UNIVERSIDADE ABERTA

Improving Social Engineering Resilience in Enterprises

Ricardo Alexandre Bentes Ribeiro

Master's Dissertation in
Information and Enterprise Systems (MISE)

Dissertation supervised by
Prof. José Henrique Pereira São Mamede and Prof. Nuno Mateus-Coelho

October 2023

Acknowledgments

I want to express my appreciation to Prof. Henrique S. Mamede and Prof. Nuno-Mateus-Coelho, my supervisors for this master's dissertation. Their invaluable insights, encouragement, and knowledge-sharing played a vital role in making this research possible.

I would also like to heartfelt thank my wonderful wife and daughter for their continuous support and enthusiasm throughout this journey. Their assistance and understanding were fundamental to conclude this work, and I am truly grateful for their presence in my life.

Furthermore, I would like to express my appreciation to all the persons who participated in the interviews, my friends and coworkers who have consistently help me to grow as an individual, during good and challenging times.

Thank you for your contributions, encouragement, and support.

Abstract

Social Engineering is a significant problem for enterprises. Cybercriminals continue developing new and sophisticated methods to trick individuals into disclosing confidential information or granting unauthorized access to infrastructure systems. These attacks remain a significant threat to enterprise systems despite significant investments in technical architecture and security measures. User awareness training and other behavioral interventions are critical for improving Social Engineering resilience. Training and education programs for users are crucial in reducing the probability of these attacks. Compliance with security policies and procedures is significantly improved through education-based training. A security culture involving all stakeholders is also essential, as open, and honest communication from management can increase user awareness of potential threats. Emotional biases such as fear, trust, and curiosity also impact susceptibility to attacks, but personal traits that make individuals vulnerable require further investigation.

This dissertation aims to provide a comprehensive assessment of the state of knowledge in this field and propose a framework by identifying best practices for improving Social Engineering resilience in organizations, while supporting the development of new research studies to address this issue. Its goal is to help enterprises of any size leverage this framework to reduce the risk of successful Social Engineering attacks and improve their culture of security awareness.

Keywords: *Social Engineering ; human behavior; personal traits; security architecture; phishing; threat actors; cybersecurity; cyberattacks; design science research; systematic literature review; framework; security awareness.*

Resumo

A Engenharia Social é um problema significativo para as empresas. Os cyber-criminosos continuam a desenvolver novos e sofisticados métodos para ludibriar indivíduos, levando-os a divulgar informações confidenciais ou a conceder acesso não autorizado a sistemas de infraestruturas. Estes ataques continuam a constituir uma ameaça significativa para os sistemas empresariais, apesar dos investimentos significativos em arquitetura técnica e medidas de segurança. A formação e sensibilização dos funcionários, entre outras intervenções comportamentais, são fundamentais para melhorar a resiliência à Engenharia Social. Os programas de formação e educação dos funcionários são cruciais para a redução da probabilidade destes ataques. O cumprimento das políticas e procedimentos de segurança é significativamente melhorado através de formação baseada na educação. Uma cultura de segurança envolvendo todas as partes é também essencial, uma vez que uma comunicação aberta e honesta por parte da direção pode aumentar a consciência dos funcionários sobre potenciais ameaças. Os preconceitos e características emocionais como o medo, confiança e curiosidade têm também impacto na suscetibilidade a este tipo de ataques, mas, no entanto, as características pessoais que tornam os indivíduos vulneráveis exigem uma investigação profunda.

Esta dissertação tem como objetivo fornecer uma avaliação abrangente do estado do conhecimento neste campo e propor uma *Framework*, identificando as melhores práticas para melhorar a resiliência à Engenharia Social nas empresas, enquanto apoia o desenvolvimento de novos estudos de investigação para abordar esta questão. O seu objetivo é ajudar as empresas de qualquer dimensão a utilizar esta *Framework* para reduzir o risco de ataques bem-sucedidos de Engenharia Social e melhorar a sua cultura de sensibilização para a segurança.

Palavras-Chave: *Engenharia social; comportamento humano; características pessoais; arquitetura de segurança; phishing; cibersegurança; ciberataques; revisão de literatura; sensibilização para a segurança.*

Contents

List of Figures

List of Tables

1 INTRODUCTION

1.1 Motivation

The threat of Social Engineering (SE) attacks on enterprise cybersecurity is more present than ever and is a growing concern for enterprises of all sizes. For example, according to Microsoft [1], phishing emails are one of the most used SE techniques in corporate environments and represent a significant problem for organizations. In addition, cybercriminals continue to develop new and sophisticated methods to trick individuals into disclosing confidential information or granting unauthorized access to infrastructure systems, leaving sensitive data vulnerable.

SE attacks remain a significant threat to enterprise systems despite significant investments in technical architecture and security measures. In addition, attackers continue to adapt and develop their tactics, therefore, the human vector of security must be addressed.

User awareness training and other behavioral interventions have become critical tools for improving SE resilience and preventing attacks, but their effectiveness still needs to be determined. Some conducted studies [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], suggest that such interventions can significantly reduce the risk of SE attacks being successful. Others report that they have a limited impact on user behavior [20], [21]. In addition, scientific research [15], [14], [19], [6], [11], [17] has identified individual factors, such as personality traits and cognitive tendencies, that may turn some individuals more susceptible to such attacks, making it difficult to find practical solutions.

According to IBM [22], phishing emails were the leading infection vector, as 41% of the attacks used phishing to gain access into an environment. This fact further exacerbates the need to explore the human factors associated with SE attacks by conducting a Systematic Literature Review (SLR) research on enterprise cyber-security and develop a framework for enterprises to implement and reduce the risk of successful SE attacks. This research aims to provide a comprehensive assessment of the state of knowledge in this field, identifying best practices and propose a framework for improving SE resilience in organizations. This research can like

so, help enterprises of any size leverage this framework to reduce the risk of success of SE attacks and create a culture of security awareness, along with the development of best practices and support the development of new research studies on innovative and effective interventions to address this issue.

1.2 The Problem

In enterprises where the security architecture has been carefully implemented and is constantly maintained, the human factor remains one of the highest vulnerabilities to cybersecurity, namely SE.

As the world experiences a digital revolution and becomes more dependent on teleworking, cloud computing, and enterprise data storage, these aspects have become essential for businesses to remain competitive and successful. However, with this growth in importance comes an increase in the frequency and sophistication of cyberattacks, which can be carried out by threat actors, hackers, groups, or even state actors. Consequently, the enterprise's employees are perceived as being the weakest link in this incessant attack & defense battle in the cyberspace, regardless of their position or status. Nevertheless, are they the primary attack vectors of cyberattacks? And are they requiring special attention, in addition to the designed, implemented, and maintained security architecture of the enterprise?

While it is yet impossible to fully pre-determine human behavior, it is vital to identify, in an enterprise context, human characteristics or personality traits that are particularly susceptible to exploitation in the context of a SE attack.

Employee resistance to security training is another perceived common issue faced by many enterprises. Despite the importance of security training in reducing the success rate of Social Engineering attacks, some employees may refuse to participate in such programs.

According to the HP Wolf Security Report [23], between 48% and 64% of office workers believe that security measures result in a lot of wasted time. Seventy-three percent said that security policies and technologies are often too restrictive, and over half (54%) of younger workers (between ages of eighteen and twenty-

four) were more worried about meeting deadlines than exposing their enterprise to a data breach.

1.3 Objectives

Answers to questions such as follows are still uncertain:

- How do employee training programs impact the success rate of Social Engineering attacks such as phishing in enterprises?
- How can companies or corporations create a culture of security to reduce the success rate of all types of Social Engineering attacks?
- What factors make businesses employees more susceptible to Social Engineering tactics?

Therefore, this dissertation aims to research and identify effective interventions that improve SE resilience, addressing objectives such as examining the literature on behavioral, technical, and organizational by performing a SLR of factors that contribute to SE attacks in enterprises and their impact on cyber security and semi structured interviews to give voice to employees on several key roles, leveraging this way a theoretical and practical understandment on the difficulties and solutions enterprises face constantly.

Furthermore, the objective is also to investigate the effectiveness of different enterprise interventions to improve SE resilience, including user awareness training, technical controls (filtering and monitoring), and organizational strategies (security culture interventions), and to identify factors that increase or prevent the success of these interventions and how they interact with each other to improve SE resilience.

As a result, this dissertation aims to propose a framework for enterprises to leverage on their operations and mitigate the success rate of SE attacks, while opening the ground to further research and development, incorporating the findings from the SLR and interviews, to improve SE resilience through identification of potential gaps in existing security infrastructures and the prioritization of interventions.

The research findings contribute to the scientific literature on enterprises cybersecurity and offer a knowledge platform for enterprises management on allocating resources to combat this persistent cyberthreat.

The following Research Question (RQ) is considered to this dissertation:

- To what extent do employee training, organizational culture, and individual susceptibility contribute to the mitigation of Social Engineering attacks, such as phishing, within enterprises?

2 THEORETICAL BACKGROUND

This section covers the definition of SE and the different types of SE attacks, that may pose a persistent threat to enterprises.
The focus research objectives of this dissertation are to establish a correlation between SE and human behavior. To appreciate the significance and distinctiveness of this investigation, an initial exploration of relevant literature was conducted through a Systematic Literature Review (SLR). The purpose of this preliminary search was to identify any prior scientific research on these topics applied to an enterprise environment.

2.1 Social Engineering

SE is a deceptive method of manipulating individuals into divulging confidential information, acting, or providing access to a secure system or facility. The success of these attacks relies on exploiting human emotions such as fear, curiosity, trust, and greed. The attackers rely, primarily, on the interactions with the victim [24], their lack of awareness, trust, and vulnerabilities to trick them into providing information or access confidential or restricted data.

SE attacks can take various forms and can be classified based on the techniques that are used, the objective, or the target of the attack. Following, are presented the most common type of SE attacks [25], being phishing one of the most common in enterprises:

Table 1 Common types of SE attacks

Attack Type	Description
Phishing	Sending fake emails or messages to trick the victim into disclosing sensitive information such as passwords, credit card numbers, or login credentials. These emails or messages often appear legitimate and are designed to lure the victim into clicking on a malicious link or opening an infected attachment [26].
Pretexting	Impersonating a trusted source such as a bank, government, or even the employer, to trick the victim into providing confidential information. The

Attack Type	Description
	attacker may use SE tactics to gain the victim's trust before requesting the information.
Baiting	Luring the victim with an attractive offer, such as free products or services, to click on a malicious link or download an infected file. The bait is designed to lure the victim into providing sensitive information or downloading malware onto their device.
Tailgating	Following a person into a restricted area without authorization. The attacker may pretend to be an employee or contractor and rely on the victim's politeness or sense of obligation to gain access.
Watering hole attacks	Compromising a website that is likely to be visited by the victim, such as a popular social media site or news outlet [27]. The attacker may infect the site with malware or use it to launch a phishing attack.
Impersonation	Posing as someone else, such as an executive or a colleague, to deceive the victim into acting or providing information. The attacker may use SE tactics such as flattery compliments or urgency to convince the victim to comply.
Spear phishing	A more targeted form of phishing by customizing the attack to the victim's specific interests, job role, or social media network. The attacker may use personal information or SE tactics to make the attack appear more legitimate.
Vishing	Using a phone call or voice message to trick the victim into disclosing sensitive information. The attacker may pose as a bank or government and may use SE tactics such as urgency or authority to persuade the victim to comply.
Smishing	Using text messages to trick the victim into clicking on a malicious link or providing sensitive information. The attacker may use SE tactics such as urgency or familiarity to persuade the victim to comply.
Quid pro quo	Offering something in exchange of sensitive information (or access). The attacker may offer a gift or service in exchange for the victim's login credentials or other confidential information.

As SE attacks become increasingly sophisticated and widespread, individuals and organizations must understand the techniques used by attackers and take steps to prevent them.

2.2 Materials and Methods

This section describes the process of the SLR used to develop this review.

2.3 Systematic Literature Review

On the systematic literature review (SLR), a thorough search is performed to evaluate which sources are most relevant to answer the research questions, identify gaps, patterns, and contradictions, segment them by themes, chronological hierarchy, methods, and theories, and finally write (synthesizing, analyzing, critically evaluate and summarize) the key findings. This SLR is performed according to the procedures for performing systematic reviews developed by Kitchenham [28]

The objective is through several stages of the process, identify the historical development in the field, validating the literature found, the errors, weaknesses, strengths, and successes, the subject experts, reputable sources, research methods, and the gaps in that literature to leverage other research questions. The SLR can be divided into three main phases (planning the review, conducting the review, and reporting the review) and the process involves the following:

- Determine the problem.
- Determine the research questions that could answer the problem.
- Research in scientific databases for similar papers in the area of study.
- Systematically review and analyze the papers collected.
- Report the results.

The detailed SLR process based on Kitchenham’s procedure [28] is covered in the "Conducting the Review" and "Reporting sections, as follows.

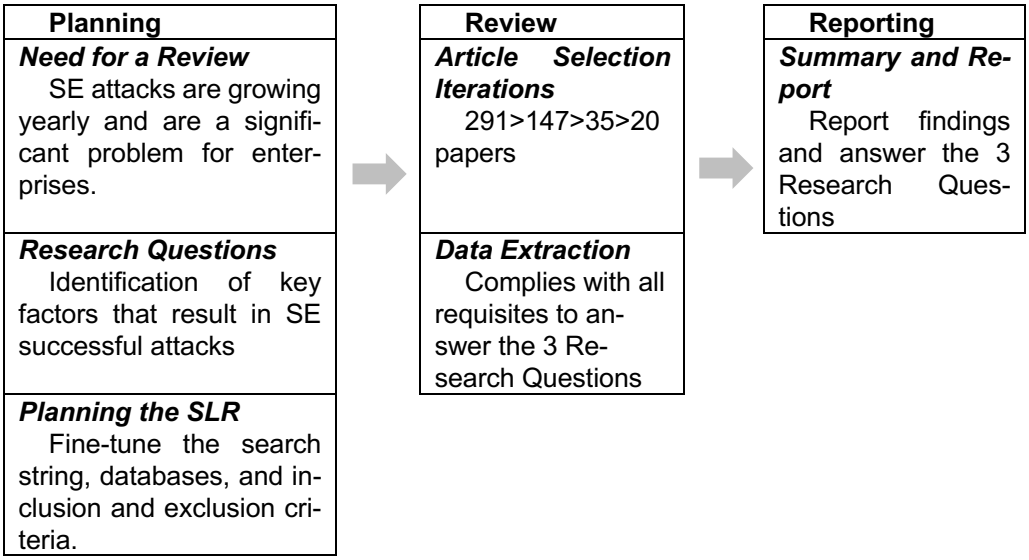

Figure 1 Systematic Literature Review Phases

Figure 1 represents the process, adapted from Kitchenham's procedure [28], divided into three sections; planning (need for a review, research questions and planning the SLR), Review (article selection iterations and data extraction) and Reporting (summary and report).

