IT department gets calls from employees who have received emails that they find suspicious. This suggests that they have gained knowledge somewhere about being vigilant for phishing emails. It's possible that they have learned this through the trainings we have provided, but we haven't been able to definitively measure if it's directly linked to the trainings. However, this is something positive we have observed in their behavior."

Structure and Delivery of Nanolearning

IR2,IR1 and IR6 emphasized the importance of tailoring the training to suit each individual's needs and skills. They saw this as a pivotal aspect for the success of the training and to effect change in employees' behaviours. IR2 highlighted how their nano-trainings are structured in short, intensive sessions. He stated, “If one happens to click on a fraudulent phishing email, the user undergoes a brief, targeted training against that specific type of phishing email. The training is therefore adapted according to the specific content of the email that was clicked on, which the program keeps track of."

IR6 echoed the views of IR2 and IR1 and added an additional layer of insight. IR6 stated, "Yes, the most important thing when it comes to organizing a training is to adapt it to the target group, and that it resembles the work environment the employees are actually in." This comment by IR6 emphasizes not only the need for individualization but also the importance of contextualizing the training to be reflective of the actual work environment.

Meanwhile, IR3 underscored the breadth and relevance of the training programs' content, "The programs cover several important aspects that employees should be aware of and consider in their daily work. On our internal intranet, the training is designed to cover specific topics related to our work, such as phishing attacks, ransomware, selection and management of secure passwords, secure remote work, conduct in public environments, and handling of fake news." In addition to this, IR3 stressed the importance of variety in the training programs to maintain engagement and ensure that employees are well-informed and prepared for security challenges. IR3 also mentioned that crucial information is shared at larger meetings and conferences where everyone can participate and receive the information at the same time. This is a viewpoint that IR2 echoed, emphasizing the importance of discussing the significance of nano-learning programs in larger groups and management meetings to incorporate them naturally into work tasks.

IR2, IR1, IR5 and IR6 rely on external programs for their nanolearninge-programs, and all three are highly satisfied with the outcome. Before starting the training, IR2 and IR1 chose to first gauge the organization's awareness level by sending out false emails. As IR1 explained, “To get an idea of where we stood, we began the training by sending out a phishing email”. This strategy provided both IR2 and IR1 with a solid basis to determine how to begin the training and at which level.

The use of external programs was something all four respondents were satisfied with, and they appreciated the automated process. However, they also saw the importance of being able to adapt the exercises more specifically. IR1 explained, “Our external training program has different modules, and we have tailored it to our needs. We took a base module and modified it, so we have gradually developed the trainings to make them more advanced and able to handle new threats."

Challenges

IR2 highlighted the initial resistance experienced when introducing nano-learning programs, primarily due to individuals' resistance to change and the additional content in their inboxes. However, this resistance was short-lived. He noted, "The change became positive when the end users realized the value, they derived from it. They received more security training without sitting through lengthy, boring courses where they did not always understand everything." This issue was not experienced by either IR1 or IR3. Instead, IR1 initially saw a challenge in getting staff to prioritize information security and to take the time for training seriously. To address this, IR1 said, "I have actively requested time during our staff meetings to discuss the importance of information security and the significance of these trainings." This approach led to greater employee engagement and seriousness toward the training.

IR3 added that it was previously challenging to engage employees, but it has recently become an expectation, and no one wants to be the one causing costly damages to the company. IR3 also mentioned that "much has come for free via media monitoring on the topic, and when big incidents have occurred, everyone has heard about it."

IR6 echoed IR1 and IR3's sentiments on engagement, focusing on the method of communication. IR6 emphasized, "It is also important not to just send out an email that says 'Click here to start the training' when at the same time we are trying to teach people not to click on links in emails without thinking. This becomes contradictory." This underscores the need for a coherent communication strategy, similar to IR1's approach of using staff meetings to address information security.

IR5 identified a mindset challenge, similar to the initial resistance mentioned by IR2, but on an individual level. He stated, "I think the biggest problem has been getting all the employees to understand that this can happen to anyone in the company. I believe many thinks: it will never happen to me and my computer." This ties back to IR1 and IR3's focus on the importance of making employees understand the significance of information security.

By promoting awareness and emphasizing the importance of cybersecurity, they saw increased engagement and more seriousness towards the trainings. Another challenge was the early integration of security awareness, particularly for new hires. To address this, IR3 has implemented an introductory training for new employees to foster early awareness and understanding of information security, aiding them in building a solid foundation of security awareness and promoting good security practices from the beginning. This aligns with IR1's sentiments, highlighting the importance of early and ongoing training.

IR2 also mentions the need for empathy towards employees, saying, "We must remember that those working in the finance department, for example, do not have the same experience with IT security. It's not their specialty. We still need to enlighten and educate them on the topic, understanding that they may not have strong prior knowledge." IR1, IR3 and IR4 agreed with this, highlighting the importance of tailoring training to employees' varied backgrounds.

Adapting the length of the training sessions was also seen as crucial to counter resistance and the risk of boring the users. IR3 illuminated the challenge of maintaining user interest without boring them, a sentiment shared by IR1 and IR2, who mentioned not making the training too tedious or lengthy. IR2 said, "If users have to spend an hour a week, they will get bored, but if it only takes 5-10 minutes a week, it doesn't seem as daunting, and interest is still maintained. This has been important for us to achieve success." IR1 added, "The exercises only take 2-5 minutes, which has been predetermined by the external provider we use, and it has worked well for us." IR3 also highlighted this, saying, "Another challenge is not to tire out the users and always maintain their interest. We've handled this by creating short, topic-specific trainings instead of lengthy ones covering multiple subjects at once, which can cause users to lose interest."

