

Implementation of methods to raise employee's cybersecurity awareness in small businesses with small-scale IT teams.

MSc Research Project
Cybersecurity

Jonas Schweizer
Student ID: x21168776

School of Computing
National College of Ireland

Supervisor: Ross Spelman

National College of Ireland
MSc Project Submission Sheet
School of Computing



Student Name: Jonas Luis Schweizer
Student ID: X21168776
Programme: MSc Cybersecurity **Year:** 2023
Module: Academic Internship
Supervisor: Ross Spelman
Submission Due Date: 14/12/2023
Project Title: Implementation of methods to raise employee's cybersecurity awareness in small businesses with small-scale IT teams
Word Count: 10393 **Page Count** 21

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Jonas Luis Schweizer

Date: 13/12/2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	<input type="checkbox"/>
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Implementation of methods to raise employee's cybersecurity awareness in small businesses with small-scale IT teams.

Jonas Schweizer
X21168776

Abstract

With the increase of cyber treats and cyber criminals targeting small business, these businesses face heightened cybersecurity challenges in the rapidly evolving digital landscape. The human factor in the cybersecurity threat landscape is responsible for a considerable part of the cyber incidents. It is necessary to ensure that small businesses are not only equipped with the technology to mitigate incidents but also with the awareness and knowledge to stop them. This study investigates the most time-efficient web-based security training and education methods tailored for Small and Medium Enterprises (SMEs). The paper utilises different areas of focus that should be considered when preparing the training campaigns and delivers cybersecurity awareness training using different web-based training methods. Through an innovative efficiency metric, the study evaluates different delivery methods, with a focus on SMEs' unique limitations. The paper presents a comprehensive structured for designing and implementing Security Education and Training Awareness (SETA) campaigns. Results indicate that gamification training method appears as the most suitable method for SMEs. Also, the time spent creating training campaigns does not directly positively or negatively affect the learning outcomes. While recommendations mentioned increase of the data population for improved results, the paper successfully presents a targeted time-efficient approach to cybersecurity awareness education in SMEs which was still a gap in the research field.

1 Introduction

As the technology in the world evolves, its adoption by people and organisations increases. Just after a pandemic that lasted more than two years, organisations of all sizes had to increase or completely start from zero their online presence to cope with new ways of doing business. With this sudden change, risks to the cybersecurity and the organisations data increases as more and more information becomes available on the internet. Even though the organisations have rapidly tried to improve and scale its cybersecurity protections, the human factor of cybersecurity has proven to be the most challenging to adapt to this new area of work. A report from Verizon in 2023 shows that 74% of all organisations breaches resulted from human elements(VERIZON, 2023). This is the reason organisations have shifted their focus to ensure that end users are aware of the internet threats. Small and Medium Enterprises (SMEs) still face difficulties to securely adapt to the changes in the cybersecurity area due to the lack of resources or the awareness of the cybersecurity threats.

SMEs represent 99.2% of the UKs (2023)and 99% of the EU's economy employing around 100 million people in the EU(ENISA, 2021a). Governments have started campaigns to upskill and make these organisations aware of the issues they can find when working

online. However, the government is not the only one that have identified the SMEs weaknesses. Cybercriminals have also noted that this type of organisations are less equipped and more for susceptible to attacks. The National Cyber Security Centre (NCSC) and the Garda National Cyber Crime Bureau (GNCCB) have reported an increase of use cybercrime targeting SMEs in Ireland (NCSC and GNCCB, 2022). Cybercriminals are starting to see a possibility to use SMEs to reach large organisations though the supply chain attacks. A survey carried out in the UK (Erdogan et al., 2023) showed that only 19% of the SMEs that replied to the survey provided cybersecurity awareness training to their employees. A different survey carried out in the 27 EU countries at the end of 2021 has showed that only 1 in 5 SMEs provide cybersecurity awareness to staff (European Commission, 2022). The same survey also demonstrated that 58% of the SMEs have suffered some type of cybercrime in 2021 that has impacted their business. This scenario is concerning as end users may not be ready or aware of any attacks or social engineer techniques used by criminals. Report from IBM (IBM, 2023) has showed that 41 % of cyber incidents involved phishing as initial access into the organisation systems.

With this setting, SMEs have now to find ways to raise awareness of their employees to the internet threats and point out the risks of human actions. With limited security budget and small-scale IT teams, this becomes an even harder task to achieve. Governments across the world have started to work to help some of these SMEs with publicly available content for training and education of cybersecurity. In Europe for example, the European Network and Information Security Agency (ENISA) publishes guidance and campaigns (ENISA, 2021b) to raise SMEs awareness in the cybersecurity field. The research field in other hand, have significant studies on how to raise awareness and methods of delivery. With the increase of remote work since the pandemic, many studies have focused the attention to online training as employees are not based in the office as often and in person training and talks cannot be easily arranged. These papers have analysed and compared delivery methods like videos, games and text-based content materials for Security and Education Training Awareness (SETA) campaigns. The results are that most of them are effective having better effectiveness with a mixture of all of them.

However, these studies fail to take in consideration organisations like SMEs that have small-scale IT teams and limited resources. The research field presents various security awareness training delivery methods, tools and software that can help organisations to deliver training and education on cybersecurity to employees. However, the gap from the research field is to how SMEs with limited resources can raise cybersecurity awareness among employees effectively and what tools and methods are better suited for their small-scale IT teams.

Having the research field gap in mind, the research questions are:

1. What is the most time efficient web-based security training and education methods to raise awareness among employees of SMEs with small-scale IT teams?
2. Is there a correlation between the amount of time spent building a security education and training awareness campaign and its learning outcome?

These questions will help IT teams to understand if long and complex training campaigns are worthwhile the time invested, while some short and simple training campaigns may be better to elevate the security awareness of employees. The goal of this research paper is to identify the work involved into raising employee's cybersecurity awareness through SETA programmes or campaigns. The study will analyse the tools and methods available in the market and register detailed information on how long it would take for IT professionals or security practitioners to configure, test and implement the campaigns to employees of a SME organisation.

Based in the research field, a framework to decide on the content was developed and a metric was used to distribute the content across each domain of knowledge. This framework helped to ensure that even with a small amount of learning time, the content would be relevant and focused on the knowledge gap of the SME. The study used two surveys (before and after training) to evaluate learning outcome of the participants. These participants were divided in groups where they had the same content time but with different learning methods like video, games and a mix of all. The results were used then in comparison to the required time to set up, and a efficiency metric helped to answer the research questions.

This research paper content is structured in the following order: Section 2 informs the literature review presented in the research field that was relevant to this study. Separated in four sections, the literature review presents in detail what was found in relation to the research question and the research gap. Section 3 describes the methodology and what activities, and analysis were conducted to achieve the results encountered. Section 4 illustrates the design of the project and Section 5 shows the implementation process of the project. This section describes the tools, surveys and other specification used during the project. Section 6 displays the results and analysis from the project with the findings generated from statistics used. Section 7 concludes the study with a discussion of the results and findings along with possible future work.

2 Related Work

During the literature review research, four main topics were identified when trying to answer the research question. The literature review is presented in a thematic framework, where each heading is a different topic addressed by different papers.

