A LITERATURE SURVEY AND ANALYSIS ON SOCIAL ENGINEERING DEFENSE MECHANISMS AND INFOSEC POLICIES

Dalal Alharthi and Amelia Regan

Department of Computer Science, University of California Irvine, Irvine, California

ABSTRACT

Social engineering attacks can be severe and hard to detect. Therefore, to prevent such attacks, organizations should be aware of social engineering defense mechanisms and security policies. To that end, the authors developed a taxonomy of social engineering defense mechanisms, designed a survey to measure employee awareness of these mechanisms, proposed a model of Social Engineering InfoSec Policies (SE-IPs), and designed a survey to measure the incorporation level of these SE-IPs. After analyzing the data from the first survey, the authors found that more than half of employees are not aware of social engineering attacks. The paper also analyzed a second set of survey data, which found that on average, organizations incorporated just over fifty percent of the identified formal SE-IPs. Such worrisome results show that organizations are vulnerable to social engineering attacks, and serious steps need to be taken to elevate awareness against these emerging security threats.

KEYWORDS

Cybersecurity, Social Engineering, Employee Awareness, Defense Mechanisms, Security Policies

1. INTRODUCTION

Information security threats can be divided mainly into two types: technical hacking and social engineering attacks. In technical hacking, cyberattackers conduct attacks using advanced techniques to gain unauthorized access to systems. However, it is difficult for hackers to successfully attack computer systems and networks using purely technical means [1]. Therefore, hackers rely on social engineering attacks to bypass technical controls. Social engineering enables attackers to gain unauthorized access to systems by psychologically manipulating users. [2], [3]. Compared to technical hacking, social engineering is generally an easier, cheaper, and more effective way to gain unauthorized access to confidential information.

Numerous previous research efforts have demonstrated the success of social engineering attacks [4], [5], [6], [7], [8]. Social engineering attacks are conducted either by person-to-person interaction (in person or over the phone) or by computer-interaction (email, pop-up window, instant message, or malicious website). Social engineers target individuals, organizations, and countries as well. Since the consequences of social engineering attacks are severe and hard to detect, employees and organizations need to be aware of the defense mechanisms that can protect against such security attacks. Mouton et al. in [9] outlined the importance of increasing the employees' awareness level against social engineering attacks.

Social engineering attacks have significant impacts on organizations. The damage can be devastating. Social engineers are looking for the easiest way into the organization systems, which is not to try and break the encryption on the organization database or type in every combination

DOI: 10.5121/ijnsa.2021.13204

of characters to guess their employees' passwords. Often, the easiest way is to trick employees into giving them the keys. Hence, social engineers aim to exploit the weakest link in a security structure by manipulating individuals and organizations to divulge valuable and sensitive data [10]. Social engineering attacks use many different techniques including, but not limited to, Business Email Compromise (BEC) and phishing in all its variations such as vishing (by voice), smishing (by SMS), and pharming (via malicious code) [11] [12]. According to [13], successful social engineering has overwhelmingly negative impacts on an organization such as data losses, financial losses, lowered employee morale, and, decreased customer loyalty. In some cases, even legal and regulatory compliance issues could result.

Due to the COVID-19 outbreak, the number of people working remotely has grown dramatically and there has been a corresponding uptick in sophisticated social engineering attacks. Under such conditions, as employees adapt to unfamiliar work environments away from the office, new coronavirus-themed phishing scams are leveraging fear, hooking vulnerable people, and taking advantage of workplace disruption [14] [15]. Organizations must ensure that their employees understand the risks of social engineering and how to avoid becoming a victim. [16] emphasized the need to adopt measures and tools, including policies and training programs, to mitigate the risk of social engineering attacks.

Additionally, recent security research [17] suggests that most organizations have unprotected data and poor social engineering cybersecurity policies in place, making them vulnerable to data loss. To successfully fight against social engineering attacks, organizations must develop and adopt Information Security Policies (ISPs). [18] defined an information security policy (ISP) of an organization as a set of rules and policies related to employee access and use of organizational information assets. Unfortunately, the research lacks well designed formal Social Engineering InfoSec Policies (SE-IPs) that organizations can adopt to protect their assets in the cyber-world.

Even though preventing social engineering attacks is crucial for organizations and countries, unfortunately, the research lacks a well-designed taxonomy of the defense mechanisms against the ever-increasing types of social engineering attack vectors. To fill this research gap, this paper provides a taxonomy of the main target points of social engineers and the defense mechanisms against various social engineering attacks and measures employees awareness level of social engineering defense mechanisms. Further, it proposes a customizable model of formal SE-IPs in organizations and measures the incorporation level of those SE-IPs in organization.

The taxonomy developed in this study will help researchers, practitioners, and organizations understand the defense mechanisms for social engineering security attacks. Organizations can use the taxonomy to elevate the awareness level of their employees about and hence better protect their organizations and their information. In addition to the taxonomy, the authors also measured employee awareness of specific social engineering defense mechanisms. To that end, the authors developed a questionnaire consisting of 48 items, then surveyed 791 employees in various public, private, and non-profit organizations in Saudi Arabia. The authors then designed, distributed, and analyzed a survey to investigate the incorporation level of SE-IPs in organizations. Then, considering the survey results as well previous work [2], [19], and [20], the paper developed a proposed model of SE-IPs that organizations can adopt.

To summarize, the authors' key contributions to this research are fourfold. The authors developed a well-designed taxonomy of the main social engineering target points along with their defense mechanisms. Then, the paper proposed a customizable proposed model of formal SE-IPs that organizations can adopt. The authors designed two survey instruments, the first one can be used to measure employee awareness of social engineering defense mechanisms, and the second one can be used to measure SE-IPs incorporation level in an organization. The authors surveyed employees in various employment sectors, then analyzed the results and reported them. Additionally, the authors made the dataset available online for researchers and practitioners in the field of cybersecurity to replicate or extend the work.

The remainder of this paper is structured as follows. Section 2 provides the necessary background for this study and presents the related research efforts on social engineering attacks against organizations. Section 3 describes the research questions this paper tries to answer. Section 4 describes the methodology for surveying the employees. Section 5 describes the taxonomy in detail. Section 6 analyzes the data collected in two survey instruments and describes the results. Section 7 calculates and describes the employees' awareness level against the various social engineering defense mechanisms. Section 8 proposes a formal SE-IPs that organizations can adopt to mitigate the risk of social engineering attacks. The incorporation level of SE-IPs in organizations is addressed in Section 9. Finally, the paper concludes with future work avenues.

2. RELATED WORK

A wide range of research efforts focuses on purely technical security attacks, while fewer researchers have focused on social engineering attacks. This section discusses the research efforts that are closely related to this study.

In 2017, Elnaim et al. [22] conducted an experimental study at Prince Sattam Bin Abdulaziz University in Saudi Arabia to examine students' familiarity with social engineering threats. The study revealed that 72% of the surveyed university students were not familiar with the term "social engineering". Another recent experimental study was conducted in 2016 by Happ et al. [23] to measure people's awareness level in Luxembourg. The authors asked 1,208 participants about their attitude towards computer security, and they also asked them about their passwords. The interviewers were carrying the University of Luxembourg bags, and they were unknown to the participants. The participants were divided into two groups: Group#1 and Group#2. Participants of Group #1 were given chocolate before being asked for their password. Whereas participants of Group#2 were given chocolate after the survey. The results revealed that a small gift could significantly increase the likelihood that participants will give their password. In Group#1, 47.9% of them revealed their passwords for a bar of chocolate while in Group#2, 29.8% of them shared their passwords. Medlin et al. [33] conducted a study to analyze the vulnerability of U.S. hospitals to social engineering attacks. Employees who volunteered to complete the survey were rewarded with both candy and a chance to win a gift card. Within the questions, employees were asked to reveal their passwords and some other confidential information. Surprisingly, 73% of the respondents shared their passwords, which raised serious concerns about the state of employees' awareness of social engineering attacks on our health care system.

