Advanced Research on Information Systems Security

ARIS²
an international journal

ISSN: 2795-4609 | ISSN: 2795-4560
Print & Online

Improving Social Engineering Resilience in Enterprises

Ricardo Alexandre Bentes Ribeiro[a,a1*], Nuno Mateus-Coelho[c,d], Henrique São Mamede[b,a]

[*a]*Universidade Aberta, Lisbon, Portugal*

[a1]*Email: ricardo.intel@outlook.com*

[b]*INESC TEC, Porto, Portugal*

[c]*Universidade Lusófona, Porto, Portugal*

[d]*LAPI2S – Laboratory of Privacy and Information Systems Security, Porto, Portugal*

Abstract

Social Engineering pose 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 paper 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 an 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 vital roles, leveraging this way a theoretical and practical understanding 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. Therefore, it 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 subject. 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.*

Citation: Ribeiro, R., N. Mateus-Coelho, and H. Mamede. "Improving Social Engineering Resilience In Enterprises". ARIS2 - Advanced Research on Information Systems Security, vol. 3, no. 1, Aug. 2023, pp. 34-65, doi:10.56394/aris2.v3i1.30.

---

* Corresponding author. Email address: ricardo.intel@outlook.com

1. Introduction

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 cybersecurity and develop a framework for enterprises to implement and reduce the risk of successful SE attacks.

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 predetermine 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 [40]. 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.

In this context, this research aims to answer to the following question: To what extent do employee training, organizational culture, and individual susceptibility contribute to the mitigation of Social Engineering attacks, such as phishing, within organizations?

This article if organized as follows: section 1, this one, presents the context and the research problem; section 2 presents the theoretical background on what is SE, the SLR process, planning, conducting the review and reporting and discussing the findings for each proposed RQ; section 3 presents the research methodology; section 4 presents the design and development, where the framework (artefact) is proposed; section 5 presents the demonstration of the proposal; section 6 presents the evaluation of the artefact, detailing the semi-structured interviews process; section 7 presents the evaluation results; section 8 presents the conclusion of this research; section 9 presents the bibliography used to support this research.

2. Theoretical Background

The focus research objectives of this paper 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], [41], [42], [43], 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. In Table 1, are presented the most common type of SE attacks [25].

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 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. Systematic Literature Review

On a 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 and proposed 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.

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).

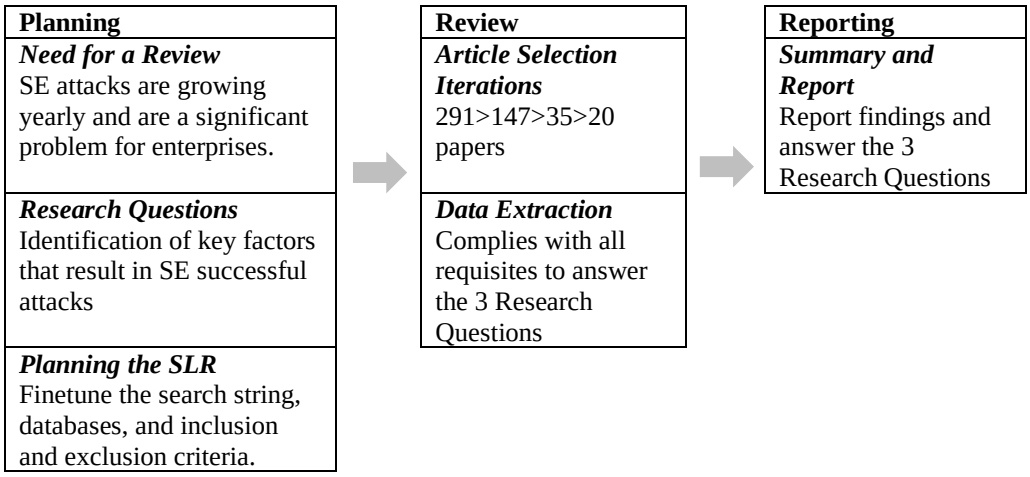

Figure 1 - Systematic Literature Review Phases

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

2.2.1. 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 paper 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 paper, including data quality assurance, statistical data analysis, data modeling, and interpretation of results.

2.2.2. 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 research questions (RQ) 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 paper, three RQs were developed:

- RQ1 - How do employee training programs impact the success rate of Social Engineering attacks such as phishing in enterprises?
- RQ2 - How can companies or corporations create a culture of security to reduce the success rate of all types of Social Engineering attacks?
- RQ3 - 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 presented in Table 3, as a criterion to frame the RQs, as suggested by Petticrew and Roberts and proposed by Kitchenham [29].