2.1 Awareness Requirements and Preparation

Numerous studies underscore the significance of conducting comprehensive requirement gathering prior to the initiation of a new training programme. It is important to gather information and requirements as every organisation will have distinct user groups and technology utilisation. (Boletsis et al., 2021) propose the integration of diagram visualisation techniques as a means to bolster cybersecurity awareness and enhance communication between technical and non-technical personnel. This paper presents a theorised scenario illustrating how the approaches are implemented and validated. It should be noted that it refrains from explaining variance implications among SMEs organisations and neither validates the work in a real-life scenario. (Ponsard and Grandclaoudon, 2020) presenting a methodological approach for information gathering and preparedness establishment preceding the commencement of any awareness program. The paper uses an analysis method on the data collected from their literature review that focus on the strengths and weaknesses inherent to SMEs. This analytical process yields important information that will guide which areas need to be addressed in awareness programs. The paper also mentioned the importance of evaluation and surveys in the start and end of the programmes.

(Wong et al., 2022) shows that recent surveys to SMEs, suggest a predominant emphasis on policy compliance over the state of awareness itself. Wong argues that the spotlight should shift from ordinary policy adherence to promoting cybersecurity awareness and good behaviour as it encourages employees to be protective instead of just compliant. The study however is based on a survey and was not applied in a SME for validation. (Parsons et al., 2014) have created a framework aimed to determine the employee's security awareness. The Human Aspects of Information Security considers different areas of knowledge and focus it to measure not only the knowledge, but also the attitude and behaviour of employees towards cybersecurity. Parsons's work holds relevance due to its

ability to differentiate deliberate from accidental behaviours. However, as the paper is a decade old, it is imperative to acknowledge that its focal areas are outdated and do not cover all the threat landscape of cybersecurity today. Nevertheless, these findings hold significance in addressing the research question, as they bring relevant techniques to help with the first steps of cybersecurity awareness initiatives.

2.2 User Personality Traits

With the rise of security tools and defence techniques, attackers direct their resources towards users to infiltrate or breach organisations. (Kalhor et al., 2022) paper points out how psychology plays a significant role in the user's behaviour. Emotions such as guilt and shame wield considerable influence over decision-making processes, especially when an individual falls a victim to social engineering tactics. This can make users perform undesired or unexpected actions that may contribute to the organisations harm. In this same subject, (Wong et al., 2022) proves that through security training and awareness programmes, users get to know threats and are more likely to spot security issues. With the cybersecurity knowledge users are more inclined towards making informed decisions.

While both papers acknowledge the significance of psychological traits in shaping end-users' cybersecurity behaviour, Kalhor's work goes deeper into this important aspect of cybersecurity awareness. In their paper, employs a methodology that categorises individuals into five categories of personalities, each characterised by unique attributes. Users that are willing to take risks or unafraid of actions without a clear outcome, are more vulnerable to cyber threats. These differences are relevant to consider when developing security awareness programmes as learning paths and methods may vary among individuals with different personality traits. Even though Kalhor's paper says that the study is focused on SMEs, there is no aspect of the paper that specifies the study is only directed to SMEs. In contrast, the focus of this paper is to raise cybersecurity awareness using security awareness programmes tailored explicitly for SMEs and that are consistent across the business. The next section discusses the importance of consistency and effectiveness when raising cybersecurity awareness.

2.3 Awareness Consistency and Results

The studies conducted by (Seda et al., 2021; Workman et al., 2022) emphasise the importance of training effectiveness. (Seda et al., 2021) explore various methods to train students and compare with traditional instructional approaches. Their findings are similar those of (Workman et al., 2022), where different learning methods, with games and simulations for example, make users perform better when compared to conventional learning methodologies. Workman's work also highlights that tailored training programmes that are designed to address specific group of users, are more effective than generic programmes. It is essential to acknowledge that to design awareness programmes and implement different training methods that are specific to groups of users is time consuming and may not suit SMEs. While both papers have made valuable contributions to our research, their primary focus leans toward cybersecurity professional education rather than the practical implementation of their findings within an organisation's end-user context. Differently from these studies, the work from (Abawajy, 2014) implements their research into end user training context. The study investigates three different methods of training delivery: game-based, video-based and text-based. Despite the results indicating that the better outcome was from groups that had a mixture of all methods, the user survey indicated that users preferred video-based training over the other deliver methods. These results establish that the correlation between learning outcome and user preference is not as significant.

(Wong et al., 2022) state that cybersecurity awareness should be encouraged and promoted making not only the users but any other stakeholders to have a security mindset and to understand threats and their severities. This promotion strengthens the credibility of awareness programmes and motivates the participants to take it seriously. (Ponsard and Grandclaoudon, 2020) takes the awareness promotion argument further and argue that cybersecurity awareness programmes and campaigns should have a broader preparation. The paper states that creating a cybersecurity culture within the organisation and integrating it into the company's strategy and roadmap is pivotal to the success towards raising awareness. Furthermore, (Uchendu et al., 2021) research studies in deeper details the aspects of building a cybersecurity culture and proposes a framework for maintaining it. The authors themselves acknowledge that certain metrics and aspects of their study remain theoretical and need to be implemented in real word for the effectiveness validation.

2.4 Awareness Implementation

(Dahabiyeh, 2021) work delves into the factors that influence on organisations decision making process when selecting an appropriate computer-based training. The paper states that several factors like quality of content, integration and compliance are significant characteristics that are considered when companies choose an online training platform. However, ease of use and implementation are the key factors when reviewing online training tools. That is of importance to the focus of our research as a choosing a complex tool would require a more substantial time commitment from the limited IT personnel typically found in SMEs. In a paper by (Bada and Nurse, 2019), survey findings explain the difficulties and challenges encountered by SMEs in their engagement with cybersecurity practices. The paper highlights that with SMEs limited resources, effective communication must be in place to achieve successful implementation of cybersecurity programmes and practices. This paper contributes with relevant points concerning the engagement and communication approaches designed to SMEs' specific needs.

When implementing raising awareness methods, it is important that the step-by step implementation process is illustrated. Simply pointing methods and tools without demonstration tends to render statements ambiguous. In their work, (Ponsard and Grandclaoudon, 2020) meticulously explains training methods and how they work. Their work explains the distinct instruments, preliminary steps for initiating an awareness program and offers concrete examples of delivery methods such as posters, guides, gamification, quizzes and assessments. Furthermore, the article then presents a practical experience carried out in Belgium where some of the proposed instruments were put into action. While in a different context, the research conducted by (Goode et al., 2018) presents a survey with experts in the cybersecurity field to identify the foundational aspects that should be covered on cybersecurity awareness raising programmes. The study focuses on the importance of identifying key foundational topics of the awareness programmes. Even though both works hold significance to this research paper, they fail to measure implementation time and effectiveness of the delivery methods. Although (Bada and Nurse, 2019) and (Ponsard and Grandclaoudon, 2020) studies are notably contributory to the research field, they primarily focus on raising awareness from an external standpoint, whereas our research paper centres its attention on small-scale IT teams from an internal perspective.

(Erdogan et al., 2023) paper presents survey results that only 19% of SMEs provide cybersecurity awareness training to their employees. The paper indicates that it may be due to the lack of tools and guidelines on this subject to help with awareness raising. The survey results also mentioned that 13% of SMEs have someone responsible for cybersecurity but do not provide awareness training. From all the paper presented in this section, a general lack of emphasis on the importance continuous learning is noted. The importance of ongoing

awareness learning is underscored in reputable cybersecurity frameworks and publications such as ISO/IEC 27001:2022 and NISP SP 800-50.

