

## Central Lancashire Online Knowledge (CLOK)

Title	Merging Policy and Practice: Crafting Effective Social Engineering Awareness-Raising Policies
Type	Article
URL	<a href="https://clock.uclan.ac.uk/id/eprint/50937/">https://clock.uclan.ac.uk/id/eprint/50937/</a>
DOI	<a href="https://doi.org/10.5220/0012410300003648">https://doi.org/10.5220/0012410300003648</a>
Date	2024
Citation	Stavrou, Eliana, Piki, Andriani and Varnava, Panayiotis (2024) Merging Policy and Practice: Crafting Effective Social Engineering Awareness-Raising Policies. Proceedings of the 10th International Conference on Information Systems Security and Privacy, 1. pp. 179-186. ISSN 2184-4356
Creators	Stavrou, Eliana, Piki, Andriani and Varnava, Panayiotis

It is advisable to refer to the publisher's version if you intend to cite from the work.  
<https://doi.org/10.5220/0012410300003648>

For information about Research at UCLan please go to <http://www.uclan.ac.uk/research/>

All outputs in CLOK are protected by Intellectual Property Rights law, including Copyright law. Copyright, IPR and Moral Rights for the works on this site are retained by the individual authors and/or other copyright owners. Terms and conditions for use of this material are defined in the <http://clock.uclan.ac.uk/policies/>

# Merging Policy and Practice: Crafting Effective Social Engineering Awareness-Raising Policies

Eliaana Stavrou<sup>1</sup><sup>a</sup>, Andriani Piki<sup>2</sup><sup>b</sup> and Panayiotis Varnava<sup>2</sup>

<sup>1</sup>*Faculty of Pure and Applied Sciences, Open University of Cyprus, Nicosia, Cyprus*

<sup>2</sup>*School of Sciences, University of Central Lancashire Cyprus, Pyla, Cyprus*

**Keywords:** Cybersecurity, Cybersecurity Policy Design, Social Engineering, Cybersecurity Awareness, Upskilling.


**Abstract:** Cybersecurity policies play a fundamental role in fostering organizational cyber governance and cyber resilience. Cybersecurity awareness-raising and training policies specify upskilling requirements and explicitly address persistent threats such as social engineering attacks. While cybersecurity awareness-raising and training activities complement the objectives of security policies, challenges including stakeholder diversity, budget constraints, generic messaging and low user engagement hinder their effectiveness. For successful policy adoption it is crucial for the workforce to grasp the relevance of these policies within their work context, understand how social engineering attacks are deployed, and apply policy rules appropriately. However, existing awareness-raising and training policies often lack specificity, leading to gaps in employee engagement and behavioural change, especially regarding social engineering threats. To address these issues, the paper proposes a dedicated social engineering awareness-raising policy, guided by Merrill's Principles of Instructions. This work aims to merge policy and practice, offering tailored examples of social engineering attacks, explicitly connecting them to relevant cybersecurity policies and making the content more engaging and relevant to the workforce. This is envisioned as a cost-effective resource for organizations with a limited training budget, which can be utilized as a starting point to enhance employee awareness, engagement, and foster a stronger organizational cyber resilience culture.


## 1 INTRODUCTION

Cyber security policies are a core element of a cyber security strategy, contributing towards an effective organizational cyber security governance (ISO/IEC, 2022). Many organizations develop a cyber security awareness-raising and training policy as part of their cyber security governance (CIS, 2023). This policy sets the requirements and focus of the training that should be undertaken by the organization. The policy's content is often written at a high level, specifying that the workforce should be made aware of the organization's cyber security policies, typical cyber threats, and best practices to address them. While this document sets the overall strategy in terms of awareness and training aspects, it does not assist for example the IT team to tailor the training according to employees' roles and responsibilities which can contribute towards more effective

behaviour change and cyber hygiene. Currently, an awareness-raising and training policy does not include relevant content to help the IT team to map cyber threats to the different cyber security policies of the organization and effectively communicate this mapping to the organization's workforce. Mapping cyber threats to specific cyber security policies could contribute to raising awareness on the problem (Stavrou, 2020) and, in turn, understanding and accepting the actions to be deployed. This can lead to more effective upskilling and to the development of a cyber security culture across an organization.