Krombholz et al. [23] illustrated some real-world examples of social engineering attacks against major companies including the New York Times, Apple, Facebook, Twitter, and the RSA Network Security LLC company. In 2013, social engineers targeted the New York Times. The initial attack was a Spear Phishing attack, which sent fake FedEx notifications. Then, the New York Times hired computer security experts to analyze the attack, and they found that some of the methods used to break into the company's infrastructure were associated with the Chinese military, i.e., were linked to a political motive. Because of this SE attack, social engineers stole the passwords of some employees in The New York Times, and hence, they were able to access the personal devices of 53 employees. Moreover, in 2011, a small number of RSA employees received an email entitled "2011 Recruitment Plan". The email was professionally written, and the readers were convinced that it was legitimate. The email contained a spreadsheet that contained a malicious payload to exploit a vulnerability on the user's device. This SE attack led to the theft of sensitive information from the RSA Secure ID system.

Aldawood and Skinner [21] suggested a few methods to be followed by organizations to reduce the effect of social engineering attacks and to educate their employees about that. These are Serious Games, Gamification, Virtual Labs, Simulations, Modern Applications, and Tournaments. The serious game is a method that allows employees to face real-time scenarios with an opportunity to use their knowledge to implement mitigation strategies. Similarly, an organization can use Gamification to assess the behavior of hypothetical victims of social engineering attacks. The use of a remote online network is another method known as Virtual Lab, which helps trainees to learn about threats of social engineering via virtual solutions. Simulations can be used as models of real scenarios to evaluate various social engineering attacks. Additionally, Modern Applications that rely on the use of software application training and learning modules can be used to assess different types of social engineering threats. Furthermore, between multiple organizations, tournaments can be constructed to engage employees, i.e., communication threats competitions.

Ghafir et al. [24] emphasized the significance of adopting a multi-layer defense, also referred to as defense-in-depth to lower the risk associated with social engineering attacks. They showed that a good defense-in-depth structure should include a mixture of security policy, user education/training, audits/compliance, as well as safeguarding the organization's network, software, and hardware. The paper also illustrated four steps of social engineering which are information gathering, developing relationships, exploitation, and execution.

Chitrey et al. [35] developed a model of social engineering attacks. The model categorized social engineering attacks under two main entities: vulnerable entities which are human, technology, and government laws, and safeguard entities which are information security awareness programs, organizational security policies, physical security, access control, technical control, and secure application development. Such a model can be used in the development of an organization-wide information security policy.

Siadati et al. [36] performed a social engineering attack to measure people's awareness level of SE attacks regarding the two-factor authentication mechanism. The experiment showed that 50% of users forwarded their authentication code to attackers. The researchers then developed principles for designing abuse-proof verification messages to reduce the susceptibility of users in forwarding the verification code to the attacker. This robust messaging approach reduced the percentage to only eight percent, or a sixth of its success against Google’s standard second-factor verification code messages.

Gupta and Sharman [25] proposed a framework for the development of a Social Engineering Susceptibility Index (SESI) based on social network theory propositions. The framework reveals the real risks of social engineering attacks that employees are exposed to. The framework suggested five indices which are social function, organizational hierarchy, organizational environment, network characteristics, and relationship characteristics.

Beuran et al. [38] used the main cybersecurity training programs in Japan as a detailed case study for analyzing the best practices and methodologies in the field of cybersecurity education and training. The paper defined a taxonomy of requirements to ensure effective cybersecurity education and training. The taxonomy has two main aspects, which are training content and training activities. As far as the training content, there are three main categories, which are attack-oriented training, defense-oriented training, and analysis/forensic-oriented training. Another perspective on cybersecurity training is considered to focus on security-related activities that include individual skills, team skills, and Computer Security Incident Response Team (CSIRT) skills.

According to [27], a combination of technical, social, economic, and psychological factors impact an employee's decision-making process when contemplating whether to comply with or ignore the terms of information security policies. A social engineer might rely on some principles to raise the effectiveness of the cyberattack, such as authority, intimidation, consensus, scarcity, familiarity, trust, and urgency. According to [1], trust, authority, and fear are contributing to the success of social engineering attacks. These internal pressures can be exploited by social engineers to achieve certain purposes, such as encouraging someone to share sensitive information that they probably should not. Additionally, when someone does something nice to us, we automatically feel obliged to return the favour [23]. Risky-shift is another critical factor that was coined by James Stoner in 1961 [28]. It occurs when an employee (as part of a team) tries to make decisions about the risk associated with the use of information technology which is different from when he is using his personal devices. At a personal level, employees tend to be more careful about their data. In contrast, when working as a team, they are more likely to make riskier decisions.

Network administrators employ a variety of security policies to protect data and services. [30] conducted a study to propose an information security policy process model for organizations. The proposed model suggests that a security governance program together with the organization’s information security office, an ongoing process of interrelated policy management activities, and the proper gauging of key external and internal influences together contribute greatly to the success of information security policies. Thus, a critical element to any organization cybersecurity program is having security controls and policies in place which are customized for their environment. [31] conceptualized and developed three dimensions of (maritime) port cybersecurity hygiene (i.e., human, infrastructure, and procedure factors), and investigated the relationships between port cybersecurity hygiene and cyber threats (i.e., hacktivism, cyber criminality, cyber espionage, cyber terrorism, and cyber war). The results indicated that organizations tended to encounter hacktivism when their human, infrastructure, and procedure factors were vulnerable. Hence, the provision of training and education to all workers, including top executives, managers, and supervisors, is necessary to ensure a cyberthreat-awareness culture at all organizational levels. Through cybersecurity awareness training, users are brought up to speed on an organization’s IT security procedures, policies, and best practices. [32] conducted an experimental study to assess end-user awareness of social engineering and phishing using a web-based survey, which presented a mix of 20 legitimate and illegitimate emails. The messages were categorized according to various characteristics of their appearance, all of which recipients may potentially use to aid their decision about whether to trust the content or not: identifiable recipient, identifiable sender, im- ages/logos, untidy layout, typos/language errors and URL/link. Participants were asked to classify them and explain the rationale for their decisions. This assessment showed that the 179 participants were 36% successful in identifying legitimate emails, versus 45% successful in spotting illegitimate ones. Additionally, in many cases, the participants who identified illegitimate emails correctly could not provide convincing reasons for their selections. According to [33], when employees are aware of their company information security policies and procedures, they are more competent to manage cybersecurity tasks than those who are not aware of their company policies. This result was based on a survey of 579 business managers and professionals after employing Structural Equations Modelling (SEM) and ANOVA procedures on the results. In contrast, [29] indicated that despite state-of-the-art cybersecurity preparation and trained personnel, hackers are still successful in their malicious acts that obtain sensitive information that is crucial to organizations.

Thus, a key concern of organizations is the failure of employees to comply with information security policies (ISPs) [34]. However, forcing individuals into compliance might trigger undesired behaviors. [35] conducted research to study determinants of early conformance toward technology-enforced security policies. The model was tested with 535 respondents from a university that implemented new password policies. The results showed that a positive attitude toward a mandatory security change leads to greater intention to comply. [18] addressed the fact that social norms related to ISPs are the product of the principle ethical climate in an organization. The study explored the role of norms in employees' compliance with an organizational information security policy (ISP) and proposed a model to examine how ISP-related personal norms are developed and then activated to affect employee's ISP compliance behavior. The results showed that ISP-related personal norms lead to ISP compliance behavior, and the effect is strengthened by ISP-related ascription of personal responsibility. Social norms related to ISP (including descriptive, injunctive and subjective norms), awareness of consequences, and ascription of personal responsibility shape personal norms. Moreover, [36] explained the issue of employees' InfoSec noncompliance that causes the majority of organizational InfoSec breaches. When InfoSec policy (ISP) is implemented, it counteracts breaches and various approaches attempted to mitigate the phenomenon of ISP non-compliance. Yet, those approaches assume that employees will passively com- ply after they are enforced, and overlooked that human feelings, behaviour, and thoughts can affect the decision on whether to comply with the ISP. However, the ISP generates a new institutional logic featuring practices that collide with the existing institutional logic. This collision represented critical changes that are perceived as threats because the ISP values embedded in the practices are contrary to the employees' practices. These value changes significantly impact ISP non-compliance because the employees' values are misaligned with the ISP values.