3 Research Methodology

3.1 Data Collection

Research participants were selected for this study based on two criteria. First, they had to be adults. Second, they needed to be employees of the organisation being investigated. Those who met both requirements received an email. The email explained that participation was sought after as part of a thesis research project and their consent would be appreciated. If they chose to accept the request, all they had to do was access a Microsoft Form with a link provided in that same email.

In both the email and Microsoft Forms, the participants were informed of their rights that included the ability to withdraw from the study without incurring any penalties. They were also assured that their data would be anonymised and wouldn't be shared with any other employees of the organisation.

Each participant was given an evaluation form twice. Once before enrolling in a training campaign and another after its completion. The first survey consisted of seven domains with 42 questions overall. This helped identify knowledge gaps within the organisation so IT staff could tailor a training program better. The primary aim of the second survey was to assess the progress, enhancements, and educational advancements achieved by all participants.

Within the literature review, it can be noticed the emphasis on the effectiveness of employing evaluation surveys at the initiation and conclusion of training programmes as a robust method for assessing the training's success. For instance, (Chaudhary et al., 2022) underscored the significance of evaluation in the context of SETA programmes. In their research, they introduced the concept of impact indicators as a primary evaluation metric. Their work was substantial to our approach, leading us to implement pre-training and post-training online assessments as the evaluation method for our SETA campaign. These online tests were devised as evaluation forms utilizing Microsoft Forms, facilitating the seamless delivery of assessments to the staff.

Microsoft Forms was used for the evaluation process due to its user-friendly survey features. Through their pre-existing business accounts, the tool seamlessly establishes connections, records respondent identities, tracks response times, and promptly notifies the researcher of each submitted response. When it comes time to export results from the survey, this platform facilitates the convenient extraction of results and the automated generation of response scores.

3.2 End-User Evaluation Tests

The primary challenge encountered concerned to the creation of the survey itself, given its length of 42 questions, mostly of multiple choice, each question with four response options and only one correct answer. In a comparative analysis of the KnowBe4 tool, it was noted that their questionnaire consisted of a total of 22 questions distributed across their seven knowledge domains. The allocation of merely three questions per domain was insufficient based on the research completed, the decision was made to double the number of questions within each domain. This increase allowed for a more comprehensive examination of the knowledge gaps inherent in each domain. The deliberate choice was made to cap the number of questions at six per domain to prevent unjustified survey lengthening, as it was observed that a 42-question survey, typically required an average of 20 minutes for completion.

Second challenge was to create two evaluation forms that comprised of the same domains and questions but still with different wording. Rephrasing tools were used to ensure questions and answers read differently but still consisted of the same subject. This approach was implemented to prevent participants from retaining or recalling questions from one survey in order to respond to the other. Additionally, the sequence of domains and questions was deliberately randomised to mitigate memory-based responses and ensure the incorporation of knowledge acquired during the training process.

3.3 Training Content Distribution

To distribute the hours of training appropriately, a metric was used to measure the average each domain scored, and which domain will require more time than others. In this way, training can be better distributed, making sure the time is better suited, and training doesn't become boring to the employees.

With the results of the first survey, an average of each domain was collected and the following formula was applied: $T - A = R$. T stands for Total, A stands for average and R stands for result. Then, all results need to be summed and divided by the number of items to obtain the total weight (TW). With this value, the following formula gives the exactly appropriate percentage of time for each domain:

$$\text{Percentage of the content} = R / TW \times 100$$

With the above formula, it is possible to calculate the appropriate time of content distribution whereas the training is short or long. Figure 1 illustrates the formula being applied to a course content with five hours of learning (300 minutes).

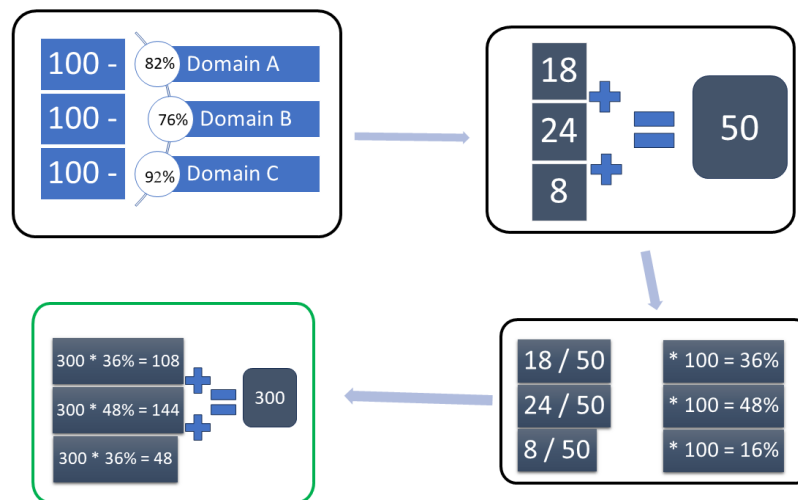


Figure 1 – Equally distributing content across domains with weight calculations.

3.4 Evaluation Metric

With a survey at the start and one at the end of the training programmes, a comparison of both surveys will be required. This will allow the research to identify the percentage mean of improvement of each group. The outcome of each group will be compared with the number of hours spend in each delivery method.

The higher the score, the better suited for SMEs: Efficiency Index = Learning Outcomes / Time Spent. The data will also be inserted into calculations to find out if there is a correlation between the time spend setting up the awareness training and the learning outcome.

4 Design Specification

4.1 Awareness Training Delivery Instrument

To deliver SETA programmes, different delivery methods can be considered. The work from (Abawajy, 2014) lists all the most popular methods of cybersecurity awareness training, ranging from instructor-led to simulation-based delivery methods. Their research identified advantages and issues with instructor-led methods. Problems with this method are that it can be fairly expensive, boring to employees and the quality of the training can vary relatively from the tutor. As we are currently transitioning into the area of remote working, it can be even harder to get employees to the office for face-to-face sessions. Meaning that organisations may be required to prepare different section for different group of employees.

A cybersecurity awareness delivery method that has been increasingly gaining popularity is the online delivery method also known as web-based delivery method (WBT). This method consists of training platforms hosted in web applications. These platforms can be accessed from most devices that support a web browser. As modern computers and smartphones have support for web browsers, this delivery method can easily reach employees working remotely or at the office. The main limitation to the WBT is the internet access dependency. (Abawajy, 2014) work mentions some disadvantages of the WBT delivery method, one of them being the employees attempting to complete the sessions with minimal time or thought.

In this paper, the use of web-based awareness training platforms was chosen over other methods for many reasons. One of them being already mentioned above is that the company where the research is being conducted has remote and hybrid workers. Conducting in person training would be time consuming and expensive if it required outsourcing the tutors. The second is the variety of material. The work from (Dahabiyeh, 2021) concludes that one of the reasons for the instructor-led methods was the capacity of tailoring training to the organisation needs. Today's WBT platforms provide a large range of material and compliance focus content. The third reason is the different training methods. WBT platform offer phishing simulation test, game-based, video-based, screensavers and newsletters. The last reason is the cost. Web-based awareness training platforms have become very accessible nowadays. Most platforms that offer similar services are ranging around one thousand euros a year for 30 users. In the end, the IT staff effort has to be taken into consideration.