By actively addressing these challenges, IR1, IR2, IR3, IR4, and IR5 have observed increased efficiency in the program and positive changes in employees' attitudes, behaviors, and understanding of cyber risks. It has become clear that early and continuous investment in security awareness is crucial for establishing a strong information culture, which is an important part of facing the challenges that arise along the way. This approach has also helped reduce cyber risks; a sentiment shared by all respondents.

5.1.2 Impact of Security Awareness Training on IT Security and Incident Reduction

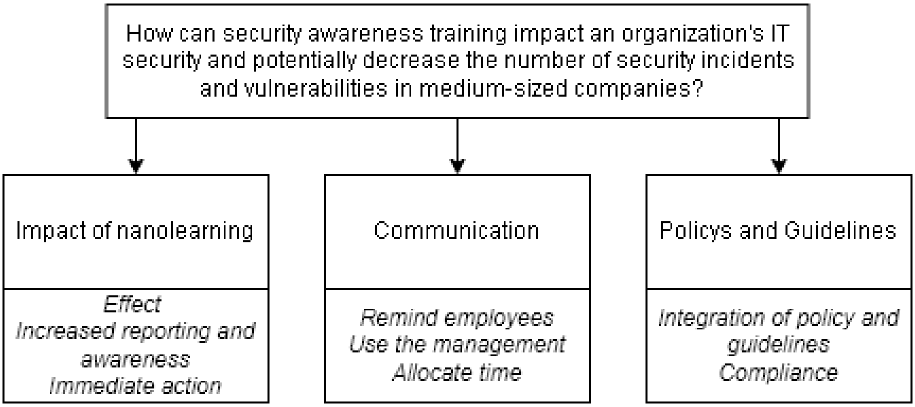
How can security awareness training impact an organization's IT security and potentially decrease the number of security incidents and vulnerabilities in medium-sized companies?
Impact of nanolearning
Effect
Increased reporting and awareness
Immediate action
Communication
Remind employees
Use the management
Allocate time
Policys and Guidelines
Integration of policy and guidelines
Compliance

Figure 3, Themes and codes related to Research Question 2 (authors own)

Impact of Nanolearning

The effect of nanolearning was clear in the insights provided by those interviewed, with their comments indicating a rise in awareness and a better response to security threats.

According to IR1, "We've noticed that people today pay more attention to vulnerabilities, which we see as clear signs when they reach out to us. We used to neither measure nor talk about incidents, but now we do, and incidents get reported." They stressed the importance of reporting incidents, even in situations when one employee clicked on seemingly reliable but compromised link. IR1 further added, "When this was found out, it was reported right away, which let us isolate the impacted computer, shut it down, and reformat it."

Similarly, IR2 pointed out the positive effects of nanolearning, stating, "We have not had any significant security incidents, but we've found vulnerabilities that weren't previously detected by employees, but instead by our IT security team." They emphasized the growing awareness among staff from different departments, who can now identify vulnerabilities before they turn into security incidents. IR2 remarked, "It's become part of every project, and it's certainly an advantage. Everyone has been able to contribute and think about security in other departments."

In agreement with the others, IR3 recognized the positive impact of nanolearning, stating, "We can see that users are daring to report and speak up if they notice anything suspicious. This is positive." They further stressed the importance of immediate reporting, saying, "We really stress that one should report right away if anything happens, so that we can make time to address the situation and not pretend like nothing is happening."

IR4 contributed by stating that nanolearning significantly increased the tendency to report, particularly in cases of suspected emails. IR4 pointed out that the main goal of raising awareness has been achieved, as evidenced by the increase in reporting, questions, and dialogue about information security. Furthermore, IR4 mentioned that self-assessments showed that 98-99% of participants felt an increase in their knowledge of information security.

IR1 explains that they don't necessarily have a concrete method to accurately measure the effect of the training programs. However, they have observed a local increase in reporting rates, indicating that people are becoming more conscious. When they initiated their nanolearning sessions, the response rate to the questions stood at 75%. In the second year, this rate increased to an average of 85%. "This is a clear sign that people are taking the nanolearnings seriously and actively discussing it with others." IR2, on the other hand, mentions that they can extract a lot of statistics from the external program they use. IR2 said, "We have access to a lot of statistics, including statistics from the other clients of the external training program. Even though we do not know their names or companies, we can compare how we manage against others who use the same service." IR3 notes that they handle everything in-house, and as a result, they cannot see any specific statistics other than noticing changes in casual conversations in the break room. Although less structured, this informal feedback provides valuable insights into the impact of their training programs.

Together, these statements demonstrate the positive influence of nanolearning in increasing awareness, encouraging incident reporting, and fostering a culture of security consciousness within the organizations.

Communication

All respondents emphasize the importance of communication and engagement regarding security awareness and nanolearning within their organizations.