In the context of enforcing an ISP, [37] suggested a simple enforcement system using a Software Defined Network (SDN) controller to block the malicious and restrict the anonymous users in the organization network. They presented a fully configurable system for an institution using POX which is a famous SDN controller. A security policy can be enforced, accessed, and controlled through it. So that a single change in policy will be reflected in all the OpenFlow switches attached to the SDN resulting in reduced cost and time, as compared to the conventional networks where each switch is managed individually.

To ensure the implementation of the organization InfoSec policies, penetration testing is required. [37] suggested two methodologies for physical penetration testing using social engineering which aims to reduce the impact of the penetration test on the employees. These two methodologies are custodian-focused (CF) and environment-focused (EF). Custodian means the employee in possession of the assets, sets up and monitors the penetration test. In EF methodology, the custodian is aware of the penetration test, which makes it more realistic, but less reliable. It does not deceive the custodian and fully debriefs all actors in the test. In the CF methodology the custodian is not aware of the test, making the methodology suitable for penetration tests where the goal is to check the overall security of an area including the level of security awareness of the custodian.

In addition, to increasing the employees awareness level of social engineering, as well as incorporating and enforcing InfoSec policies, organizations should have a disaster recovery plan that describes scenarios for resuming work quickly and reducing interruptions in the aftermath of a disaster. The significance of an organized planned disaster management strategy to overcome unexpected event and help to recover was emphasized by [37]. [39] suggested engaging the public in planning for disaster recovery, which will lead to increased stakeholder awareness of risk, available resources, and support for policies that build resilience.

3. RESEARCH QUESTIONS

Social engineering attacks challenge the security of all networks regardless of the robustness of their firewalls, cryptography methods, intrusion detection systems, and anti-virus software systems [40]. Because social engineering is such a threat in today workplace, it is vital to increase employees awareness level of such attacks and incorporate and enforce security policies in organizations to keep organization's networks safe from such attacks. To that end, this section presents the research questions this study tries to answer four questions, which are (RQ1) What are the main defense mechanisms against social engineering attacks that employees and organizations should be aware of?, (RQ2) What is the current employees' awareness level of social engineering defense mechanisms?, (RQ3) what are the formal SE-IPs that should be incorporated in organizations?, And (RQ4) what is the current level of formal SE-IPs incorporation in organizations?

4. RESEARCH METHODOLOGY

4.1. Building the Taxonomy of Social Engineering Defense Mechanisms

To develop the taxonomy, the authors followed a systematic literature review as well as the SANS institute guidelines. Below is a brief description of each one.

4.1.1. Systematic Literature Review (SLR)

To develop a taxonomy of the defense mechanisms of social engineering attacks, the authors followed a Systematic Literature Review (SLR) technique as recommended by Okoli and Schabram in [41]. To do that, the authors conducted a literature review of recent journals and conference papers that contained "social engineering" in their title. Then, extracted the target points of social engineers and any suggested defense mechanism from each paper.

4.1.2. The SANS Institute

SANS (SysAdmin, Audit, Network, Security) Institute is a private company based on the United States founded in 1989. SANS is the largest source for cybersecurity training in the world. It provides guidelines that organizations need for rapid development and implementation of information security policies. These guidelines are divided into four categories: general category, network security, server security, and application security. To build the taxonomy, the authors followed some of the guidelines in the SANS InfoSec Policies and SANS Awareness Survey.

4.2. Measuring Awareness Level Methodology

To measure the awareness level of employees in public, private, and non-profit organizations, the authors designed a questionnaire, distributed it to a large number of employees, and then analyzed the collected data. To build the questionnaire, the authors relied on the developed taxonomy, the Human Aspects of Information Security Questionnaire (HAIS-Q) [26], SANS Awareness Survey, and the Essential Cybersecurity Controls created by the Saudi National Cybersecurity Authority in 2018 [42]. The resulted questionnaire consists of 48 questions. To distribute the questionnaire, the authors used SurveyMonkey [43], an online cloud-based survey service, to publish and distribute the survey. The participated organizations have different sizes, belong to different sectors, and are geographically distributed over 13 regions of Saudi Arabia to allow a diverse and representative sample. The questionnaire can be used by organizations to measure the awareness level of their employees against various social engineering defense mechanisms. The average time to complete the survey is 7 minutes.

4.3. Surveyed Employees

Over several months, the survey was received by thousands of employees either through their organizations or directly from us over email or social media accounts. Reminders were sent also to remind the employees to answer the survey. In the end, 1523 employees in various public, private, and non-profit organizations in Saudi Arabia participated in the survey.

4.4. Selected Country

As a case study, this research focuses on public, private, and non-profit organizations in Saudi Arabia. According to the Saudi General Authority for Statistics, the Saudi population was 34.2 million in 2020 [44]. And according to The Statista Portal [45], the number of Internet users in Saudi Arabia is increasing rapidly, reaching about 89% of the population in 2020, which increases the need for enhanced cybersecurity awareness to defend sensitive information in cyberspace. The authors selected Saudi Arabia as a country of this study for the following reasons. Saudi Arabia is the most targeted country in the Middle East and North Africa (MENA) region. For example, in 2012, over 35,000 of Aramco computers were infected by a virus called Shamoon, which operated like a time bomb (logic bomb malware). These devices were partially wiped or totally destroyed [46], [47], [48]. Saudi Arabia designed and sponsored many governmental programs to prevent cybersecurity attacks as well as to increase the awareness level of its employees regarding cybersecurity. According to the Global Cybersecurity Index (GCI) created by the UN International Telecommunication Union (ITU) [49], Saudi Arabia achieved ranking first at the Arab level and 13 at the global level out of 175 countries for its commitment to cybersecurity. This paper is an extension of the research work in [11], [19], and [20], which used the same sample for a related survey but had a lower response rate.

4.5. Measuring the Incorporation of Formal SE-IPs

To measure the level of SE-IPs incorporation, the authors carefully designed a survey instrument. To build the survey, the authors relied on the taxonomy of social engineering defense mechanisms [11] and the resulting survey consisted of 30 questions 9. The survey was distributed using SurveyMonkey [43], an online cloud-based service, to publish and distribute the survey. The participating organizations have different sizes, belong to different sectors, and are geographically distributed over 13 regions of Saudi Arabia to allow a diverse and representative sample. The questionnaire can also be used by organizations to measure their incorporation level of SE-IPs. The average time to complete the survey was 6 minutes.

4.6. Developing a Formal SE-IPs Model

To develop the SE-IPs, the authors relied on the Taxonomy of Social Engineering Defense Mechanisms [11] as well as the results of the survey. Additionally, the authors developed a Systematic Literature Review of recent studies published on the subject. The literature review examined recent journals and conference papers that contained “Social Engineering”, “Cyber Attacks/Threats”, and/or “Information Security Policies” in their titles. The authors then extracted Social Engineering InfoSec Policies (SE-IPs) from each paper.

5. TAXONOMY OF SOCIAL ENGINEERING DEFENSE MECHANISMS

To answer the first research question, RQ1 (What are the main defense mechanisms against social engineering attacks that employees and organizations should be aware of?), the authors conducted a thorough investigation of the literature and found that there are five main target points for social engineers.

Social engineers try to achieve their malicious goals through these five target points, which are the main assets of any organization. These five target points are People, Data, Software, and Hardware (SW/HW), and Networks. Figure 1 depicts a tree-structure taxonomy of the main target points and the defense mechanisms for each target point.