2.3.1 Background

The SLR is conducted to identify state of the art in this field [28]. This investigation consists of summarizing and synthesizing different scientific literature (scientific papers, scientific publications, thesis, books, and others) found on the SE in the enterprise environment topic. This allows to position this dissertation in relation to existing knowledge and to formulate thoughtful reflections on this topic.

The SLR involves the research of relevant information (on arguments and authors relevant to SE in an enterprise context), allowing a deeper understanding and identifying gaps and problems in the available literature. The SLR research is based on a search string (Table 2) performed on the EBSCO database, considering specific parameters and filters (Table 3).

Data processing from the SLR is detailed in the "Conducting the Review" and "Reporting sections. This data processing and analysis involves methodologies and actions performed on data to help identify and describe facts and patterns and

develop explanations and test hypotheses to the problem object of this dissertation, including data quality assurance, statistical data analysis, data modeling, and interpretation of results.

2.3.2 Planning the Review

A methodical review of existing literature was conducted with the objective to observe the state of the art in this field. This section outlines the scientific paper selection and the search process applied. To determine suitable Search Strings/Expressions, it was necessary first to define the RQs of this SLR, according to the procedures for performing systematic reviews developed by Kitchenham [28] as described in Section 2.3. According to the objective of this dissertation, three RQs were developed:

- How do employee training programs impact the success rate of Social Engineering attacks such as phishing in enterprises?
- How can companies or corporations create a culture of security to reduce the success rate of all types of Social Engineering attacks?
- What factors make businesses employees more susceptible to Social Engineering tactics?

Given the focus on the enterprise environment, several synonyms were used on the first part of the search string to cover more possible results. On the second part of the search string, “social engineering ” and “phishing” were used because using only “social engineering ” resulted in fewer results, and the same principles can be applied to phishing – the most common form of SE in enterprises (Table 1). The complete search string resulted in the search expression shown as follows.

Table 2 Search string used.

Search string
(enterprise OR corporation OR company OR business) AND ("social engineering" OR phishing)

A PICOC (Population, Intervention, Comparison, Outcome, Context) table was created as a criterion to frame the RQs, as suggested by Petticrew and Roberts and proposed by Kitchenham [29].

Population	Enterprises of all sizes, sectors of activity or country
Intervention	Improving SE resilience in enterprises (framework)
Comparison	Social Engineering events, such as phishing attacks, on other enterprises
Outcomes	Improved security, reduced long-term costs and improved enterprise credibility
Context	Enterprises of all sizes with employees whose activities rely on using technology, such as computers, for their work-related activities

The inclusion and exclusion of the papers used in this SLR can be found in the following table.

Table 3 Users training awareness impact.

Inclusion criteria	Exclusion criteria
Directed to at least one of the research topics; Social Engineering or Enterprise	Not in scope
Full text available	Not related to any form of Social Engineering
Academic Journals	Dated before 2008
Scientific Magazines	Not peer-reviewed
Scientific Conference Proceedings	

2.3.3 Conducting the Review

This section highlights the review protocol and the methods used to undertake this SLR, based on Kitchenham's recommendations [28]. A major and significant

scientific database was considered for this literature review, EBSCO (EBSCOhost web - https://web.p.ebscohost.com/ehost/search/).

The EBSCO search engine used in this dissertation was accessed using the advanced search option. To not limit the results, the search period was left as default. In this process, the option to search for words in the abstract (AB) was selected. The search was limited to available academic journals, scientific magazines, conference materials and proceedings, and full texts. These applied filters ensured and assessed the quality of the primary studied to be used.

During each of the scientific paper's selection processes, papers were classified into three categories: "Include," "Maybe," and "Exclude," based on their relevance to the research questions.

Papers that added no value to the research (or were not in scope) were marked as "Exclude" and were not included in subsequent iterations. The "Maybe" papers were those for which it was unclear whether they would add value, and "Included" papers were considered relevant to the study. Although both "Included" and "Maybe" papers were considered for the following selection phase, the "Maybe" papers were reviewed to determine the factor that placed them in this category and were finally considered or discarded.

The selection phase of the papers was done cumulatively and considered the inclusion and exclusion criteria detailed in Table 4. The search in EBSCO with the search string (Table 2) returned 291 results. These results were then exported to Rayyan (https://www.rayyan.ai) in the “bib” format. After this import into Rayyan, one duplicate was detected and eliminated.

The selection process of the papers began with reading the 290 abstracts. Then, 143 papers were excluded, either “Not related to any form of SE” or “Not in scope”, resulting in 147 selected papers.

The 147 papers introductions and conclusions were read in the following selection phase, from which 112 were excluded by not being in scope, although mentioning SE, resulting in 35 selected papers.

In the final selection phase, the entire 35 papers were read. Eleven more papers were excluded by needing to be more pertinent or in scope, resulting in 24 papers. Four papers were finally excluded by being unable to respond to any research questions, concluding in 20 relevant papers.

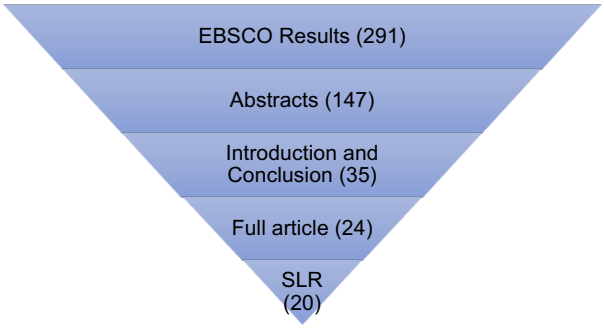

Figure 1 Selection phases

The following table presents the number of papers that were included and excludes according to the inclusion and exclusion criteria presented in Table 4.

Table 4 Papers included/excluded according to inclusion/exclusion criteria.

Inclusion criteria	Included	Exclusion criteria	Excluded
Directed to at least one of the research topics; Social Engineering or Enterprise	274	Not in scope	144
Full text available	291	Not related to any form of Social Engineering	35
Academic Journals	123	Dated before 2008	0
Scientific Magazines	168	Not peer-reviewed	0
Scientific Conference Proceedings	0		

Regarding the publication year of the papers, the following graphic (Figure 2) shows the distribution of SE-released papers over the years in the final 20 articles used in this review. It is observable an increase in releases over the recent years regarding this topic.

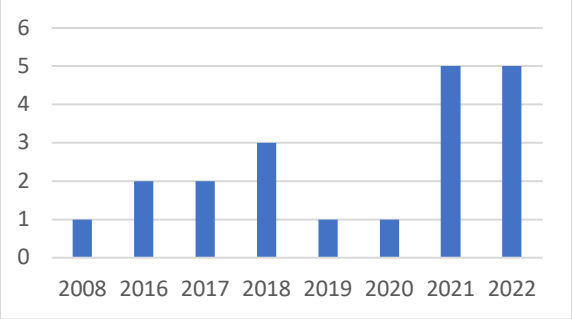

Figure 2 Release SLR final papers over the years

The following table presents the mapping of the final papers used in this review, the publication year, and the number of citations.

Table 5 Mapping of the Selected Papers

Publication	Publication Year	Number of Citations
[15]	2017	20
[20]	2022	13
[5]	2022	13
[11]	2017	13
[18]	2008	11
[17]	2022	10
[8]	2021	10
[2]	2022	9
[9]	2016	8
[16]	2018	8
[19]	2021	8
[12]	2018	7
[3]	2020	6
[6]	2021	5
[4]	2019	4
[7]	2016	4
[10]	2018	4
[13]	2022	4
[14]	2021	3
[1]	2017	3

The data synthesized was performed on a comprehensive matrix. Excerpts from the papers were compiled on the matrix and analyzed on their relevancy and/or by matching the search strings. The combination and analysis of the selected papers allowed, therefore, to formulate conclusions directly derived from this evidence.

2.3.4 Reporting

This section presents the resulting findings for the three RQs of the SLR.

RQ1: How do employee training programs impact the success rate of Social Engineering attacks such as phishing in enterprises?

SE has several approaches, focusing from the technical side to the human behind the machine. However, while the network of any enterprise can be architected, patched, and updated with the best security frameworks and recommendations, the human component is more difficult to control due to its susceptibility to emotional influence [19]. This review observes that any enterprise needs to provide users with cybersecurity training and awareness (mainly focused on phishing) to identify SE threats and promptly react to them [7], influencing user behavior in terms of defending against information security risks [15].

User awareness and training programs should not, however, be one-size-fits-all. To create a resilient defensive and awareness behavior against cyberattacks such as SE, management should thoroughly consider identifying groups of employees according to their level of information security awareness and skills. Then, tailoring specific high-intensity and narrowly focused training [19] through methodical, structured, consistent, and measurable training programs [10], [11] like internal phishing campaigns or game-based learning can be applied. These training programs should also focus on cognitive and emotional factors. Also, training should give attention to phishing emails inspection and technical authentications [11]. When preparing for training delivery, the programs should consider decreasing the biases caused by perceived familiarity [8] and being adjusted not to be extremely hard (frustrating the user), or extremely simple (giving the user overconfidence), being challenging enough to stimulate the learning process.

Throughout the review it is noticeable the correlation between information security/cybersecurity, and employee awareness of cyber threats. Therefore, human resource's function must be involved from the start, both in terms of employee selection (i.eg, induction trainings on cybersecurity) and the periodic training plans [19], to maximize user awareness and minimize the enterprise's overall vulnerability to being a cyberattack victim.

Most of the literature and scientific papers identified in this field are directly related to phishing, the most common type of SE attack (usually seen in an enterprise environment), not covering the several facets and complexity of what SE comprehends and its effect on the human susceptibility. These factors impact this review because several studies only focus on phishing and phishing email interpretation rather than on the core concepts of SE. Therefore, the training programs and their impact on the success rate of SE attacks in enterprises and the mitigation procedures are often specific to phishing.

According to the scientific papers relevant to this study, the majority (17) relates user awareness training provided to employees with preventing SE attacks, especially the most common form of SE - phishing emails. However, one article stated that awareness training is ineffective [20] or is not cost-effective [21]. Another stated that there are insufficient studies on security training for individual users [9], even though recognizing that user awareness is essential when reducing the risk of SE.

Table 6 Employee's training awareness impact

Impact	Number of Papers	Papers
Increase in cybersecurity and Information security within an enterprise	18	[2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19]
Not adequate for cybersecurity and Information security improvement	2	[20], [21]

RQ2: How can companies or corporations create a culture of security to reduce the success rate of all types of Social Engineering attacks?

On the previous researched question, most papers [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19] related user awareness training provided for employees with success on preventing SE attacks, and correlate the user awareness training as a part of security culture on the enterprise.

Three papers [20], [16], [14] identified the key point to create a culture of security and consequently reduce the success rate of a SE attack to be a cooperative effort by involving users collectively in addressing SE. Two papers [9], [14] referred to it as the continuous training and simulation programs, and two [16], [14] as the involvement of the management and human resources functions. One article [21] refers the use of Machine Learning technology as the best way to achieve higher security, and one article [17] identified that the roles' accesses at an enterprise need to be compartmentalized.

The perceived severity of threats directly correlates to the user's motivation in preventing them from happening [14], directly impacting results in the enterprise security culture. Due to this relevant impact, user awareness, motivation, and engagement efforts to protect sensitive information cannot be lightly planned as a one-fit-all or a set it and forget it [16], [14] approach. The key is to embed core concepts into users' everyday tasks by simulating attacks on the enterprise for them to retain the information more efficiently, with continuous training and simulation programs[9] that are engaging, relevant, and beneficial.

The security culture must be set as a whole, from management, executives, human resources [16] functions, regulators, Information Technology (IT), and all user departments [9]. All enterprise employees should be aware of potential risks to the enterprise. Through open and honest communications, management increases trust and the security mindset [14].

Employee engagement is, therefore, the key to developing a cybersecurity culture, along with a risk management plan, part of the overall organizational strategy and business continuity plans [16].

This involvement and join effort resulting from an open disclosure of what is at risk and what users can contribute to the overall enterprise security culture can also be complemented, for instance, by an anti-phishing approach to prevent phishing attacks, while using intelligent Machine Learning (ML) technology [21]. In addition, a contributing factor can be the need-to-know approach regarding users' access to critical sensitive information by compartmentalizing user access [17] (and risk) and minimizing the risk of possible information exfiltration.

Only six out of the twenty papers in scope mention directly or indirectly the security culture in an enterprise. However, the findings associated with RQ2 show that user awareness training (with specific characteristics) is also part of the "formula" to increase enterprise security.

Table 7 Actions for creating a culture of security.

Actions	Number of Papers	Papers
Addressing Social Engineering on a collective level (employees' engagement)	3	[20], [16], [14]
Involvement of executive level and engagement of human resources function	2	[16], [14]
Continuous training and simulation programs	2	[9], [14]
Using intelligent machine learning (ML) technology	1	[21]
Compartmentalize roles	1	[17]

RQ3: What factors make businesses employees more susceptible to Social Engineering tactics?

Mapping what factors can make someone more vulnerable or prone to a SE attack is challenging due to the complexity of human behavior and individual traits. Only six papers [15], [14], [19], [6], [11], [17] offer a few mentions related to what can make individuals more susceptible to SE attacks; the remaining papers do not aboard this subject [12], [9], [16], [21], [13], [2], [18], [8] or enumerate what personal traits or human characteristics, attackers may leverage or exploit on a SE attack [3], [4], [5], [7], [20], [10].

