UNIVERSITY OF CALIFORNIA,
IRVINE

Social Engineering Defense Mechanisms and InfoSec Policies: A Survey and Qualitative Analysis

DISSERTATION

submitted in partial satisfaction of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

in Computer Science

by

Dalal Naser Alharthi

Dissertation Committee:
Professor Amelia Regan, Chair
Professor Sergio Gago
Professor Joshua Garcia

2021

DEDICATION

Dedicated to the strongest person I know: me, and to my children Nawaf, Ilan, and Farrah, without whom this dissertation would have been completed two years earlier... I love you! I also dedicate this dissertation to my husband (Sultan) and my family, for their love and support!

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

Having reached this important milestone in my academic career, I would like to thank many important people who cheered me along this path.

The ultimate thanks and glory is given to the best and most patient advisor, Professor Amelia Regan, who has helped me develop as a researcher and as a person. During my time at the Department of Computer Science at the University of California, Irvine, she has been my mother away from home. Her guidance, support, optimism and encouragement have been invaluable throughout the entire time of my PhD studies.

I am grateful to the committee members of my final defense, Professor Sergio Gago and Professor Joshua Garcia. Also, I'd like to say thanks to my colleagues during my entire PhD studies. I am fortunate to have the support of great friends in department of computer science, and more specifically Amelia Regan's lab members, Reza Asadi, Amari Lewis, Arash Nabili, Karina Hermawan, and Caesar Aguma. I also learned a lot from my collaborators, whom I have crossed paths during my experience in industry in Farmers Insurance, Palo Alto Networks, and Dell. Throughout the entire of my PhD, I have had valuable experience as a teaching assistant of graduate classes,and I have learned valuable skills in my Division of Teaching Excellence and Innovation (DTEI) Fellowship.

In addition, a big thank you to my dad, my mom, and all my family members and relatives for their support and encouragement throughout my PhD and my intellectual development more broadly.

Each person I mentioned here contributed to this dissertation in some fashion. With their help, support, and love this dissertation has become a work that I am proud to have my name on.

Finally, I thank Shaqra University for their generous fellowship. Additionally, I would like to thank the Future of Information and Communication Conference (FICC), the Computing Conference, the International Conference on Network Security Applications (CNSA), and the International Journal of Network Security Its Applications (IJNSA) for giving me permissions to include my previously published papers in this dissertation.

VITA

Dalal Naser Alharthi

EDUCATION

Ph.D. in Computer Science **2021**
University of California, Irvine *Irvine, California*

Master of Science in Computer Science **2018**
University of California, Irvine *Irvine, California*

Master of Public Administration **2014**
King Saud University *Riyadh, Saudi Arabia*

Bachelor of Science in Computer Sciences **2008**
Princess Nourah Bint Abdul Rahman University *Riyadh, Saudi Arabia*

RESEARCH EXPERIENCE

Researcher **2016-2021**
University of California, Irvine *Irvine, California*

TEACHING EXPERIENCE

Teaching Assistant **2020-2021**
University of California, Irvine *Irvine, California*

Lecturer **2018-2021**
Shaqra University *Riyadh, Saudi Arabia*

Teaching Assistant **2015-2018**
Shaqra University *Riyadh, Saudi Arabia*

INDUSTRY EXPERIENCE

Resident Engineer - Senior Prisma Cloud Consultant **2020-2021**
Palo Alto Networks *Houston, Texas*

Cloud Security Engineer - Information Security Consultant **2019-2020**
Farmers Insurance *Woodland Hills, California*

Director of Electronic Media Department **2014-2015**
Ministry of Civil Service *Riyadh, Saudi Arabia*

Programmer **2009-2014**
Princess Nourah Bint Abdul Rahman University *Riyadh, Saudi Arabia*

REFEREED JOURNAL PUBLICATIONS

A Literature Survey and Analysis on Social Engineering Defense Mechanisms And Infosec Policies **March 2021**
International Journal of Network Security and Its Applications (IJNSA)

REFEREED CONFERENCE PUBLICATIONS

Social Engineering InfoSec Policies (SE-IPs) **January 2021**
14th International Conference on Network Security and Applications (CNSA)

Social Engineering Defense Mechanisms: A Taxonomy and a Survey of Employees Awareness Level **July 2020**
Science and Information Conference

A Taxonomy of Social Engineering Defense Mechanisms **March 2020**
Future of Information and Communication Conference (FICC) 2020

ABSTRACT OF THE DISSERTATION

Social Engineering Defense Mechanisms and InfoSec Policies: A Survey and Qualitative Analysis

By

Dalal Naser Alharthi

Doctor of Philosophy in Computer Science

University of California, Irvine, 2021

Professor Amelia Regan, Chair

Social engineering attacks can be severe and difficult to detect before considerable damage is done. Therefore, to prevent such attacks, organizations should be aware of social engineering defense mechanisms. The application of security policies is essential for mitigating the risk of social engineering attacks. However, incorporating and enforcing successful security policies in an organization is not a straightforward task. To that end, we developed a taxonomy of social engineering defense mechanisms and a customizable model of formal Social Engineering InfoSec Policies (SE-IPs) that can be adopted by a wide variety of organizations. We also designed and distributed a survey to measure employees awareness of social engineering defense mechanisms and a survey to measure the incorporation of formal SE-IPs in organizations. After collecting and analyzing the data from the two surveys which included over fifteen hundred responses, we found that more than half of employees are not aware of social engineering attacks, and on average, organizations incorporated just over fifty percent of the identified formal Social Engineering InfoSec Policies. Such worrisome results show that organizations are vulnerable to social engineering attacks, and serious steps need to be taken to elevate the awareness level against these emerging security threats.