4.2 Selecting Awareness Campaign Platform

The work from (Dahabiyeh, 2021) looks into the criteria and factors that customers take in consideration when selecting a security awareness solution. Some of these factors are ease of use and implementation, quality of content, integration and customisation. Ease of use and implementation is about the employees that will be accessing the platform and completing the training. How easy it is to navigate and for the IT professionals to set up and implement a training campaign. Integration is about how easily integrated is the platform with other businesses solutions. For the example of phishing emails, how can the solution be integrated with the emails solutions each company uses. Customisation can be important as each company may want to tailor their training to their needs or knowledge gap. How easy can the platform be customised to support training needs.

The above factors have been considered when looking for a WBT platform solution. When researching the market on the internet, different results can be found. One of these results is the G2 software reviews¹, which is a software marketplace. One of the leaders of the G2 Grid for security awareness training solutions is KnowBe4 (as September 2023). KnowBe4 does meet the criteria mentioned above and is one of the market leaders. Another important factor to choose this solution was that the organisation where the research was

¹ <https://www.g2.com/categories/security-awareness-training#grid>

being conducted was already using KnowBe4 for phishing simulation with its employees. Implementation and adaptation of the solution was not required as IT and non-technical staff were familiar with the solution.

4.3 Knowledge Domain Areas

As technology adoption among employees has increased exponentially over the past two decades, the cybersecurity landscape has expanded significantly. Given the array of diverse threats and aspects within the areas of IT that are a concern, the scope of content to be covered varies depending on the users within an organisation. To cover fully all concerned areas, training campaigns will take long and may not be achievable. As explained by (Ponsard and Grandclaoudon, 2020), prior to initiating any training or awareness campaign, it is imperative to establish one's current position and target objectives. Ponsard's research outlines the essential steps for achieving a successful SETA programme. The determination of the target scope can be achieved by addressing pressing issues or by assessing the existing knowledge gaps within the organisation and subsequently allocating resources to address these gaps.

Furthermore, (Ponsard and Grandclaoudon, 2020) emphasizes that cybersecurity awareness campaigns should not be regarded as singular, isolated efforts. SETA programs and other awareness-raising initiatives should be recurring events integrated into the organisation's long-term strategy. By making recurrent programmes, you can ensure that the learning is continuous and that emerging areas can be addressed in timely manner.

It is worth noting that leading organisations and established cybersecurity frameworks, such as NIST and ISO 27001, recommend training to be performed once a year the least, with some supporting for biannual sessions. While market best practices and academic research have not definitively specified a precise frequency or duration required to achieve the minimum acceptable level of cybersecurity awareness, the consensus underlines the importance of continuous and consistent learning to keep employees informed.

(Parsons et al., 2014) recognised during interviews with senior managers of Australian organisations that a significant proportion of cybersecurity breaches occur due to human oversight rather than malicious intent. The study resulted in the identification of seven focus areas representing common human errors leading to data breaches. These focus domains appear to align with findings in works by (Liginlal et al., 2009), (Schultz, 2005), and (Wood and Banks, 1993).

In this study, the seven focus areas identified in Parsons' work were considered alongside the mapping of security behaviours to risk-related outcomes by SebDB(CybSafe, 2023) and the knowledge areas delineated by KnowBe4 (KnowBe4, 2023) (refer to Figure 2). Both SebDB, a cybersecurity behaviour database maintained by the community, and KnowBe4, a private organisation specializing in elevating user cybersecurity awareness, presented their respective areas of focus. These resources facilitated the development of a unique classification of domains within the state of the art of cybersecurity awareness. This new classification combines the cybersecurity research literature with the proprietary field, up-to-date taxonomies.

Figure 2 illustrates the combination of various focus areas, resulting in the establishment of seven distinct domains called the "Knowledge Domains of Cybersecurity Awareness" (KDCA). The 7 domains are briefly mentioned below along with the domain letter which is later used for identification in the implementation section.

- Domain A = Password, Authentication and Accounts
- Domain B = Email Security
- Domain C = Personal Exposure, Internet Use and Social Media

- Domain D = Data Theft, Data Leak, Information Handling
- Domain E = Mobile Devices and Remote Working
- Domain F = Fraud & Identity Theft
- Domain G = Incident Reporting

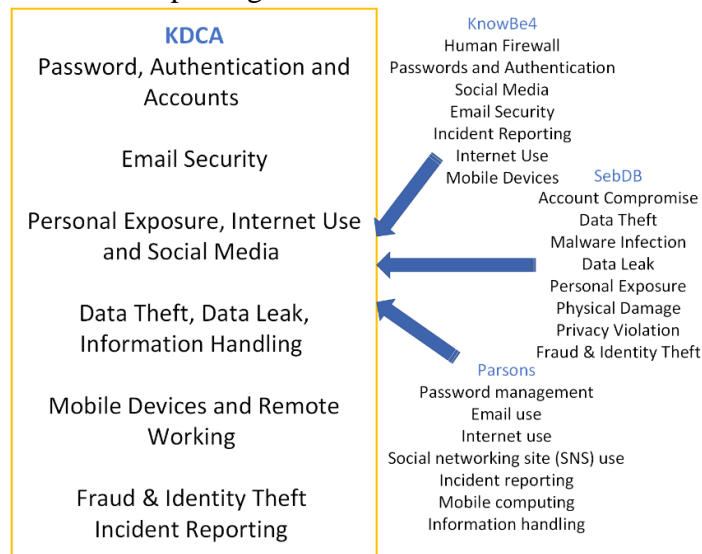


Figure 2 – Creation of up-to-date knowledge areas of cybersecurity awareness

5 Implementation

5.1 Learning Groups

The creation of the learning groups involved a randomised selection process for participants to ensure an absence of interference in the results. Given that the study concentrates on the efficacy of methods rather than individual participant characteristics, selecting individuals based on gender or other personal attributes would be considered unfair. A total of 30 participants have taken part in the research. It was possible to allocate two groups of eight participants and an additional two groups consisting of seven participants each. Further details regarding the delivery methods of these groups are available in section 5.4.

5.2 Content Distribution

During the literature review research, it was observed that the only stipulation regarding the time commitment for training programs was the requirement for them to be recurrent, with no specific mention of a minimum time duration. The organisation granted authorisation for a maximum training duration of four hours. In my analysis, I determined that each participant would need to dedicate a minimum of 30 minutes per week to complete the training over a two-month period. This approach was designed to ensure that even if participants were on annual leave for certain days, the training requirements would not become overly burdensome if some days or even an entire week was missed. The selection of training content was based on identifying areas with the most significant knowledge gaps.

A subset of participants that could not commit to the workload received one phishing email per week for the duration of the two-month training period. Simultaneously, this group had their desktop wallpaper replaced with educational images related to cybersecurity and the desktop wallpaper images were set to change at least once daily.

The data collected on the first survey was used to identify how the content time should be distributed across different areas. The mean of each domain was collected and subtracted by the total possible score (100%). This allowed us to find the gap number of each domain and

then sum all seven knowledge domain gaps finding the weight. With the following formula, it was possible to distribute all the 240 minutes of training appropriately among all domains.

The table 1 below explains the manner in which the outcomes derived from the initial evaluation form contributed to the identification of knowledge gaps within the organisation. These results, in conjunction with the formula detailed in Section 3.3, provide the necessary framework for tailoring the training campaign with a specific emphasis on addressing deficiencies in appropriate areas.

Table I – Discovering cybersecurity awareness gap with evaluation form results.