What makes SE attacks successful is the fact that Threat Actors trigger emotional biases [20], appealing to strong emotions or feelings like fear [20], [3], [4], excitement [20], trust [7], [11], [18], [20] commitment [20], lust [30], curiosity [18], greed [3], pity [3], anxiety [3], urgency [3], [18], [4], need [18] and authority [18]. These emotional biases are commonly used to influence users to, for instance, open a phishing email, using the Principles of Persuasion in SE; authority, social proof, liking, similarity and deception, distraction, commitment, integrity, and reciprocation [5]. On the other hand, IT professionals are less prone to fall for an SE attack [15], [14], [19], so as employees working in larger teams [6], higher job levels [6], new joiners [6], users unable to focus [11], frequent internet users [11].

Users that received recent (and periodic) security awareness training are also less prone to fall for a SE attack [14]. Despite this, some users may fall prey to a self-serving bias by believing they are more likely to identify a phishing email and therefore, being more prone to fall for a SE attack like a phishing email [11].

Some studies also reveal that variables like individual differences are not significant to identify the increase in the probability of someone falling more easily to a SE attack [11]. Furthermore, mental tactics proneness cannot be point out for specific groups of people, especially the vulnerable ones [4].

Table 8 Individual factors more susceptible to SE

Factors	Number of Papers	Papers
Employer characteristics		
Technical skills (not working in IT)	3	[15], [14], [19]
Role (lower job level)	2	[6], [14]
Gender (female)	2	[6], [19]
Time employed (longer time)	2	[6], [14]
Part-time	1	[6]
Team (working in a large team)	1	[6]
Age (older)	1	[6]
Age (younger)	1	[19]
Gender (male and female are similar)	1	[14]
Personality traits		
Boredom proneness	1	[11]
Trustworthy (known source)	1	[11]
Focus (more focused)	1	[11]
Normative commitment (high)	1	[17]
Continuance commitment (high)	1	[17]
Trust (more trustworthy)	1	[17]
Neuroticism (high)	1	[19]

2.3.5 Discussion

The choice of the three research questions derives directly from the increasing number of cyberattacks like phishing on enterprises, that often start (and end) with an SE attack, even when this cybersecurity threat has stayed the same over time. The purpose of this dissertation is, therefore, to establish a correlation between what is currently being done in enterprises regarding user training awareness programs, how enterprises are performing to stimulate the increase of a cybersecurity culture, and what makes a person, or a group of persons more susceptible to fall prey for SE attacks. The approach to answering these questions included a scientific and methodological SLR to determine the state of the art in this field addressed in studies, and to open ground for future development work to improve enterprises' cybersecurity.

Regarding RQ1, the “Reporting” section results demonstrated a widespread agreement that user training awareness is an essential central point in an enterprise’s cybersecurity. These results highlight the importance of addressing the human element in cybersecurity, particularly concerning SE attacks, through tailored user awareness and training programs. These programs should be consistent, measurable, and challenging while involving human resources function from the pre-planning phase. While most studies suggest the importance of user awareness training, some studies suggest ineffectiveness or cost-ineffectiveness. Additionally, there are limitations of studies only focusing on phishing, one of the most common forms of attack of SE, highlighting the need for a comprehensive understanding the effects human susceptibility on SE.

The findings related to the RQ2 demonstrate that the security culture must be set as a whole, Involving management, executives, human resources, regulators, IT, and all user departments. Open and honest communication from management increases trust and the security mindset, as employees should be aware of potential risks to the enterprise. The “Reporting” section also notes that only six of the twenty papers directly or indirectly mention security culture in an enterprise, even though, as discussed in the previous research question, user awareness training with specific characteristics should consider as part of the formula to increase the enterprise security culture.

Regarding RQ3, the findings demonstrate the difficulty in identifying personal traits or human characteristics that make individuals more susceptible to SE attacks. Only six reviewed papers mention such traits, while the remaining refer the need to address the topic. SE attacks are successful because they trigger emotional biases such as fear, trust, and curiosity, amongst others, which can be used to influence users to fall for a phishing email, for example, using persuasion principles. These findings also suggest that IT professionals, employees in larger teams, higher job levels, new joiners, and users who received recent security awareness training are less prone to fall prey to SE attacks. However, individual differences and mental tactics cannot be used to identify vulnerable groups of people. We can also observe

in the findings that some users may fall to self-serving bias by believing they are less likely to fall for SE attacks.

2.3.6 Further investigation

While the reviewed literature focuses primarily on phishing attacks in many cases, other SE attacks could be explored, such as spear phishing, pretexting, baiting, quid pro quo, tailgating, scareware, vishing, and smishing. Investigating these other types of attacks could provide a deeper understanding of the attacker's tactics.

Regarding the importance of user awareness training and the security culture of an enterprise, further research can explore whether immersive simulations or gamification, as stated by Alsawaier [31], the application of game features, like video game elements, into non-game context with the purpose of motivate and engage in learning. These methodologies can therefore be more effective than traditional training methods.

The results of the SLR note the difficulty in identifying personal traits or human characteristics that make individuals more susceptible to SE attacks. However, it would be valuable to investigate this topic further to understand how attackers choose their targets and how enterprises can better prepare their users.

Finally, results show that only a few papers mention the security culture in an enterprise, and more research can explore how an organization's culture affects its vulnerability to SE attacks. This could include the focus on examining the role of leadership, the effectiveness of different communication strategies, the level of psychological safety and the impact of user engagement on an organization's security posture.

Employee resistance to security training is another common issue in many enterprises. Despite its importance in reducing SE attacks, some employees refuse to participate for various reasons. Resistance can occur from a lack of understanding about the significance of security training, such as fully comprehending the potential risks of SE attacks and their impact on the enterprise. Additionally, employees may view security training as an extra burden on their workload, leading them to prioritize

other tasks over attending training sessions. Cultural resistance may also contribute to the problem, with factors such as lack of support from management, insufficient emphasis on security culture, or the belief that security is only the responsibility of the IT department. Further investigation is also necessary to determine the root causes of employee resistance to security training in enterprises.

2.3.7 SLR Conclusions

Several findings could be observed in the SLR. The findings suggest that educating employees with regular and tailored training awareness programs are part of the procedures for reducing the probability of a SE attack. Furthermore, by ensuring compliance with security policies and procedures, education-based training is significantly more effective in gaining compliance [14], [17], as cybersecurity knowledge and beliefs of employees have a significant impact on their intentions to comply with organizational cybersecurity controls [19]. However, while there is broad agreement about employees training and awareness, some studies suggest that specific training programs may need to be more effective or cost ineffective.

Moreover, the importance of a security culture involving all organizational stakeholders must be considered. For example, open and honest communication from management can increase trust and the security mindset among employees, making them more aware of potential threats to the enterprise. However, the limited mention of security culture in the reviewed literature highlights the need for more future research to explore the effectiveness of different communication strategies and the role of employee engagement in an enterprise's security posture.

While the reviewed literature identifies emotional biases such as fear, trust, and curiosity as crucial factors that can make individuals more susceptible to SE attacks, the difficulty in identifying personal traits or human characteristics that make individuals vulnerable highlights the need for further investigation on how human factors impact the level of enterprises' cybersecurity.

3 RESEARCH METHODOLOGY

This section covers the researched methodology used. In the first stage of this research, a Literature Review was conducted to identify the problem addressed in the previous section. As mentioned before in the “Further Investigation” section, there are still further investigation to be conducted.

Therefore, to continue and guide the investigation of this dissertation and answering the research question mentioned in section 1.3 Objectives, the activities of Design Science Research (DSR), proposed by Peffers *et al.* [30], have been selected as the primary research methodology. Once the initial artifact (framework) has been developed, the next step is to conduct an evaluation phase. Finally, to support the preliminary research findings and refine the artifact, semi-structured interviews will be used to gather data to be analyzed.

3.1 Design Science Research

Design Science Research (DSR) is a research approach that aims to address organizational issues by creating and evaluating IT artifacts. This methodology, that will be used in the paper, involves a systematic process of designing artifacts to solve identified problems, contributing to research, evaluating the effectiveness of the designs, and communicating the results to relevant stakeholders.

The created artifacts can consist of several elements, such as constructs, models, methods, and instantiations, that can lead to innovations and new features in technical, social, or informational resources [22].

DSR is an iterative process that involves several phases, starting with problem identification, then developing a design solution evaluated using a set of defined criteria. These criteria usually consider factors such as feasibility, efficiency, effective-ness, and usability of the artifact and its potential impact on the enterprise. DSR emphasizes the importance of rigor and systematic analysis to ensure designs are grounded in theory and evidence-based practices.

In addition, DSR recognizes the importance of considering the human factors involved in using and adopting IT artifacts. Therefore, it considers the social,

cultural, and organizational context in which the artifacts are intended. DSR aims to create artifacts that are technically feasible, are socially acceptable and culturally appropriate.

According to Peffers *et al.* [30], the Design Science Research Methodology (DSRM) involves six steps detailed as follows.

1. ***Identify the problem and motivation:*** which involves understanding the current state of the problem, the limitations of existing solutions, and the potential benefits of a new solution. As mentioned on Section 1 (Introduction), the problem is the increase of SE attacks in enterprises and the effects that user awareness, through training programs and personal traits, has on reducing these types of cyberattacks.

2. ***Define the objectives:*** which should be specific, measurable, achievable, relevant, and time-bound (SMART) [22]. It involves identifying the outcomes that the research aims to achieve and the criteria for evaluating the success of the research. In this case, proposing a framework to improve SE resilience in enterprises.

3. ***Design and develop the artifact:*** which is the new solution that addresses the problem. It involves defining the requirements of the artifact, designing the solution, and developing a prototype or a working model of the artifact (framework) to improve SE resilience in enterprises.

4. ***Demonstrate the artifact:*** which involves evaluating the artifact's effectiveness and usability in a real-world setting. It involves testing the artifact with users, collecting feedback, and identifying areas for improvement. In this stage, the proposed framework is implemented on a corporate environment and tested.

5. ***Evaluate the artifact:*** which involves assessing the artifact's effectiveness, efficiency, and usability. It involves measuring the outcomes achieved by the artifact, comparing it with existing solutions, and identifying the limitations

and challenges of the artifact. This stage uses the semi-structured interviews detailed in the Section 4.2 (Semi-structured Interviews)

6. ***Communicate the results:*** which involves sharing the findings, conclusions, and implications of the research with the relevant stakeholders. It involves writing papers and a master's dissertation.

These phases of the DSRM are presented in Figure 3, regarding the actions per each phase of the process [22].

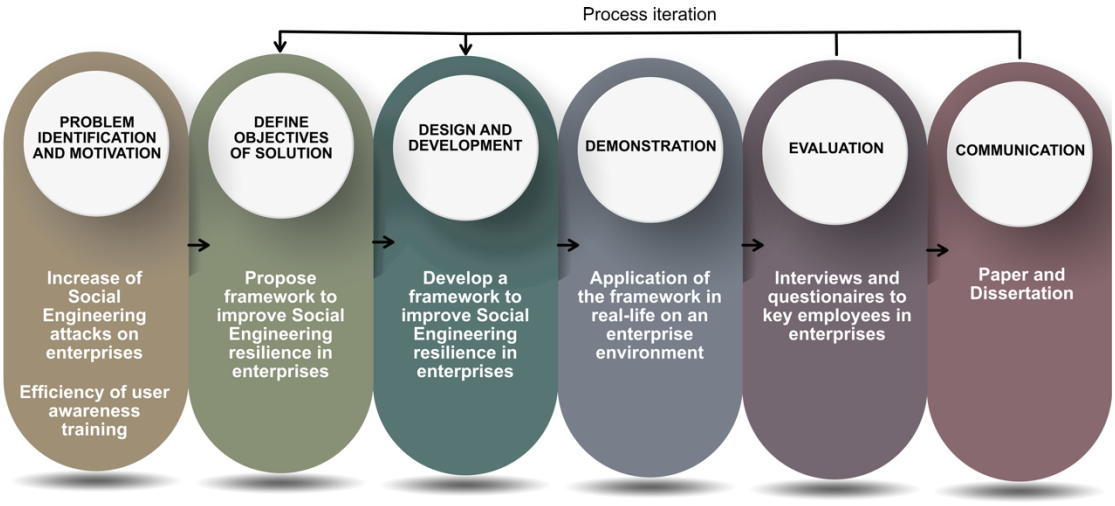

Figure 3 Adapted DSRM Process Model

3.2 Semi-structured Interviews

The semi-structured interviews conducted within several organizations, evaluates the enterprise's SE prevention or resilience capabilities, and their relationship to user's personal traits and awareness levels. Before the interviews, an interview protocol is prepared, and potential participants are informed of the research objectives and asked for their consent to participate.

Semi-structured interviews are a commonly utilized approach in development research, as they offer insights into the mental processes behind decision-making and behaviors where the interviewer follows a guide, but can, when it feels appropriate, pursuit the understanding on certain topics within the course of the

interview [32] and enhancing therefore, the quality of the research [33]. Additionally, they often provide valuable information previously unknown to the researcher. In this study, the semi-structured interviews explored the enterprise's practices, capabilities, and Key Performance Indicators (KPI's) used in user awareness and SE attack prevention. The framework will then be examined from the perspective of these capabilities and their related KPI's.

Semi-structured interviews are beneficial in the following scenarios:

- Asking open-ended questions to gain insight into individual perspectives within a group.
- Conducting one-on-one evaluations with critical stakeholders (different roles, positions, and experience).
- Exploring unexplored topics with potentially significant issues.

This method is standard in qualitative research and involves using an interview guide [32], which outlines a list of questions and topics to be covered during the conversation. However, the interviewer has the flexibility to explore additional topics if appropriate. This guide can be found in Appendix A.

The Interviews were conducted in national and international enterprises to sixteen key subjects and positions: management, security team, cloud architecture, consulting, vendors, finance, and end (non-IT) users, with different levels of expertise and experience in Information Security.

During the interviews, an interview protocol was used, mainly informing the participants about the research goals, and asking for their consent to the interview.

The interview protocol for this study considers the finding identified in the SLR conducted before. Furthermore, this protocol of semi-structured interviews, enables an inside view of how this framework can impact and answer the remaining open answers initiated by the Research Questions, as they offer the interviewer the opportunity to deeply develop topics that arise during conversations [32].