Chapter 1

Introduction

1.1 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 [11]. 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 [36][17]. Compared to technical hacking, social engineering is generally an easier, cheaper, and more effective way to gain unauthorized access to confidential information.

Hence, social engineers aim to exploit the weakest link in a security structure by manipulating individuals and organizations to divulge valuable and sensitive data [43]. 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) [6] [51].

According to [62], successful social engineering has an overwhelming negative impact 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. Numerous other research efforts addressed the significant impact of social engineering attacks on the organizational level [33], [44], [73], [55], and [14]. Social engineers are looking for the easiest way into the organizations systems, which is not to try and break the encryption on the organization's database or type in every combination of characters to guess their employees passwords. Often, the easiest way is to trick employees into giving them the keys. 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. [52] outlined the importance of increasing the employees awareness level against social engineering attacks.

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 [2] [61]. The Verizon data breach investigations recent report stated that 33% of actions used to attack organizations come through social engineering-based attacks and addressed that most organizations have unprotected data and poor social engineering cybersecurity policies in place, making them vulnerable to data loss [70].

To successfully fight against social engineering attacks, organizations must ensure that their employees understand the risks of social engineering and how to avoid becoming a victim. Additionally, its imperative to develop and adopt Information Security Policies (ISPs). [74] defined an information security policy (ISP) of an organization a set of rules and policies

related to employee access and use of organizational information assets. [4] emphasized the need to adopt measures and tools, including policies and training programs, to mitigate the risk of social engineering attacks.

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. The research also lacks a formal model of Social Engineering InfoSec Policies (SE-IPs) that organizations can adopt to protect their assets in the cyber-world. To fill these research gaps, our research provides the following key contributions. We 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. We 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. We surveyed employees in various employment sectors, then analyzed the results and reported them. Additionally, we made the dataset available online for researchers and practitioners in the field of cybersecurity to replicate or extend the work.

1.2 Problem Statement

Measuring employees awareness level of social engineering defense mechanisms and investigating the incorporation level of formal Social Engineering InfoSec Policies (SE-IPs) in organizations.

1.3 Research Objective and 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 [59]. Most cyber-criminals consider it much easier to abuse a persons trust than to use technical means to hack into a secured computer system; they have learned how to trick their targets into giving them information by exploiting certain qualities in human nature. They use various forms of communication, such as email, the Internet, the telephone, and even face-to-face interactions, to perpetrate their schemes of defrauding and infiltrating organizations. Because social engineering is such a threat in todays workplace, it is vital to incorporate, teach, and enforce security policies in organizations to keep organization's networks safe from such attacks.

To that end, the main objectives of our research is to develop a taxonomy of social engineering defense mechanisms and propose a formal model of Social Engineering InfoSec Policies (SE-IPs). To achieve these objectives more effectively, the following four research questions are created:

- 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 SE-IPs that should be incorporated in organizations?
- RQ4: What is the current level of SE-IPs incorporation in organizations?

1.4 Research Scope and Limitation

We are aware that the study might have limitations such as using a scenario-based questionnaire instead of conducting a real social engineering attack study, but this was considered unavoidable due to ethical considerations. However, the questions in the developed questionnaires were designed carefully to match recent and real social engineering-based attacks on organizations.

1.5 Structure of Dissertation

The dissertation is divided into six chapters. The first chapter is written to present the problem and motivation of this research. The detailed research objectives and questions are also presented in this chapter as well. Chapter two is used to present the literature review. Chapter three introduces the methodology for the whole research process from data collection to data analysis. Chapter four is used to illustrate our taxonomy of social engineering defense mechanisms and analyze employees awareness level of that. Chapter five proposes a formal Social Engineering InfoSec Policies (SE-IPs) that organizations can adopt, and analyzes the current incorporation level of those SE-IPs. Finally, the dissertation concludes with future work avenues addressed in chapter 6.

Chapter 2

Literature Review

A wide range of research efforts focuses on purely technical security attacks, while fewer researchers have focused on social engineering attacks. This chapter provides an overview of the different kinds of common social engineering security attacks addressed in the Background Section. Then, it discusses the research efforts that are closely related to this dissertation.

2.1 Background

Organizations mainly focus on deploying high quality and sophisticated security tools to detect security vulnerabilities or even prevent security attacks. However, security is only as strong as the weakest point in the system, which includes the human actors. Since humans are the weakest point in the information security chain, they are being targeted by social engineers. According to [25], misuse of information systems by humans, both intentionally and unintentionally, accounts for 50% to 75% of cybersecurity threats.

As stated by Granger [32], social engineering is "the art and science of getting people to comply with your wishes." It can be defined as the practice of acquiring information through

technical and non-technical means [46]. Therefore, social engineering attacks rely on convincing people that a social engineer is a trusted friend or colleague. Social engineering attacks can be carried out either by a human or by a machine through a software system [48]. Social engineering attacks have no limit, and they only depend on the creativity of social engineers. In the past few years, the number and the sophistication of social engineering attacks have increased and became more diverse. These attacks are difficult to detect and prevent, resulting in loss of confidential data, intellectual property, financial data, money, and organizational credibility with customers [3].

Figure 2.1 depicts the primary social engineering (SE) attack vectors [6]. As shown in the figure, there are two types of attacks: technical SE attacks and non-technical SE attacks. This paper provides a brief description of each one so the reader can understand the discussion that ensues.