Calculating weights Weigh = 100 - results	Normalising Weights = Results / 61 * 100	Allocation time = Weight % * time
Domain A: 100 - 87 = 13	Domain A: (13 / 61) * 100 =	21.31% * 240 = 51 minutes
Domain B: 100 - 88 = 12	Domain B: (12 / 61) * 100 =	19.67% * 240 = 47 minutes
Domain C: 100 - 92 = 8	Domain C: (8 / 61) * 100 =	13.11% * 240 = 31 minutes
Domain D: 100 - 97 = 3	Domain D: (3 / 61) * 100 =	4.91% * 240 = 12 minutes
Domain E: 100 - 96 = 4	Domain E: (4 / 61) * 100 =	6.55% * 240 = 16 minutes
Domain F: 100 - 80 = 20	Domain F: (20 / 61) * 100 =	32.78% * 240 = 79 minutes
Domain G: 100 - 99 = 1	Domain G: (1 / 61) * 100 =	1.63% * 240 = 4 minutes
Weight Total = 61		Total minutes = 240

5.3 Campaign Content Selection

The time spent for each training group within the respective groups was relatively brief. This efficiency was made possible due to the capabilities of the awareness training platform. The platform provides an advanced search feature enabling the detailed targeting of specific categories such as popular topics, attack vectors, risk management, and regulatory aspects.

The screenshot displays the 'Topics' section of the KnowBe4 Modstore. At the top, there is a search bar labeled 'Search' with a magnifying glass icon. Below the search bar, the content is organized into four columns, each with a title and a list of items with checkboxes:

- Attack Vector:** CEO Fraud, Malware, Phishing, Ransomware, Smishing, Social Engineering, Spear Phishing, Tailgating, USB, Vishing.
- Popular Topics:** Cybersecurity Awareness Month, Data Privacy, Data Protection, Diversity, Equity and Inclusion, Email Security, Human Firewall, Internet Use, Mobile Devices, NIST, Passwords & Authentication, Professional Development, Red Flags, Social Media, WiFi, Working Remotely.
- Regulatory:** FCPA, FERC, FERPA, FMLA, GDPR, HIPAA, LGPD, NERC, PCI, PHI, PII, PIPEDA, POPIA.
- Risk Management:** Discrimination, Employment Law, Ethics, Harassment, Incident Reporting, Personal Security, Physical Security, Workplace Safety.

Figure 3 – Content selection in KnowBe4 Modstore awareness platform

As illustrated in Figure 3, each piece of content is systematically tagged, allowing for content selection based on these tags. Many of these tags matched or related to the seven knowledge domain areas, facilitating the tailoring of content for each learning group. In that way, I was able to filter and preview each piece of content before choosing it. Special consideration was given to content that was interactive, engaging, and of moderate complexity, recognising that this was the participants' initial exposure to the training

campaign. The tool also featured a content-type filter, facilitating the categorisation of modules by training module, video module, game and others, which helped choosing the material for the different learning groups. Without the benefits of these advanced filtering and searching capabilities, the workload for the IT team in crafting each training campaign can experience a significant increase.

5.4 Awareness Campaign Build-Up

The SETA campaign was separated in 4 groups, with each group having a different learning delivery method. Group A consists of learning through (1) wallpaper images that display different cybersecurity advises and best practices and (2) phishing email simulations with different email templates. Group B comprises of learning through games and quizzes. Group C was made of video modules and group D of games, quizzes and videos altogether. The following will explain how they were created and the recorded length of time used in process.

5.4.1 Group A – Wallpaper & Phishing

The selection and implementation of wallpaper image arts for Group A, involved visualising and downloading suitable wallpapers. As a result, 27 wallpaper images were chosen based on the knowledge domains, avoiding heavily coloured and ominous design to enhance the overall user experience. Due to the variability in users' duration of visual engagement with each wallpaper, it was not feasible to precisely allocate time over the wallpapers chosen. The platform provided the same categorisation and filtering available over the other content types used in the other groups. The overall time for this content selection took 20 minutes.

To display these images to the selected users, it was necessary to create a Group Policy Object (GPO) setting within the Domain Controller (DC) server. In that way the computer would have these images displayed in their desktop wallpaper. The configuration necessary was more advanced as simple windows GPO policies only allow for one wallpaper image, and this would require manual intervention every time a new image needed to be displayed. Two scripts were implemented and a task scheduler along with the GPO so staff would get at least one different image every day when logging into their computers if working from the office network. It is important to note that this variation may not be consistent for remote staff, as they lack a connection to the DC server when logging in from home. In practice, most staff members would cycle through the entire collection over the course of 60 days, repeating each image twice. This configuration took two hours and 27 minutes to be completed.

Concerning the phishing templates selection, a pragmatic approach was adopted, dedicating 45 minutes to the selection and preparation of the phishing simulation campaign. Crafting templates from scratch was deemed impractical due to the substantial time investment. Template choices were guided by difficulty ratings of four or five stars and content relevance. While templates related to Ireland or Irish businesses were prioritised, constraints in filtering options only relating to business field or language limited alignment with specific knowledge domains. Additional time was given for modifying email information in selected templates and choosing a landing page. The landing page served the purpose of guiding the end users to understand that they have failed a test and offers the opportunity to watch or read some information on how to improve their cybersecurity habits. Unfortunately, only one landing page can be chosen per campaign. The cumulative time invested in both wallpaper and phishing components totalled 192 minutes, equivalent to three hours and 12 minutes.

5.4.2 Group B – Gamification (Games & Quizzes)

The gamification method within KnowBe4 presents limitations, offering only 29 game modules. Although content selection was initially performed based on the knowledge domain, the cumulative training minutes proved insufficient. By incorporating all 29 games/quizzes, the overall content time reached 241 minutes. It is noteworthy that, in summary, all gamification content available in the platform was added to Group B so the training duration was the same as the other groups. The main difference from this delivery method from the remaining is that a substantial portion of the content was amalgamated, encompassing diverse knowledge domains within the same game module. Group B required a total of one hour and 10 minutes for completion.

5.4.3 Group C - Videos

Group C required a total of one hour and 50 minutes for completion. Unlike gamification, video content was notably more extensive, comprising over 500 modules. The consideration of domains played an essential role in the selection of video content; however, certain domains lacked sufficient available video content. Domains with greater content availability were used to fill the training content gap. Like the gamification delivery method, some video modules covered multiple domains, but it was possible to find much more targeted content. The diversity of educational and entertaining material was substantially broader in the case of videos compared to gamification.

5.4.4 Group D - Gamification & Videos

The platform offers over 1300 choices of material when applying all content types. The seven domains were considered in the content selection process for this group, and it is noteworthy that the only domain lacking sufficient content was Fraud & Identity Theft. Particularly, the area of identity theft appears to be the area where not many games or video content is available. The allocated time was dedicated to addressing the needs within all domains, effectively utilising the entirety of the 240 minutes assigned. Group D used a total of two hours and 10 minutes for completion.

6 Evaluation

The end results were combined into a single dataset, serving as the foundation for evaluation analysis. Table II presents an extract of the dataset, where the full dataset will be available in the configuration manual.