A major cyber threat that organizations continue facing is social engineering (SE). The digital transformation that occurred during COVID-19 pandemic provided a great opportunity to cyber criminals (Venkatesha et al., 2021) to attack organizations and/or individuals through SE. Awareness-raising and training have been proved to

<sup>a</sup> <https://orcid.org/0000-0003-4040-4942>

<sup>b</sup> <https://orcid.org/0000-0003-0376-1713>

complement the objectives of security policies and to be the most effective way to address SE attacks (Smith et al., 2013). However, several challenges exist that can hinder the adoption of upskilling solutions, with the economic factor being the most prevailing challenge (GOV.UK, 2023). The impact from a SE attack can be devastating for an organization, especially when this attack is launched as the starting point for delivering more advanced attacks, such as ransomware. This should prompt the cybersecurity community to design new interventions and increase cyber resilience against SE attacks. As indicated in ENISA's latest Cyber Security Threat Landscape 2023 (ENISA, 2023), the problem remains and efforts should continue to empower organizations becoming cyber resilient against this type of attacks. Another challenge that is identified across the provision of different SE training and awareness programs (Aldawood & Skinner, 2019) is that often the same message or content is communicated across different audiences. This approach does not help the workforce to relate to the problem, realize the threat and how it can be transformed in their work context (Stavrou, 2020). This lack of contextualised understanding can hinder employees' engagement with awareness-raising efforts and the motivation to change their behaviour.

There is a timely and critical need to return to the basics and reconsider the design of awareness-raising policies, by developing a dedicated and contextualizable SE awareness-raising policy. Such a policy can provide tailored examples of SE attacks and link them to relevant policies. Organizations that do not currently have the budget to allocate for external training can utilize the policy to educate their employees and better prepare them for follow up awareness-raising and training sessions that can be scheduled as soon as the budget permits. Overall, the aim of creating a dedicated SE awareness-raising policy is twofold: first, to create more engaging, demonstrative, and relevant content to the organization so that the workforce can easily relate to the security policies' content and be motivated to apply it in practice (hence merging policy enforcement with practical application); and second to serve as a reference point to design purposefully tailored awareness-raising and training sessions. This work investigates the use of Merrill's Principles of Instructions (MPI) to support the proposed policy design objectives. Moreover, a questionnaire is being developed to assess policy-related aspects with the aim to inform policy design.

The paper is structured as follows: section 2 presents the methodology; section 3 briefly discusses

related work; sections 4 and 5 discuss how MPI can be utilized and the key aspects that can inform the design of a SE awareness-raising policy, respectively. Section 6 presents the proposed policy design and some preliminary evaluation results. Finally, section 7 concludes the work performed in this study.

## 2 METHODOLOGY

Initially, research was performed to identify and analyse standards and frameworks related to design aspects of information security policies. The objective was to identify the typical structure and content of security policies. Through the investigation, it was also important to identify specific security policies that can be applied in the context of a variety of SE attacks. Moreover, Merrill's Principles of Instruction were analysed to explore how this model can potentially guide the design of an engaging and effective SE awareness-raising policy. Another aspect that could inform the design of such a policy relates to the workforce's perceptions regarding different policy-related aspects that might contribute to a false sense of security. A questionnaire was developed to assess these aspects. The questionnaire was administered in the context of a small organisation with a limited training budget. Investigation results informed the design of a novel SE awareness-raising policy. An initial evaluation with a follow-up questionnaire was performed to assess the design principles of the proposed policy.

## 3 RELATED WORK

Different frameworks, standards and guidelines exist to guide the design of cyber security policies. The purpose of security policies is twofold. On one hand to guide the general workforce of an organization on the best practices that should be followed, the actions that are not endorsed, and guide them to report incidents to the organization. On the other hand, to guide the technical team to implement appropriate technologies and procedures to comply with the security policies.

The ISO/IEC 27002:2022 standard (ISO/IEC, 2022) provides guidelines to organizations, to determine and implement commonly accepted information security controls as part of an information security management system (ISMS). Usually, an organization defines a high-level information security policy to set the approach to

manage its information security. This policy is then supported by a bundle of other topic-specific policies to guide the implementation and applicability of other controls. Examples include, among others, email policy, backup policy, information classification and handling, acceptable use policy, etc. Some of these policies are applicable by the general workforce of the organization while others are meant to be considered by the technical team.