4 PROPOSAL

This section covers the proposal in the form of an artifact. In the case will be a conceptual framework for improving SE resilience in enterprises, which requirements are resumed in Table 7.

This conceptual framework will be a crucial element establishing the significance and relevance of this study, and its contribution. It provides a solid rationalization for the research questions and outlines the research design, including data collection and analysis methods, to ensure that this research is appropriately and scientifically conducted.

Furthermore, it contextualizes the study within multiple dimensions and positions of the research against another research. It acknowledges the biases, assumptions, and values that may affect the research outcomes, articulating the study's underlying theoretical foundations, enabling the understatement of the study's research questions, data collection, analysis methods and how this study fits into the larger theoretical and research context.

This conceptual framework aims to provide a roadmap to ensure that the research design and methods are aligned with the research questions and the theoretical perspective, identifying gaps in the existing research, understanding the complexities of the research problem, and ultimately generate new knowledge [33].

Table 9 *Proposed Artifact (simplified): Framework for improving SE resilience in enterprises.*

Components	Description
User Awareness and Training	Develop a tailored and measurable training program that involves Human Resources starting from the pre-planning phase.
Security Culture	Create and nurture a culture of open and honest communication that provides regular training sessions, seminars, and workshops on cybersecurity.
Address Emotional Biases	Use persuasion principles to educate employees on how to identify and avoid SE attacks.

	Target different user groups with emphasis on IT professionals and new joiners.
Continuous Evaluation	Continuously evaluate the effectiveness of the training program, security culture, and persuasion techniques using metrics and KPI's. Make all necessary improvements.
Empower Reporting	Empower employees to report suspicious activity through an anonymous mechanism without fear of reprisal. Provide regular feedback on the effectiveness of the reporting and any actions taken.

Table 9 describes in a high-level detail, the proposed artifact (framework), object of this dissertation.

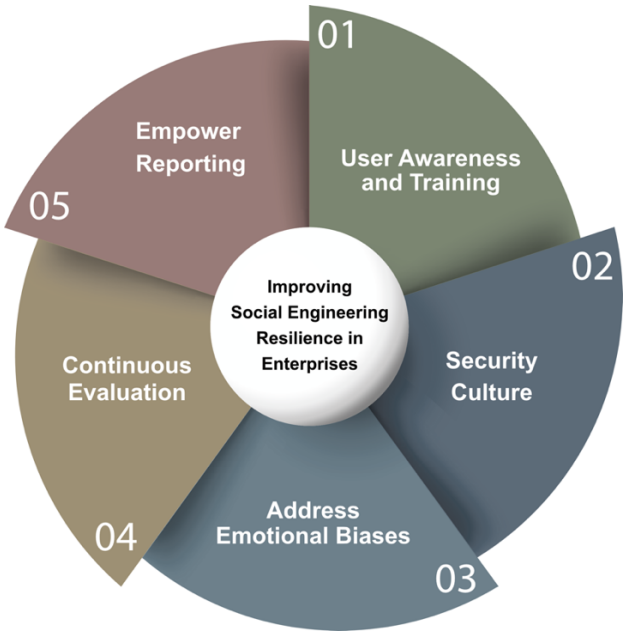

Figure 4 Proposed framework sectioning

Following, it is presented a detailed description of every component of the proposed framework.

Table 10 *Proposed framework detailed description.*

Component	Proposed framework
User Awareness and Training	• Conduct a baseline assessment of employee's knowledge and awareness of SE attacks to identify gaps and areas for improvement. • Develop a training program that includes different delivery methods (e.g., videos, simulations, gamification, quizzes) and is tailored to the different roles and responsibilities within the enterprise. • Integrate meaningful SE awareness into new employee onboarding and ongoing training programs. • Develop metrics and KPI's to measure the effectiveness of the training program as phishing simulation results and users feedback surveys. • Ensure that awareness training is up to date, adapted to the enterprise reality and with the latest SE tactics and threats.
Security Culture	• Develop a communication plan that includes periodic security awareness messages and reminders. • Encourage a culture of openness and transparency where users feel comfortable reporting incidents and sharing information about potential threats. • Provide incentives for employees who demonstrate responsible security practices and behavior. • Ensure collaboration and communication between different departments and teams to promote a shared responsibility for security. • Establish a security working group to overlook and coordinate security related activities across the enterprise.

Component	Proposed framework
Address Emotional Biases	• Develop educational materials that use persuasive communication techniques to increase users understanding of SE threats and their emotional responses to them. • Provide examples and case studies that illustrate the impact of SE attacks on users and the enterprise. • Use positive reinforcement such as recognition and rewards, to encourage users to adopt reasonable security practices. • Use gamification or other interactive approaches to engage users and increase their motivation to learn about SE.
Continuous Evaluation	• Develop a set of metrics to measure the effectiveness of the different components of the framework, specifically user awareness, security culture and reporting. • Use these metrics and KPI's to identify areas for improvement and perform necessary adjustments. • Conduct regular reviews and evaluations of the framework to prove its relevancy and effectiveness in facing ever-evolving SE threats.
Empower Reporting	• Develop or improve a reporting mechanism that is easy to use, anonymous, and secure. • Provide clear guidance to users on what types of incidents should be reported and how to report them. • Establish a process for triaging and responding to reported incidents. • Provide regular feedback to employees on the status of their reported incidents and any actions taken.

Overall, this framework takes a comprehensive approach to improving SE resilience in enterprises by addressing the human element of cybersecurity and focusing on user awareness, a security culture, and on emotional biases. Therefore, the proposed framework aims to improve SE resilience in enterprises by addressing these key factors.

In Figure 5, it is presented the process diagram for the framework to improve SE resilience in organizations.

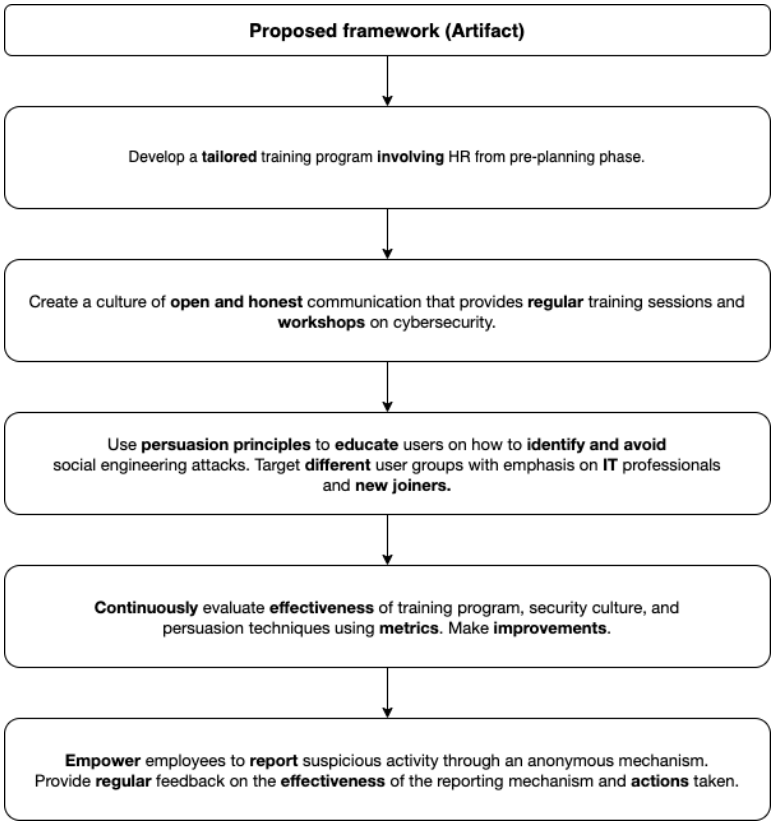

Figure 5 Process diagram of the Artifact

The following section will detail the Evaluation phase of this dissertation.

5 EVALUATION

The evaluation will be done using semi-structured interviews as detailed in Section 3.2. Semi-structured interviews are an accepted method in development research that differentiated itself from other types of interviews, which follow a specific set of predetermined questions, focusing on certain themes and topics but, like mentioned by Raworth *et al.* [34] conducted in a conversational approach.

5.1 Interviews

The semi-structured interviews were conducted using a set of twenty pre-defined questions, including follow-up questions. The questions were primarily open-ended, as detailed in Appendix A, to allow detailed responses, and cover the three research questions identified previously.

The interviews were conducted by phone using Microsoft Teams, WhatsApp, Telephone or performed in person, facilitating the maximum participation and convenience for the interviewees. All interviews, when possible, were audio recorded to ensure that all the details of the responses were captured accurately for further review. The interviews were also, when possible, automatically transcribed to allow easy analysis of the data and to identify common themes and patterns that emerged across the interviews.

Subsequent data analysis involves a combination of approaches to identify insights that can inform the development of the framework for improving SE resilience in enterprises. In addition, the data collected from the interviews was compared to the findings from the SLR conducted earlier to identify any gaps or areas where additional research was needed.

The results of the interviews were used to validate the artifact of the DSR proposed by Peffers et. al. [30]. In addition, the feedback and insights provided by the interviewees allows to refine and improve the framework, ensuring that it is both comprehensive and practical for use in real-world settings in an enterprise environment.

Conducting these semi-structured interviews was a critical step in gathering valuable insights and data, which contributes to the development of the framework for improving SE resilience in enterprises.

5.1.1 Preparation

To conduct the semi-structured interviews, individualized preparation was done for each participant to expedite and facilitate the interview process. Once the participants provided consent to start the interview, the interviews started following the structure as shown in Appendix A, which covered the research questions presented in the Reporting section.

Before each subsequent semi-structured interview, close observation was conducted on the previous interview results to gain a thorough understanding of the issue and to reformulate appropriate semi-structured questions when needed. This process allowed better open-ended questions relating to the problem, providing the opportunity to discover new approaches, to challenge and comprehend the evolution of the framework. This approach was based on recommendations from prior research [32].

5.1.2 Participants Characterization

To leverage and gather a broader and significant sample as possible, several company sizes, sectors, positions, and countries were considered. Likewise, the sixteen interviews comprised from IT savvy practitioners to non-IT users. Like summarized in Table 11, the interviewee's current positions in IT are diversified as CISO (Chief Information Security Officer), SOC (Security Operation Center) Manager, Cybersecurity Engineer, Support Engineer, Security Analyst, System Engineer, Senior Software Developer and Security Architect. And not IT related positions range from Consulting Partner, Manager, General Manager, Project Manager, Quality, Environment and Energy Coordinator, Production Supervisor and Office Administrator. The countries (Portugal, Spain, Ireland, Germany, India, and Switzerland) and the number of employees (from 40 to 240000) of each working place of the interviewees are also diversified. Five of the interviewees have ages below forty years, nine of them between forty and fifty, and two more than fifty years old.

Table 11 *Interviewees characterization*

ID	Date	Current Position	Enterprise sector	Employees	Country	Age
#101	15/06/2023	Quality, Environment and Energy Coordinator	Express transportation & Logistics	600	Portugal	46
#102	14/06/2023	Manager	Finance	4300	Portugal	46
#103	13/06/2023	Security Analyst	IT Services	240000	India	39
#104	13/06/2023	Cybersecurity Engineer	IT Consultancy	1000	India	44
#105	07/06/2023	Support Engineer	Business software	50000	Ireland	44
#106	06/06/2023	Project Manager	Engineering services	8000	Germany	42
#107	06/06/2023	Office Administrator	Public Education	200	Portugal	38
#108	05/06/2023	Consulting Partner	Sustainability Consulting	8000	Spain	45
#109	05/06/2023	General Manager	Education	40	Portugal	46
#110	06/09/2023	System Engineer	IT Services	240000	India	38
#111	08/06/2023	Security Architect	IT Development	500	Spain	29
#112	06/07/2023	SOC Manager	Commodity Trading	11000	Portugal	39
#113	06/07/2023	CISO	Commodity Trading	11000	Switzerland	56
#114	14/06/2023	Senior Software Developer	Finance	300	Spain	47
#115	15/06/2023	Production Supervisor	Manufacturing	160	Portugal	55
#116	17/06/2023	Pharmaceutical	Healthcare	61000	Spain	46

Table 11 details the sixteen interviewees characterization used to perform the interviews.

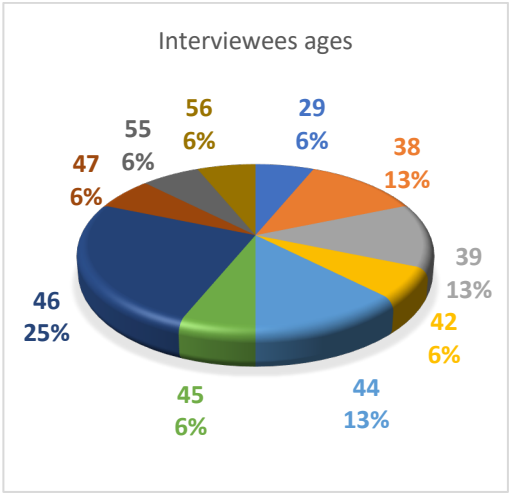

Figure 6 *Interviewee's ages*

In Figure 6, it can be observed that the percentage of the interviewees ages are situated between 38 and 46 years old.