Table 3 - PICOC

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 are listed in table 4.

Table 4 - 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	

2.2.3. Conducting the Review

The review protocol and the methods used to undertake this SLR were 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 paper 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.

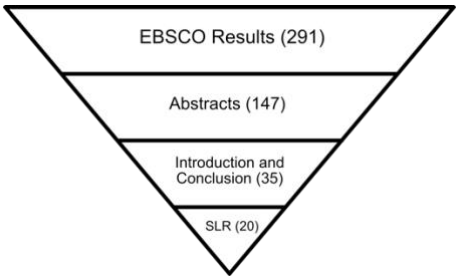

Figure 1 - Selection phases

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 5 - 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 released papers over the years in the final 20 articles used in this review. It is observable an increase in scientific work on the topic across the recent years.

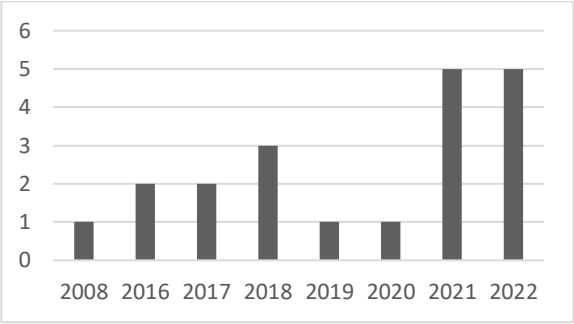

Figure 2 - Release SLR final papers over the years

Table 5 presents the mapping of the final papers used in this review, the publication year, and the number of citations.

Table 6 - 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 presented in Table 7. Excerpts from the papers were compiled on the matrix and analyzed on their relevancy and/or by matching the search strings and if the topics are covered or not by each paper.

Table 7 - Synthetized data matrix

Paper	How do employee training programs impact the success rate of social engineering attacks in enterprises?	How can enterprises create a culture of security to reduce the success rate of social engineering attacks?	What factors make individuals more susceptible to social engineering tactics?	Can the implementation of cybersecurity policies and procedures reduce the success rate of cyberattacks in enterprises?
Paper 1	Relevant	Not covered	Not covered	Not covered
Paper 2	Relevant	Not covered	Relevant	Not covered
Paper 3	Relevant	Not covered	Relevant	Relevant
Paper 4	Not covered	Not covered	Relevant	Not covered
Paper 5	Not covered	Not covered	Relevant	Not covered
Paper 6	Relevant	Not covered	Relevant	Relevant
Paper 7	Relevant	Not covered	Not covered	Not covered
Paper 8	Relevant	Relevant	Relevant	Not covered
Paper 9	Relevant	Relevant	Not covered	Not covered
Paper 10	Relevant	Not covered	Not covered	Not covered
Paper 11	Relevant	Not covered	Relevant	Not covered

Paper 12	Relevant	Relevant	Not covered	Relevant
Paper 13	Relevant	Not covered	Not covered	Relevant
Paper 14	Relevant	Not covered	Not covered	Not covered
Paper 15	Relevant	Relevant	Relevant	Relevant
Paper 16	Relevant	Not covered	Relevant	Relevant
Paper 17	Relevant	Relevant	Not covered	Not covered
Paper 18	Relevant	Relevant	Relevant	Relevant
Paper 19	Relevant	Not covered	Relevant	Not covered
Paper 20	Relevant	Not covered	Relevant	Relevant

The combination and analysis of the selected papers allowed, therefore, to formulate conclusions directly derived from this evidence.

2.2.4. 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 8 presents the employee's training impact according to the increase in cybersecurity and Information security within an enterprise or by not being adequate for cybersecurity and Information security improvement.

Table 8 - 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 9 presents the actions mentioned in the papers for creating a security culture in enterprises.

Table 9 - 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]. 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]. 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]. Table 10 presents the individual factors that are more susceptible to SE attacks mentioned in the papers.

Table 10 - 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]
Parttime	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. 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 paper 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.

RQ1 emphasizes the crucial role of user training awareness in enterprise cybersecurity, with varying opinions on its effectiveness and cost efficiency. The need for a comprehensive understanding of human susceptibility beyond phishing is underscored. Regarding RQ2, the findings stress the holistic nature of establishing a security culture within enterprises. However, limited mentions of security culture in the literature suggest room for integrating it more effectively with user awareness training. Concerning RQ3, the paper highlights the challenge of identifying personal traits influencing susceptibility to SE attacks. Emotional biases, such as fear and trust, contribute to attack success. Certain groups, like IT professionals and those recently trained, may be less susceptible, but individual differences and self-serving bias complicate identifying vulnerable groups.