ISO/IEC 27002:2022 standard includes two specific controls that are relevant to upskilling the workforce. Control 5.27 “Learning from information security incidents” aims to reduce the likelihood or consequences of future incidents. The control mandates that knowledge gained from security incidents should be used to strengthen and improve security controls, including enhancing “User awareness and training” (control 6.3). As per control 5.27, this can be achieved by “providing examples of what can happen, how to respond to such incidents and how to avoid them in the future”. This approach indicates that awareness and training should be tailored to reflect the threats that are relevant to the organization’s business environment and operations. With regards to the user awareness and training control, the standard specifies that employees should be made aware of the security policies and be trained, considering their job function. Such educational activities should be scheduled regularly to help employees learn and retain the knowledge gained. In essence, this approach should adopt a micro-training plan (Kävrestad, 2023) to maximize the benefits of upskilling initiatives. Moreover, it is highlighted that it is essential to not only focus on the ‘what’ and ‘how’, but also the ‘why’ so employees realize the problem, its impact and the objective of the controls that should be applied.

The Cyber Security Framework (CSF) proposed by the National Institute of Standards and Technology (NIST, 2018) is another framework that guides organizations to manage cybersecurity risks by applying a set of best practices. The framework assembles guidelines and practices under five cybersecurity functions (identify, protect, detect, respond, recover), providing a holistic approach and empowering organizations to improve their cyber resilience. The framework can be utilized by organizations as a tool to align policy, business, and technological approaches to managing cybersecurity risks. Different policy templates, (e.g., CIS & MS-ISAC, 2019a, 2019b; Healthit.gov, 2018; SANS, 2022) have been developed to assist organizations apply the CSF.

With regards to SE attacks, Alharthi & Regan (2021) have proposed a model of SE ‘infosec’ policies and designed a survey to measure their adoption level. The policies are categorised under four areas (people, data, hardware and software, and network) that can be impacted by SE attacks. The proposed policies target both end-users and IT teams. The latter are expected to implement the relevant policies’ rules. Aldawood (2020) emphasizes that it is essential to understand people’s behaviour and prior knowledge to provide them with customized and effective SE security training. The author proposes to group people based on their awareness of SE threats prior to providing tailored security training. Steinmetz et al. (2023) interviewed social engineers and IT professionals about their perceptions related to different aspects of security policies. Results highlighted the need to consider the elements that make for an effective policy document; the way it is written and communicated, and the supporting mechanisms to aid its implementation.

## 4 SECURITY POLICY DESIGN POWERED BY INSTRUCTIONAL DESIGN PRINCIPLES

### 4.1 Merrill's Principles of Instruction

This paper explores the applicability of the MPI model (Merrill, 2002) in guiding the design of engaging and effective security policies. The MPI model consists of five interrelated principles that can effectively promote learning:

- *Problem-Centred*. Learning can be more effective when knowledge is acquired in the context of real-life tasks or problems.
- *Activation*. Learning activities should help learners to activate prior knowledge and to process and structure the new knowledge to make associations between the past and the new knowledge.
- *Demonstration*. Learners can retain knowledge longer when real tasks or problems are demonstrated.
- *Application*. Learners can build new knowledge and skills effectively when they carry out real tasks or investigate real problems.
- *Integration*. The learning activities should encourage the learners to integrate the new

knowledge they have acquired into their professional and/or personal environment.

The work by Charalambous & Stavrou (2023) has demonstrated how MPI can be used to design SE awareness-raising and training activities that support the key objective of a culture of cyber situational awareness, e.g. enabling people to recognise when they are being attacked in a professional and/or personal context, understanding the means of attack and the bad practices to avoid, and recognising the measures to counter SE attacks. This paper extends the work proposed by Charalambous and Stavrou (2023) by providing guidelines on how MPI can drive the design of effective SE awareness-raising policies.

## 4.2 Guidelines Towards Designing Effective Social Engineering Awareness-Raising Policies

Given that crafting a novel SE awareness-raising policy, which is envisioned to encompass educational content for raising security awareness while being packaged as a policy programme, it is essential to first investigate typical policy designs, how they are structured and what content needs to be included. Such an investigation can provide insights regarding gaps that need to be addressed to support the design of a SE awareness-raising policy.