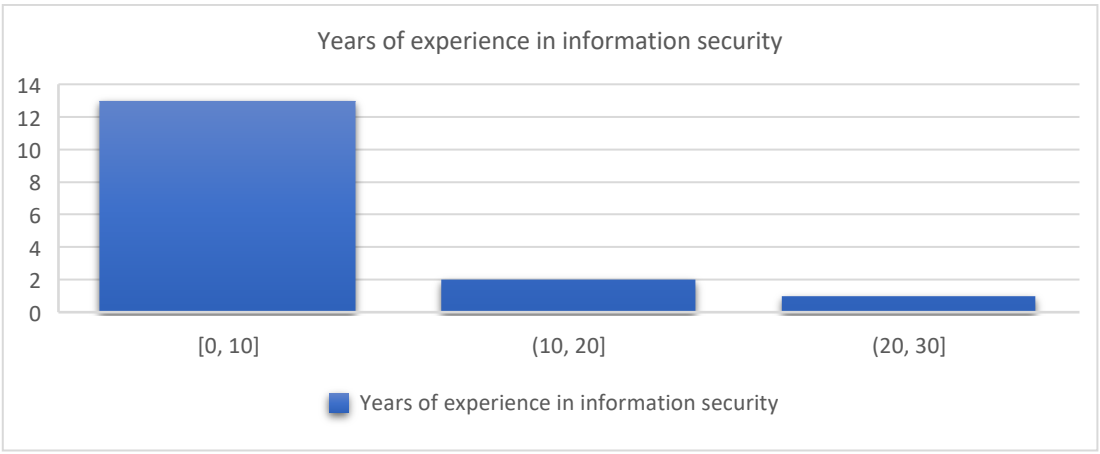

Figure 7 *Years of experience in information security*

In Figure 7, it can be observed that most of the interviewees have between 0 and 10 years of experience in the field of Information Security.

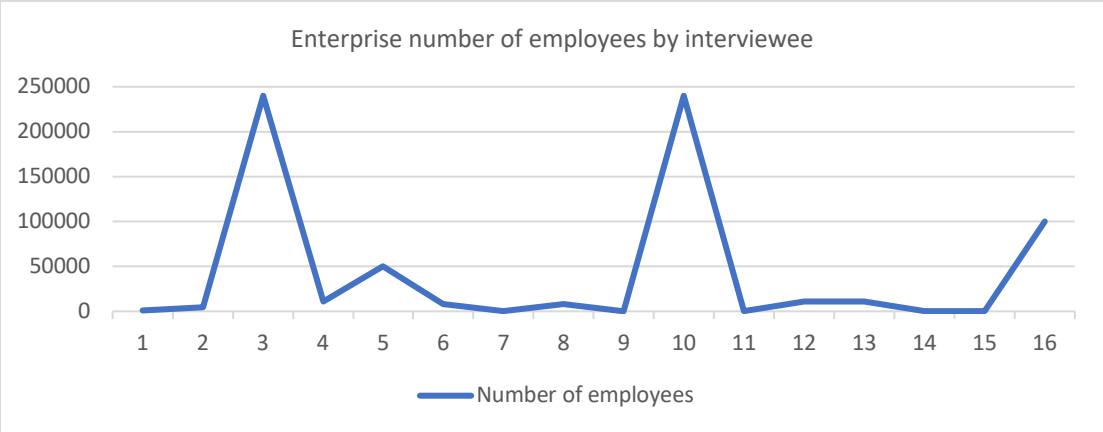

Figure 8 *Enterprise number of employees by interviewee*

As it can be observed, most employees is situated below five thousand employees, one enterprise at around ten thousand, and another around twenty-four thousand employees.

5.1.3 Conducting the Interviews

This section transcribes the summary of the interviews conducted according to Table 11. All the interviews were performed as detailed in Annex A, focusing on validating the framework proposed in Section 5 “Proposed Artifact”, and responding to the tree research questions presented in the section 3.1.5 “Reporting”.

Table 12 *Interviews summary - key takeaways*

Interview number	Key takeaways
#101	• The effectiveness of regular reminders, phishing campaigns, and information reinforcement in educating employees about SE attacks. • The lack of resistance among employees towards security awareness programs. • Regular training, phishing campaigns, and email alerts on emerging security trends contribute to the security culture, along with being an international company and maintaining a specialized IT department. • To ensure policy compliance, she recommended audits, relevant examples, and informative materials. • Factors such as lack of attention and distraction contribute to individual

	susceptibility, and enhancing SE resilience requires reinforcing awareness, sharing real-life examples, and emphasizing information security's importance.
#102	• Employee training programs and establishing a security culture is essential to mitigate SE attacks. • Effective employee education methods include enforcing solid passwords, closing idle computers, being cautious with client orders via email, and avoiding leaving accessible information. • The company implements internal phishing campaigns and e-learning training to prevent SE attacks, resulting in a 60% to 70% reduction in successful attacks. • Resistance to training is minimal due to mandatory requirements and strict internal rules. • Compliance with security policies is ensured through e-learning results and measured using key performance indicators. • Common SE tactics encountered include phishing emails, smishing, and vishing. • Individual factors influencing SE attacks includes lack of awareness, training, and understanding of threats.
#103	• Highlights the importance of security awareness training covering several types of attacks, focusing on human-based tactics. • They have implemented programs targeting phishing emails, SE attacks, and sends regular awareness emails. They also do internal phishing campaigns to assess employees and provide training when necessary. • Training programs have proven effective in reducing the success rate of SE attacks by an estimated 60 to 70% when employees are knowledgeable about the tactics and procedures involved. • Resistance to training is minimized through strict enforcement and the potential consequences of low scores on their cybersecurity scorecard. • Initiatives like the “Cybersecurity Week”, regular communication from the Information Security and training contribute to a better security culture. • Consistent application of security policies is ensured through a comprehensive security management plan involving senior management, middle management, IT teams, and end users. • Phishing attempts are the most common SE tactic encountered
#104	• The enterprise conducts phishing campaigns every two months, followed by training for successful phishing victims, reducing SE attack success rates, mainly through mandatory training for failed phishing campaign participants.

- Employee resistance to security awareness programs derive from factors such as workload, disinterest in security, limited risk awareness, uninspiring training, and the absence of consequences.
- Suggests a system that restricts tool access for phished or non-compliant individuals. Gamification through a points-based system could engage employees and reinforce security practices.
- Consistent application of policies can be achieved through management and HR collaboration, emphasizing security in presentations and corporate meetings.
- Most common SE tactics in the enterprise are phishing attacks.

#105
- The effective methods to educate employees on SE tactics include formal training that highlights the types of attacks they encounter, with management playing a role in cautioning employees during team meetings and emails.
- They have implemented yearly refreshers on SE and other threats, introductory training, and internal phishing campaigns.
- Employee training resistance may be originated from skepticism, lack of communication about attacks, and security being considered secondary. To enhance participation and effectiveness, he suggests providing real-life examples and showcasing the impact of attacks.
- They promote a security culture through top and middle management feedback, communication in meetings, and board initiatives.
- Common SE tactics the enterprise has encountered include phishing emails, unauthorized building access, and phone calls.
- Factors influencing SE attacks include a sense of urgency, exploitation of willingness to help others, and establishing personal, friendly, trusting, and polite interactions.

#106
- Effective ways to educate employees on SE tactics include workshops tailored to different age groups, with older employees receiving more training sessions and younger employees requiring fewer sessions.
- Emphasizes having qualified personnel, up-to-date hardware, and addressing IoT security and suggests compensating employees for avoiding security incidents.
- To prevent cyberattacks they have implemented small training and regular reminders about phishing. Employees need access to specific data on the effectiveness of these programs or may cause disinterest in the security culture.
- Employee resistance to security awareness programs is attributed to age and workload.
- The enterprise promotes a security culture through training guidelines and email

reminders with deadlines.

- Security policies and practices can be managed through automated software systems, increased advertising, information sharing, and sensitization.
- Common SE tactics encountered by the organization include phishing emails and tailgating.
- Regarding individual factors influencing SE attacks, he believes that ignoring problems and a lack of proactive behavior are the contribution.

#107

- The best way to educate employees on SE tactics is through training. They have not implemented any training programs.
- Resistance to security awareness programs among employees may be due to the lack of appeal and the perception that security incidents only happen to others.
- Suggested that organizations should use language easily understandable by all participants.
- Common SE tactics the organization encounters include phone calls and phishing emails.
- To ensure the consistent application of security policies and practices, suggests implementing concrete rules and security systems on computers.
- Believes that a lack of knowledge plays a significant role in influencing the SE attacks.

#108

- The creation of awareness on SE tactics includes building awareness and conducting interactive virtual training, group discussions, and sharing sessions.
- They primarily use scenario-based presentations, such as phishing emails, to train employees on SE attacks.
- Resistance to security awareness programs among employees may be originated from language barriers.
- Organizations should consider using face-to-face or interactive virtual training that are engaging and applicable to employees' specific sectors or roles.
- They promote a security culture through training and management discussions.
- Mentions that organizations focused solely on delivering products or services may prioritize security less, leading to a weaker security culture.
- Deploying skilled employees in different regions and implementing assurance programs, internal or by third parties, can help assess compliance with policies and procedures.
- Common SE tactics encountered include mobile texting, phishing emails, and fake calls.
- Highlights awareness, knowledge, and a focused work vision as crucial factors

influencing SE attacks. Individuals who use social networks may be more vulnerable due to attackers exploiting their preferences and interests.

#109

- The most effective way to educate and create awareness on SE tactics is through training.
- Resistance to security awareness programs among employees, are related to the lack of knowledge and difficulties in understanding technology and security concepts. To improve training participation rates and effectiveness, she suggests sensitizing employees before and after the training sessions.
- To promote a security culture, they have implemented security protocols but need to be better understood and taken seriously by employees.
- Organizational factors that contribute to a better security culture include the literacy of employees, training programs, and tech literacy.
- Consistent application of security policies and practices throughout the organization would be achieved by evaluating risks.
- Suggests implementing employee training programs to improve enterprise resilience.

#110

- For employee's education, mentions regular training sessions, sending awareness emails, and offering instructional training on a quarterly or monthly basis. They have implemented various employee training programs, such as phishing awareness and training.
- These programs have effectively reduced the success rate of SE attacks by approximately 50-60%.
- Resistance to security awareness programs among employees, particularly non-IT employees, is attributed to a lack of knowledge and by considering it an unusual task.
- To improve training participation rates and effectiveness, suggests implementing mandatory training for employees, sending reminder emails, involving managers in monitoring attendance and taking appropriate actions.
- They promote a security culture through email communications, an education portal, and mandatory training for new employees.
- Regarding individual factors influencing SE attacks, mentions the importance of paying attention to emails, being cautious when sharing data, and complying to policies.

#111

- The most effective ways to educate employees on SE tactics include regular awareness sessions, simulated phishing tests, and case studies showcasing real life examples.

- They have implemented several programs such as phishing awareness training, SE simulations, and security awareness campaigns, being highly effective in reducing the success rate of such attacks.
- Resistance to security awareness programs among employees may come from a lack of perceived relevance, time constraints, and insufficient engagement from leadership.
- To improve training participation rates and effectiveness, suggests making training sessions interactive, tailoring content to different job roles, and providing incentives for participation.
- The company promotes a culture of security by regularly communicating security best practices, fostering a "security-first" mindset, and recognizing employees for security behaviors.
- For the application of security policies and practices, recommends conducting regular security audits, providing training, training reinforcements, and by establishing clear accountability for adherence to policies.
- Common SE tactics encountered include phishing emails, pretexting, and baiting through malicious attachments or USB drives.
- Individual factors that influence SE attacks include a lack of security awareness, human curiosity, and the tendency to trust others.
- Suggests ongoing security awareness training, emphasizing the importance of skepticism and verifying requests and promoting a culture of reporting of all suspicious activities, to improve SE resilience.

#112

- Effective ways to educate employees involve constant training in a fun and engaging manner. Suggests incorporating visual elements such as banners in the office and organizing activities throughout the year that employees can participate, believing that traditional training methods, such as lengthy videos may contribute to resistance.
- They have implemented mandatory phishing training and security awareness programs, which have effectively reduced the click rate on phishing emails and increased awareness among employees.
- To improve training participation rates and effectiveness, suggests creating benefits for employees and ensuring that the training is engaging and enjoyable.
- Emphasizes the importance of small exercises throughout the year to promote a security culture rather than relying solely on occasional management meetings.
- A promotion of a security culture could be more effective on a top-down approach, with the CEO leading and emphasizing the importance of security.
- Factors contributing to a better security culture include technological maturity, investment in security, and active engagement with employees.

- Security policies and practices can be ensured through security controls and periodic checks, and compliance with policies and practices can be measured using KPI's specific to each policy.
- The most common SE tactics encountered includes phishing, phone calls, and impersonation of users.
- Individual factors that influence these types of attacks include greed, fear, a sense of urgency, and the desire to please others.

#113

- They create awareness through face-to-face or online training with a "personal touch", emphasizing the importance of delivering training that captures employees' attention by making it more relatable/personal.
- They have implemented online training programs to prevent SE attacks, being quite effective in reducing the success rate of such attacks.
- Employee training resistance to security awareness programs may be due to competing priorities and work-related stress and suggests using HR sanctions to improve training participation rates and effectiveness.
- The security culture is achieved through training and communications, via email.
- Suggests using different controls and tests to ensure the consistent application of security policies and practices throughout the enterprise.
- Common SE tactics encountered are impersonation of internal employees, managers, or individuals associated with the enterprise and the tactics used include WhatsApp messages, email, and phone calls.
- Individual factors that influence SE attacks include training and awareness levels, naivety, fatigue, and lack of attention.

#114

- The promotion of awareness includes regular security awareness sessions, interactive workshops, and real case studies.
- Practical and engaging approaches are beneficial for understanding and recognizing SE tactics.
- They have implemented several employees training programs, including phishing campaigns, training, and continuous education on SE tactics, effectively reduced the success rate of SE attacks.
- Lack of time, perception that security prevents productivity, and inadequate communication are several of the reasons for employee training resistance to security awareness programs. To improve participation and effectiveness, suggests offering flexible training schedules, using gamification elements, and aligning security training with determined roles and responsibilities.
- They promote a culture of security among employees through regular communication of security policies and best practices, security-focused newsletters, and

	recognition for employees following security guidelines. • Strong security leadership, frequent audits, and a sense of shared responsibility for security, contribute to a better security culture. • Common SE tactics encountered include impersonation via email or phone, and texting to retrieve sensitive information. • Individual factors that influence SE attacks includes the lack of awareness, human trust, curiosity, and susceptibility to manipulation.
#115	• The way to educate employees are regular security talks, providing examples, and reminding employees to be cautious. Believes that raising awareness and vigilance is crucial in preventing SE attacks. • The main employee training programs implemented are security training and encouraging employees to report suspicious activities. These programs have increased awareness and vigilance among employees. • Employee training resistance may originate from the lack of time and the perception that security is someone else's responsibility, suggesting practical examples and involving employees in creating security policies to improve training participation rates and effectiveness. • Updated machines, as well as constant supervision, contribute to a better security culture. • Management should enforce the rules to ensure the consistent application of security policies and practices. • Common SE tactics encountered includes phishing emails and attempts to make purchases on behalf of others. • Individual factors that influence SE attacks includes trusting others too quickly.
#116	• To educate employees on SE tactics, they conduct workshops and regular training sessions, considering the constantly changing techniques. • They implement programs such as internal phishing campaigns and use tools like exchanges online and segregate its internal structure into multiple companies, which helps to contain any attacks and prevents hackers from reaching all areas. Different credentials are assigned to users to ensure the segregation of access to enterprise data. • Training programs have been around 80% successful in reducing the success rate of SE attacks. However, acknowledges that resistance to security awareness programs can exist due to mandatory training requirements and employees feeling overwhelmed with multiple training sessions each year. • To improve training participation rates and effectiveness, suggests the gamification of the training process, providing a sandbox for failed attempts, and

simulating potential causes of failure and consequences for the user.