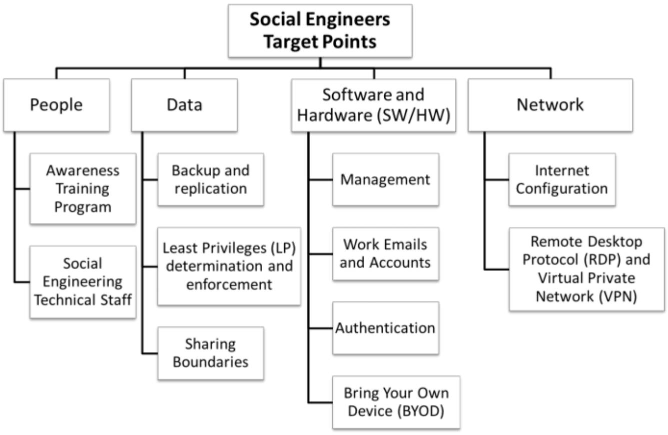
Social Engineers Target Points
People
Data
Software and Hardware (SW/HW)
Network
Awareness Training Program
Social Engineering Technical Staff
Backup and replication
Least Privileges (LP) determination and enforcement
Sharing Boundaries
Management
Work Emails and Accounts
Authentication
Bring Your Own Device (BYOD)
Internet Configuration
Remote Desktop Protocol (RDP) and Virtual Private Network (VPN)

Fig1. Social Engineering Defense Mechanisms

Next, the paper provides a description of each target point and the defense mechanisms against social engineering attacks targeting these target points.

- **People (Employees):** Social Engineers target organizations' employees using social intelligence techniques to convince them to perform tasks that they should not do, such as giving their passwords or sharing private data, etc. To protect this asset, organizations should consider (1) educating their employees periodically and (2) hiring IT technical staff knowledgeable of social engineering security attacks.
- **Data:** Data is a valuable asset for any organization, and it is a critical target point for cyber attackers either at the personal level or at the organizational level. To defend this asset, organizations need to (1) perform backup and replication to their data periodically, (2) determine the minimum information each employee and system needs to perform their tasks and grant only that information to that employee or system, and (3) create clear security policies to identify the sharing boundaries of the information so employees would know what to share and with whom.
- **Software and Hardware (SW/HW):** Organizations should educate their employees about the importance of the hardware and the software of their organizations. To secure organizations' equipment and systems against social engineering attacks, the organizations need to educate their employees regarding (1) the management process of the organization's hardware and software, (2) work emails and accounts, (3) any authentication policy, and (4) the Bring Your Own Device (BYOD) policy.
- **Network:** Employees access databases and other servers through a network. Each network has a different security policy. Most organizations nowadays allow VPN (Virtual Private Network) or RDP (Remote Desktop Protocol) to allow their employees to access the local network remotely. To protect organizations' networks from potential social engineering attacks, employees should be aware of the different Internet configurations as well as the different network security policies regarding the VPN and the RDP.

6. RESEARCH ACHIEVEMENTS

6.1. Questionnaire I: Measuring Employees Awareness Level of Social Engineering Defense Mechanisms

In light of the taxonomy of social engineering defense mechanisms illustrated in Figure 1, the authors carefully designed a survey and distributed it among employees working in public, private, and non-profit organizations in Saudi Arabia. The survey has a total of 48 questions. The average time to complete it was about 7 minutes. 791 employees responded to the authors' calls and answered the survey. The sample represented a wide range of ages. Approximately 1% of the participants are less than 20 years old, 18% are from 20-29, 42% from 30-39, 25% from 40-49, 11% from 50-59, and 3% of the participants are 60 and above years old. Regarding the qualifications of the participants, 89% of the employees have at least a Bachelor's degree. Nearly half of the employees, 48% of them, earned a degree in an IT field. Furthermore, as far as their usage of the Internet, 71% of the employees use it for more than three hours daily. Moreover, 61% of the participants work for the government, 30% of them work in private sectors, and 9% of them work in non-profit organizations. 80% of employees' organizations have an Information Technology (IT) department/center and 26% of these IT departments have a separate cybersecurity team. Participants have various job titles and work at different levels in the organizational structure. After distributing the survey, the authors collected the data and performed an analysis. This section sheds light on some of the interesting results and findings from the survey. Regarding the employees' awareness of social engineering attacks and their defense mechanisms, the survey found that 45% of the employees mistakenly think that they are not targeted by cyberattackers. 84% of the participants were overconfident and stated that their work computers are very secure. Approximately 45% of the participants stated that they can tell if their work computer is hacked or infected. 36% of the employees have found a virus on their work computer at least once, and 22% of them were not sure whether their work computers were infected or not. Additionally, 27% of the participants' accounts have been hacked or stolen at least once. The participants were asked to write about these incidents. The authors found that different platforms such as personal and work computers, bank accounts, credit card information, personal and work emails, social media account, etc., have been hacked or stolen. While the reasons behind some of these incidents were unknown, other incidents were due to phishing emails, downloading malicious email attachments, not using multi-factor authentication, shoulder surfing, blackmailing for money (Ransomware), providing credential informing to unsecured websites, or not updating their Anti-virus tools. Interestingly, in some reported incidents, social engineers acted as IT technicians who came to the victims' offices to repair their computers. While some of these incidents were solved, others have not been solved due to many reasons including that social engineers have changed the password of the stolen accounts. Additionally, 39% of the participants received a phone call requesting personal information from someone they do not know, and nearly 60% received emails requesting personal information from someone they do not know. 40% of the employees indicated that they are not familiar with the term "phishing attack". From those employees who are not familiar with the phishing attacks, 77% of them received emails and 8% of them received phone calls requesting their passwords. When it comes to scam emails, only 42% of the participants are aware of them. Regarding password protection, 28% of the employees have been asked about their passwords from co-workers and 24% of them have disclosed the password of their work-related accounts to someone else. These dangerous numbers show that organizations are vulnerable to social engineering attacks. Surprisingly, the authors found that 66% of the employees read/open spam emails. This percentage, if generalizable, means that more than half of the employees are vulnerable to phishing, spear phishing, and other social engineering attacks. As far as opening email attachments, only 54% of the employees are careful and reluctant to open the contained attachments, while the rest are not. 66% of the employees do read or open spam emails. Based on these results, organizations' computers can be easily infected with malicious software or viruses. The participants were asked also if their organizations have security policies accessible to the employees. Only 22% of the employees know/understand those policies. Contributors were asked if they know who to contact in case their work computers hacked or infected. Only 66% of them answered "Yes" whereas the rest do not know what to do in such cases. Moreover, the survey revealed that only 58% of the organizations have Information Exchange Policies (IEPs). Nearly, half of the Saudi employees follow their instincts regarding information exchange. The participants were asked the following question "If you receive an unusual request from your boss or a co-worker via email, such as sending sensitive information to an unknown email, what do you do?". 59% of them would send the email right away. Only 41% of the employees stated that they would not send sensitive information to an unknown email. About passwords construction and protection, 34% of the participants use the same password for all their work accounts, and 23% of them use the same password for their work accounts and their personal accounts as well. Contributors were asked about any regular security maintenance of their work computers. Specifically, the authors asked if they have anti-virus or not and if that anti-virus tool is up-to-date or not. To that end, 61% of them claimed that they have up-to-date anti-virus software, while the rest were divided evenly between having an outdated anti-virus and not knowing if they even have an anti-virus tool or not. The participants were also asked if the firewall is enabled on their work computers. 62% of them answered "Yes", while the rest do not know if they have a firewall or not. 63% of the employees stated that their work computers are configured to automatically update the operating system. On the other hand, 8% of the contributors store their personal data such as their bank's credit card numbers on their computers. 54% of them do not check if the accessed website is secure (HTTPS) or not before signing in. Only 44% of the employees have never clicked on a link that looks malicious whereas the rest click on all links even the ones that look malicious or contained in strange emails. Moreover, the data analysis of the survey revealed that 39% of the employees have downloaded and installed software on their work computers. 38% of the employees are using their own personal devices, such as their mobile phones and laptops to store or transfer confidential organization's information. 94% of the employees perform work-related tasks on their personal devices and 40% of them do that daily. And while 19% of the participants have logged into work accounts using public computers, only 20% of them use VPN to do so. As far as the network security policies, only 34% of the participants declared that their organizations have policies about which websites they can and cannot visit while at work and they are aware of such policies. The rest, 66%, were divided evenly between not knowing the policies or not having them from the first place. Participants were asked a similar question to determine whether they can access their social media accounts, such as Twitter and Facebook, using their work computers and 33% of them answered "Yes". The employees were also asked if their organizations have clear policies about the use of their work emails. While 39% of the participants stated that there are such policies, and they are aware of them, 18% indicated that there are such policies, but they do not know them and 22% indicated that there are no policies regarding the work emails and you are free to use them as a personal email. The participants were also asked three questions about the boundaries to share information within and outside their organizations. The survey revealed that 59% of the employees know what type of information they can exchange with other co-workers on the same or different departments within their organizations, with other employees from different organizations, and share information publicly. 41% of the employees are not aware of any regulations about that and they just follow their insects when it comes to sharing information. Moreover, the survey revealed that only 25% of the participants know that their organizations have cybersecurity policies that he should read and follow. 34% of the employees stated that the cybersecurity policies in their organizations are not clear or not accessible to everyone, and 44% of them do not know if their organizations have security policies or not. Another question asked to determine the existence of any social engineering awareness training programs offered by their organizations. In response to this question, 33% of the employees answered "No", and 33% of them are not sure if there are such training sessions.