### 4.2.1 Design Limitations of Security Policies

Security policies usually provide a set of statements covering what employees can or cannot do, actions to take in case of an incident and the procedures to verify compliance with the policy. Different types of security policies (e.g., Alharthi & Regan, 2021; CIS & MS-ISAC, 2019a, 2019b; Healthit.gov, 2018; ISO/IEC, 2022; SANS, 2022) can address the threat of SE attacks. From the investigations performed, a set of security policies was identified pertinent to: emails, passwords, internet usage, encryption, social media and internet postings, acceptable use, data classification, clean desk, access control, removable media, anti-malware tools, security event reporting, communications management, and software installation. Usually, these policies include statements relevant to the respective topic but do not provide a reference to the relevant SE attack(s). Also, as per the recommended guidelines (e.g., ISO/IEC, 2022; Steinmetz et al., 2023), the policy statements should be brief, concise, and clear. While this is an important aspect, these statements are usually generic rather than contextualized in the working environment of the workforce.

### 4.2.2 Human-Centred Security Policy Design

Considering the MPI model, a SE awareness-raising policy should adopt a human-centred approach. Such a policy should contextualize the problem within the specific industry the workforce is employed, in line with *Problem-centred* principle of MPI. This means that policy statements should not be generic but tailored to an organization's scope of work and aligned to the workforce's job responsibilities. Employees could better comprehend the policy when this is relevant to their working environment.

The structure and presentation of the policy can also play a significant role in helping people understand and relate with the policy's content. Arbitrary policy statements could not help people easily activate prior knowledge and experiences related to SE attacks. Following the *Activation* principle of MPI and informing employees in a structured approach on how SE attacks work in real life, could help activate prior knowledge and relate with the problem and the policy content. This aspect can be further enhanced through the MPI *Demonstration* principle. Storytelling scenarios could be utilized to present SE attacks that are relevant to the business environment and tasks. This can further contribute to better understanding the problem as employees can relate SE attacks with their work. A logical scenario sequence could be to name the attacks, outline the attack means, and then present short scenarios elaborating the lures, techniques, and impact, with a direct link to the policy statements and the expected response actions. These scenarios should be further tailored to cover different job roles. A diagrammatic format (e.g., using flow charts, tables, etc.) could aid the presentation of these scenarios. The proposed approach could make policy content more relevant to employees, aid their understanding, motivate them to accept and comply with policies, promoting an organizational culture of cyber situational awareness.

Organizations can consider the *Application* principle of the MPI model to confirm whether employees understood the problem, can adapt their knowledge in new situations and apply the policy accordingly. This can be achieved by presenting new attack scenarios to employees in the context of their work towards enhancing and assessing their knowledge and skills. Results can indicate whether further guidance and training are needed. Of course, the ultimate assessment would be in real conditions, considering MPI *Integration* principle. Lessons learned could inform policies' updates, and this



should be a continuous process, contributing towards an effective cybersecurity governance.

## 5 ASSESSING THE WORKFORCE'S SENSE OF SECURITY

A key challenge organizations face with regards to information security policies is the false sense of security (Stavrou, 2020) their workforce might display. Ignorance or lack of awareness can put an organization at immense risk as its employees may not consider the importance of applying policies, thinking that they are secure 'by default'. In this work, we deemed important to assess whether the employees: 1) knew if the organization applied security policies, 2) were aware whether the organization was applying security measures against cyber threats, 3) were familiar with a variety of SE attacks, 4) were implementing bad practices, and 5) recognized the need for continuous education about cyber threats. Results can provide insights to the organization on the extent that employees are feeling a false sense of security which can pose a great threat to the organization. If such a case occurs, the organization needs to take actions to increase awareness and training of employees to rectify the situation.

An assessment was performed in the context of a small organization which did not have any security policies in place. Forty four (n=44) employees responded to the questionnaire we administered with the objective to investigate their security awareness level and provide insights to design the organization's security policies. Initially, the emphasis was on the design of a SE awareness-raising policy.

The questionnaire first investigated whether employees had knowledge of the organization's security policies. The majority of employees (96%) responded that their organization has applied security policies. In reality, the organization did not have any security policies. Security policies are a core element of a cybersecurity strategy that guide the general workforce to protect the assets of an organization. Therefore, it is crucial for an organization to have a clear view of the employees' awareness level and their perception regarding implemented security measures. The result alerted the organization that realized that its workforce was having a false sense of security.