The literature review primarily focuses on phishing attacks, the exploration of other social engineering (SE) attacks could be relevant for comparison. In terms of user awareness training and enterprise security culture, future research could investigate the effectiveness of gamification to motivate and engage employees, potentially surpassing traditional training methods. The SLR results highlight the challenge of identifying personal traits making individuals susceptible to SE attacks, suggesting the need for further research to understand how attackers choose targets and how enterprises can better prepare their users. Additionally, only a few papers mention security culture in enterprises. Further research could explore how organizational culture affects vulnerability to SE attacks, examining leadership roles, communication strategies, levels of psychological safety, and the impact of user engagement on an organization's security posture. Employee resistance to security training can be a common issue. Further investigation is needed to identify the root causes of this resistance in enterprises and improve the effectiveness of security training.

Several findings could be observed in this 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

To continue and guide the investigation of this paper and answering the research question mentioned in Introduction, the activities of Design Science Research (DSR), proposed by Peffers et al. [30], have been selected as the primary research methodology. Once the initial artefact has been developed, the next step is to conduct an evaluation phase. Finally, to support the preliminary research findings and refine the artefact, 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 artefacts. This methodology, that will be used in the paper, involves a systematic process of designing artefacts to solve identified problems, contributing to research, evaluating the effectiveness of the designs, and communicating the results to relevant stakeholders. The created artefacts 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, effectiveness, and usability of the artefact 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 artefacts. Therefore, it considers the social, cultural, and organizational context in which the artefacts are intended. DSR aims to create artefacts 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 timebound (SMART) [22]. It involves identifying the outcomes that the research aims to achieve and the criteria for evaluating the research success, proposing a framework to improve SE resilience in enterprises.

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

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

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

identifying the limitations and challenges of the artefact. 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 a paper.

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

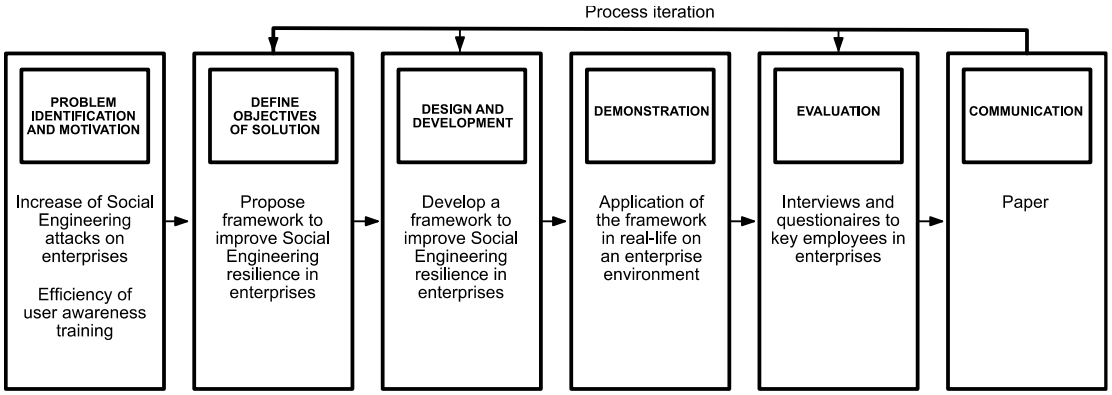

Figure 3 Adapted DSRM Process Model

3.2. Semi structured Interviews

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. 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 opportunities to develop topics that arise during conversations [32].

4. Design and Development

In this section, which corresponds to step 3 of the DSR, it is described the proposal.

As a result of the findings on the literature review, the proposal will go on the direction of proposing a framework for organizations to leverage on their operations and mitigate the success rate of SE attacks, to improve SE resilience through identification of potential gaps in existing security infrastructures and the prioritization of interventions.

4.1. Requirements

Table 11 outlines both functional and non-functional requirements, adapted from Johannesson [38] work on Design Science, stating they need to identify and outline an artefact that can address the explicated problem and to elicit the requirements on that artefact [38]. These requirements are integral to the design and development of the framework. Each component addresses specific organizational aspects.