6.2. Questionnaire II: Measuring SE-IPs Incorporation Level

The survey has a total of 30 questions. The average time to complete it was 6 minutes. 1523 employees responded to the survey. The sample represented a wide range of ages. Approximately 1% of the participants are less than 20 years old, 16% are from 20-29, 40% are from 30-39, 26% are from 40-49, 14% are from 50-59, and 3% of the participants are 60 and above years old. 60.44% of the participants work for the government, 36.29% of them work in the private sector, and 3.27% work in the non-profit sector. The authors asked the participants about the department that they are working in. Only 30.62% of them work in IT department. After distributing the survey, the authors collected the data and performed an analysis. This section sheds light on some of the interesting results and findings from the survey. Regarding the participants' cybersecurity knowledge and behaviour, one of every two employees mistakenly believes they are not a target for cyberattackers. The result showed that only 49.17% of participants think that their work computer would be valuable for hackers/social engineers. Additionally, only 33.42% of organizations have a cybersecurity awareness training program for their employees. Moreover, when suspecting that a theft, breach, or exposure of organizations protected data has occurred, only 70.31% of employees feel comfortable notifying the appropriate team in their organizations. However, 48.03% of them responded that they do not have an email address specifically assigned for reporting phishing emails. In regards of the existence of a Data Protection Policy, the authors asked some questions about a data backup policy, an information sharing policy, and transmitting, storing, labelling, and handling sensitive information. The results illustrated that only 47.70% of computerized systems save backups of the employees' work. 60.11% of employees do backup their work using USB and/or cloud storage periodically, and 84.66% of them do not encrypt their work-related files. Moreover, only 25.75% of the participants addressed that their organizations have policies regarding what not to discuss over phone calls with your colleagues (i.e., organization information that is too sensitive to be discussed over phone). Additionally, only 21.88% of organizations have policies regarding verifying who is on the other end of the phone call. The survey showed also that only 42.23% of organization have policies regarding transmitting, storing, labelling, and handling sensitive information within/outside the organization. After that, a question was asked about having policies regarding transferring organizations data to a personal email account, i.e., sending a work-related email to a personal email account. Only 38.56% of organizations have those policies. Additionally, a question was asked regarding a Removable Storage Policy. Only 42.49% of employees addressed that they must have an approval before using any portable storage device on your work-computer (such as USB/external hard drive). To summarize data protection related results discussed above, 60.11% of employees do backup their data, 38.56% forward work emails to their personal emails, and 42.49% of them use external storage devices to store organization data. Hence, employees can take their organization data with them upon their departure, which raises the risk of data loss in organizations. Other survey questions were asked regarding hardware/software (HW/SW) protection policies. 60.31% of employees addressed that their work-computer is current with virus protection and software patches. Moreover, the survey showed that only 55.17% of organizations grant the access to IT services and infrastructure under the principle of least privilege. The authors also asked employees if they are required to request an approval prior to installing software to their work-computer. Only 64.38% of organizations have policies regarding that, which means that 35.62% of organizations are susceptible to downloading copyrighted software, offensive material, or files that are infected with harmful computer viruses. Regarding Password Policies, 73.58% of organizations have password creation requirements/guidelines, and

65.18% of them enforce employees to change their passwords periodically. 31.02% of employees addressed that they use the same pass- word for their work-related accounts as their personal online accounts. The survey asked some questions regarding a Mobile Device Policy. Only 42.29% of organizations have a Bring Your Own Device (BYOD) Policy, while 46.50% of them allow their employees to store work-related data via mobile device such as iOS and/or Android. However, 52.91 % of employees reported that they do not regularly patch their phones OS within 90 days of the new OS release, which can lead to cyberattacks. Regarding Internet Usage and Social Media Policies. Only 66.91% of organizations block access to some internet websites and services when using work-computer, the rest allow their employees to have an unlimited access to internet websites including websites that may be harmful and dangerous. Additionally, 66.31% of organizations do not have a Proxy/URL Configuration Policy, and employees in those organizations can access social media without applying for proxy exception. 38.96% of employees have logged in their work-related accounts using public WiFi, such as from a cafe shop or a hotel lobby. Using public WiFi can lead to cyber-risks such as Man-in-the-Middle, malware distribution, snooping and sniffing. While using VPN services can help establish secure and encrypted connections, only 38.23% of participants addressed that they use it when transmitting organizations data or accessing organizations resources remotely.

7. Employees Awareness Level of Social Engineering Defense Mechanisms

To answer the second research question, RQ2 (What is the current employees' awareness level of social engineering defense mechanisms?), the authors analyzed the data obtained from the survey to measure the awareness level of employees against the various defense mechanisms as shown in the taxonomy (Figure 1). To that end, the authors grouped the questions into different groups where each group measures the awareness level of a defense mechanism in the taxonomy. As a result, Figure 2 depicts the correlation between questions from the survey to the defense mechanisms from the taxonomy.

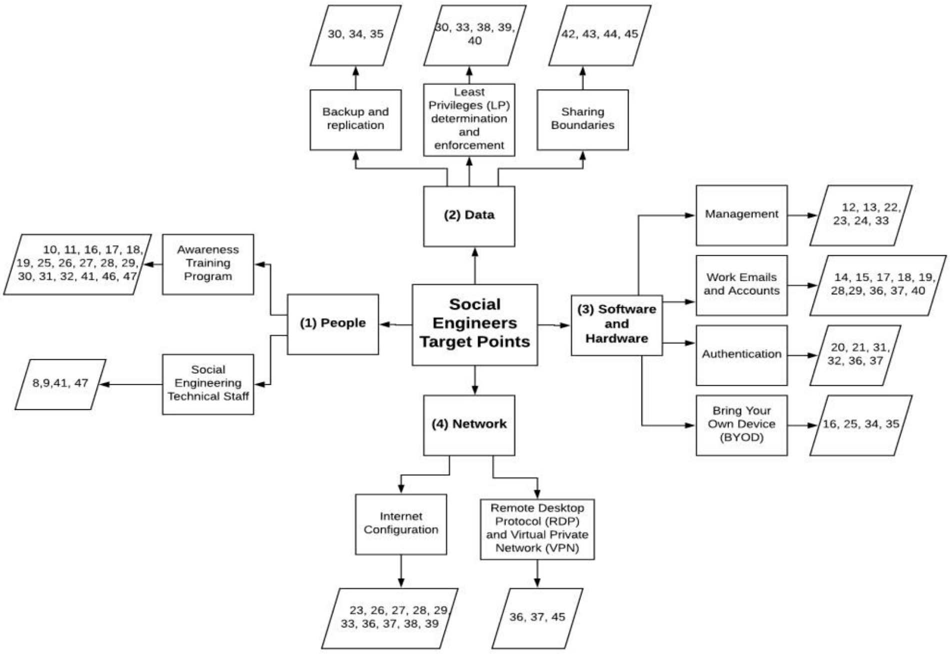

Fig 2. The correlation between the survey questions to the defense mechanisms in the taxonomy

Using Figure 2, the authors calculated the employees' awareness level regarding each social engineering defense mechanism. From figure 3, we see that, for example, only 49% of the employees attended training programs about social engineering, 50% of the employees aware of the data sharing boundaries in their organizations. Regarding the software and hardware, only 53% of the employees use their work email and account appropriately to avoid any potential social engineering attack, and finally, the figure shows that only 42% of the employees are aware of the right usage of the VPN and RDP protocols.