- They promote a culture of security through color-coded banners in emails (internal vs. external).
- States that enterprises tend to act and implement security measures only after a breach or attack occurs.
- Consistent application of security policies and practices is ensured through a top-down application of global policies and standards, measured using KPI's of the enterprise's security status against specific standards.
- The most common SE tactic encountered is human-based SE, particularly phishing.
- Emphasizes that human factors play a significant role in SE attacks, with humans being the weakest link. Factors such as a sense of urgency and perceived risk are exploited, causing individuals to lower their defenses and react impulsively.
- To improve SE resilience, suggests providing exercises or training where employees feel a personal risk or threat to their lives, simulating real-life scenarios that exploit human characteristics and personal traits.

These key takeaways were extracted from the transcripts of each interview and represent the uniqueness and ideas expressed by each interviewee. Detailed information on each interviewee can be found on Table 11.

5.1.4 Data Saturation

In this research, a data saturation process was carried out to evaluate the status of the artifact (framework) and prepare it for the evaluation stage. Data saturation, a qualitative research methodology concept, aims to determine when further data collection and analysis are unnecessary based on the gathered and analyzed data [35]. Saturation becomes evident when newly obtained data becomes redundant compared to the existing data.

The decision to cease data collection is justified by the consistent observation of similar comments and a declining trend in the percentage of suggested changes by participants, indicating that data saturation has been achieved, being appropriate to conclude the data collection at this point and proceed to the evaluation phase [36].

Therefore, after conducting 16 interviews, the data collection phase was concluded to progress to the next step of the Design Science Research (DSR) process, which involves the evaluation process (Section 6 "Evaluation").

Table 13 *General overall unique contributions by interviewee*

Interview	Employee Training Programs and Security Culture	Resistance and Improvement Suggestions	Policy Compliance and Measurement	Factors Influencing Attacks and Resilience Enhancement
#101	3	1	1	3
#102	1	1	1	3
#103	1	1	1	2
#104	1	1	1	4
#105	0	1	1	1
#106	1	1	0	2
#107	0	1	0	0
#108	1	0	0	1
#109	0	0	0	0
#110	1	0	0	0
#111	0	1	0	1
#112	0	0	0	0
#113	0	1	0	2
#114	0	0	0	0
#115	0	0	0	0
#116	0	0	0	0

The count by each interviewee were structured according to the unique contributions provided by each interviewee on responding to the research topics proposed in this dissertation, mainly the RQ “To what extent do employee training, organizational culture, and individual susceptibility contribute to the mitigation of Social Engineering attacks, such as phishing, within enterprises?”.

The following figure illustrates the unique overall contribution of each interviewee, on the several research topics.

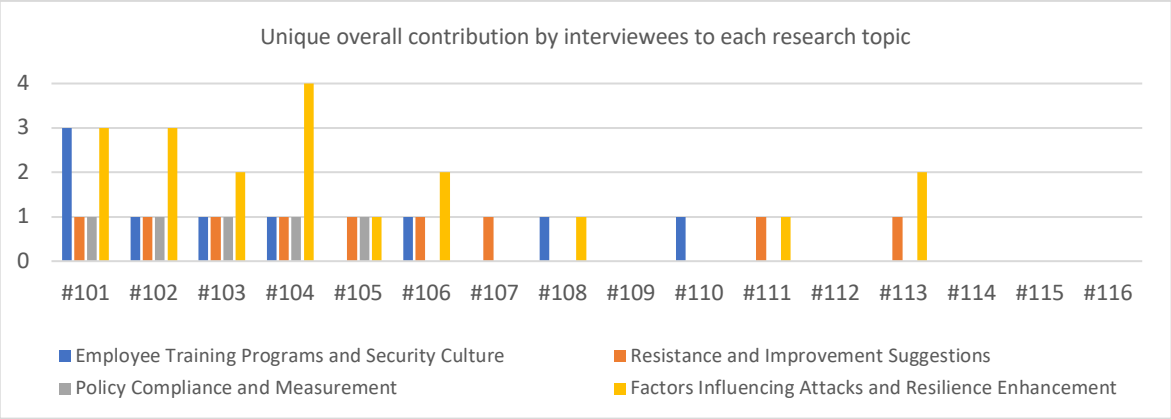

Figure 9 *Unique overall contribution by interviewees to each research topic*

Figure 9 maintains the same research structure topics as Table 13, highlighting the unique overall contribution by each interviewee on the several research topics.

6 DISCUSSION

This section presents the interview findings as proposed in Table 11 “Resumed interviewees characterization” to address the research questions and validate the proposed framework detailed in Section 4, "Proposal."

6.1 Evaluation Results

The conducted interviews allowed to gather more information and insights regarding the “missing holes” identified in the SLR phase that originated the 3 RQ of the SLR (Section 2.3.2). The following sections present the discussion according to each SLR RQ.

6.1.1 SLR RQ1

How do employee training programs impact the success rate of Social Engineering attacks such as phishing in enterprises?

The responses provide valuable insights into the impact of employee training programs on the success rate of SE attacks in enterprises, and strongly align with the proposed framework, emphasizing the importance of continuous training, awareness, and testing to educate employees on SE tactics.

One common and recurring theme in the interview responses is the significance of regular reminders. Interviewees highlighted the effectiveness of periodically reminding employees about the risks associated with SE attacks. Employees are reminded of the potential threats by incorporating regular reminders into training programs, being more likely to maintain vigilance and implement security measures daily.

Another critical aspect mentioned by the interviewees is the need for regular testing. By conducting simulated SE attacks such as internal phishing campaigns, enterprises can assess the effectiveness of their training programs and identify areas that require further improvement. Regular testing helps to reinforce the knowledge and skills acquired during training, ensuring that employees remain aware and capable of identifying and mitigating potential SE threats.

The interviewees also emphasized the importance of reinforcing information, including providing ongoing support and resources to employees to ensure that the knowledge acquired during training is continually reinforced. By providing accessible materials, such as well translated materials, technically suitable for the employee's levels or online resources, organizations can empower employees to refresh their knowledge of SE tactics and respond effectively to potential attacks.

Furthermore, the interviews responses highlighted the need for a culture of skepticism and critical thinking when handling suspicious emails, phone calls, or requests for sensitive information. This cautious behavior can significantly reduce the likelihood of falling victim to SE attacks.

While these practices align with the proposed framework and emphasize the importance of continuous training, awareness, and testing, it is worth mentioning that other security practices as using strong passwords, closing computers when not in use, and confirming requests through other means, can contribute to overall security but are not directly focused on educating employees about SE tactics. However, these practices can still be considered part of a broader security awareness program that complements the efforts to mitigate SE attacks.

6.1.2 SLR RQ2

How can companies or corporations create a culture of security to reduce the success rate of all types of Social Engineering attacks?

The responses obtained validates the strategies enterprises can implement to create a culture of security, and ultimately reducing the success rate of SE attacks.

One common theme in interviewee's responses is the emphasis on regular training, highlighting the importance of regular training sessions focused on SE tactics, and the need to keep employees informed about the latest security threats and trends. These insights align with the proposed framework's emphasis on conducting a baseline assessment and implementing tailored training programs. By regularly providing employees with up-to-date training, enterprises can nurture a culture of security

awareness and empower employees with the knowledge and skills necessary to identify and mitigate SE attacks.

Internal phishing campaigns and email alerts were also mentioned as effective practices. Interviewees acknowledged the value of phishing campaigns to test and enhance employees' ability to recognize and respond to internally simulated SE attacks. Sending “fake” phishing emails (internal phishing campaigns) helps to raise awareness, highlight vulnerabilities, and reinforce training efforts. Additionally, email alerts about security trends ensure that employees are kept informed about emerging threats, enabling them to stay vigilant and take proactive measures to protect sensitive information.

Initiatives like a “Cybersecurity Week” on a yearly basis can create a culture of security, highlighting the significance of organizing dedicated events that focus on educating employees about SE tactics, best practices, and the importance of maintaining strong security measures. These initiatives provide opportunities for in-depth discussions, knowledge sharing, and employee engagement, fostering a collective commitment to cybersecurity.

Regarding security culture, feedback from management and communication in team meetings are important to reinforce the importance of security measures, expectations, and encouraging the compliance to security measures and internal protocols. Regular meetings provide a means for discussing security concerns, sharing best practices, and addressing emerging issues. The establishment of a security committee and collaboration between departments to promote a culture of security is another way to involve stakeholders from different areas of the organization. This can create a collaborative and holistic approach to security, ensuring that security is prioritized at all levels, from top to bottom.

Creating an environment where employees feel comfortable reporting security incidents or suspicious activities is crucial for early detection and mitigation of SE attacks. Incentives, such as recognition or rewards, can further motivate employees to actively participate in reporting and contribute to the overall security posture of the enterprise.

Addressing emotional biases is another crucial aspect highlighted in the interview responses. Using educational materials and persuasive communication techniques, such as storytelling, can appeal to employees' emotions and increase their understanding of the impact of SE attacks. Positive reinforcement and gamification to engage employees and nurture a sense of achievement and personal responsibility in maintaining security practices are also good strategies that align with the proposed framework's approach of increasing understanding, providing examples, and using positive reinforcement to mitigate emotional biases.

Regarding continuous evaluation, the usage of metrics to measure the effectiveness of security initiatives and conducting regular reviews are good ways to monitor the effectiveness of training programs, internal phishing campaigns, and other security awareness efforts allows enterprises to identify areas for improvement and adapt their strategies accordingly. These facts highlight the importance of developing metrics and making necessary adjustments based on the evolving threat landscape, further highlighting the value of continuous evaluation as basilar part of creating an overall security culture.

Furthermore, a streamlined and user-friendly reporting system encourages employees to report suspicious activities promptly, facilitating a swiftly response to potential SE attacks. Establishing a process for triaging and responding to reported incidents, ensuring that reported incidents are addressed effectively , allows these responses to align with the framework's focus on establishing reporting mechanisms and providing employee’s feedback.

6.1.3 SLR RQ 3

What factors make businesses employees more susceptible to Social Engineering tactics?

The interviews provided valuable insights into the factors that make employees more susceptible to SE tactics. The SE tactics mentioned by the interviewees, including phishing emails, impersonation, smishing, vishing, tailgating, pretexting, baiting, malicious attachments, or USB drives, were consistent with those

considered in the proposed framework. This alignment validates the framework's relevance in addressing common SE tactics and their impact on employees.

The interview responses clarified several factors contributing to susceptibility to SE attacks. One key factor identified is a need for more attention and awareness. Interviewees highlighted how personal and professional distractions could compromise an employee's ability to evaluate suspicious communications or requests with a critically mindset, reinforcing the importance of user awareness and training initiatives that educate employees about the several SE techniques, providing guidance on how to remain vigilant while facing potential real attacks.

Personal vulnerabilities, such as fear and greed, were also identified as factors that make individuals more susceptible to SE tactics. They confirmed that social engineers often exploit these emotions and personal traits to manipulate employees into divulging sensitive information or performing unauthorized actions. Addressing these emotional biases becomes crucial in developing effective countermeasures. The proposed framework recognizes the significance of addressing emotional biases by suggesting strategies such as providing examples and using positive reinforcement to promote critical thinking and reduce the influence of these biases.

The willingness to help others was another factor mentioned in the interviews. Social engineers often exploit the inherent good faith of employees by posing as someone in need or in a position of authority like a hierarchical superior, leveraging their trust to gain access to sensitive information or resources. Educating employees about the potential risks associated with blindly complying with such requests is essential in mitigating the success of SE attacks. By promoting critical thinking and verification, enterprises can empower individuals to question and validate requests before taking any action.

Ignorance and human trust were additional factors identified in the interviews, acknowledging that employees may be unaware of the various tactics used in SE attacks and may place excessive trust in digital communications or seemingly legitimate sources. Training and awareness programs can significantly address these factors by equipping employees with knowledge about used SE tactics and teaching

them to adopt caution and a critical mindset when interacting with unfamiliar or potentially risky situations.

The interviewees provided a diverse range of suggestions to improve SE resilience, and these suggestions align with the components of the proposed framework, reinforcing awareness through ongoing training and face-to-face awareness sessions was a commonly mentioned strategy. By continually updating and reinforcing employee's knowledge of SE tactics and evolving threats, enterprises can enhance their resistance to attackers' manipulation.

Performing audits and training exercises using real examples was another recommendation proposed. By simulating real-life SE scenarios, enterprises can assess employee's responses, identify vulnerabilities, and tailor training programs accordingly. This hands-on approach can significantly enhance understanding of SE tactics and the ability to detect and respond appropriately.

The involvement of all stakeholders was stated as a critical factor in improving SE resilience. By engaging employees, management, and relevant departments, organizations can share responsibility for security and establish a collective defense against SE attacks. This collaborative approach aligns with the framework's emphasis on creating a security culture that permeates throughout the organization, from top to bottom.

Implementing policies and controls, using gamification, reducing workloads to alleviate stress, providing easily understandable information, conducting ongoing security awareness training, promoting skepticism and verification, and fostering a culture of reporting and sharing real-life examples were among the other suggestions provided by the interviewees. These recommendations converge with the framework's components, further validating its effectiveness in addressing the factors that make individuals more susceptible to SE tactics.