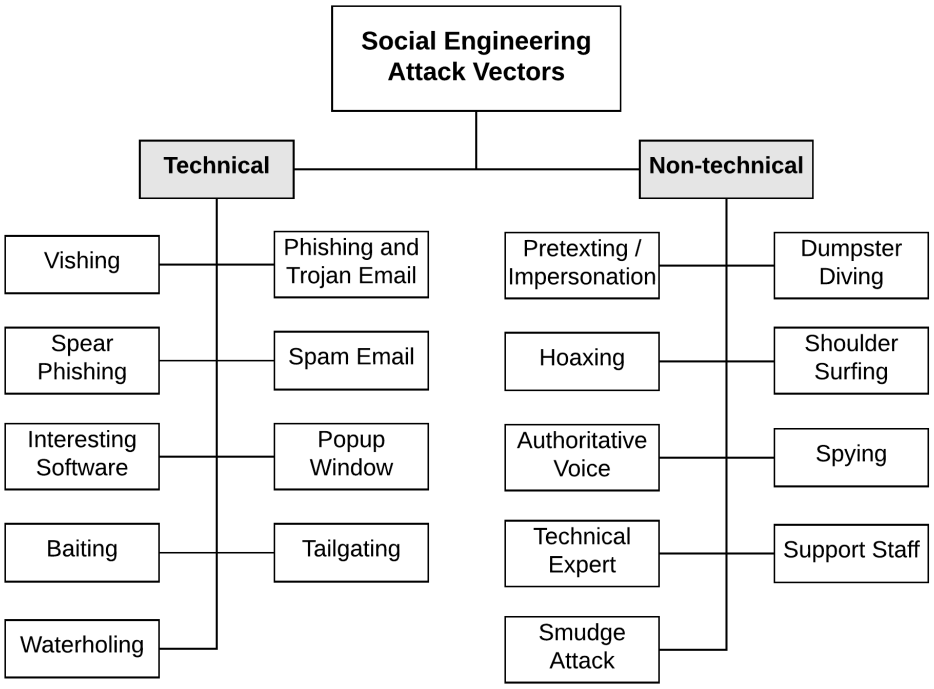

Figure 2.1: Social Engineering Attack Vectors [6]

Technical Social Engineering Attacks

As shown in the left side of Figure 2.1, technical social engineering attacks are Vishing, Phishing, Spear Phishing, Spam Email, Interesting Software, Popup Window, Baiting, Tailgating, and Waterholing.

- *Phishing and Trojan Email* rely on carefully crafted messages to entice victims to open attachments or click on embedded hyperlinks [11]. In this security attack, the victim is entirely unknown to the social engineer.

  The phishing attack is one of the most successful social engineering attacks. One of the biggest phishing attacks occurred in March of 2016 during the U.S. presidential election. It targeted John Podesta, the former chairman of Hillary Clinton's U.S. presidential campaign, and through his account, some of Clinton's emails. The target of the attack was Clintons personal Gmail account, which had messages from 2007 through 2016 [72], [64]. On that phishing email, there was a "change password" link, once John Podesta clicked on it and changed his password, social engineers maliciously retrieved his password and locked his account.

- *Vishing* (voice phishing) occurs by tricking people into revealing sensitive information through a phone call.

- *Spear Phishing* similar to the phishing attack, but in this attack, the victim's information is known to social engineers. Therefore, the social engineer can launch customized cyberattacks.

- *Spam Email* is an email that offers friendships, diversion, gifts and various free pictures and information in order to plant malicious code on the reader's machine.

- *Interesting Software* and *Popup Windows* are other social engineering techniques in which a social engineer convinces a victim to download and install a useful program

or application such as a CPU performance enhancer or displays a pop-up window that prevents a victim from proceeding with the session unless he reenters his username and password.

- *Baiting* happens when a malware-infected storage medium is left in a location where it is likely to be used by targeted victims [46].

- *Tailgating* aims at accessing unauthorized places by getting help from an authorized person.

- *Waterholing* means compromising a website that is likely to be of interest to a chosen victim [11].

Non-Technical Social Engineering Attacks

There are several social engineering attacks where technology is not involved such as Pretexting/Impersonation, Dumpster Diving, Shoulder Surfing/Spying, Hoaxing, Authoritative Voice, Smudge Attack, Support Staff, and Technical Expert.

- *Pretexting/Impersonation* occurs when a social engineer pretends to be someone else who is known to a target person.

- *Dumpster Diving* happens by sifting through the trash of an organization to find discarded items that include sensitive information.

- *Shoulder Surfing* and *Spying* use direct observation techniques to get information [46]. When a social engineer attempts to extract sensitive information about the recent activity of a user using, for example, residual oils on touch screen devices to detect the user's input, such an attack called *Smudge Attack*. This attack method can be applied to a significantly large set of devices such as touch screens of ATMs and DRE voting machines [13].

- *Hoaxing* an attempt to trick an audience into believing that something false is real [71].

- *Authoritative Voice* is another SE attack, discussed in [71], in which a social engineer calls a company's computer help desk and pretend to have access to a troubleshooting system.

- *Support Staff* and *Technical Expert* are physical attacks used by social engineers by acting as support staff or as technical staff. As an example, a man dressed as a cleaning crew member, walks into a work area, carrying cleaning equipment, then in the process of appearing to clean a desk area, he can snoop around and get valuable information such as passwords, or confidential files that an employee forgot to hide, or even make a phone call impersonating an employee from his desk.

According to a 2018 Verizon report [1], phishing and pretexting combined account for 98% of social engineering incidents and email is the most common media to carry social engineering attacks.

Major Successful Social Engineering Attacks

The following table provides some real world examples of how small security mistakes can cost large organizations huge amounts of money and the respect of their customer and constituents.