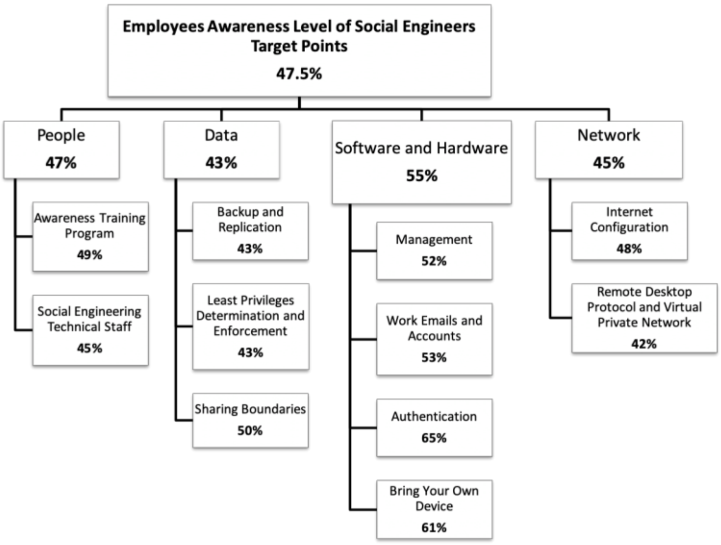

Fig 3. Employee’s awareness level against the social engineering defense mechanisms

Figure 4 below compares the awareness level of employees against social engineering defense mechanisms in public, depicted in blue bars, and private, depicted in orange bars, organizations. The figure indicates that the awareness level of employees in private organizations is more than the awareness level of employees in public organizations.

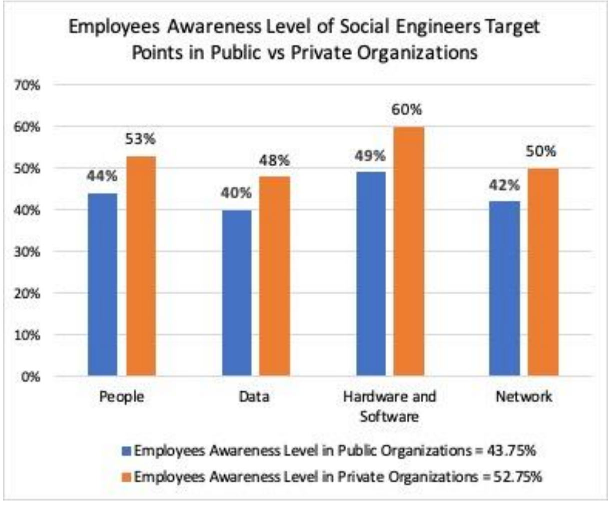

Fig 4. Comparison of employees awareness level in public and private organizations

Overall, this study shows that only 47.5% of the employees in both public and private organizations are aware of the social engineering attacks and their defense mechanism.

8. SOCIAL ENGINEERING INFOSEC POLICIES

This section aims to answer the third research question, RQ3 (what are the formal SE-IPs that should be incorporated in organizations?) by defining the security requirements for the proper and secure use of Information Technology services in organizations. According to [50], Confidentiality refers to the protection of sensitive information from unauthorized disclosure, Integrity is defined as the accuracy, completeness, and validity of information by business values and expectations, and Availability relates to information being available when required by the business process now and in the future. Hence, to reach a high cybersecurity maturity level in an organization and to protect its CIA, this paper suggested incorporating 18 formal Social Engineering InfoSec Policies (SE-IPs) shown in Figure 5.

Below are the policies and their short descriptions.

1. **Security Awareness Policy:** To outline the requirements for security awareness and training. To protect organizational assets, all employees need to defend the integrity and confidentiality of the organizations' resources. One of the best ways to achieve a significant and lasting improvement in information security practice is through raising awareness of everyone who interacts with information assets.
2. **Exception Management Policy:** To address the required approvals for any exceptions to the organizations' policies and procedures.
3. Data Classification Policy: To cover the different types of data classifications and how each should be handled based on the level of confidentiality required. Different levels of data classifications exist, ranging from public to highly confidential, and specific levels of security are required for storing and transmitting data.
4. **Data Ownership Policy:** To outline the details regarding data ownership, including creation, responsibilities, and control over the data.
5. **Data Breach Policy:** Data breaches can lead into severe operational, financial, reputational, and legal impacts in organizations [50]. Hence, it is vital to incorporate/enforce a Data Breach Policy to outline the procedures required for reporting a data security breach. This will help protecting the organization employees, partners, and stakeholders from illegal or damaging actions by individuals, either knowingly or unknowingly.
6. **Encryption Policy:** To cover the requirements for encryption technologies used to secure organization's data.
7. **Business Continuity and Disaster Recovery Policy**: Most organizations are equipped with the latest technological tools but lack disaster recovery plans [37]. The IT Business Continuity (BC) and Disaster Recovery (DR) standards provide requirements to manage business continuity related risks and effectively address crisis situations.
8. **Access Control Policy:** To cover the requirements for proper and secure control of access to IT services and infrastructure in the organization.
9. **Vendor Risk Management Policy:** This Policy should outline the requirements for assessing third-party vendor security risks.
10. **Mobile Device Policy:** Mobile devices create added risk and potential targets for data loss. Usage of such devices must be in alignment with appropriate standards and encryption technology must be used. This policy should be applied to any mobile device issued by the organization or used for conducting business (i.e., BYOD Bring Your Own Device) which transmits or store data.
11. **Application Security Policy:** To cover secure coding practices, assessments, and remediation for any applications being developed or integrated with the organizations environment. Web application vulnerabilities account for the largest portion of attack

vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities be remediated prior to production deployment. Additionally, organizations must be aware of web application threats. According to [51], SQL injection attack and Denial-of-Service (DoS) attack are two most important security threads found in the web applications.

12. **Security Risks and Controls:** The Consolidated IT Controls Catalog (CITCC), known as the Blue Book, is a baseline of IT security controls intended to provide IT Management, information custodians, and staff with a set of consolidated control requirements that must be in place to minimize and manage the organizations IT risks. The controls outlined are mandatory requirements based on the applicability to specific IT environments and follow the premise of, implement once, satisfy many requirements.
13. **General IT Usage Policy:** To outline the acceptable use of computer equipment in the organization. It should cover general IT usage of the organization’s resources including, but not limited to: Acceptable Use, Internet Usage, Electronic Mail, Wireless Connections Remote Access, Workstation Security, Removable Storage Media, Software Installation, and Social Media.
14. **Physical Security Policy**: For any security-conscious businesses, physical security must be enforced throughout the organization, without exception [52]. Hence, it is significant to incorporate/enforce a policy that outlines the requirements for physically securing the organization’s assets, including but not limited to computer hardware, workstations, servers, printers, and building/room access.
15. **Password Policy:** To cover the requirements for passwords that secure systems and accounts. Any system that handles valuable information must be protected with a password-based access control system. Password Policy must address Password Creation Policy, Password Change Policy, and Password Protection Policy.
16. **Network Security Policy:** To cover the standards for maintaining a secure network infrastructure to protect the integrity of organization data and mitigate risk of a security incident.
17. **Server Security Policy:** To establish standards for the base configuration of internal server equipment that is owned and/or operated by the organization. Effective implementation of this policy will reduce the risk of unauthorized access to the proprietary information and technology. [25] conducted a study about firewall informed by web server security policy.
18. **Proxy/URL Configuration Policy:** To outline the baseline of websites which should be blocked or permitted at the web proxy. End users should only be able to access websites as required for their job responsibilities. A web-filtering tool is used in order to prevent access to the site from a web browser. When access is prevented, a screen should show that local governance has prevented access. This should also provide contacts for users if they feel there is a legitimate business reason for access.