Table 11 - Functional and Non-Functional requirements for framework development

Components	Functional Requirements	Non-Functional Requirements
User Awareness and Training	• Tailored and measurable training program involving HR from the pre-planning phase. • Modules for different employee groups, with an emphasis on IT professionals and new joiners. • Tracking system to monitor employee participation and completion of training modules.	• *Usability:* Intuitive and user-friendly interface for the training program. • *Scalability*: Training program can scale to accommodate a growing number of employees. • Reliability: Training modules are available and reliable during scheduled sessions.
Security Culture	• Create and nurture a culture of open and honest communication, providing regular training sessions, seminars, and workshops on cybersecurity. • Schedule and content for regular cybersecurity awareness sessions.	• *Compliance*: Cybersecurity sessions comply with relevant regulatory standards and industry best practices. • *Auditability*: Logging mechanisms to track employee participation in cybersecurity awareness sessions.
Address Emotional Biases	• Persuasion principles to educate employees on identifying and avoiding SE attacks. • Educational content to target different user groups, focusing on IT professionals and new employees.	• *Compatibility*: Compatibility with various emotional intelligence training tools and resources. • *Maintainability*: Design the framework to easily incorporate updates to psychological principles and educational content.
Continuous Evaluation	• Metrics and KPIs to measure the effectiveness of the training program, security culture initiatives, and persuasion techniques. • Continuous evaluation process to assess the impact of the framework on reducing SE vulnerabilities. • Metrics and KPIs reviews to identify areas for improvement and make necessary adjustments to	• *Performance:* Metrics for the continuous evaluation process to ensure timely and accurate assessments. • *Documentation:* Comprehensive documentation for the continuous evaluation process.

Components	Functional Requirements	Non-Functional Requirements
	enhance overall effectiveness.	
Empower Reporting	• Anonymous reporting mechanism to empower employees to report suspicious activity without fear of reprisal. • Clear guidelines on how to use the reporting mechanism and ensure its accessibility to all employees. • Feedback to communicate regularly with employees about the outcomes of reported incidents and actions taken to address them.	• *Security:* Robust security measures to protect the anonymity and integrity of the reporting mechanism. • *Usability:* Reporting mechanism user-friendly and easily accessible for all employees. • *Maintainability:* Reporting mechanism to allow for updates and improvements based on user feedback.

The objective is to create a comprehensive and adaptable solution through a framework that aims to provide a structured approach to improving SE resilience while ensuring usability, reliability, and scalability across all enterprise contexts.

4.2. Proposal

The proposed 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 10 describes in a high-level detail, the artefact.

Table 12 - Proposed Artefact (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 preplanning 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.

Because the components of the artefact must be used in a certain sequence, in Figure 4 this sequence is presented.

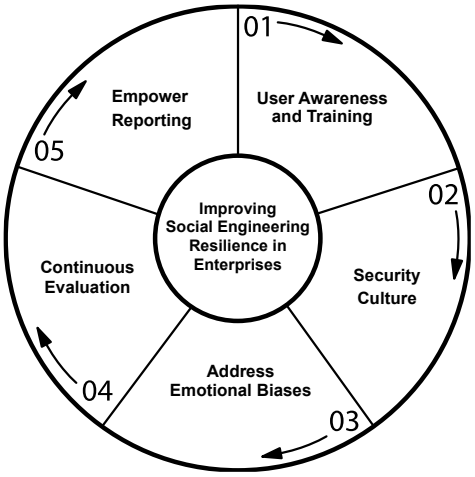

Figure 4 - Proposed framework sectioning

In Table 11, is presented a detailed description of every component of the proposed framework.

Table 13 - Proposed framework detailed description (Adapted from Johannesson [38]).

Components	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.
Address Emotional	• Develop educational materials that use persuasive communication techniques to increase

Biases	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 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.

4.3. Requirements Coverage

It is important to make a check to establish the coverage of the initial requirements by the framework. Table 14 provides a quick overview of how each functional and non-functional requirement is covered by the proposed framework.

Table 14 - Initial requirements coverage check (Adapted from Johannesson [38]).

Components	Functional Requirements Coverage	Non-Functional Requirements Coverage
User Awareness and Training	✓ Module tracking system. ✓ Tailored modules for different groups. ✓ Involvement of HR.	✓ *Usability:* Intuitive and user-friendly interface. ✓ *Scalability:* Framework pair growing user base. ✓ *Reliability:* Training modules available and reliable.
Security Culture	✓ Regular cybersecurity sessions scheduled. ✓ Open and honest communication culture.	✓ *Compliance:* Sessions comply with regulatory standards. ✓ *Auditability:* Logging mechanisms for session participation.
Address Emotional Biases	✓ Persuasion principles. ✓ Tailored content for different user groups.	✓ *Compatibility:* Framework compatible with emotional intelligence tools. ✓ *Maintainability:* Framework can be easily

Components	Functional Requirements Coverage	Non-Functional Requirements Coverage
		updated.
Continuous Evaluation	✓ Metrics and KPIs. ✓ Continuous evaluation process. ✓ Regular review and improvement cycle.	✓ *Performance:* Defined metrics for timely assessments. ✓ *Documentation:* Comprehensive documentation.
Empower Reporting	✓ Anonymous reporting mechanism. ✓ Guidelines for reporting mechanism usage. ✓ Feedback for reported incidents.	✓ *Security:* Robust measures for anonymity. ✓ *Usability:* User-friendly reporting system. ✓ *Maintainability:* Reporting system easily updatable.