Social Engineering Attack	Implications	Lesson Learned
Twitter Bitcoin Scam (2020)	Twitter employees fell for social engineering exploits that allowed the bad actors a backdoor into highly-sensitive login information. As a result, social engineers tweeted double your Bit-coin offers from Verified Twitter users, telling their followers that they would double donations made on a select link, which allowed them to steal hundreds of thousands dollars.	The biggest weakness to most companies may be the employees themselves. Hence, educating employees is essential to improve an organizations cybersecurity posture.
Toyota Boshoku Corporation (2019)	Social engineering and Business Email Compromise (BEC) targeted cost Toyota a lost of 37 million USD. Using persuasion, attackers persuaded a finance executive to change recipients' bank account information in a wire transfer.	Employees should be aware of the detection mechanisms of BEC Scam as well as fraudulent payments submitted as a result.
US Presidential Election Email Leak (2016)	Social engineers sent a series of spear phishing emails to employees The Democratic National Conventions network. The email shortened the URL link to hide its true redirect path, which allow social engineers to gain full access to employees Google accounts.	Employees must be cautious of shortened URL links that can raise the risk of malware infection.

2.2 Related Work

Most of the proposed measures to mitigate cyber threats in the related work are focused on one element of cyber threats, which is technical threats. Despite the importance and effectiveness of technical solutions, social engineers try to exploit the weakest link of an organization's security, human vulnerabilities [26] [5]. Hence, we require solutions that understand and guard against human weaknesses.

A good understanding of user security behavior can help reduce the success of social engineering attacks [10]. In this context, Elnaim et al. [28] conducted an experimental study in 2017 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 experimental study was conducted in 2016 by Happ et al. [37] 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. Furthermore, Medlin et al. [50] 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. Moreover, Siadati et al. [65] 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 8%, or a sixth of its success against Googles standard second-factor verification code messages.

Krombholz et al. [46] 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. As another example, leveraging *Waterholing* SE attacks in 2013 against Apple, Facebook, and Twitter, social engineers were able to exploit a zero-day vulnerability. Specifically, they were able to sneak into the corporate networks and inject malicious code onto their websites. Once a user visited the infected website, his device would be compromised. Moreover, in 2011, a small number of RSA employees received an email entitled "2011 Recruitment Plan". The email was well 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 stealing sensitive information of the RSA SecureID system.

Several research efforts studied social engineering attack vectors. I.e., Chitrey et al. [24]

developed a model of social engineering attacks. The model categorized social engineering attacks under two main entities: (1) vulnerable entities which are human, technology, and government laws, and (2) safeguards entities which are information security awareness program, 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. On the other hand, Gupta and Sharman [34] 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 (1) social function, (2) organizational hierarchy, (3) organizational environment, (4) network characteristics, and (5) relationship characteristics. Furthermore, Parsons et al. [56] suggested a Human Aspects of Information Security Questionnaire (HAIS-Q) to measure Information Security Awareness (ISA) of Australian organizations. The authors demonstrated the effectiveness of the HAIS-Q to measure ISA.

Aldawood and Skinner [3] 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 the Gamification to assess the behavior of hypothetical victims of social engineering attacks. 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. On the other hand, Orgill et al. [55] demonstrated

two metrics for determining security compliance in an organization. These are user education and security auditing. They emphasized the importance of educating employees about social engineering attacks and how to prevent them. Moreover, Ghafir et al. [31] 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.

Beuran et al. [18] 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 [39], a combination of technical, social, economic, and psychological factors affect 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 [11], 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 favor [37]. Risky-shift is another critical factor that was coined by

James Stoner in 1961 [69]. 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 the organization's data and services. [45] 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 organizations 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 an organizations information security policies. Thus, a critical element to any organization's cybersecurity program is having security controls and policies in place which are customized for their environment. [63] 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 cyberthreats (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. [44] 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 are 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, images/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 [47], when employees are aware of their companys information security policies and procedures, they are more competent to manage cybersecurity tasks than those who are not aware of their companies policies. This result was based on a survey results from 579 business managers and professionals after employing Structural equation modeling and ANOVA procedures on the results. In contrast, [5] 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) [67]. However, forcing individuals into the compliance might trigger undesired behaviors. [16] conducted a 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. [74] 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 employees 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 injunctive and subjective norms),

awareness of consequences, and ascription of personal responsibility shape personal norms. Moreover, [22] 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 comply after they are enforced, and overlooked that human feelings, behavior 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 represent 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 impacts ISP non-compliance because the employees values are misaligned with the ISP values. In the context of enforcing an ISP, [35] suggested a simple enforcement system using a Software Defined Network (SDN) controller to block the malicious and restrict the anonymous users in the organization's 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's InfoSec policies, penetration testing is required. [27] suggested two methodologies for physical penetration testing using social engineering, which aim 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 increase 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 the unexpected event and help to recover was emphasized by [68]. [40] 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.

Chapter 3

Methodology

This chapter describes the research methodology we followed to develop the taxonomy of social engineering defense mechanisms, to measure the employees awareness level of that, to create a formal model of SE-IPs, and to measure SE-IPs incorporation level in organizations.

3.1 Building the Taxonomy Methodology

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

3.1.1 Systematic Literature Review (SLR)

To develop a taxonomy of the defense mechanisms of social engineering attacks, we followed a Systematic Literature Review (SLR) technique as recommended by Okoli and Schabram in [54]. To do that, we conducted a literature review of most recent journals and conferences papers that contained "social engineering" in their title. Then, extracted the target points

of social engineers and any suggested defense mechanism from each paper.

3.1.2 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 divided into four categories: general category, network security, server security, and application security. To build the taxonomy, we followed some of the guidelines in the SANS InfoSec Policies as well as the SANS Awareness Survey.

3.2 Measuring Awareness Level Methodology

To measure the awareness level of employees in public, private, and non-profit organizations, we designed a questionnaire, distributed it to a large number of employees, and then analyzed the collected data.