Table II – Research results dataset snapshot

Group	ID	Outcome	Completed	timestaff	timeit	Metric
B	13	0	100	173	70	0
A	35	5	0	0	192	0.026041667
C	24	8	100	426	110	0.072727273
D	23	2	100	236	130	0.015384615
D	20	-2	100	279	130	-0.01538462
C	18	3	20	50	110	0.027272727
B	28	3	0	0	70	0.042857143

The "Group" column labels the training group to which each staff member belonged during the data recording. "ID" represents a unique identifier assigned to participants to ensure anonymity. "Outcome" signifies the numerical difference between the second and first

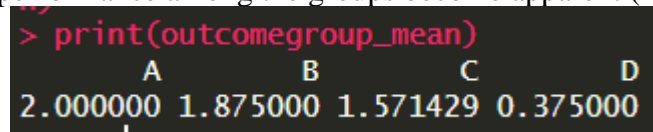
evaluation forms (second – first evaluation form). The "Completed" column indicates the percentage of training content completed by the staff. "Timestaff" denotes the time in minutes spent by the staff on the training content, whether completed or not. It is important to note that Group A did not record any time in either column ("Completed" & "timestaff"). This is due to their receipt of training through simulations and wallpaper images, rendering content time measurement impractical. The "timeit" column records the time in minutes dedicated by the IT to creating each delivery method group, with this duration remaining constant within each group. Finally, the "Metric" column represents the main data pursued in this research. As detailed in the methodology, the metric is calculated by dividing the outcome by the time spent by the IT department (Outcome / "timeit"), which results in the efficiency index. A higher metric value indicates greater suitability of the delivery method for SMEs.

R Studio was employed for a comprehensive analysis of these results gathered in the dataset. Various statistical tests were conducted to assess the significance of the results, where the tests can be seen in the following subsections. The complete dataset and scripts employed for research evaluation will be accessible in the thesis configuration manual.

6.1 Case Study 1 – Learning methods general results and outcomes.

Group A was the only one that did not have any negative outcome. The remaining groups all had at least one negative outcome. Group B presented outcomes ranging from a minimum of -2 to a maximum of +7. Group C faced the most adverse outcomes, with a minimum of -8; however, it also achieved notable positive results, reaching a peak of 10, making it the group with the highest overall outcomes among all learning groups. Group D, while outstanding in terms of least negative outcomes after group A, displayed a lack of significant positive results. The range of outcomes for Group D varied from a minimum of -2 to a maximum of +5. Remarkably, Group B held the highest average outcome among all learning groups that had training content opposed to phishing simulations. Overall, group A has the highest mean among all delivery methods.

When looking at simple results like the average of outcome for each learning group, visible variations in performance among the groups become apparent (Figure 4).



```
> print(outcomegroup_mean)
      A      B      C      D
2.000000 1.875000 1.571429 0.375000
```

Figure 4 – The mean of each learning group knowledge outcome.

While these results suggest that Group A is the most proficient for learning overall, it is imperative to recognise that this observation, in isolation, does not contribute substantially to the research and research questions. Our primary objective is to identify a measurement or metric that can ascertain whether a particular training delivery method can return the best positive outcome with minimal time investment from the IT department. This specific analysis will be addressed in the following section.

6.2 Case Study 2 – Most time efficient learning method.

The primary answer we want to discover is what awareness training delivery method returns best outcomes with the least time involvement from the IT department. As previously mentioned, the metric serves as an indicator of training efficiency for each participant and groups. Some outcome results were negative, indicating a decline in scores in the second evaluation form post-training. Despite this, the contributions of these staff to the dataset influence the average score of their respective training groups. In Figure 5, we are utilising the R summary command to provide a summary overview of the metric column.


```
> summary(Fullresults$Metric)
   Min. 1st Qu.  Median    Mean 3rd Qu.    Max.
-0.07273 0.00000 0.00000 0.01368 0.02825 0.10000
```

Figure 5 – The summary of the metric variable using R command.

Here, "Fullresults\$" refers to the dataset in use, and "Metric" points to the column storing metric values. The summary reveals a minimum result of -0.07273 (ID 12), where the individual obtained an outcome of -8 with 110 minutes spent by IT during campaign creation. In opposition, ID 22 achieved the maximum metric of 0.10000, managing an outcome score of 7+ with only 70 minutes spent by IT. In Figure 6, "tapply" R command is used to get the metric's average by group.

```
#Grouping the Metric Means by Group
metricgroup_mean <- tapply(Fullresults$Metric, Fullresults$Group, mean)
print(outcomegroup_mean)
```

Figure 6 – Tapply command used in R to group means of variable together.

Here, "metricgroup_mean" serves as the variable to store the data, with "<-" used for recording. The "tapply" command facilitates the application of functions to data rows for easy display. The two specified values are the metric and the groups, while "mean" signifies the mean of the "metric." The print function displays the first two values enclosed within parentheses.

```
> print(groups_mean)
      A      B      C      D
0.010416667 0.026785714 0.014285714 0.002884615
```

Figure 7 – Comparison of means of the Metric displayed by learning group.

With these results and as displayed in Figure 7, we observed that group B has the higher efficiency index, followed by Group C, Group A, and lastly, Group D. The metric and collected results affirm that Group B holds the highest mean efficiency index among all groups. For this part of the analysis, we are also interested in knowing if the average value of the metric differs between groups or not. For that, we can use the Analysis of Variance (ANOVA) test in R:

```
anova <- aov(Metric ~ Group, data = Fullresults)
> summary(anova_oneway)
      Df Sum Sq Mean Sq F value Pr(>F)
Group    3 0.00238 0.0007945    0.518  0.674
Residuals 26 0.03988 0.0015338
> |
```

Figure 8 – One-way ANOVA results using R.

As shown in the results displayed in Figure 8, the one-way ANOVA revealed that there was not a statistically significant difference between outcomes and groups ($p=[0.674]$). The p-value of this ANOVA table is higher than 0.05 which says that the dataset size was not large enough to produce statistically significant results. This means that we do not have statistical significance to deny that the average value of the metric is the same between groups.

6.3 Case Study 3 – Learning outcomes vs time investment correlation.

In this case study, there are two hypotheses:

- H0, Null Hypothesis. This hypothesis says that a correlation between the time invested by IT creating a training campaign and its learning outcomes does not exist.
- H1, Alternative Hypothesis. This hypothesis says that a correlation between the time invested by IT creating a training campaign and its learning outcomes exists.

To prove the alternative hypothesis, it is necessary to create a simple linear regression to test if “timeit” significantly predicted “Outcome”. In Figure 9, we can see the output of the linear regression calculated using R.

```
> summary(outcome_model)

Call:
lm(formula = Outcome ~ timeit, data = Fullresults)

Residuals:
    Min       1Q   Median       3Q      Max
-9.430 -1.447 -1.420  1.578  8.570

Coefficients:
            Estimate Std. Error t value Pr(>|t|)
(Intercept)  1.4018193   2.1468178    0.653   0.519
timeit        0.0002546   0.0163512    0.016   0.988

Residual standard error: 3.916 on 28 degrees of freedom
Multiple R-squared:  8.656e-06, Adjusted R-squared:  -0.03571
F-statistic: 0.0002424 on 1 and 28 DF,  p-value: 0.9877
```

Figure 9 – Simple linear regression model results using R.

As shown on the simple linear regression result, it was found that “timeit”, the times spent by IT, did not significantly predict “outcome”, the knowledge outcome ($\beta = [0.0002546]$, $p = [0.988]$). The p-value is notably higher than 0.05, meaning that the study does not have enough power to prove a significant correlation exists, so we fail to reject null hypothesis. This means that it is not possible to guarantee that more time spent building a training campaign will result in better learning outcomes.