The checkmarks presented in Table 14, indicate that the corresponding requirement is addressed by the framework.

5. Demonstration

This section covers the demonstration of the proposed framework (artefact) to a use-case. To demonstrate the framework, a real-world use case will be used, based on the framework proposed by Johannesson [38].

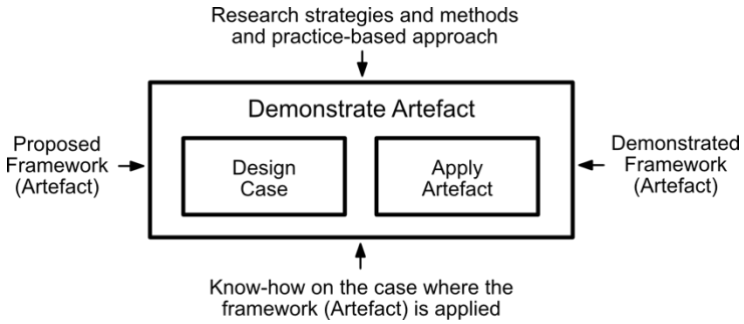

Figure 5 - Demonstrate artefact process (Adapted from Johannesson [38]).

5.1. Introduction to the Use Case

The enterprise used to demonstrate the framework is in the commodity sector. It has more than ten thousand employees, and it operates at an international level. It has a SOC team and has implemented a user awareness program based mainly on internal phishing campaigns. The training is managed by several teams and assigned by the LMS (Learning Management Team) at a global level. The user awareness level is on par with the sector, but the number of employees that fall for phishing emails is still high in some regions, as there is training resistance. Despite the high efforts to secure the environment, the human factor is still an issue, and SE's resilience must be addressed.

5.2. Application of User Awareness and Training

To showcase the framework's effectiveness, training is sectored by regions and groups of employees, and therefore, depending on their sector, the content of the phishing campaign and training module will differ. HR has

been involved since the beginning by providing the updated group lists and reviewing and working with the remaining teams throughout the year on the content of each campaign.

The content of each campaign (phishing email and training) is tailored according to specific user groups. More tech-savvy employees, such as IT employees, receive more technical training, and where the content is being prepared, considering the capabilities and understandings of some topics. On employee groups not as tech savvy, such as facility operators, the content is more introductory level on the principles of phishing and how to avoid these types of social engineering attacks.

5.3. Implementation of Security Culture

The emphasis lies in cultivating a robust security culture through a multifaceted approach when implementing a security culture. To prioritize regular awareness sessions, workshops, and seminars, fostering an environment where employees are continuously informed about emerging cybersecurity threats. Cross-departmental collaboration and a shared responsibility mindset are integral components, ensuring that security considerations permeate every aspect of our organization. Leadership is pivotal in supporting and actively participating in cybersecurity initiatives, setting the tone for the entire workforce. Implemented recognition and reward programs serve as powerful tools, acknowledging and reinforcing positive security behaviors to nurture a culture where vigilance is celebrated. Also important is recognizing the workforce's diverse needs, prioritizing tailored content, and employing various learning approaches to different learning styles. Metrics serve as a compass for ongoing assessment, allowing us to measure the effectiveness of the initiatives and make continuous improvements, ensuring that the security culture remains dynamic and resilient.

5.4. Addressing Emotional Biases in the Use Case

A strong emphasis on using persuasion principles and real-world examples is enforced to address emotional biases, ensuring that the training content is informative but also practical and relatable. To recognize the diversity in emotional profiles across the enterprise, the content is tailored to address the unique needs of different user groups. It focuses on addressing IT professionals and non-tech-savvy employees, such as simulated scenarios incorporating emotional elements, providing a realistic and immersive training experience. Additionally, prioritization and establishment of feedback mechanisms and robust support systems allow employees to share their experiences and navigate emotional challenges within a supportive environment. Continuous evaluation serves as a guiding principle, allowing the assessment and improvement of emotional resilience initiatives, ensuring their relevance and effectiveness over time.