3.3 Questionnaires

To measure the awareness level of employees against the social engineering defense mechanisms and the SE-IPs incorporation level, we have carefully designed two questionnaires. To build the questionnaires, we relied on (1) the developed taxonomy, (2) the Human Aspects of Information Security Questionnaire (HAIS-Q) [56], (3) SANS Awareness Survey, (4) NIST Cyber Security Framework, (5) ISO 27001 Standard, and (6) the Essential Cybersecurity

Controls created by the Saudi National Cybersecurity Authority in 2018 [53].

To distribute the questionnaires, we used SurveyMonkey [41], an online cloud-based survey service, to publish and distribute the survey instruments. Then, a letter of invitation was sent to several Saudi organizations informing them about the project and asking them to circulate it among their employees. The participated organizations have different sizes, belong to different sectors, and geographically distributed over 13 regions of Saudi Arabia to allow a diverse and representative sample. The questionnaires can be used by organizations to measure the awareness level of their employees against various social engineering defense mechanisms and the incorporation level of formal SE-IPs.

3.4 Surveyed Employees

Over several months, the survey received by thousands of employees either through their organizations or directly received it from us over the email or social media accounts. Many reminders were sent also to remind the employees to answer the survey. At the end, 791 employees participated in the first survey and 1523 employees participated in the second one. Participants are working in various public, private, and non-profit organizations in Saudi Arabia

3.5 Selected Country

As a case study, we focuses on public, private, and non-profit organizations in Saudi Arabia. According to the Saudi General Authority for Statistics, the Saudi population is 33.5 million in 2019. And according to The Statistics Portal, the number of Internet users in Saudi Arabia is increasing rapidly, reaching about 90.4% of the population in 2020, which increases the

need for enhancing cybersecurity awareness to defend sensitive information in the cyberspace. We 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, on 2012, over 35,000 Aramco's computers were infected by a virus called Shamoon, which operates like a time bomb (logic bomb malware). These devices were partially wiped or totally destroyed [20], [23], [15].
- 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 International Telecommunication Union (ITU) [42], Saudi Arabia ranked number 13 out of 194 countries in 2018.

Chapter 4

Social Engineering Defense Mechanisms: A Survey of Employees Awareness Level

We start this chapter by presenting the taxonomy of social engineering defense mechanisms. Then, we analyze the data we collected using our developed questionnaire and report our results. We conclude the chapter by measuring employees awareness level of social engineering defense mechanisms.

4.1 Taxonomy of Social Engineering Defense Mechanisms

To answer the research question, RQ1 in Chapter 1, we conducted a thorough investigation of the literature, and found that there are five main target pints for social engineers. Social engineers try to achieve their malicious goals through these five target points, which are

the main assets of any organizations. These five target points are *People*, *Data*, *Software and Hardware (SW/HW)*, and *Network*. For each target point, we determined the defense mechanisms to prevent any potential social engineering security attack targeting that target point. Figure 4.1 depicts a tree-structure taxonomy of the main target points and the defense mechanisms for each target point. Next, this section provides a detailed description of each target point and the defense mechanisms against social engineering attacks targeting these target points. Employees and organizations should be aware of these defense mechanisms to prevent any social engineering attack [6].

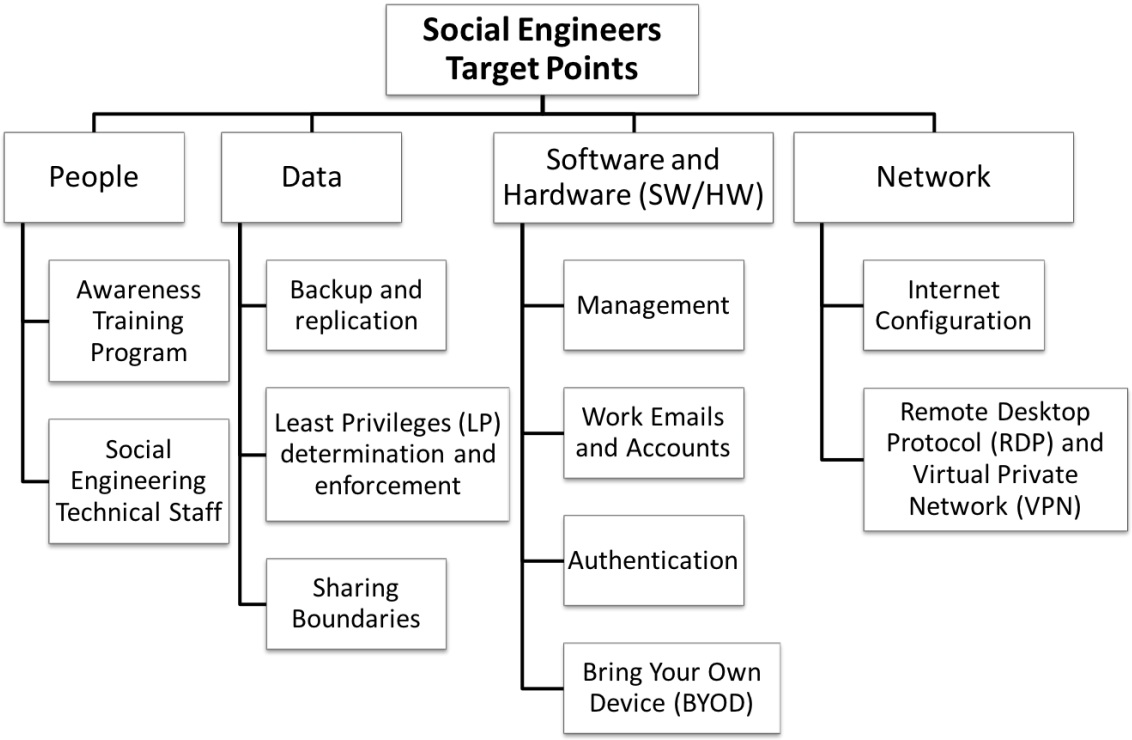

Figure 4.1: A comprehensive taxonomy of social engineering defense mechanisms for each target point [7]

4.1.1 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 share

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. Below the description of these two defense mechanisms.