What is more alarming, was the employees' perception of implemented measures against SE attacks. Approximately half of the participants (52%)

reported they do not know the measures taken by the organization. Although this is acceptable as the organization did not implement something specific, the majority of the employees were certain that security policies were in place to protect the organization, including policies related to SE attacks. Another 16% reported that there are measures implemented, contributing to an elevated false sense of security across the organization's workforce. The rest of the participants (32%) reported that they do not actually know if measures are taken by the organization.

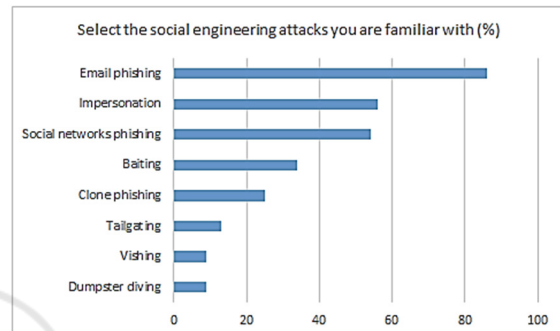


Figure 1: Investigating familiarity with SE attacks.

It was also important to assess employees' awareness level related to SE attacks. The organization did not offer any specific training related to SE attacks. A high percentage of employees (87%) reported that they did not participate in any training in the past. Only a small cohort (13%) reported attending such a training, probably in the context of their previous employment. Even though employees did not undertake a formal training, it was assumed that some of them may be familiar with different types of SE attacks, e.g., due to personal experience, awareness campaigns on social media, etc. As indicated in Figure 1, employees were mostly familiar with email phishing attacks and attacks delivered through social networks. Employees seem to be less aware of physical-related SE attacks such as dumpster diving, tailgating, etc. Moreover, it was significant that the assessment indicated that most employees were not familiar with vishing, an attack which is often utilized by cyber criminals.

Moreover, the questionnaire assessed whether bad practices are applied. Specifically, it was of interest to the organization to investigate whether the physical security could be easily compromised. This was indicated by the positive response of 37% of participants who declared that they share their access card with colleagues. This indicates that they do not realize the risk of physical security compromise, which is a typical SE attack scenario (tailgating).

Table 1: Proposed social engineering awareness-raising policy.

Social Engineering Attack	Means	Example of attack	Related policies													
			Email policy	Password policy	Internet usage	Encryption policy	Social media and internet postings	Acceptable use	Data classification	Clean desk	Access control	Removable media	Anti-malware policy	Security event reporting	Communications management	Software installation
Phishing *	Email, social media	Appendix A	x	x	x	x	x							x		
Smishing	Phone	Appendix B						x						x		
Vishing	Phone	Appendix C						x	x					x		
Tailgaiting	In person	Appendix D								x	x			x		
Dumpster diving	In person	Appendix E								x				x		
Shoulder surfing	In person	Appendix F								x				x		
Baiting	In person, Online	Appendix G							x			x	x	x		
BEC	Email	Appendix H												x	x	
Scare-ware	Online	Appendix I			x									x		X
* Phishing (spear phishing, whaling, clone phishing)																

\* Phishing (spear phishing, whaling, clone phishing)

A critical aspect related to mitigating a false sense of security, concerns the perception of employees related to the need for continuous education (Stavrou, 2023) about cyber threats. This aspect can be assessed through their perception about the awareness-raising and training frequency. A high percentage of participants (57%) reported that awareness-raising initiatives should occur once a year, about one in three (27%) indicated twice a year, and 16% answered just once. These results indicate that many employees may not realize the importance of life-long learning and continuous professional development (CPD) for staying up to date with the cyber threat landscape and the cyber hygiene practices that should be applied to protect themselves and their organization. Thus, it becomes imperative for organizations to take actions to help their workforce realize the importance of life-long learning and cultivate relevant skills using engaging learning methods (Piki et al., 2023).

## 6 PROPOSED SOCIAL ENGINEERING AWARENESS-RAISING POLICY

Typically, an organization should have several security policies as part of an information security management system (ISMS). At the top of the

hierarchy lies the enterprise security policy that sets the overall security objectives at a strategic level. This endeavour is supported by a set of other policies, covering different areas that are important to the organisation. These are called topic-specific policies. Moreover, system-specific policies can be specified to focus on a particular type of system, e.g., a firewall. This structure fits well with the purpose of the proposed SE awareness-raising policy which is linked to attack-specific security policies. The proposed policy will specify the SE attacks that are relevant to the business environment of the organization and which the workforce should be made aware of. In turn, the workforce is expected to demonstrate the ability to identify, protect, detect, respond, and recover from such attacks, in accordance to the CSF.