6.2 Validated Artifact

If the previous discussion of three RQ questions used in the SLR, in Section 6, can provide valuable insights that were identified and missing in the SLR phase, this

section takes those insights into account to respond to the RQ of this dissertation, and how, furthermore, the interviews responses performed in the DSR phase, strongly support, and validate the proposed framework.

6.2.1 Dissertation RQ

To what extent do employee training, organizational culture, and individual susceptibility contribute to the mitigation of Social Engineering attacks, such as phishing, within enterprises?

Interviewees emphasized the importance of regularly conducting training sessions to ensure employees remain aware of the risks associated with SE attacks, aligning with the proposed framework's emphasis on the key factor of continuous employee's training and awareness.

Simulated attacks, such as internal phishing campaigns, were also highlighted as effective measures to educate employees and test their ability to recognize and respond to SE tactics. Interviewees acknowledged the value of these exercises in raising awareness, identifying vulnerabilities, and reinforcing the knowledge and skills acquired during the several training iterations.

In addition to training and simulated attacks, awareness sessions were considered valuable components of an effective and proper employee education program. These training sessions provide opportunities for employees to learn about the latest SE techniques and understand the potential impact of falling victim to such attacks.

Real-life examples were also emphasized as practical tools to educate employees about SE tactics. Sharing stories and case studies of actual real incidents helps employees understand the tactics used by attackers and the consequences of their actions. This firsthand knowledge enables employees to recognize and respond appropriately to similar situations.

To further enhance the effectiveness of training programs, interviewees suggested using interactive and engaging methods. Gamification, for example, can make training sessions more enjoyable and increase employee participation rates. By incorporating elements of competition, rewards, and challenges, enterprises can

motivate employees to engage in training and retain knowledge more effectively and actively.

The interview responses also validated the importance of relevant and well translated training materials. It was emphasized that training programs should be tailored to the employee's technical level and cultural context. Providing materials that are easily understandable and accessible to all employees ensures that the training is practical and inclusive.

Furthermore, these remarks provided by the interviewees align with the proposed framework's components, reinforcing its effectiveness in addressing SE attacks. The interviewees mentioned the importance of creating a security culture within the enterprise, addressing emotional biases, continuously evaluating the training program's effectiveness, and empowering employees to report suspicious activities as vital strategies to mitigate the success rate of SE attacks.

The data gathered from the interviews strongly supported the proposed framework for mitigating SE attacks. By implementing regular training, internal simulated attacks (like phishing campaigns), awareness sessions, and using real-life examples, enterprises can effectively educate employees and reduce the success rate of these types of attacks. The proposed suggestions stated by the interviewees, such as relevant and well-translated training materials, gamification, and interactive methods of education, offer valuable guidance for enterprises searching to enhance their training programs and create a culture of security. By aligning with the proposed framework and incorporating these strategies, enterprises can improve their security posture and better protect against SE attacks.

7 CONCLUSION

This section concludes the dissertation research done with communication, research conclusions, limitations, and future work.

7.1 Communication

The SLR conducted in this research *("Improving Social Engineering Resilience In Enterprises: A Systematic Literature Review"*) has been submitted to the *ARIS2 - Advanced Research on Information Systems Security* journal on April 2, 2023 and accepted in May 3, 2023 by the editors, being in the phase of Copyediting for future publication. Also, a full paper will be prepared for submission on conference, describing the work in this dissertation. Finally, this dissertation is also part of the communication step of DSR.

7.2 Research Conclusions

The research conducted through the SLR, DSR and interviews, provided valuable insights regarding the effectiveness of employee training and awareness programs, to create a security culture and mitigate SE attacks in enterprises. Combining the findings from both methodologies enabled to draw a comprehensive verified conclusions that can guide enterprises in strengthening their cybersecurity posture to external threats. It is now possible to have a better understanding on the importance of the RQ proposed in this research and make some notations regarding its answers.

The SLR highlights the significance of educating employees through regular and tailored training awareness programs to reduce the probability of successful SE attacks. Employees cybersecurity knowledge significantly impact their intentions to comply with cybersecurity controls. Therefore, continuous training initiatives that address specific SE tactics are essential to equip employees with the necessary knowledge and skills to identify and respond effectively on facing potential threats. The interviews further emphasize the importance of periodic reminders and regular testing to reinforce employee knowledge and maintain vigilance and awareness against SE attacks. Continuous ongoing support and accessible resources, such as

well-translated and online training materials, are also fundamental in ensuring that the knowledge acquired during the training sessions are continually reinforced.

Creating a security culture within an enterprise involves all stakeholders, from employees to management. The SLR suggests that open and honest communication from management can increase trust and promote a security mindset among employees. A collaborative approach to security involving all departments and stakeholders can promote a collective cyber defense against SE attacks. Furthermore, regular team meetings can provide a platform for discussing security concerns, sharing best practices, and addressing emerging issues. The interviews further validate the importance of a security culture to promote cybersecurity. A "Cybersecurity Week" dedicated on educating and creating awareness on employees about SE tactics and best practices exemplifies how specific events can reinforce the security culture in enterprises. Additionally, establishing a security team that collaborates with all departments further emphasizes the role of employee engagement in an enterprise's security posture.

Although employee training is critical, integrating technical solutions enhances an enterprise's security posture. Implementing technical controls such as Multi-Factor Authentication (MFA), encryption, and advanced intrusion detection systems can prove to be effective tools against numerous SE tactics. However, the SLR points out the potential risk of over-reliance on technology that could potentially lead to employee complacency. Therefore, it is essential to balance technical measures and human awareness, with employees acting as the first defense line against SE attacks.

Emotional biases such as fear, trust, curiosity, and a willingness to help others are key factors that make employees more susceptible to SE attacks. Threat actors often exploit these emotions and personal traits to manipulate them into divulging sensitive information or performing unauthorized actions. The proposed framework addresses these emotional biases by recommending strategies such as providing real-life examples and using positive reinforcement to promote critical thinking and reduce the influence of these human biases. By educating employees on SE tactics and risks, enterprises can empower employees to question and validate requests

before acting by without increasing their cognitive effort, create muscular plasticity, as mentioned by Wolpaw [37] “the entire function of the nervous system is to ensure that sensory input (experience) leads to appropriate motor output (behavior)”, pp.256.

Both the SLR and DSR, including the interviews, highlight the significance of continuous evaluation and enhancement of the enterprise's SE resilience. Monitoring the effectiveness of training programs and awareness initiatives, internal phishing campaigns, and other security awareness efforts allows enterprises to identify areas for improvement and adapt their strategies and resources accordingly. Implementing employee-friendly reporting mechanisms and incident response processes as well as using metrics and KPI’s to measure the effectiveness of security initiatives and conducting regular reviews allows enterprises to stay ahead of emerging threats.

Engaging employees, management, and key departments in the security process nurtures a collective defense, collaboration, and shared responsibility for security, resulting on a security culture that permeates the enterprise from top to bottom. Rewarding positive behaviors and providing incentives for reporting security incidents encourages active employee participation in security, that combined with process for triaging and responding to reported incidents ensures that potential threats are addressed in an effective manner.

There is present an emphasis on the importance of educating employees about proeminent SE tactics and their impact not only on the enterprise, but also on a personal level. By providing real-life examples, simulations, and ongoing security awareness training, employees can better recognize and respond appropriately to these attacks. The proposed framework's approach of using educational materials, persuasive communication techniques, and gamification aligns with the interviewees suggestions for appealing to employees’ emotions and promoting understanding of the real impact of SE attacks.

With both methodologies we can now have more enlightenment on the RQ covered in this dissertation. Regarding on how managers can mitigate the risk of employees

suffering targeted SE attacks, managers can mitigate the risk of employees suffering targeted SE attacks by implementing a multi layered approach, including regular and tailored employee training, periodic reminders and testing to reinforce knowledge, fostering a security culture through open communication and collaboration, and balancing technological measures with human vigilance. By combining these strategies, managers can empower employees to recognize and respond effectively to SE attacks, reducing the likelihood of successful attacks.

According to the observed results of this research, user training awareness effectively reduces the success rate of SE attacks. The root causes for employee traction to training (that is not the reality in most of the interviews) include using real-life examples and simulations, ongoing security awareness, persuasive communication techniques, and the incorporation of gamification elements. These factors enhance employee engagement and understanding, making the training more impactful in equipping employees to defend against SE attacks.

On what human behavior or personality traits can be identified that are more susceptible to these attacks, we can conclude that human behavior and personality traits that make individuals more susceptible to SE attacks include fear, trust, curiosity, and a willingness to help others. Threat actors exploit these emotions and traits to manipulate employees into divulging sensitive information or performing unauthorized activities. To mitigate vulnerabilities, training programs can provide examples and use positive reinforcement to promote critical thinking and to question and validate requests before acting.

It is now clear that enterprises can improve the overall cybersecurity culture by promoting a collective defense against SE attacks. This involves nurturing a security culture through open and honest communication from management, which increases trust and promotes a security mindset among employees. Regular team meetings and dedicated events can reinforce the importance of security and create a collaborative approach involving various departments and stakeholders. Incentives for reporting security incidents and establishing a process for incident response also contribute to a positive security culture.

By combining employee training and awareness programs while establishing a security culture, integrating technological solutions, and promoting collaboration and critical thinking, enterprises can significantly reduce their susceptibility to SE threats. By progressively and constantly evaluating and adapting their strategies, enterprises can become proactive against emerging threats. Educating employees about SE tactics and addressing emotional biases play central roles in strengthening the human element of cybersecurity. With a collective commitment to cybersecurity and a culture of vigilance, enterprises can significantly increase their overall security posture and protect against the ever-evolving SE attacks.

7.3 Limitations

This research employed semi-structured interviews, compelling to a diverse and ample sample size to ensure both precision and a comprehensive range of opinions. A total of 16 interviews were conducted, enabling a more thorough exploration of the subject matter.

One limitation worth noting is that, even though some non-English publications were used in this research, the focus on English-only publications could inadvertently overlook valuable insights and perspectives from other linguistic sources.

Finally, regarding the SLR, common search methods relying solely on search terms and search engines can lead to insufficient materials. To mitigate this, formal searches were performed, with specific keywords to improve the reliability and replication this research in the future.
Furthermore, the data analyzed in the selected papers were sourced from a single database (EBSCO) and collected at a single time, which limits the ability to establish causality and may bias the sample towards the paper submission acceptance terms of the EBSCO database. Future work can expand the SLR to other relevant scientific databases and on different time periods.
It is also recognized the difficulty in effectively measuring personality traits and human behavior, even in a corporate environment, to measure the overall complexity of cybersecurity applied to a human conditional factor.

Additional work is needed to evaluate the effectiveness of different training programs and explore new strategies, such as immersive simulations or gamification, explore the effectiveness of different defense mechanisms, examine how attackers choose their targets to better protect organizations from SE attacks and explore the effectiveness of different communication strategies, and the role of employee engagement in an enterprise's security posture.

7.4 Future Work

The cybersecurity landscape is constantly evolving. Threat actors rely increasingly on new technologies, tools, and techniques that allow a better success rate in their efforts. Some of the SE attack attempts through phishing are now using massive, automated email campaigns, more and more sophisticated to pass undetected into users' email inboxes. Future research can focus on how emerging tools like Artificial Intelligence (AI) can help mitigate and further automate the detection rates of those phishing attacks.

Since phishing is one of the most common SE attacks in enterprises, it would be interesting to investigate further the process and success rate of spear phishing versus phishing. This topic was out of the scope of this research, but that could be leveraged in future work better to understand the implications on both enterprise and personal levels.

Future researchers are also encouraged to consider longitudinal studies to evaluate the effectiveness of different training and education programs applied to different human traits and characteristics, to enhance employees' overall security awareness and improve enterprise cybersecurity.

7.5 Conflicts of Interest

The author declares that there are no conflicts of interest regarding the publication of this dissertation.

8 BIBLIOGRAPHY

[1] Microsoft, “Phishing trends and techniques.” Accessed: Aug. 10, 2023. [Online]. Available: https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/phishing-trends?view=o365-worldwide

[2] M. Carlton and Y. Levy, “Cybersecurity skills: Foundational theory and the cornerstone of advanced persistent threats (APTs) mitigation.,” *Online Journal of Applied Knowledge Management*, vol. 5, no. 2, pp. 16–28, 2017, Accessed: Aug. 10, 2023. [Online]. Available: https://www.researchgate.net/publication/318276855_Cybersecurity_skills_Foundational_theory_and_the_cornerstone_of_advanced_persistent_threats_APTs_mitigation

[3] K. Chetioui, B. Bah, A. O. Alami, and A. Bahnasse, “Overview of Social Engineering Attacks on Social Networks.,” *Procedia Comput Sci*, vol. 198, no. 1, pp. 656–661, 2022, Accessed: Aug. 10, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050921025412?via%3Dihub

[4] M. de Oliveira Fornasier, N. M. Paiva Knebel, and F. V. da Silva, “PHISHING E ENGENHARIA SOCIAL: ENTRE A CRIMINALIZAÇÃO E A UTILIZAÇÃO DE MEIOS SOCIAIS DE PROTEÇÃO.,” *Meritum: Revista de Direito da Universidadee FUMEC*, vol. 15, no. 1, pp. 147–165, 2020, Accessed: Aug. 10, 2023. [Online]. Available: http://revista.fumec.br/index.php/meritum/article/view/7771

[5] A. Ferreira and S. Teles, “Persuasion: How phishing emails can influence users and bypass security measures.,” *Int J Hum Comput Stud*, vol. 125, pp. 19–31, 2019, Accessed: Aug. 10, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1071581918306827

[6] M. Frank, L. Jaeger, and L. M. Ranft, “Contextual drivers of employees’ phishing susceptibility: Insights from a field study.,” *Decis Support Syst*, no. Preprints, 2022, Accessed: Aug. 10, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0167923622000896

[7] T. Grassegger and D. Nedbal, “The Role of Employees’ Information Security Awareness on the Intention to Resist Social Engineering.,” *Procedia Comput Sci*, vol. 181, no. 1, pp. 59–66, 2021, Accessed: Aug. 10, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050921001381

[8] W. Jingguo, L. Yuan, and H. R. Rao, “Overconfidence in Phishing Email Detection.,” *J Assoc Inf Syst*, vol. 17, no. 11, pp. 759–783, 2016, Accessed: Aug. 10, 2023. [Online]. Available: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1757&context=jais

[9] I. , Lim, Y.-G. , Park, and J.-K. Lee, “Design of Security Training System for Individual Users,” *Wirel Pers Commun*, vol. 90(3), pp. 1105–1120, 2016.