IR3 states, "We communicate the importance of nanolearning to our employees in various ways. One of our main strategies is to consistently highlight and discuss the significance of 'security awareness training' during meetings, larger gatherings, and conferences. These events provide us with excellent opportunities to highlight the constant need to stay updated with the latest security principles and procedures." IR3 continues: "In addition to this, we use our internal intranet to continuously share vital information and updates about security and nanolearning." By disseminating this information in an accessible and regular manner, IR3 mentions that they can reach all employees regardless of their position or job responsibilities. IR3 also mentions that they aim to implement security thinking early in new employees by initially providing them with more extensive security training, laying a foundation from the start. IR1 shares a similar strategy with IR3, stating that their employees undergo MSB's DISA training as part of their introduction.

IR4 adds that communication is partly achieved by informing and anchoring the training with management and managers, who are responsible for motivating and following up with their employees, and partly through information on the intranet. Additionally, IR4 mentions other concurrent activities, such as information security training with each unit and information campaigns.

IR3 notes that their operation handles quite sensitive information, "As we handle sensitive information in our operation, our employees are already aware of the importance of security, and we don't always need to communicate its importance." "This awareness has made it easier for us to motivate them to actively participate in the nanolearning programs. They understand that their engagement in these programs protects the organization, their personal data, and the sensitive work they perform."

IR5 emphasizes the utilization of emails and reminders to ensure that everyone completes the mandatory nanolearning programs.

IR2 notes, "Before we introduced the security awareness training program for the employees, I and the program's responsible sent out a phishing email to assess the current level of the employee's awareness. This was done to gain insight into how well-prepared we were for cyber threats. After this step, we informed everyone about the new program. From that point, everything is more or less automated". The program IR2 uses adapts the training based on each individual's knowledge level and the areas they have previously struggled with. Providing extra motivation to employees has not been deemed necessary in this context, as the program itself and the employee interactions appear to promote this naturally. The visibility of statistics regarding which departments have yet to complete their training encourages a form of mutual motivation. IR2 explains that the program's ranking system is a significant motivating factor in this dynamic. "It taps into a competitive spirit, with many striving to attain higher rankings, making the learning process more fun."

Getting the management team involved is very important for successful communication to the employees. This is something both IR1, IR3, and IR6 emphasize. IR1: "Despite some considering they have more important things to do, we have made it clear to everyone, primarily the management team who has passed it on to all employees, that this is a priority." IR1 continues, "We are quite pleased that almost 90% participate this year". IR3 mentions that "The management team is also involved in the process. They have access to all statistics and keep the employees updated on the importance of participating in the nanolearning programs."

IR6 highlights the role of external factors in communication, stating, "Yes, it's about communicating through the management how important it is and that we continuously remind and discuss this subject. Right now, we are also naturally supported by what is happening in the outside world, as social media, and news report on related events. This in itself serves as a form of education when the subject is brought up in the media, on TV, and so on."

All respondents underscore the importance of feedback and continuous updates within their IT security and nanolearning programs. IR3: "Taking in feedback is also a crucial part; this allows employees to communicate with us about what they think about the training and what needs to be improved." IR1 agrees with this and emphasizes the importance of direct communication and feedback after introductory training, creating opportunities for continuous improvements based on employee experiences and insights. Additionally, IR4 stated, "Absolutely, evaluation and follow-up of the intended effect are an important part of educational efforts. We have conducted an evaluation that includes design, method, and with the opportunity to also leave other comments." This highlights the importance of evaluating the effectiveness of the educational programs.

Policies and Guidelines

All respondents agreed on the important role that written policies, standards, and governance documents have in their respective organizations' nanolearning programs. IR1 noted that many components included in the nanolearning programs are detailed in their guidelines or governing documents. Specifically, they have user guidelines for information security that serve as a foundational platform. Additionally, IR1 shared that at the end of the nanolearning programs, there are often links to their governing documents where users can further read about a particular topic or similar. "This has been crucial for us in order to enhance knowledge," says IR1. IR3 follows a similar approach where their intranet allows further reading on certain topics and offers quizzes to test the users' knowledge. IR3 also emphasizes the importance of policies and guidelines as an additional resource for employees. The nanolearning programs address key components that are further elaborated on in the governing documents and policies. IR3 notes that the nanolearning programs, governance documents, and policies genuinely complement each other. "If you want to know more about anything, the information is in our other documents," states IR3.

IR5 adds, "All employees will read and sign the IT Use policy on an annual basis. If significant changes to the policy are made, employees may be required to read and sign the policy at that time. All policy documents are available on the intranet. The nanolearning modules that are sent out often involve a review of the previously mentioned policies and understanding how to detect threats and other things that can affect IT security."

Furthermore, IR6 mentions that they are nearing completion in updating their governing documents and policies to communicate best practices more effectively for cybersecurity. IR6 states, "We are almost done with this and are in the process of finalizing them. They don’t cover everything, but they explain the importance of cybersecurity and other things that are important to know."

However, IR2 has not exactly taken the same approach but mentions: "Besides the training program itself, I have created guidelines for information classification. This helps employees understand how different types of data should be handled. For example, if an email contains a certain type of personal data, it will be classified at a specific level according to the guidelines I have developed. This provides employees with a clear indication of what can and cannot be sent to external recipients, and it complements the information given in the nanolearning programs.

6. Discussion

In this chapter, the discussion draws upon the findings from the systematic literature review (SLR) and the interviews conducted with all the respondents. The goal is to understand the study's implications regarding the role of security awareness training and nanolearning in organizations. Evidence from academic research and real-world experiences is considered to explore the connection between these two different but related perspectives. By connecting findings from the SLR and the interviews, a complete understanding of the topic is presented, evaluating how effective security training programs are at dealing with cyber threats.