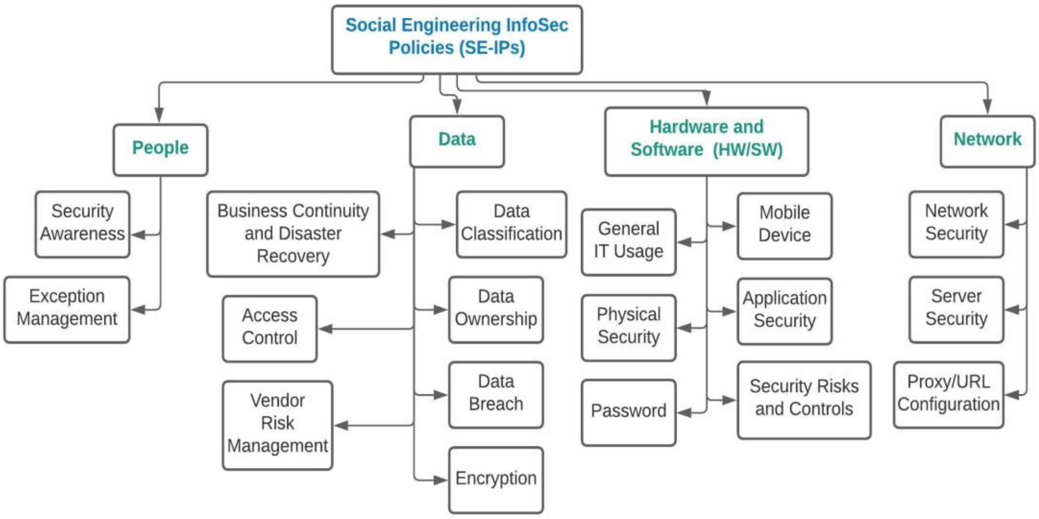

Fig. 5: Proposed Formal Social Engineering InfoSec Policies (SE-IPs)

9. Formal SE-IPs Incorporation Level

To answer the fourth research question, RQ4 (What is the current level of formal SE-IPs incorporation in organizations?), the authors analyzed the data obtained from the survey, to measure the current incorporation level of SE-IPs in organizations. To that end, the survey questions were grouped so that each group measures the incorporation level of a SE-IP. As a result, Figure 6 depicts the correlation between questions from the survey to the social engineering security policies in the SE-IPs taxonomy.

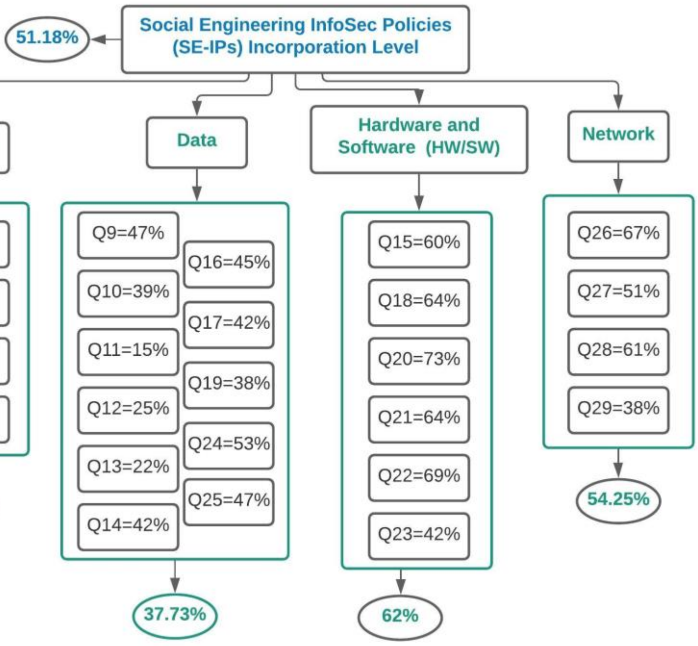

Fig. 6: Formal SE-IP Incorporation at the Organizational Level

Employees in the private sector are more aware of social engineering attacks than employees in the public sector [11]. Moreover, this paper indicates that the incorporation level of SE-IPs in private organizations is more than in public organizations as shown in Figure 7 that compares SE-IPs incorporation level in public, depicted in blue bars, and private, depicted in orange bars, organizations. The figure indicates that 58.25% of SE-IPs are incorporated in private organizations, comparing to 47.25% of them in public organizations.

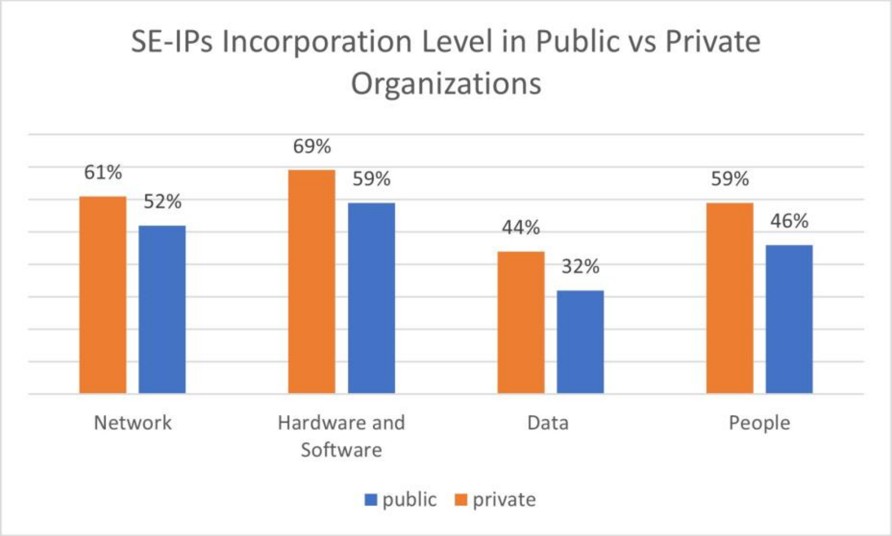

Fig. 7: Formal SE-IPs Incorporation Level in Public vs Private Organizations

10. CONCLUSION

Humans have become the weakest link in the security pipeline, and social engineers are taking advantage of the knowledge gap that exists in this area. To mitigate the risk of social engineering attacks, organizations and their employees must be aware of social engineering defense mechanisms and incorporate Social Engineering InfoSec Policies (SE-IPs). After surveying employees in various employment sectors, the paper found that 47.5% of employees are aware of social engineering defense mechanisms and 51.18% of formal SE-IPs are incorporated. To help increase this percentage, the authors proposed a customizable model of SE-IPs that consists of 18 SE-IPs categorized into four main categories. After developing well-designed SE-IPs, the next step is to provide some recommendations regarding enforcing those written policies and translating them to technical processes within the organizations' systems. Moreover, as another venue of future directions, the authors are planning to develop an awareness training session for organizations to educate their employees about mitigating the risks of social engineering security attacks.

ACKNOWLEDGMENT

The first author was supported by a generous fellowship from Shaqra University. All errors and omissions are the responsibility of the authors alone. Additionally, the authors gratefully acknowledge and appreciate the significant contributions from managers in the Saudi public and private organizations, whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication.

REFERENCES

[1] S. D. Applegate, Social engineering: hacking the wetware! Information Security Journal: A Global Perspective 18 (1) (2009) 40–46.

[2] C. Hadnagy, Social engineering: The art of human hacking, John Wiley & Sons, 2010.3. A. Berg, Cracking a social engineer, [online]. lan times (1995).

[3] A. Berg, Cracking a social engineer, [online]. lan times (1995).

[4] T. Greening, Ask and ye shall receive: a study in social engineering, ACM SIGSAC Review 14 (2) (1996) 8–14.

[5] A. Karakasiliotis, S. Furnell, M. Papadaki, Assessing end-user awareness of social engineering and phishing.

[6] M. Workman, A test of interventions for security threats from social engineering, Information Management & Computer Security 16 (5) (2008) 463–483.

[7] G. L. Orgill, G. W. Romney, M. G. Bailey, P. M. Orgill, The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems, in: Proceedings of the 5th conference on Information technology education, ACM, 2004, pp. 177–181

[8] T. Bakhshi, M. Papadaki, S. Furnell, A practical assessment of social engineering vulnerabilities., in: HAISA, 2008, pp. 12–23.