5.5. Continuous Evaluation in Action

For continuous evaluation, establishing and regularly reviewing Key Performance Indicators (KPIs) are highlighted, ensuring a clear focus on measurable outcomes. Adaptive training content evolves based on evaluation results, emphasizing real-time responsiveness. Showcase comprehensive analysis of incident response data and user feedback mechanisms, also provide insights for continuous improvement. Benchmarking against industry standards ensures practices align with best-in-class approaches, value scenario-based testing, and collaborate with external auditors to fortify the defenses. Transparent communication of results and lessons

learned fosters a culture of openness. The iterative improvement cycle is a core element, reflecting the commitment to constant refinement and enterprise resilience against SE threats.

5.6. Empowering Reporting in the Use Case

An anonymous and secure reporting mechanism is in place for reporting empowerment, with clear guidelines and procedures. Regular communication highlights the impact of reporting on the security posture, integrated with ongoing awareness training. Furthermore, accessibility, diverse reporting options, and metrics to measure effectiveness are offered. Feedback on reported incidents is crucial and encourages reporting at all organizational levels, fostering a shared responsibility culture. Integration with incident response procedures ensures a quick and cohesive approach, while a commitment to continuous improvement underlines the dedication to refining the security measures responsively.

5.7. Results and Impact

Analyzing the results and the impact of the framework implementation, we can analyze the quantitative data demonstrating a reduction in successful attacks and increased reporting rates. Assessments and surveys reveal enhanced user awareness levels, complemented by qualitative feedback that reflects employee engagement and a positive response to our initiatives. Observable cultural shifts towards a security-conscious environment emphasize the dedication to fostering a proactive mindset. A comparison of organizational metrics with industry standards and benchmarks showcases an alignment with sector best practices. An analysis of the return on investment confirms the framework's cost-effectiveness, while discussions on challenges, lessons learned, and insights gained provide valuable context for continuous improvement. Instances of employee recognition and rewards underscore the tangible impact of the efforts on individual and collective security awareness.

5.8. Challenges and Lessons Learned

The data resulting from the framework implementation highlights the quantitative success with reduced attacks and increased reporting. Survey results highlight enhanced user awareness, and qualitative feedback confirms proactive employee engagement. Operational efficiency is evident in positive incident response evaluations and cultural shifts towards a security consciousness. Comparative metrics demonstrate alignment with industry standards and Return On Investment (ROI) analysis assesses the cost-effectiveness of the framework. Discussions on challenges, lessons learned, and insights gained provide context for improvement. Employee recognition highlights the framework's success in generating a security-aware mindset permeable to all employee sectors.

5.9. Conclusion and Generalizability

The framework, demonstrated in the commodity sector, strategically addresses social engineering threats. It effectively tackles human factor challenges through tailored training, a robust security culture, and measures to address biases. Results present tangible success with reduced attacks and increased awareness, supported by metrics and ROI analysis. The framework's adaptability and proactive approach make it relevant across industries,

offering a blueprint for building a security culture and improving resilience in a dynamic threat landscape.

6. Evaluation

In this section, corresponding to step 5, is conducted the evaluation of the artefact.

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.

6.1. Interviews

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 artefact 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.

6.2. 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].

6.3. 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 12, the interviewee's current positions in IT are diversified.

Table 15 - 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

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

6.4. Data Saturation

In this research, a data saturation process was carried out to evaluate the status of the artefact (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. 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. 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]. Table 14 represents the general overall unique contributions by each of the sixteen interviewees.

Table 16 - 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 paper, 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?". Fig. 9 illustrates the unique overall contribution of each interviewee, on the several research topics.

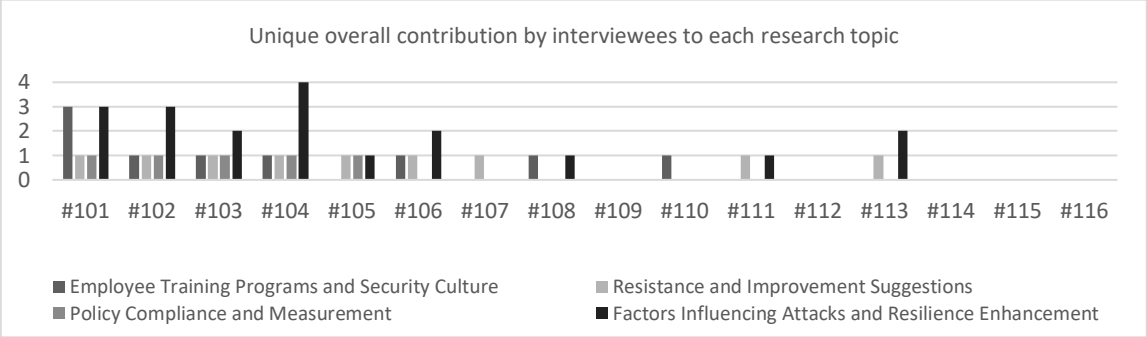

Figure 6 *Unique overall contribution by interviewees to each research topic*

Figure 9 highlights the unique overall contribution by each interviewee on the several research topics.