6.1 Key insights from Interviews focused on RQ1

The interviews reveal an important shift in employee attitudes towards cyber risks, a factor found to be significant in the SLR. According to all respondents, continual security awareness training, when effectively implemented, leads to a noticeable change in employee behavior. This aligns with the findings of Sas et al. (2021) and Alshaikh, Maynard, and Ahmad (2021), who pointed out that security knowledge and positive attitudes towards security are linked to secure behavior.

Moreover, the interviewees emphasize the importance of management support in instilling a strong security culture in the organization. IR3 specifically states, "you need the bosses on board to build a real security culture in the company." This observation echoes the findings of Dahabiyeh (2021), who identified top management support as one of the crucial factors in improving Security Awareness Training (SAT) programs.

As noted by IR1, IR3, IR4 and IR6 the increased engagement of employees and their cautious behavior towards potential cyber threats suggest a heightened security awareness. This increased awareness is likely to have been brought about by the consistent and effective training, as postulated by Tschakert and Ngamsuriyaroj (2019), who highlighted the benefits of training programs in reducing susceptibility to phishing attacks.

Regarding the delivery of nanolearning, both IR2 and IR1 emphasized tailoring the training to meet individual needs and skill levels, an approach that Kwak et al. (2020) advocated. This personalized training approach is seen as crucial to engaging employees effectively and promoting secure behavior. IR6 also emphasized the importance of adapting the training to the target group and making it reflective of the actual work environment. This comment by IR6 aligns with the insights from Alyami et al. (2022) regarding the importance of tailoring SETA programs to employees' learning styles and job roles. This need for customization is also underlined by Pattinson et al. (2020), who found that alignment of training type with participants' learning preferences and demographics is crucial for Information Security Awareness enhancement. This personalized training approach is seen as crucial to engaging employees effectively and promoting secure behavior.

IR6 highlighted the importance of a coherent communication strategy in training, illustrating the need for consistent messaging and methods in education, which is in line with IR1's approach of using staff meetings to address information security.

Finally, the noticeable change in the behavior of employees towards handling sensitive information, as noted by IR1, aligns with the idea proposed by Fagade et al. (2017) that pre-employment background checks and other mechanisms can help identify agents that pose behavioral risk, and the more cautious behavior is indicative of an increased awareness of these risks.

Overall, the findings from the interviews provide practical insights that align with the theoretical research from the SLR, reinforcing the value of ongoing, tailored security awareness training and strong management support, coherent communication strategies, and employee engagement in enhancing employees' cybersecurity behavior. The personalization and alignment with employee needs, as emphasized by IR6 and supported by Alyami et al. (2022) and Pattinson et al. (2020), are essential in fostering engagement and meeting the unique security needs of both individuals and organizations.

6.2 Key insights from interviews focused on RQ2

Cyber threats such as phishing attacks pose significant risks to organizations. As noted by Kwak et al. (2020), they are common tools for hackers. Training programs aimed at raising awareness about these threats have shown efficacy in both decreasing the number of victims and boosting participants' self-assurance in spotting and avoiding these dangers (Tschakert & Ngamsuriyaroj, 2019). The improvement in reporting rates post-nanolearning programs initiation, as seen in the interviews conducted, corroborates this. Participant IR1 noted an increase from 75% to 85% in response rate within two years of implementing the nanolearning sessions, hinting at the efficacy of these training programs in heightening awareness about such threats.

The relationship between employee's security knowledge, their attitudes towards security issues, and their behavior has been well-established in studies like those by Sas et al. (2021) and Alshaikh, Maynard, and Ahmad (2021). Employees with greater security knowledge and a more positive attitude towards security are likely to engage in more secure behaviors. In the interviews conducted, participants IR1, IR2 and IR4 echoed these findings, mentioning employees becoming more aware and actively participating in discussions on security issues after the training programs. IR3 cited noticeable changes in casual conversations in the break room, indirectly indicating a shift in attitudes and behaviors.

However, the efficacy of security training programs can be impeded by setbacks into old habits or neglect to adhere to recommended policies. Therefore, it is essential to design these programs according to the needs and preferences of the target audience (Alshaikh, Maynard, and Ahmad, 2021; Sas et al., 2021). This was reinforced by interviewees IR1, IR2, IR3, IR4 and IR6, who stressed the importance of communication and engagement in security awareness and nanolearning. They highlighted the crucial role of management in endorsing these programs and the need to adjust them based on individual knowledge levels.

Another common conclusion that emerged from both the SLR, and the interviews was the role of written policies, standards, and governance documents. They guide and shape security awareness training and nanolearning programs.

Stewart and Jürjens (2017) accentuated the importance of organizational policies as fundamental rules protecting an organization's assets. This view was somehow mirrored by all the respondents, whom all acknowledged that these documents were essential in their respective organizations' training programs.

Interestingly, IR6's experience of sending out fake phishing emails and providing training when recipients clicked on them is in line with the approach highlighted by Kävrestad et al. (2023), called Context-Based Micro-Training (CBMT). CBMT emphasizes providing training at the moment it is needed, ensuring it is timely and directly applicable. This approach is beneficial because it addresses the challenges of knowledge retention and ensures that the training is timely, directly applicable, and less likely to be viewed as an interruption, thereby encouraging user participation and engagement. This effectiveness is exemplified through IR6's practice, demonstrating how immediate feedback and training can significantly impact users' awareness and behavior.