- Awareness Training Program:

  Previous research has shown that Information Security Awareness (ISA) is vital in mitigating the risks associated with information security breaches [12]. Raising employees awareness level is the best way to limit the effect of social engineering techniques. Employees need guidance to make the right decisions in the digital world. According to [66], "without any guidelines to follow when exceptional situations arise, an employee is liable to take actions that compromise the organization's data or cause the organization to miss out on lucrative business prospects.". Therefore, organizations need to provide well-rounded awareness training programs to their employees to stay secure.

- Social Engineering Technical Staff:

  To prevent social engineers from performing their tricks on people, each organization should be equipped with a social engineering technical staff. This team needs to be knowledgeable about social engineering security attacks and their consequences. The existence of this team can be helpful and beneficial to educate employees and to prevent social engineering attacks.

4.1.2 Data

Data is a valuable asset for any organization, and it is a critical target point by cyberattacker either at the personal level or at the organizational level. At the personal level, social engineers might target personal data of a high profiled employee such as family pictures, videos, salary, etc. At the organizational level, many types of sensitive information can be

targeted, such as planning documents, employees personally identifiable information (PII), financial information, or any private organizational data. 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.

- Backup and Replication:

  Constantly backing up the data and creating replication of the data, either inline or offline replication, ensure the integrity and the availability of the data. Employees should be aware of any backup and replication policy in their organizations so they can consider it for the organization's data stored either on the servers or even on their work computers. Providing consistent rules for backup and replication management is critical to ensure the High Availability (HA) of the organization's data.

- Least Privileges (LP) Determination and Enforcement:

  Determining the exact data each employee or system needs could be a complex task, but it is crucial for security comprehension as well as preventing a data breach or, at least, minimizing it. Applying the least privilege security principle ensures that each employee has access only to the data he needs to perform his work. According to [38], protecting organizations' systems and securing their data require correct enforcement of the "least user rights" and administrator privileges.

- Sharing Boundaries:

  This defense mechanism ensures that employees are aware of the sharing boundaries policies of each information they have access to within and outside their organizations. For example, some information can be shared only between workers in the same depart-

ment, whereas others can be shared only between workers on the same organization, etc.

4.1.3 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, organization 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.

- SW/HW Management:

  Managing software systems and hardware components to prevent social engineering attacks requires that each organization have clear policies regarding software installation, configuration, updates, hardware maintenance plan, etc. Such clear security policies, if exists and employees are aware of, would prevent many social engineering attacks such as *Technical Expert* and *Support Staff*.

- Work Emails and Accounts:

  Protecting work emails by filtering any potential spams are critical since, in most cases, they are considered as a formal way of communication. Therefore, if a social engineer was able to send an email from an employee's work email, this could lead to severe consequences. On the other hand, social engineers mainly use emails as a medium to spread their malicious intent. Therefore, employees need to know about security policies. Organizations must ensure that their employees are aware of what is acceptable and unacceptable use of the work emails and accounts as well as preventing any unauthorized computers or locations from accessing employees work emails and accounts.

- Authentication:

  To prevent social engineers from impersonating employees, an authentication process should include "something they have", such as biometric information or their phone devices, in addition to the "something they know", such as username and password, as described in [72]. If organizations incorporate such a policy, then employees are protected against many social engineering attacks. There are many techniques to increase the security of the authentication process, including two-factor authentication, using captcha, complex passwords, specific IP address, open a service during certain hours, etc.

- Bring Your Own Device (BYOD):

  Many organizations allow their employees to use their own devices for work purposes to increase the efficiency and the productivity of employees during the working hours. However, many employees do not pay attention to the security risks associated with this BYOD policy. Therefore, such employees need to be aware of any security risks that theses devices might pose. According to [30], the lack of understanding of BYOD by organizations puts them at risk of losing control of their critical information resources and assets. Hence, it is essential to ensure that these devices are not compromising the confidentiality, integrity, and availability goals of information security. This can be done by incorporating effective security and privacy policies to manage BYOD.

4.1.4 Network

Employees access databases and other servers through a network. The network could be a Local-Area Network (LAN), Wide-Area Network (WAN), wireless network or wired network, etc. Each network has a different security policy. For example, if an employee is connecting to the LAN network of an organization, he might have access to servers that he would

not have access to if he is connecting from his home network. Moreover, most organizations nowadays allow VPN (Virtual Private Network) or RDP (Remote Desktop Protocol) to allow their employees to access the local network remotely. All of these different network security policies bring security threats to organizations if the employees are not aware of them. For example, if an employee accesses his/her organization's local network using a VPN from a public computer or his/her friend's computer, if that computer is compromised, then that employee risks his/her organization. To protect organizations' networks from potential social engineering attacks, employees should be aware of the different Internet configuration as well as the different network security policies regarding the VPN and the RDP.

- Internet Configuration:

  The Internet has enabled interconnection of different computer networks all over the world. Protecting confidential information has been made especially challenging due to the ever-changing array of social engineering tactics using the Internet. Thus, for any organization, it is vital to secure its networks, including the wired and the wireless networks. Additionally, employees should be aware of the different network configurations in their organizations.