6.4 Case Study 4 - Learning outcomes and other correlations.

In order to try and find more possible correlations among all available variables, we can use the correlation command below. In the series of commands we used “subset” to create a reduced dataset and we use “select= -Group” in order to remove any variables that may not be numeric. The command “round” uses the input 2 to round all results to decimals not displaying long numbers. The command “ggcorrplot” uses the attributes within parentheses to display the correlation values from the selected subset of data in a easy visual way.

```
reduced_data <- subset(nophish, select = -Group)
corr_matrix = round(cor(reduced_data), 2)
ggcorrplot(corr_matrix, hc.order = TRUE, type = "lower",
lab = TRUE)
```

In this correlation, we remove the phishing group as they do not have recorded times, and this would affect the outcome. The results are displayed in Figure 10.

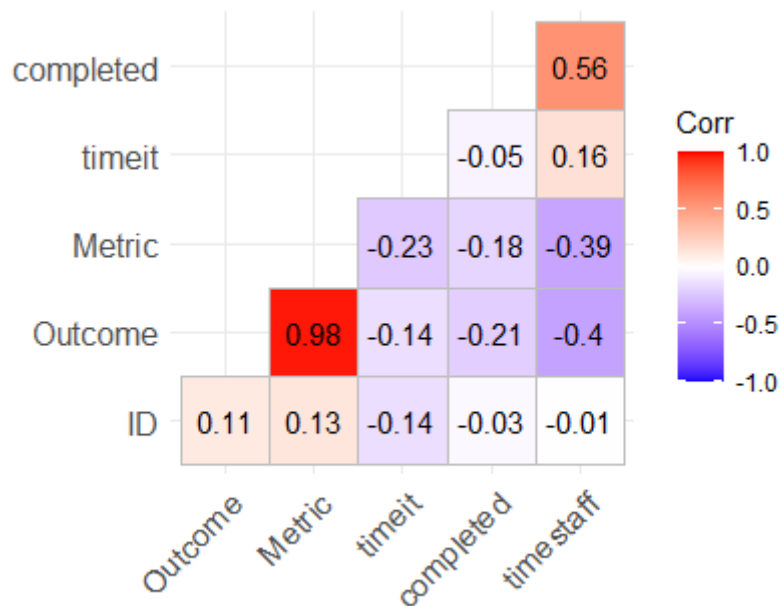


Figure 10 – Graphical visualization among all dataset variables.

Outcome x Metric have a positive correlation as Outcome was used in the generation of the Metric. Variables like “completed” and “timestaff” are positively related as the more time someone spends doing the course the higher the chance of them finishing. But this is not necessarily the case as the dataset shows one staff member that took 15 hours to finish the training while other staff members in the same group finished the training in less than 4 hours. We can see on Figure 10 that no correlations can be found on the dataset.

Analysing the results above we can also see that there is no correlation between the time spent by staff completing the training and the learning outcomes. This means that even though some staff may have spent more time completing or finishing training, it does not mean their knowledge outcome was superior to others that didn’t.

6.5 Discussion

Overall, all learning groups have returned a positive average learning outcome from the participants. Some of the groups have returned a few negative results, which means learning outcome was reduced when comparing first and second evaluation forms. All groups had at least one participant that even after completing the training, scored the same in both evaluation forms. Group A, phishing simulations and wallpaper images learning group, was the only learning group that did not experience any negative outcome. The remaining groups had a mix of high positive or negative as well as zero improvement outcomes results. The fact that three of the learning groups involved content completion and one of the learning groups didn’t, made the analysis a slightly more difficult. When trying to find any multicollinearity among the variables, it is necessary to separate this group from the remaining dataset as this group would make the results inaccurate. Another issue with the recorded data is also related to the dataset. When adapting the data and trying to statistically analyse each case, the dataset becomes too small to have statistically significant results.

The research was performed with two research questions in mind. When analysing the results, I was able to answer both questions. The first question sought the most time efficient web-based security training and education methods. This research showed that when simply analysing the outcome results, group A with the phishing simulation, has performed better than the other learning groups but it also required more time from the IT department to create

it. A metric was created to put the data collected from the staff training delivered a suitable analysis. It was evident from the evaluation that group B outperformed the other groups when using this metric and this is why group B is the most time efficient delivery method among the ones tested in this research. This means that gamification method group is the best security education and training awareness method to SMEs.

In contrast to the findings presented by (Abawajy, 2014), our study demonstrates that gamification delivery method has outperformed all the other delivery methods, including the group utilising mixed delivery methods. Divergences between our results and Abawajy's work can be attributed to two principal factors. Firstly, the approach taken in this work for training campaign preparation is more structured and comprehensive, encompassing various knowledge areas and ensuring uniformity in knowledge domains across all training groups. Unlike Abawajy's work, which lacked such preparation and campaign development, this paper methodology involves a more systematic preparation process. Secondly, the changes in this paper results arises from our evaluation metric. Unlike studies solely considering student outcomes, this research incorporates the amount of time invested by IT professionals, leading to a more accurate assessment designed to the context of SMEs. No prior literature has undertaken a comparative analysis of delivery method efficacy with a specific evaluation metric focused on SMEs.

The second research questions being pursued was to understand if a correlation between the amount of time spent building a SETA campaign and its learning outcome exists. From the evaluation, it was discovered that the correlation between these two variables was of -0.14 (Figure 10). This means a very small negative correlation between the two variables. However, it is evident in the linear regression test results that the data being analysed did not have enough statistically significance meaning it fails to reject the null hypothesis. This paper has also looked at all the variables collected and no other significant correlation between the outcome and the other variables can be explained.

In summary, it can be considered that the group B learning with gamification is considered the most appropriate to small business with small-scale teams. However, we have also to consider that group A learning through phishing simulations and image wallpapers has performed exceptionally well considering the amount of time it requires to be created. It is important to take in to consideration that training campaigns have its limitations when time is required from staff to stop their work tasks and watch videos or complete quizzes. Even though the videos and quizzes were in average around 5 minutes in length each, the content time overall was 4 hours. Depending on the team or organisation, this time may not be available and communicating the importance of this training time to the company management can be challenging. This is why all methods should be considered and should be implemented accordingly with the company culture and environment.

7 Conclusion and Future Work

The cybersecurity state of the art has seen an increase on the cyber threats related to the human factor. The Small and Medium Enterprises (SMEs) are the most vulnerable to these threats as their resources are limited and their lack of awareness to the threats is concerning. This research aimed to analyse the current methods, techniques and tools available to raise employee's cybersecurity awareness with focus in SMEs. It was possible to not only find the correct tools to raise cybersecurity awareness but also develop a plan to implement Security Education and Training Awareness (SETA) campaigns and a new metric to evaluate training effectiveness. In this research, we sought to answer to research questions: (i) What is the most time efficient web-based security training and education methods to raise awareness among employees of SMEs with small-scale IT teams; and (ii) Is there a correlation between

the amount of time spent building a security education and training awareness campaign and its learning outcome? We conducted the training campaign with four different learning groups having four different learning delivery methods. With the evaluation metric created and the results collected from the evaluation forms answered before and after the training, it was possible to answer the first research question and state that Web-based training (WBT) games and quizzes are the most time efficient delivery method among all the methods evaluated. With statistical tests to the data collected, I was able to answer the second research question and state that there is no relationship between the time spent by IT professionals and the students' learning outcomes. Other tests were performed with other variables collected during the campaigns, but no significant correlations were found. The research then has brought significant value to the research field, reinstating the importance of SETA campaign and its preparation as well as its recurrence. The Knowledge Domains of Cybersecurity Awareness (KDCA) along with the evaluation metric have brought up to date areas of concern when implementing SETA campaigns and a SME focused evaluation method.