7. 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.

The interview responses focus the impact of employee training programs on SE attack success rates in enterprises, aligning with the proposed framework's emphasis on continuous training, awareness, and testing. Interviewees stress the importance of regular reminders, incorporating them into training programs to enhance employee vigilance against SE threats. Regular testing through simulated attacks, like internal phishing campaigns, are relevant in assessing and improving training program effectiveness, ensuring employees can identify and mitigate SE threats. Ongoing support and accessible resources are crucial for reinforcing training knowledge. The need for a skeptical and critical culture when handling suspicious communications is underscored to reduce vulnerability to SE attacks. While practices like using strong passwords contribute to overall security, they are not directly focused on SE tactics education. However, they can complement broader security awareness efforts to mitigate SE attacks.

The interviews conducted in this study validates strategies for fostering a security culture and reducing success in SE attacks. Key findings include the emphasis on regular SE training, internal phishing campaigns, and email alerts. Regular training enhances awareness and equips employees to identify and counter SE attacks. Internal phishing campaigns and email alerts effectively test and reinforce security measures. Initiatives like a "Cybersecurity Week" promote awareness and education. Management feedback, team meetings, and a security committee contribute to a culture of security. Encouraging reporting through incentives is vital for early SE attack detection. Addressing emotional biases using educational materials and positive reinforcement aligns with the proposed framework. Metrics and continuous evaluation are crucial for adapting strategies to the evolving threat landscape. A streamlined reporting system facilitates prompt responses to potential SE attacks, aligning with the framework's focus on reporting mechanisms and feedback.

The interviews brought valuable insights into factors increasing susceptibility to SE tactics, validating the proposed framework's relevance. The mentioned tactics aligned with the proposed framework, confirming its applicability. Key susceptibility factors identified included the need for attention and awareness, distractions compromising critical evaluation, and personal vulnerabilities like fear and greed. Addressing emotional biases, promoting critical thinking, and offering examples are vital countermeasures. The willingness to help others was noted, emphasizing the importance of educating employees about potential risks and promoting verification before compliance. Ignorance and excessive trust in digital communications were acknowledged, highlighting the role of training and awareness programs. Recommendations for improving SE resilience included ongoing training, face-to-face awareness sessions, audits, and training exercises with real examples. Involving all stakeholders and implementing policies, controls, gamification, stress reduction, easily understandable information, skepticism, verification, and a culture of reporting align with the framework, validating its effectiveness in mitigating enterprise’s susceptibility to SE tactics.

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, the interviews responses performed in the DSR phase, strongly support, and validate the proposed framework.

8. Conclusion

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

After the development of the artefact and as result of the interviews, it has been emphasized the importance of regular training sessions, aligning with the proposed framework's emphasis on continuous employee training. Awareness sessions were considered valuable components of a comprehensive employee education program, offering insights into the latest SE techniques and potential impacts of falling prey to such attacks. Simulated attacks, like internal phishing campaigns, were highlighted as effective measures to educate and test employees' SE tactics recognition and response abilities, raising awareness and identifying vulnerabilities. Real-life examples were mentioned as practical tools, aiding employee understanding of attacker tactics and consequences. To enhance training effectiveness, interviewees suggested interactive methods like gamification, making sessions enjoyable and increasing participation. The importance of relevant and well-translated training materials, tailored to employees' technical and cultural levels, was emphasized for practical and inclusive training.

These insights align with the proposed framework, emphasizing the importance of creating a security culture, addressing emotional biases, continuously evaluating training effectiveness, and empowering employees to report suspicious activities. The gathered data strongly supports the proposed framework for mitigating SE attacks. Implementing regular training, simulated attacks, awareness sessions, and real-life examples also are aligned, offering valuable guidance for enterprises aiming to enhance their training programs and establish a security culture. By incorporating these strategies, enterprises can improve their security posture and effectively protect against future SE attacks.

The research, comprising a Systematic Literature Review (SLR), Design Science Research (DSR), and semi-structured interviews, brought valuable insights into enhancing employee training and awareness programs, fostering a security culture, and mitigating Social Engineering (SE) attacks in enterprises. The combined findings provide comprehensive conclusions guiding enterprises to enhance their cybersecurity posture against external threats. The key takeaways include the significance of continuous and tailored trainings to reduce SE attack probabilities, the importance of employee cybersecurity knowledge, and the need for periodic reminders, regular testing, and ongoing employees' awareness.