- Remote Desktop Protocol (RDP) and Virtual Private Network (VPN):

  Although both RDP and VPN protocols support secure Internet communications, provide traffic integrity, confidentiality and authentication, it remains a complex and error-prone task. Hence, it is important to ensure the creation of a secure connection to an organization's network from any host by incorporating effective security policies. Such security policies need to be specified correctly in order to enforce access control and traffic protection appropriately. Moreover, employees should be aware of these security policies and the risks these protocols might bring to their organizations. Fu et al. [29] indicate that RDP and VPN security policies require considering two levels: requirements level and implementation level. The correctness of implementation level security

policy can be verified by checking satisfaction of requirement level security policy.

4.2 Questionnaire 1: Measuring Employees Awareness Level of Social Engineering Defense Mechanisms

This section sheds some light on the results of our first questionnaire and analyzes employees awareness level of social engineering defense mechanisms.

4.2.1 Data Analysis and Results

In light of the taxonomy of social engineering defense mechanisms (Figure 4.1), we carefully designed a survey and distributed it among employees working in public, private, and non-profit organizations in Saudi Arabia [7]. 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. 58% of participants are male, whereas the rest are females. The sample represented a wide range of ages. Approximately 1% of 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 participants are 60 and above years old.

Regarding the qualifications of 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 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, we 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 participants were overconfident and stated that their work computers are very secure. Approximately 45% of 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 participants' accounts have been hacked or stolen at least once. Participants were asked to write about these incidents. We 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 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 85% of them received phone calls requesting their passwords.

When it comes to scam emails, only 42% of 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, we 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. Based on these results, organizations' computers can be easily infected with malicious software or viruses.

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 organizations have Information Exchange Policies (IEPs). Nearly, half of employees follow their instincts regarding information exchange.

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 participants use the same password for all of 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, we 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 stated 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. 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 on a daily basis. And while 19% of 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 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 are allowed to 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 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.

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 are allowed to 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 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.

Finally, participants were asked to share their thoughts and concerns regarding cybersecurity

policies in their organizations. Below are some answers (translated from Arabic to English):

- "The reason behind neglecting security policies is the way these are designed and written. These are complicated, unreadable, and not-understandable."
- "It would be better to separate the IT team and cybersecurity team. The latter should be linked directly to the organization's head/leader."
- "Supporting researchers/experts in cybersecurity is needed to make a difference."
- "Education is the key to protect the organizations assets. Special training programs should be designed for educational purposes, and should focus more on new employees as well as old employees who reject computerizing the organization's process/procedures."
- "There should be restricted sanctions for any employee who ignores the security policies of the organization."

4.2.2 Employees Awareness Level of Social Engineering Defense Mechanisms

To answer the second research question, RQ2, we 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 4.1).

To that end, we grouped the questions into different groups where each group measures the awareness level of a defense mechanism in the taxonomy. As a result, Figure 4.2 depicts the correlation between questions from the survey to the defense mechanisms from the taxonomy [7].

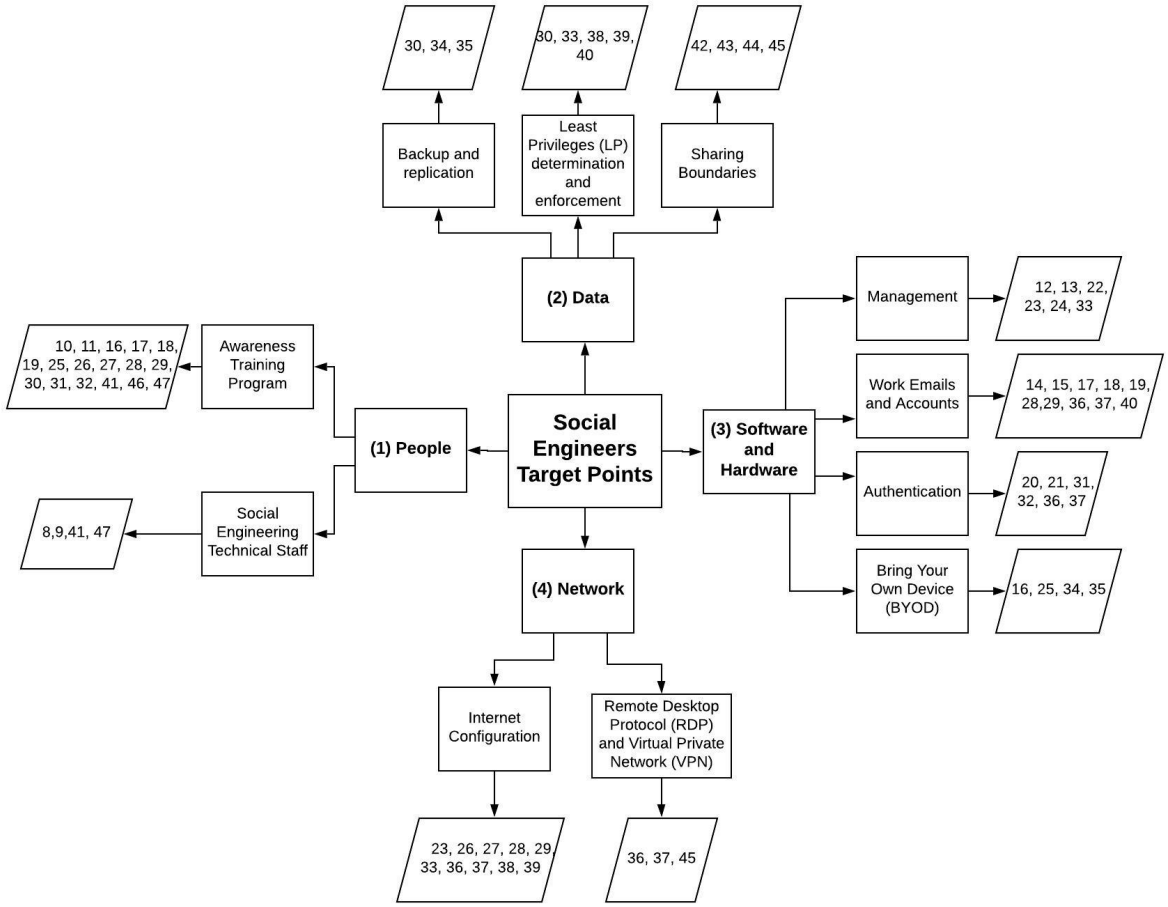

Figure 4.2: The correlation between the questions in the survey to the defense mechanisms in the taxonomy [7]