A limitation of the research project was the low number of participants. As this was performed in a SME, only 30 participants took part. These number was then split down by four groups leaving only a small number of participants per group, reducing the significance of the analytical tests performed. A recommendation for future work is to have the methods and metrics created in this research implemented in a number of different SMEs. The evaluation forms should also be scheduled along with the participants to ensure they are not completed under pressure. The same data should be collected, and the evaluation forms completion time should be recorded in a different way as it was discovered in this research that Microsoft Forms seem to fail to correctly record the time in some of the evaluation forms. More learning deliver methods could also be used to expand the contribution to the research field.

References

- Abawajy, J., 2014. User preference of cyber security awareness delivery methods. *Behav. Inf. Technol.* 33, 237–248. <https://doi.org/10.1080/0144929X.2012.708787>
- Bada, M., Nurse, J.R.C., 2019. Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Inf. Comput. Secur.* 27, 393–410. <https://doi.org/10.1108/ICS-07-2018-0080>
- Boletsis, C., Halvorsrud, R., Pickering, J.B., Phillips, S., Surridge, M., 2021. Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment, in: *Proceedings of the 16th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications - IVAPP*. French Civil Aviation University (ENAC), France;University of Glasgow, United Kingdom;Escola Superior de Tecnologia de Setúbal, Portugal;University of Rennes 1, France, pp. 266–274.
- Chaudhary, S., Gkioulos, V., Katsikas, S., 2022. Developing metrics to assess the effectiveness of cybersecurity awareness program. *J. Cybersecurity* 8, tyac006. <https://doi.org/10.1093/cybsec/tyac006>
- CybSafe, 2023. Welcome | SebDB [WWW Document]. URL <https://www.cybsafe.com/research/security-behaviour-database/> (accessed 12.12.23).
- Dahabiyeh, L., 2021. Factors affecting organizational adoption and acceptance of computer-based security awareness training tools. *Inf. Comput. Secur.* 29, 836–849. <https://doi.org/10.1108/ICS-12-2020-0200>

- ENISA, 2021a. SME Cybersecurity. [WWW Document]. ENISA. URL https://www.enisa.europa.eu/topics/cybersecurity-education/sme_cybersecurity (accessed 4.3.23).
- ENISA, 2021b. Cybersecurity for SMEs - Challenges and Recommendations (Report/Study). ENISA, Europe.
- Erdogan, G., Halvorsrud, R., Boletsis, C., Tverdal, S., Pickering, J., 2023. Cybersecurity Awareness and Capacities of SMEs:, in: Proceedings of the 9th International Conference on Information Systems Security and Privacy. Presented at the 9th International Conference on Information Systems Security and Privacy, SCITEPRESS - Science and Technology Publications, Lisbon, Portugal, pp. 296–304. <https://doi.org/10.5220/0011609600003405>
- European Commission, 2022. SMEs and Cybercrime - May 2022 - - Eurobarometer survey. Europe.
- FSB, The Federation of Small Business, 2023. UK Small Business Statistics [WWW Document]. URL <https://www.fsb.org.uk/uk-small-business-statistics.html> (accessed 11.25.23).
- Goode, J., Levy, Y., Hovav, A., Smith, J., 2018. Expert assessment of organizational cybersecurity programs and development of vignettes to measure cybersecurity countermeasures awareness. *Online J. Appl. Knowl. Manag.* 6, 67–80. [https://doi.org/10.36965/ojakm.2018.6\(1\)67-80](https://doi.org/10.36965/ojakm.2018.6(1)67-80)
- IBM, 2023. IBM Security X-Force Threat Intelligence Index 2023 [WWW Document]. URL <https://www.ibm.com/reports/threat-intelligence> (accessed 11.25.23).
- Kalhor, S., Ayyasamy, R.K., Jebna, A.K., 2022. How Personality Traits Impacts on Cyber Security Behaviors of SMEs Employees. Presented at the International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Sakheer, Bahrain, pp. 635–641.
- KnowBe4, 2023. Smart Groups: SAPA Automation Guide [WWW Document]. Knowl. Base. URL <https://support.knowbe4.com/hc/en-us/articles/8355412499859-Smart-Groups-SAPA-Automation-Guide> (accessed 12.12.23).
- Liginlal, D., Sim, I., Khansa, L., 2009. How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Comput. Secur.* 28, 215–228. <https://doi.org/10.1016/j.cose.2008.11.003>
- NCSC, GNCCB, 2022. National Cyber Security Centre (NCSC) and the Garda National Cyber Crime Bureau (GNCCB) launch joint public awareness campaign for European Cyber Security Month [WWW Document]. MerrionStreet.ie. URL https://merrionstreet.ie/national_cyber_security_centre_ncsc_and_the_garda_national_cyber_crime_bureau_gnccb_launch_joint_public_awareness_campaign_for_european_cyber_security_month.html (accessed 4.11.23).
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C., 2014. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Comput. Secur.* 42, 165–176. <https://doi.org/10.1016/j.cose.2013.12.003>
- Ponsard, C., Grandclaudon, J., 2020. Guidelines and Tool Support for Building a Cybersecurity Awareness Program for SMEs, in: Information Systems Security and Privacy, Communications in Computer and Information Science. Springer International Publishing, Prague, Czech Republic, pp. 335–357. https://doi.org/10.1007/978-3-030-49443-8_16
- Schultz, E., 2005. The human factor in security. *Comput. Secur.* 24, 425–426. <https://doi.org/10.1016/j.cose.2005.07.002>
- Seda, P., Vykopal, J., Švábenský, V., Čeleda, P., 2021. Reinforcing Cybersecurity Hands-on Training With Adaptive Learning, in: 2021 IEEE Frontiers in Education Conference

- (FIE). Presented at the 2021 IEEE Frontiers in Education Conference (FIE), IEEE, Lincoln, NE, USA, pp. 1–9. <https://doi.org/10.1109/FIE49875.2021.9637252>
- Uchendu, B., Nurse, J.R.C., Bada, M., Furnell, S., 2021. Developing a cyber security culture: Current practices and future needs. *Comput. Secur.* 109, 102387. <https://doi.org/10.1016/j.cose.2021.102387>
- VERIZON, 2023. Data Breach Investigations Report 2023 - Verizon.
- Wong, L.-W., Lee, V.-H., Tan, G.W.-H., Ooi, K.-B., Sohal, A., 2022. The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *Int. J. Inf. Manag.* 66, 102520. <https://doi.org/10.1016/j.ijinfomgt.2022.102520>
- Wood, C.C., Banks, W.W., 1993. Human error: an overlooked but significant information security problem. *Comput. Secur.* 12, 51–60. [https://doi.org/10.1016/0167-4048\(93\)90012-T](https://doi.org/10.1016/0167-4048(93)90012-T)
- Workman, M.D., Luévanos, J.A., Mai, B., 2022. A Study of Cybersecurity Education Using a Present-Test-Practice-Assess Model. *IEEE Trans. Educ.* 65, 40–45. <https://doi.org/10.1109/TE.2021.3086025>