In summary, both the SLR and the interviews conducted emphasize the criticality of security awareness training programs in managing information security and fostering a security-conscious behavior amongst employees. Both traditional methods and the key role of policies and guidelines are highlighted in both studies. The real-world experiences from the interviews further validate academic research, underscoring the significance of these elements in establishing effective security training programs.

6.3 Limitations

The study has several limitations that should be acknowledged, despite the rigorous research design and careful consideration of the data collection methods. One potential limitation is the use of a qualitative research approach, which may limit the generalizability of the findings to other settings. Qualitative research aims to explore a particular phenomenon in-depth and does not aim to produce statistically representative results. Therefore, the findings of this study may not be applicable to other types of organizations or industries.

Another limitation is the use of semi-structured interviews as the primary data collection method. While this approach allows for a more open-ended and exploratory approach to data collection, it may also introduce potential biases, such as interviewer or participant bias. The interviewers' personal beliefs and experiences may influence the interpretation of the data, and the participants' responses may be influenced by social desirability bias or their desire to present themselves in a positive light.

Additionally, the selection of interviewees using a non-random approach may limit the generalizability of the findings. While this approach was chosen to ensure that the interviewees possessed valuable insights into the IT departments and knowledge of security awareness training in medium-sized companies, it may also limit the range of perspectives represented in the study.

Finally, the sample size of 6 medium-sized companies may also be a limitation of this study. While the sample was selected strategically to provide a comprehensive understanding of the general operations and practices of medium-sized companies in Sweden, the findings may not be applicable to other types of organizations or industries.

In conclusion, while this study provides valuable insights into the topic of security awareness training in medium-sized companies, the limitations should be considered when interpreting the findings and generalizing the results to other settings.

6.4 Methods, implementation, and results

The choice of combining a structured literature review (SLR) and interviews, allowed for a more holistic understanding of the topic. The SLR provided a broad overview of the academic perspective on security awareness training, whereas the interviews offered real-world insights from the professionals in the field. The triangulation of data from these different sources enhanced the validity and credibility of the findings.

As with any research, different understandings of the results are possible. For instance, changes seen in how employees act might be due to things other than security training. This could include changes in the company's way of doing things or outside factors. Also, since interviews depend on each person's views, their answers could be shaped by personal bias or way of seeing things. This could impact the understanding of the results.

The findings from this study highlight the importance of implementing effective security awareness training in organizations. The interviews and the results from the SLR suggest that tailored and ongoing training programs, supported by management, can lead to more secure employee behaviors. Therefore, organizations may benefit from including such training strategies.

6.5 Validity

In reflecting on the validity of the research, there are several factors to consider. The study initially sought to conduct interviews with eight or more companies, but due to limited participation, only three were accomplished. This gap might impact the generalizability of the results. Fewer perspectives could leave out potentially diverse experiences and approaches to security awareness training, leading to a somewhat limited understanding. This issue may be further compounded by the possibility that many organizations, especially those primarily focused on financial operations, may not implement security awareness training since they have no one that works with it. Therefore, the sample may not be representative of all types of organizations. Interviews naturally present some validity issues. Participants may be prone to providing socially desirable responses or could be influenced by the phrasing of the questions, unintentionally introducing bias into the results. Measures were taken to mitigate this, but there is always a risk of it affecting the responses to some extent.

A language aspect is also crucial to consider. The interviews were conducted in Swedish and then translated into English. Kapborg & Berterö (2002) highlights that translating from one language to another can be very complex due to subtle differences in meaning. While some languages may share similarities with English, others do not. Moreover, certain words or concepts might not have direct translations due to cultural differences or non-equivalent terms. The translation process might introduce semantic changes, affecting the precision of the data and its subsequent analysis. Additionally, it is important to recognize the potential impact of the researcher's own biases and preconceptions on the interpretation of the data. As highlighted by M.Berndtsson et al. (2008) the background and values of the researcher can “colour” their perception, observation, and interpretation of the data. Despite these potential validity issues, this research delivers valuable insights into security awareness training in the companies involved. It lays the groundwork for further, perhaps more extensive, investigations into this area.

6.6 Ethical and Societal Aspects

6.6.1 Ethical Aspects

To ensure that the ethical aspects have been addressed, all respondents has been informed that anonymity applies to them and to companies they work for. The names of the interviewed respondents, personal information, or which companies they work for are not important and do not affect the results of the study. Offering anonymity can help to obtain selected respondents more easily and to express themselves honestly and confidently in the interviews.

Beyond confidentiality, the study's ethical aspects also include the implications of the results on organizations and their stakeholders. Security awareness training can affect an organization’s reputation, employee morale, and trust between stakeholders. The results can guide organizations in making informed decisions regarding security practices, and this holds ethical weight as it can impact not only the organization but also its internal and external stakeholders. For instance, adequate security awareness training can protect customer data, and the ethical handling of such data is critical to maintaining trust and ethical business practices.

6.6.2 Societal Aspects

The study also has broader societal implications. Security awareness training is not just an organizational tool but holds significance in the larger societal context.