[10] M. J. A. Miranda, “Enhancing Cybersecurity Awareness Training: A Comprehensive Phishing Exercise Approach.,” *International Management Review*, vol. 14, no. 2, pp. 5–10, 2018, Accessed: Aug. 10, 2023. [Online]. Available: http://www.imrjournal.org/uploads/1/4/2/8/14286482/imr-v14n2art1.pdf

[11] G. D. Moody, D. F. Galletta, and B. K. Dunn, “Which phish get caught? An exploratory study of individuals′ susceptibility to phishing.,” *European Journal of Information Systems*, vol. 26, no. 6, pp. 564–584, 2017, Accessed: Aug. 10, 2023. [Online]. Available: https://link.springer.com/content/pdf/10.1057/s41303-017-0058-x.pdf

[12] A. , Șandor, G. Tont, and E. Simion, “A Mathematical Model for Risk Assessment of Social Engineering Attacks,” *TEM Journal*, vol. 11(1), pp. 334–338, 2022, Accessed: Aug. 10, 2023. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4180646

[13] S. Sankhwar, D. Pandey, R. A. Khan, and S. N. Mohanty, “An anti-phishing enterprise environ model using feed-forward backpropagation and Levenberg-Marquardt method.,” *Security and Privacy*, vol. 4, no. 1, 2021, Accessed: Aug. 10, 2023. [Online]. Available: https://www.researchgate.net/publication/344308446_An_anti-phishing_enterprise_environ_model_using_feed-forward_backpropagation_and_Levenberg-Marquardt_method

[14] N. Sebescen and J. Vitak, “Securing the human: Employee security vulnerability risk in organizational settings.,” *J Assoc Inf Sci Technol*, vol. 68, no. 9,

pp. 2237–2247, 2017, Accessed: Aug. 10, 2023. [Online]. Available: https://asistdl.onlinelibrary.wiley.com/doi/abs/10.1002/asi.23851

[15] R. Torten, C. Reaiche, and S. Boyle, “The impact of security awarness on information technology professionals’ behavior.,” *Comput Secur*, vol. 79, no. 1, pp. 68–79, 2018, Accessed: Aug. 10, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404818304656

[16] C. C. Trumbach, D. M. Payne, and K. Walsh, “Cybersecurity in business education: The ‘how to’ in incorporating education into practice.,” *Industry and Higher Education*, no. Preprints, 2022, Accessed: Aug. 10, 2023. [Online]. Available: https://journals.sagepub.com/doi/abs/10.1177/09504222221099389?journalCode=ihea

[17] M. Workman, “Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security.,” *Journal of the American Society for Information Science and Technology*, vol. 59, no. 4, pp. 662–674, 2008, Accessed: Aug. 10, 2023. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/asi.20779

[18] A. Yasin, R. Fatima, L. Liu, J. Wang, R. Ali, and Z. Wei, “Understanding and deciphering of social engineering attack scenarios.,” *Security and Privacy*, vol. 4, no. 4, 2021, Accessed: Aug. 10, 2023. [Online]. Available: https://www.researchgate.net/publication/350387721_Understanding_and_deciphering_of_social_engineering_attack_scenarios

[19] Т. Т. В., “Психологические аспекты информационной безопасности организации в контексте социоинженерных атак.,” *Administrative Consulting*, vol. 157, no. 2, pp. 123–138, 2022, Accessed: Aug. 10, 2023. [Online]. Available: https://www.acjournal.ru/jour/article/view/1893/0

[20] N. Klimburg-Witjes and A. Wentland, “Hacking Humans? Social Engineering and the Construction of the ‘Deficient User’ in Cybersecurity Discourses.,” *Sci Technol Human Values*, vol. 46, no. 6, pp. 1316–1339, 2021, Accessed: Aug. 10, 2023. [Online]. Available: https://www.researchgate.net/publication/348574895_Hacking_Humans_Social_Engineering_and_the_Construction_of_the_Deficient_User_in_Cybersecurity_Discourses

[21] I. Qabajeh, F. Thabtah, and F. Chiclana, “A recent review of conventional vs. automated cybersecurity anti-phishing techniques.,” *Comput Sci Rev*, vol. 29, no. 1, pp. 44–55, 2018, Accessed: Aug. 10, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1574013717302010

[22] IBM, “Threat Intelligence Index 2023,” *IBM Security X-Force* , 2023, Accessed: Aug. 10, 2023. [Online]. Available: https://www.ibm.com/reports/threat-intelligence

[23] HP, “HP Wolf Security.” Accessed: Aug. 10, 2023. [Online]. Available: https://www.hp.com/us-en/security/endpoint-security-solutions.html

[24] M. A. Siddiqi and W. Pak, “A study on the psychology of Social Engineering-based cyberattacks and existing countermeasures,” *Applied Sciences*, vol. 12(12), p. 6042, 2022, Accessed: Aug. 10, 2023. [Online]. Available: https://www.mdpi.com/2076-3417/12/12/6042

[25] W. Syafitri, Z. Shukur, U. Asma’Mokhtar, R. Sulaiman, and M. A. Ibrahim, “Social Engineering attacks prevention: A systematic literature review,” *IEEE Access*, vol. 10, pp. 39325–39343, 2022, Accessed: Aug. 10, 2023. [Online]. Available: https://ieeexplore.ieee.org/iel7/6287639/6514899/09743471.pdf

[26] H. Finch, A. Abasi-Amefon, J. Woosub, L. Potter, and X.-L. Palmer, “Commentary on Healthcare and Disruptive Innovation,” *International Conference on Cyber Warfare and Security*, p. 77, 2023.

[27] N. Krithika, “A study on wha (watering hole attack)–the most dangerous threat to the organization,” *Int. J. Innov. Sci. Eng. Res.(IJISER)*, vol. 4, pp. 196–198, 2017, Accessed: Aug. 10, 2023. [Online]. Available: http://www.ijiser.com/paper/2017/vol4issue8/Aug2017p101.1.pdf

[28] B. Kitchenham, “Procedures for performing systematic reviews,” *Keele, UK, Keele University*, vol. 33.2004, pp. 1–26, 2004, Accessed: Sep. 24, 2023. [Online]. Available: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=29890a936639862f45cb9a987dd599dce9759bf5

[29] B. Kitchenham, “Guidelines for performing Systematic Literature Reviews in Software Engineering,” *EBSE Technical Report*, vol. 33, no. 5, 2007, Accessed: Sep. 25, 2023. [Online]. Available:

https://www.researchgate.net/publication/258968007_Kitchenham_B_Guidelines_for_performing_Systematic_Literature_Reviews_in_software_engineering_EBSE_Technical_Report_EBSE-2007-01

[30] Ken Peffers, Tuure Tuunanen, Marcus A. Rothenberger, and Samir Chatterjee, “A Design Science Research Methodology for Information Systems Research,” *Journal of Management Information Systems*, pp. 45–77, 2007, Accessed: Aug. 10, 2023. [Online]. Available: https://www.researchgate.net/publication/284503626_A_design_science_research_methodology_for_information_systems_research/link/616fed20766c4a211cfb5b47/download

[31] R. S. Alsawaier, “The effect of gamification on motivation and engagement,” *The International Journal of Information and Learning Technology* , vol. 35.1 (2018), pp. 56–79, 2018, Accessed: Aug. 10, 2023. [Online]. Available: https://rex.libraries.wsu.edu/view/pdfCoverPage?instCode=01ALLIANCE_WSU&filePid=13350057080001842&download=true

[32] D. Cohen and B. Crabtree, “Semi-structured Interviews,” 2006, Accessed: Aug. 10, 2023. [Online]. Available: http: //www.qualres.org/HomeSemi-3629.html

[33] Sharon M. Ravitch and Matthew Riggan, *Reason & Rigor: How Conceptual Frameworks Guide Research*, 2nd Edition., vol. ISBN: 9781483340401. Thousand Oaks, CA.: SAGE Publications, Inc., 2017.

[34] K. Raworth, C. Sweetman, S. Narayan, J. Rowlands, and A. Hopkins, “Conducting semi-structured Interviews,” *Oxfam*, 2012, Accessed: Aug. 10, 2023. [Online]. Available: https://books.google.com/books/about/Conducting_Semi_structured_Interviews.html?id=-dHtAQAAQBAJ

[35] B. Saunders *et al.*, “Saturation in qualitative research: exploring its conceptualization and operationalization,” *Qual Quant*, vol. 52, no. 4, pp. 1893–1907, Jul. 2018, Accessed: Aug. 10, 2023. [Online]. Available: https://link.springer.com/article/10.1007/s11135-017-0574-8

[36] M. P. Grady, “Qualitative and action research: A practitioner handbook,” *Phi Delta Kappa International*, 1998, Accessed: Aug. 10, 2023. [Online]. Available: https://books.google.com/books?hl=pt-PT&lr=&id=JOr3-A3-LbwC&oi=fnd&pg=PA1&dq=%5B32%5D.%09M.+P.+Grady,+%E2%80%9C

Qualitative+and+action+research:+A+practitioner+handbook%E2%80%9D.&ots=hC-NVcoEQ4&sig=ythTRSi_ZbSot3r8EFh7U00jxg

[37] J. R. Wolpaw and Jonathan S. Carp, “Plasticity from muscle to brain,” *Progress in neurobiology* , vol. 78.3–5, pp. 233–263, 2006, Accessed: Aug. 10, 2023. [Online]. Available: https://www.neurotechcenter.org/sites/default/files/misc/Plasticity%20from%20muscle%20to%20brain.pdf

Appendix A: Interview Outline

The following details the interview outline performed. It is based on the type of questions, correspondent relevance to the study, research questions addressed in the SLR and the correspondent questions. By leveraging the responses to these questions, the objective of this interview outline is to respond to this dissertation RQ: To what extent do employee training, organizational culture, and individual susceptibility contribute to the mitigation of Social Engineering attacks, such as phishing, within enterprises?

Type	Relevance	Research Question	ID	Question
Closed	Background		Q001	In what sector does your organization operate?
			Q002	How long do you work in your current organization?
			Q003	What is your current position?
			Q004	How many years of experience do you have in the field of information security, if any?
			Q005	How familiar are you with Social Engineering attacks?
			Q006	Have you received any formal training in Social Engineering?
Open	RQ (DSR RQ1)	How do employee training programs impact the success rate of social engineering attacks in enterprises?	Q007	In your opinion, what are the most effective ways to educate employees on Social Engineering tactics?
			Q008	What are the main employee training programs your organization has implemented to prevent Social Engineering attacks?
			Q009	Follow-up: How effective have these programs been in reducing the success rate of Social Engineering attacks?
			Q010	If existent, what do you think are the underlying factors contributing to employee training resistance to security

				awareness programs?
			Q011	Follow-up: And how do you think organizations can improve training participation rates and effectiveness?
Open	RQ (DSR RQ2)	How can enterprises create a culture of security to reduce the success rate of social engineering attacks?	Q012	How does your organization promote a culture of security among employees?
			Q013	Follow-up: What organizational factors in your current company or the company you worked for before do you think contribute to a better or worse security culture?
			Q014	How would you ensure that security policies and practices are consistently applied throughout the organization?
			Q015	Follow-up: What methods would you use to measure compliance with these policies and practices?
Open	RQ (DSR RQ3)	What factors make individuals more susceptible to social engineering tactics?	Q016	What common Social Engineering tactics has your organization encountered?
			Q017	Either by an internal simulation or a real external threat, did you ever fall for any Social Engineering attack?
			Q018	Follow-up: If yes, what factors do you think were the cause?
			Q019	In opposition to organizational factors, what individual factors do you believe influence Social Engineering attacks?
			Q020	Follow-up: According to those individual factors, how would you improve Social Engineering resilience in your organization?

The following questionnaire analysis vector represents the relevance, utility, usage, and improvements that are relevant to the questionnaire used in this research.

Appendix B: Questionnaire analysis vector

ID	RQ	Relevance	Utility	Completeness	Usage	Improvements
Q001	Background	Medium	High	-	High	-
Q002	Background	Medium	High	-	High	-
Q003	Background	Medium	High	-	High	-
Q004	Background	Medium	High	-	High	-
Q005	Background	High	High	High	High	-
Q006	Background	High	High	High	High	-
Q007	RQ (DSR RQ1)	High	High	High	High	-
Q008	RQ (DSR RQ1)	High	High	High	High	-
Q009	RQ (DSR RQ1)	High	High	High	High	-
Q010	RQ (DSR RQ1)	High	High	High	High	-
Q011	RQ (DSR RQ1)	High	High	High	High	-
Q012	RQ (DSR RQ2)	High	High	High	High	-
Q013	RQ (DSR RQ2)	High	High	High	High	-
Q014	RQ (DSR RQ2)	High	High	High	High	-
Q015	RQ (DSR RQ2)	High	High	High	High	-
Q016	RQ (DSR RQ3)	High	High	High	High	-
Q017	RQ (DSR RQ3)	High	High	High	High	-
Q018	RQ (DSR RQ3)	High	High	High	High	-
Q019	RQ (DSR RQ3)	High	High	High	High	-
Q020	RQ (DSR RQ3)	High	High	High	High	-

The questionnaire analysis vector is based on the relevance, utility, completeness, usage, and improvements of each question, as follows.

- **Relevance:** The degree to which the interview question is related to the research questions and the study's overall goal.
- **Utility:** The extent to which the interview question helps address the research questions and generate data that can validate the artifact of the DSR.

- **Completeness:** The degree to which the interview question covers all relevant aspects of the research question and provides a comprehensive understanding of the topic.
- **Usage:** The extent to which the interview question is practical and feasible for use in the research study, including considerations such as time, resources, and access to participants.
- **Improvements:** Opportunities for improving the interview question to better align with the research questions and improve the quality of data generated.