Considering ISO/IEC Control 5.27 “Learning from information security incident” and Control 6.3 “User awareness and training”, a new SE awareness-raising policy is proposed with two key design aspects that reflect the key guidelines provided by the controls as discussed above, in the Related Work section. One key design aspect focuses on the need to make the workforce aware of the different types of SE attacks, the techniques utilized to deploy such attacks, and the actions that should be taken to detect and respond to these attacks. The actions relate to the rules that the workforce needs to follow, and which can be listed across different security policies. This can be made evident to the workforce by mapping SE attacks to the relevant security policies implemented

by the organization. The aim is to empower employees to demonstrate resilience against malicious attempts that are elusively trying to collect sensitive information through various techniques to compromise the organization's infrastructure and impact its operations. Table 1 provides a potential list of SE attacks that can be relevant to an organization's business operation and indicates the means that can be utilized in each case. Appropriate attack scenarios can be provided in Appendices, demonstrating how these attacks can be implemented in an organization's context. The work performed by Charalambous and Stavrou (2023) provides guidelines on how to contextualize SE attacks in a healthcare ecosystem.

The second key design aspect relates to the provision of SE awareness-raising and the practices that the organization should implement. This is elaborated taking into consideration that small businesses might not have the budget to purchase third party training services. The lack of a security training budget does not mean that a business should not consider other cost-efficient actions, fortifying their workforce against SE attacks. This challenge is also highlighted in CIIS (2023) where respondents indicated that "those most at risk are people and organisations that do not have the resources to protect themselves [...] What it all shows is that protecting against the economic impact on security is a societal challenge. Like vaccination, the more people and businesses that are protected, the less opportunity there is for threats to breed or break out". Therefore, two SE awareness-raising levels are proposed to accommodate different situations when security budgets are limited and until resources are available. The provided guidelines are envisioned to enhance the guidelines provided under ISO/IEC 27002:2022 Control 6.3 – User awareness and training. Appropriate policy rules are expected to be spawned from this work's guidelines.

**Level 1 – Directed Reading Activity.** The IT/Security officer of the organisation should provide to employees an attack scenario from Table 1 and the related security policies. Employees are expected to read the attack scenarios to realize how a SE attack might be deployed in the context of their working environment. This is expected to help employees associate the policy rules with the problem and understand the benefit from applying them. Given that there are different examples of SE attacks that employees should understand, it is recommended to have weekly reading activities so that people have the time to relate to each case, process the provided information and increase the chance to retain the

developed knowledge. Following the completion of the reading activities, the IT/Security officer should launch brief assessments to confirm that employees can acknowledge which security policies are relevant to specific SE attacks. These can be in the form of quizzes or may embrace digital game-based learning approaches as proposed in Piki et al. (2023).

**Level 2 – Development of Tailored Awareness - Raising and Training Activities and Material.** This level should also take into consideration the attack scenarios and security policies provided in Table 1 to create engaging and effective awareness raising activities. The activities might be developed in-house (if there is expertise) or externally when there is a budget available. Moreover, the initial attack examples can be further tailored to specific departments and job roles to help people understand how attacks can be transformed given different business contexts.

An initial policy document was developed considering the proposed guidelines. The policy was delivered in a small company as part of a SE awareness-raising program. Following the awareness-raising activity (policy distribution across the workforce), a preliminary evaluation was performed to assess the key design aspect of the proposed policy – the tailored attack scenarios. Through a questionnaire all employees acknowledged that they better understood the policies through the provided real-life attack examples. Providing real-life attack examples in a security policy can help people to better understand the situation, compared to the case of just providing an attack definition. Various attack scenarios were also presented to the employees, receiving promising results which indicated that a high percentage (75%) of the workforce was able to recognize the attacks and to identify where to report the potential incidents. Evidently, the proposed intervention is considered an initial step towards increasing awareness on SE attacks and relevant policies implemented by an organization. It should serve as a complementary measure along with other interventions to contribute towards a workforce with solid cyber resilient capabilities against SE attacks.