In consideration to the United Nations 17 Sustainable Development Goals (SDGs) The use of security awareness training and ethical conduct in the research aligns with several of the goals. The research promotes security awareness training which can be contributed to Goal 4: Quality Education. Goal 4.4 to be exact which aims to increase the number of individuals with relevant technical skills for employment, decent jobs, and entrepreneurship by 2030 (UN, 2018). Security awareness training is a crucial technical skill in the current digital workplace. By empowering employees with the knowledge and tools to navigate the digital environment safely, this research can help to create a workforce that is better equipped for the evolving demands of modern employment. As such, security awareness training is not just a tool for risk mitigation, but it's also an instrument for fostering sustainable growth and enhancing vocational skills.

The research also aligns with Goal 9: Industry, Innovation, and Infrastructure (UN, 2018). By fostering awareness on mitigating cyber threats and risks, it contributes to building resilient infrastructure in the digital era and supports new and well-working approaches for security.

Lastly, this study's emphasis on security awareness training fits well with Goal 17.8 of the United Nations' Sustainable Development Goals. This goal calls for increased use of helpful technologies, especially information, and communication technology (UN, 2018) Security awareness training teaches how to use information and communication technology responsibly and effectively. It helps people understand the dangers and the importance of being safe when using digital technologies. By strengthening these skills and knowledge, this study indirectly supports the better and safer use of these crucial technologies, which can help economic and social growth in areas that are not as advanced in technology.

In summary, ethical considerations ensure the responsible conduct of the research and its implications for stakeholders, while societal aspects emphasize the broader consequences and contributions of security awareness training to the welfare and development of society.

7. Conclusion

The study aimed to investigate the impact of security awareness training on employee attitudes and behaviors related to cyber risks and on IT security within an organization. These were the research questions:

Research question 1: How does security awareness training impact employees' attitudes, behaviours, and knowledge related to cyber risk in medium-sized companies?

Research question 2: How can security awareness training impact an organization's IT security and potentially decrease the number of security incidents and vulnerabilities in medium-sized companies?

The research utilized a SLR to understand the effectiveness of various methods of security awareness training and how they contribute to reducing cyber risks. Key findings included the importance of continuous training, the correlation between security knowledge and attitudes, the effectiveness of unconventional training methods, and the ways to enhance the quality and relevance of these training programs.

Interviews, which was the primary source of information was conducted with representatives from different medium-sized companies, supported the findings of the SLR, highlighting the positive shift in employee attitudes towards cyber risk due to ongoing training. The interviews further emphasized the importance of management support, tailored training methods, and proactive addressing of challenges in promoting secure behaviour among employees.

The impact of nanolearning, a specific method of training, was another central theme in the interviews. Respondents discussed how nanolearning led to increased awareness and improved response to security threats, underscoring the value of consistent communication and management support for successful implementation. The role of feedback, regular updates, and well-defined policies and guidelines also emerged as essential aspects of these training programs.

Additionally, it was highlighted in this study that one of the reasons why nanolearning was particularly effective was due to the thoughtful approach taken by those responsible for its implementation. The organisations didn't just implement nanolearning without prior notice. Instead, they prepared the employees for these trainings, and actively sought feedback. They also engaged in discussions during conferences or seminars with the organisations to understand whether nanolearning was truly making an impact. This indicated that the responsible parties had a well-thought-out plan for the roll-out and assessment of nanolearning, which likely contributed to the successful implementation and positive outcomes seen with this study.

The findings from the interviews provided a practical perspective to the academic research from the SLR, confirming the importance of continuous, customized security awareness training, supported by strong management commitment, in enhancing cybersecurity behaviour among employees.

In summary, the research validates that security awareness training significantly promotes a culture of cybersecurity awareness within organizations. For these programs to be effective, they should be ongoing and personalized to accommodate individual requirements, with full backing from the organization's management. Additionally, when properly executed, such training initiatives can decrease the incidence of security breaches, thereby enhancing the overall IT security posture of an organization.

7.1 Future work

The findings from this study offer several promising approaches for future work. While this research demonstrated the significant impact of security awareness training on employee attitudes and behaviors and on IT security in an organization, there are several aspects that could be further explored. One of these aspects could be the Effectiveness of Various Training Methods. Since this research highlighted the benefits of nanolearning and continual security awareness training. Future work could investigate the comparative effectiveness of different training methods, such as workshops, short videos, simulations, e-learning, and one-on-one sessions, in fostering cybersecurity awareness. Understanding the effectiveness of various training methods can significantly benefit organizations. With such information, they could tailor their training pro-grams more efficiently, choosing the method that has the most significant impact on employees' attitudes, behaviors, and knowledge related to cybersecurity. A comparative study of this nature could result in more effective and efficient security awareness training programs, further strengthening the cybersecurity posture of organizations.

Additionally, since it was highlighted in this study that one of the reasons why nanolearning was particularly effective was due to the thoughtful approach taken by those responsible for its implementation, future work could also examine how the planning and execution strategies contribute to the success of these training methods. Investigating the best practices in preparing employees, collecting feedback, and evaluating the impact through conferences or seminars could provide valuable insights for organizations seeking to maximize the effectiveness of their training programs.

The research setting was also limited to a single country, and cultural factors influencing attitudes and behaviors toward cybersecurity were not considered. Future research could include cross-cultural studies to investigate the influence of different cultural contexts on security awareness and training effectiveness.

These are just a few possibilities for future work in this field, with many more to explore. Cybersecurity is a critical area in our society, with the safety of individuals and organizations constantly being challenged by cyber threats. As such, it is essential to continue to explore and develop the best methods to keep people and organizations secure.