Creating a security culture involves all stakeholders, with open communication and collaboration being crucial, as highlighted in both the SLR and interviews. A collaborative approach, reinforced through regular team meetings and events like a "Cybersecurity Week," generates a collective cyber defense effort. Balancing technical controls with human awareness, such as Multi-factor Authentication (MFA), encryption, and intrusion detection systems, enhances an enterprise's security, although, caution is advised against overreliance on technology.

Educating employees about SE tactics and addressing emotional biases like fear, trust, curiosity, and a willingness to help others play central roles in strengthening the human element of cybersecurity. The proposed framework addresses these biases through strategies like real-life examples and positive reinforcement. Continuous evaluation and enhancement of SE resilience are emphasized, along with the need for engaging employees, management, and key departments in the security process. Positive reinforcement and incentives contribute to a

security culture throughout the enterprise.

By progressively and constantly evaluating and adapting their strategies, enterprises can become proactive against emerging threats. 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. This can be achieved by using real-life examples, simulations, and ongoing awareness training, that enhances their ability to recognize and respond appropriately. Managers can mitigate SE attack risks through a multi-layered approach, combining training, reminders, testing, nurturing a security culture, and balancing technological measures with human vigilance. Finally, training programs can mitigate vulnerabilities by promoting critical thinking and validating requests before acting.

8.1. Limitations

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. 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.

8.2. 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.

8.3. Conflicts of Interest

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

9. Bibliography

[1] Microsoft, "Phishing trends and techniques." Accessed: Aug. 10, 2023. [Online]. Available: https://learn.microsoft.com/enus/microsoft365/security/intelligence/phishingtrends?view=o365worldwide

[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 Universidade 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/imrv14n2art1.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/s413030170058x.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_antiphishing_enterprise_environ_model_using_feedforward_backpropagation_and_LevenbergMarquardt_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. KlimburgWitjes 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 antiphishing 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 XForce , 2023, Accessed: Aug. 10, 2023. [Online]. Available: https://www.ibm.com/reports/threatintelligence

[23] HP, "HP Wolf Security." Accessed: Aug. 10, 2023. [Online]. Available: https://www.hp.com/usen/security/endpointsecuritysolutions.html

[24] M. A. Siddiqi and W. Pak, "A study on the psychology of Social Engineeringbased cyberattacks and existing countermeasures," Applied Sciences, vol. 12(12), p. 6042, 2022, Accessed: Aug. 10, 2023. [Online]. Available: https://www.mdpi.com/20763417/12/12/6042

[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. AbasiAmefon, 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_EBSE200701

[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, "Semistructured Interviews," 2006, Accessed: Aug. 10, 2023. [Online]. Available: http: //www.qualres.org/HomeSemi3629.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 semistructured 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/s1113501705748

[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=ptPT&lr=&id=JOr3A3LbwC&oi=fnd&pg=PA1&dq=%5B32%5D.%09M.+P.+Grady,+%E2%80%9CQualitative+and+action+research:+A+practitioner+handbook%E2%80%9D.&ots=hCNVcoEQ4&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

[38] Johannesson, P., Perjons, E. (2021). An Introduction to Design Science. Springer, Cham. https://doi.org/10.1007/978-3-030-78132-3_8

[39] Mateus-Coelho, Nuno, and Manuela Cruz-Cunha, editors. Exploring Cyber Criminals and Data Privacy Measures. IGI Global, 2023. https://doi.org/10.4018/978-1-6684-8422-7

[40] Daniel Jorge Ferreira, Nuno Mateus-Coelho and Henrique S. Mamede, Methodology for Predictive Cyber Security Risk Assessment (PCSRA), Procedia Computer Science, Volume 219, 2023, Pages 1555-1563, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2023.01.447.

[41] Mario Saraiva, Nuno Mateus-Coelho, CyberSoc Framework a Systematic Review of the State-of-Art, Procedia Computer Science, Volume 204, 2022, Pages 961-972, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2022.08.117.

[42] M. Saraiva and N. Coelho, "CyberSoc Implementation Plan," *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*, Istanbul, Turkey, 2022, pp. 1-6, doi: 10.1109/ISDFS55398.2022.9800819.

[43] Filipe Alves, Nuno Mateus-Coelho, Manuela Cruz-Cunha, Encryption File System Framework - Proof of Concept, Procedia Computer Science, Volume 181, 2021, Pages 1237-1246, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2021.01.322.