## 7 CONCLUSIONS

The workforce's acceptance and adherence to cybersecurity policies is a critical factor that can contribute towards an effective organizational cyber



security governance. Organizations should consider different interventions to assist the workforce realize the nature of cyber threats, how attacks are delivered, the impact to individual safety and business operations, recognize what behaviours can put the organization at risk and what actions they need to apply when they are under attack. A common cyber threat that organizations and individuals are facing is SE. A typical approach to address SE attacks is to deliver awareness-raising training to empower and upskill the workforce. However, this should not be perceived as a solution that can be adopted by all organizations as this depends on different factors, with the economic aspect and lack of engagement being the most prevailing. Given that awareness-raising and training activities can complement the objectives of security policies, this should be taken into account to propose new interventions to empower small businesses that have limited budgets to increase awareness of their workforce. This work proposes the development of a social engineering awareness-raising policy, incorporating awareness-raising and educational principles alongside policy rules. The aim is to offer an open, cost-free baseline intervention that can help the workforce realize how SE attacks can be delivered in the context of their working environment and job role, better understand the objectives of specific security policies, identify and apply the relevant policy rules that can help in addressing SE attacks. Future work will expand upon the concept of delivering tailored SE awareness-raising and training initiatives.

## REFERENCES

- Aldawood, H., Skinner, G. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues, *Future Internet*, vol. 11, no. 3, p. 73.
- Aldawood, H. (2020). A Policy Framework to Prevent Social Engineering, 3rd International Conference Middle East and North Africa Conference of Information System, Casablanca, Morocco.
- Alharthi, D., Regan, A. (2021). A Literature Survey and Analysis on Social Engineering Defense Mechanisms and INFOSEC Policies, *Int. Journal of Network Security & Its Applications (IJNSA)* Vol.13, No.2.
- Charalambous, A., Stavrou, E. (2023). Building societal resilience against social engineering attacks: Unleashing the power of instructional design and microtargeting, 16th Annual International Conference of Education, Research and Innovation (ICERI).
- CIS, MS-ISAC. (2019a). NIST Cybersecurity Framework, SANS Policy Templates.
- CIS, MS-ISAC. (2019b). NIST Cybersecurity Framework, Policy Template Guide.
- CIS. (2023). Security Awareness Skills Training Policy Template, CIS Critical Security Controls. <https://www.cisecurity.org/insights/white-papers/security-awareness-skills-training-policy-template-for-cis-control-14>. (Accessed on 28/10/2023)
- CIIS. (2023). Chartered Institute of Information Security - The Security Profession 2022/23.
- ENISA. (2023). ENISA Threat Landscape 2023. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>. (Accessed on 28/10/2023)
- GOV.UK. (2023) Cyber security skills in the UK labour market 2023.
- Healthit.gov. (2018). Info Security Policy Template. <https://www.healthit.gov/resource/information-security-policy-template>. (Accessed on 28/10/2023)
- ISO/IEC. (2022). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection: Information security controls
- Kävrestad, J., Furnell, S., Nohlberg, M. (2023). User perception of Context-Based Micro-Training – a method for cybersecurity training, *Information Security Journal: A Global Perspective*
- Merrill, M. D. (2002). First principles of instructional design, *Educational Technology Research and Development*, vol. 50, no. 3, pp. 43–59.
- NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity
- Piki, A., Stavrou, E., Procopiou, A., Demosthenous, A. (2023). Fostering Cybersecurity Awareness and Skills Development Through Digital Game-Based Learning, 10th International Conference on Behavioural and Social Computing (BESC)
- SANS (2022). SANS Security Policy Templates. <https://www.sans.org/information-security-policy>. (Accessed on 28/10/2023)
- Smith, A., Papadaki, M., Furnell, S. M. (2013). Improving awareness of social engineering attacks, *IFIP Advances in Information and Communication Technology*, vol. 406, pp. 249-256.
- Stavrou, E. (2020). Back to basics: Towards building societal resilience against a cyber pandemic, *Journal on Systemics, Cybernetics and Informatics (JSCI)*, vol. 18, no. 7, pp. 73-80.
- Stavrou, E. (2023). Planning for Professional Development in Cybersecurity: A New Curriculum Design. International Symposium on Human Aspects of Information Security and Assurance (HAISA), UK.
- Steinmetz, K.F., Holt, T.J. Brewer, C.G. (2023). Developing and implementing social engineering-prevention policies: a qualitative study. *Security Journal*.
- Venkatesha, S., Reddy, K.R., Chandavarkar, B.R. (2021). Social Engineering Attacks During the COVID-19 Pandemic. *SN Computer Science*, vol. 2, no. 78.