References

Abu-Amara, F., & Tamimi, H. (2021). Cyber shield security awareness program. *Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development, INDIACom 2021*, 422–425. https://doi.org/10.1109/INDIACom51348.2021.00075

ACM Digital Library. (2023). 2023. https://dl.acm.org/about [Accesed: 2023-04-02]

Akinyelu, A. A., & Adewumi, A. O. (2014). Classification of phishing email using random forest machine learning technique. *Journal of Applied Mathematics, 2014*. https://doi.org/10.1155/2014/425731

Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017). Security awareness training: A review. *Lecture Notes in Engineering and Computer Science*, *2229*, 446–451.

Alkhazi, B., Alshaikh, M., Alkhezi, S., & Labbaci, H. (2022). Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior. *IEEE Access*, *10*(November), 132132–132143. https://doi.org/10.1109/ACCESS.2022.3230286

Alshaikh, M., Maynard, S. B., & Ahmad, A. (2021). Applying social marketing to evaluate current security education training and awareness programs in organisations. *Computers and Security*, *100*, 102090. https://doi.org/10.1016/j.cose.2020.102090

Alyami, A., Sammon, D., Neville, K., & Mahony, C. (2022). The Critical Success Factors for Security Education, Training and Awareness (SETA) Programmes. *2022 Cyber Research Conference - Ireland, Cyber-RCI 2022*. https://doi.org/10.1109/Cyber-RCI55324.2022.10032674

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information and Computer Security*, *27*(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Berndtsson, M., Hansson, J., Olsson, B., & Lundll, B. (2008). *Thesis Projects - A Guide for Students in Computer Science and Information Systems*.

Chapman, P. (2021). Defending against insider threats with network security's eighth layer. *Computer Fraud and Security*, *2021*(3), 8–13. https://doi.org/10.1016/S1361-3723(21)00029-4

Dahabiyeh, L. (2021). Factors affecting organizational adoption and acceptance of computer-based security awareness training tools. *Information and Computer Security*, *29*(5), 836–849. https://doi.org/10.1108/ICS-12-2020-0200

Denscombe, M. (2014). *The good research guide: Research methods for* *small-scale social research projects. London: Open University Press, McGraw Hill.*

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing*, *62*(1), 107–115. https://doi.org/10.1111/j.1365-2648.2007.04569.x

FBI. (2022). *2022 Internet Crime Report FBI's Internet Crime Complaint Center (IC3). 2022*(I), 10–13. [Accesed: 2023-05-12]

Furnell, S., Khern-am-nuai, W., Esmael, R., Yang, W., & Li, N. (2018). Enhancing security behaviour by supporting the user. *Computers and Security*, *75*, 1–9. https://doi.org/10.1016/j.cose.2018.01.016

Haney, J., & Lutters, W. (2020). Security Awareness Training for the Workforce: Moving beyond "check-the-Box" Compliance. *Computer*, *53*(10), 91–95. https://doi.org/10.1109/MC.2020.3001959

Hielscher, J., Kluge, A., Menges, U., & Sasse, M. A. (2021). "Taking out the Trash": Why Security Behavior Change requires Intentional Forgetting. *ACM International Conference Proceeding Series*, 108–122. https://doi.org/10.1145/3498891.3498902

IEEE Xplore. (2023). 2023. https://ieeexplore-ieee-org.libraryproxy.his.se/Xplorehelp/overview-of-ieee-xplore/about-ieee-xplore [Accesed: 2023-04-02]

Jain, A. K., & Gupta, B. B. (2017). Phishing detection: Analysis of visual similarity based approaches. *Security and Communication Networks*, *2017*(i). https://doi.org/10.1155/2017/5421046

Jesson, J., & Lacey, F. (2006). How to do (or not to do) a critical literature review. *Pharmacy Education*, *6*(2), 139–148. https://doi.org/10.1080/15602210600616218

Kapborg, I., & Berterö, C. (2002). Using an interpreter in qualitative interviews: Does it threaten validity? *Nursing Inquiry*, *9*(1), 52–56. https://doi.org/10.1046/j.1440-1800.2002.00127.x

Kwak, Y., Lee, S., Damiano, A., & Vishwanath, A. (2020). Why do users not report spear phishing emails? *Telematics and Informatics*, *48*(August 2019), 101343. https://doi.org/10.1016/j.tele.2020.101343

Kävrestad, J., Furnell, S., & Nohlberg, M. (2023). User perception of Context-Based Micro-Training–a method for cybersecurity training. *Information Security Journal*, *00*(00), 1–17. https://doi.org/10.1080/19393555.2023.2222713

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2020). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the paandemic. *ArXiv*, 1–20.

Lancet, T. (2023). *Facts about ScienceDirect*. 2. https://www.elsevier.com/solutions/sciencedirect [Accessed: 2023-04-02]

Lang, M., & Connolly, L. (2022). Managing the Cybersecurity Risks of

Teleworking in the Post-Pandemic "New Normal." *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4146506

Leal Filho, W., & Kovaleva, M. (2015). Research Methods. *Environmental Science and Engineering*, *5*(3), 81–82. https://doi.org/10.1007/978-3-319-10906-0_5

Li, L., He, W., Xu, L., Ivan, A., Anwar, M., & Yuan, X. (2014). Does explicit information security policy affect employees' cyber security behavior? A pilot study. *Proceedings - 2nd International Conference on Enterprise Systems, ES 2014*, 169–173. https://doi.org/10.1109/ES.2014.66