[9] F. Mouton, M. M. Malan, L. Leenen, H. S. Venter, Social engineering attack framework, in: 2014 Information Security for South Africa, IEEE, 2014, pp. 1–9.

[10] R. Kalnin,š, J. Purin,š, and G. Alksnis, "Security evaluation of wireless network access points," Applied Computer Systems, vol. 21, no. 1, pp.38–45, 2017.

[11] D. N. Alharthi, M. M. Hammad, and A. C. Regan, "A taxonomy of social engineering defense mechanisms," in Future of Information and Communication Conference. Springer, 2020, pp. 27–41.

[12] F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack examples, templates and scenarios," Computers & Security, vol. 59, pp.186–209, 2016.

[13] N. Saxena, E. Hayes, E. Bertino, P. Ojo, K.-K. R. Choo, and P. Burnap, "Impact and key challenges of insider threats on organizations and critical businesses," Electronics, vol. 9, no. 9, p. 1460, 2020.

[14] T. Ahmad, "Corona virus (covid-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity," Available at SSRN3568830, 2020.

[15] N. Sarginson, "Securing your remote workforce against new phishing attacks," Computer Fraud & Security, vol. 2020, no. 9, pp. 9–12, 2020.

[16] H. Aldawood and G. Skinner, "Contemporary cyber security social engineering solutions, measures, policies, tools and applications: Acritical appraisal," International Journal of Security (IJS), vol. 10, no. 1, p. 1, 2019.

[17] V. Systems, "Varonis 2019 global data risk report," 2019.

[18] A. Yazdanmehr and J. Wang, "Employees' information security policy compliance: A norm activation perspective," Decision Support Systems, vol. 92, pp. 36–46, 2016.

[19] D. N. Alharthi and A. C. Regan, "Social engineering defense mechanisms: A taxonomy and a survey of employees' awareness level," in Science and Information Conference. Springer, 2020, pp. 521–541.

[20] D. N. Alharthi and A. C. Regan, "Social engineering InfoSec Policies (SE-IPs)," in the 14th International Conference on Network Security & Applications (CNSA 2021). CICT, 2021, pp. 521–541. NIAI - 2021 pp. 57-74, 2021.

[21] H. Aldawood, G. Skinner, An academic review of current industrial and commercial cyber security social engineering solutions, in: Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, ACM, 2019, pp. 110–115.

[22] B. M. E. Elnaim, H. A. S. W. Al-Lami, The current state of phishing attacks against Saudi Arabia university students.

[23] C. Happ, A. Melzer, G. Steffgen, Trick with treat–reciprocity increases the willingness to communicate personal data, Computers in Human Behavior 61 (2016) 372–377.

[24] I. Ghafir, V. Prenosil, A. Alhejailan, M. Hammoudeh, Social engineering attack strategies and defence approaches, in: 2016 IEEE 4th International Conference onFuture Internet of Things and Cloud (FiCloud), IEEE, 2016, pp. 145–149.

[25] M. Gupta, R. Sharman, Social network theoretic framework for organizational socialengineering susceptibility index, AMCIS 2006 Proceedings (2006) 408.

[26] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, T. Zwaans, Thehuman aspects of information security questionnaire (hais-q): two further validation studies, Computers & Security 66 (2017) 40–51.

[27] T. Herath, H. R. Rao, Encouraging information security behaviours in organizations: Role of penalties, pressures and perceived effectiveness, Decision Support Systems47 (2) (2009) 154–165.

[28] J. A. Stoner, Risky and cautious shifts in group decisions: The influence of widely held values, Journal of Experimental Social Psychology 4 (4) (1968) 442–459.

[29] H. Aldawood and G. Skinner, "Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues," Future Internet, vol. 11, no. 3, p. 73, 2019.

[30] K. J. Knapp, R. F. Morris Jr, T. E. Marshall, and T. A. Byrd, "Information security policy: An organizational-level process model," computers &security, vol. 28, no. 7, pp. 493–508, 2009.

[31] C. Senarak, "Port cybersecurity and threat: A structural model for prevention and policy development," The Asian Journal of Shipping and Logistics, 2020.

[32] A. Karakasiliotis, S. Furnell, and M. Papadaki, "Assessing end-user awareness of social engineering and phishing," 2006.

[33] L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan, "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior," International Journal of Information Management, vol. 45, pp. 13–24, 2019.

[34] M. Siponen, M. A. Mahmood, and S. Pahnila, "Employees' adherence to information security policies: An exploratory field study," Information& management, vol. 51, no. 2, pp. 217–224, 2014.

[35] F. Bélanger, S. Collignon, K. Enget, and E. Negangard, "Determinants of early conformance with information security policies," Information& Management, vol. 54, no. 7, pp. 887–901, 2017.

[36] K.-c. Chang and Y. M. Seow, "Effects of it-culture conflict and user dissatisfaction on information security policy non-compliance: A sense-making perspective," 2014.

[37] F. Hadi, M. Imran, M. H. Durad, and M. Waris, "A simple security policy enforcement system for an institution using sdn controller," in 2018 15th International Bhurban Conference on Applied Sciences and Technology (IBCAST). IEEE, 2018, pp. 489–494.

[38] V. D. Soni, "Disaster recovery planning: Untapped success factor in an organization," Available at SSRN 3628630, 2020.

[39] J. Horney, M. Nguyen, D. Salvesen, O. Tomasco, and P. Berke, "Engaging the public in planning for disaster recovery," International journal of disaster risk reduction, vol. 17, pp. 33–37, 2016.

[40] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," Future Internet, vol. 11, no. 4, p. 89, 2019.

[41] C. Okoli, K. Schabram, A guide to conducting a systematic literature review of information systems research.

[42] NCSC, National Cybersecurity Centre (Accessed 2019). link

[43] S. Inc., Surveymonkey (Accessed 2019). link

[44] Stats, "Saudi general authority for statistics," Accessed 2020. [Online]. Available: https://www.stats.gov.sa/

[45] Statista, "Statista," Accessed 2020. [Online]. Available: https://www.statista.com/

[46] C. Bronk and E. Tikk-Ringas, "The cyber-attack on Saudi Aramco," Survival, vol. 55, no. 2, pp. 81–96, 2013.

[47] D. D. Cheong, "Cyberattacks in the gulf: lessons for active defence," 2012.

[48] S. S. Basamh, H. Qudaih, and J. B. Ibrahim, "An overview on cybersecurity awareness in Muslim countries," International Journal of Information and Communication Technology Research, 2014.

[49] ITU, "Committed to connecting the world," Accessed 2020. [Online]. Available: https://www.itu.int/en/Pages/default.aspx

[50] T. McClelland, "The insider's view of a data breach-how policy, forensics, and attribution apply in the real world," 2018.

[51] R. Bhor and H. Khanuja, "Analysis of web application security mechanism and attack detection using vulnerability injection technique," in 2016 International Conference on Computing Communication Control and automation (ICCUBEA). IEEE, 2016, pp. 1–6.

[52] J. Saleem and M. Hammoudeh, "Defense methods against social engineering attacks," in Computer and network security essentials. Springer, 2018, pp. 603–618.

Authors

Dalal Alharthi is a Ph.D. Candidate in Computer Science at the University of California, Irvine. She is also a Resident Engineer at Palo Alto Networks and a Senior Prisma Cloud Consultant at Dell. She is equipped with 12+ years of work experience between academia and industry. Her research interests are in the field of Cybersecurity, Network Security, Cloud Security, Privacy, Human-Computer Interaction (HCI), and Artificial Intelligence (AI).

Amelia Regan received a BAS in Systems Engineering from the University of Pennsylvania, an MS degree in Applied Mathematics from Johns Hopkins University, and an MSE degree and Ph.D. degree at the University of Texas. She is a Professor of Computer Science at the University of California, Irvine. Her research interests include network optimization, cyber-physical transportation systems, machine learning tools for temporal-spatial data analysis, and cybersecurity.