Marshall, M. N. (1996). *Sampling for qualitative research*. *13*(6), 522–525. https://www.semanticscholar.org/paper/Sampling-for-qualitative-research.-Marshall/12dff0acfdd704217a7e89b842ca4ebc902023eb

Matli, W., & Wamba, S. F. (2023). Work from anywhere: inequalities in technology infrastructure distribution for digit workers. *Digital Transformation and Society*, *2*(2), 149–162. https://doi.org/10.1108/dts-08-2022-0042

Medvet, E., Kirda, E., & Kruegel, C. (2008). Visual-similarity-based phishing detection. *Proceedings of the 4th International Conference on Security and Privacy in Communication Networks, SecureComm'08*. https://doi.org/10.1145/1460877.1460905

Okoli, C. (2015). A guide to conducting a standalone systematic literature review. *Communications of the Association for Information Systems*, *37*(1), 879–910. https://doi.org/10.17705/1cais.03743

Okoli, C., & Schabram, K. (2010). Working Papers on Information Systems A Guide to Conducting a Systematic Literature Review of Information Systems Research. *Working Papers on Information Systems*, *10*(2010). https://doi.org/10.2139/ssrn.1954824

Pattinson, M., Butavicius, M., Lillie, M., Ciccarello, B., Parsons, K., Calic, D., & McCormac, A. (2020). Matching training to individual learning styles improves information security awareness. *Information and Computer Security*, *28*(1), 1–14. https://doi.org/10.1108/ICS-01-2019-0022

Sas, M., Reniers, G., Ponnet, K., & Hardyns, W. (2021). The impact of training sessions on physical security awareness: Measuring employees' knowledge, attitude and self-reported behaviour. *Safety Science*, *144*(August), 105447. https://doi.org/10.1016/j.ssci.2021.105447

Shahi, C., & Sinha, M. (2021). Digital transformation: challenges faced by organizations and their potential solutions. *International Journal of Innovation Science*, *13*(1), 17–33. https://doi.org/10.1108/IJIS-09-2020-0157

Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information and Computer Security*, *25*(5), 494–534. https://doi.org/10.1108/ICS-07-2016-0054

Tonkin, A., & Kosasih, W. (2023). *Simulating cyber security management : A gamified approach to executive decision making*. https://doi.org/10.1145/3551349.3561148

Tschakert, K. F., & Ngamsuriyaroj, S. (2019). Effectiveness of and user preferences for security awareness training methodologies. *Heliyon*, *5*(6), e02010. https://doi.org/10.1016/j.heliyon.2019.e02010

UN. (2018). *The 2030 Agenda and the Sustainable Development Goals An opportunity for Latin America and the Caribbean Thank you for your interest in this ECLAC publication*. https://repositorio.cepal.org/bitstream/handle/11362/40156/25/S1801140_en.pdf [Accesed: 2023-05-15]

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A. (2012). Experimentation in software engineering. In *Experimentation in Software Engineering* (Vol. 9783642290). https://doi.org/10.1007/978-3-642-29044-2

Young, J. C., Rose, D. C., Mumby, H. S., Benitez-Capistros, F., Derrick, C. J., Finch, T., Garcia, C., Home, C., Marwaha, E., Morgans, C., Parkinson, S., Shah, J., Wilson, K. A., & Mukherjee, N. (2018). A methodological guide to using and reporting on interviews in conservation science research. *Methods in Ecology and Evolution*, *9*(1), 10–19. https://doi.org/10.1111/2041-210X.12828

Zhang, Z. (Justin), He, W., Li, W., & Abdous, M. (2021). Cybersecurity awareness training programs: a cost–benefit analysis framework. *Industrial Management and Data Systems*, *121*(3), 613–636. https://doi.org/10.1108/IMDS-08-2020-0462

Appendices A

Interview questions:

General questions

1. Can you tell me a bit about yourself and your role in the organization?
2. How long have you worked within the IT department, and what are your primary responsibilities concerning security awareness training/nanolearning?
3. Before we delve into the subject of nanolearning, could you share a bit of your experience with IT security . Studies/work experience

Questions related to RQ1: How do security awareness training impact employees' attitudes, behaviours, and knowledge related to cyber risk in medium-sized companies?

1. Which nanolearning programs or similar is used in your organization to manage vulnerabilities and cyber risks?
2. What are the key components of these programs, and how are they provided to employees? In other words, in what form are the trainings given?
3. Can you give some specific examples of changes you have observed in employees' attitudes, behaviors, and knowledge of cyber risks following the introduction of security awareness training?
4. In your experience, what are the most common challenges or barriers to successfully implementing nanolearning programs, and how does your organization handle these challenges?

Questions related to RQ2: How can security awareness training impact an organization's IT security and potentially decrease the number of security incidents and vulnerabilities in medium-sized companies?

1. Can you share your organization's experience with nanolearning and its impact on reducing the number of security incidents or vulnerabilities previously observed? Can you see that the number of incidents decreased since the introduction of the trainings?
2. How do you measure the effect of nanolearning when it comes to reducing the number of security threats or cyber incidents within your organization?
3. How do you communicate the importance of these security trainings to your employees and motivate them to actively participate in nanolearning programs?
4. How do governance documents, policies, or other standards influence the nanolearning programs for employees? Can you give an example of their application? Do these documents contain guidelines, requirements, or expectations to promote cybersecurity and security awareness in the organization?