Using Figure 4.2, we calculated the employees awareness level regarding each social engineering defense mechanism as shown in Figure 4.3. From the figure, 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.

Figure 4.4 compares the awareness level of employees against social engineering defense mechanisms in public, depicted in blue bars, and private, depicted in orange bars, organizations.

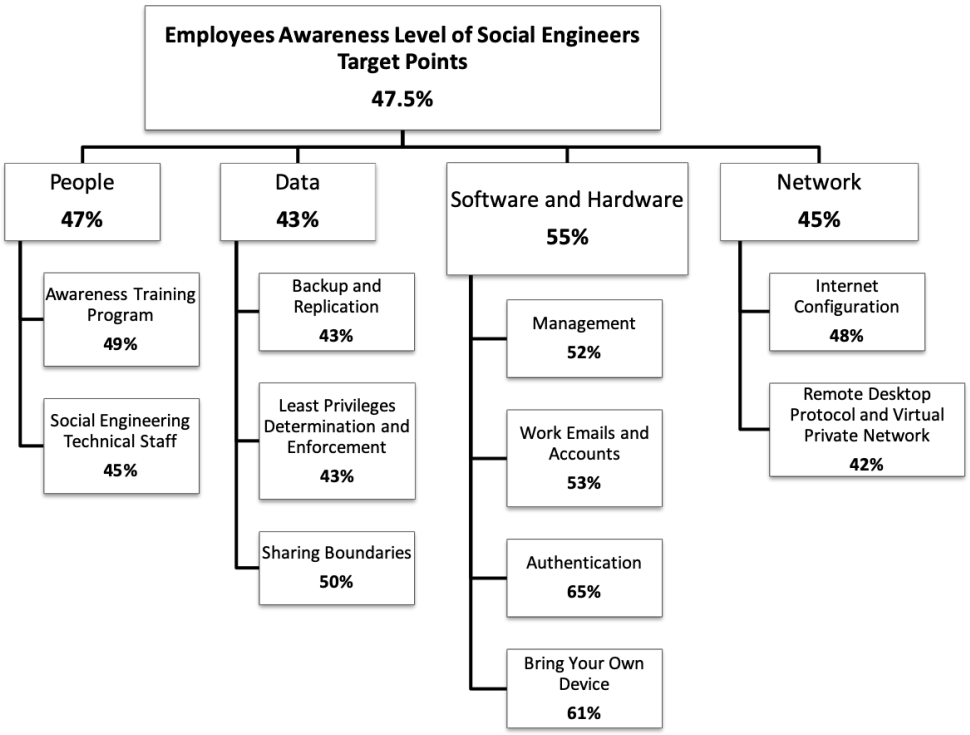

Figure 4.3: Employees' awareness level against the social engineering defense mechanisms [7]

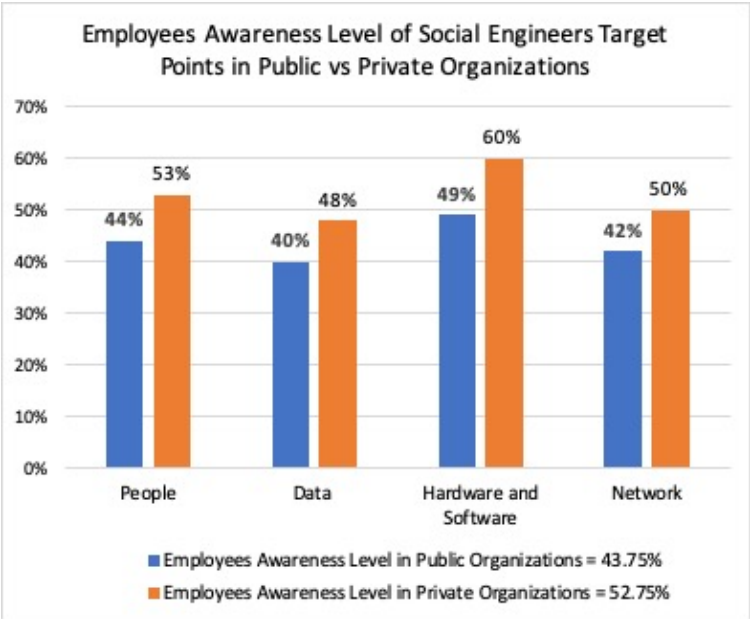

Figure 4.4: Comparison of employees awareness level in public and private organizations [7]

The figure indicates that the awareness level of employees in private organizations is more than the awareness level of employees in public 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. Such a worrisome number calls for urgent actions need to be taken from organizations to increase the awareness level of their employees.

Chapter 5

Social Engineering InfoSec Policies (SE-IPs)

In this chapter, we analyze the data we collected using our developed questionnaire and report our results. Then, we propose a Formal Model of SE-IPs that organizations can adopt. We conclude this chapter by measuring the incorporation level of SE-IPs in organizations.

5.1 Questionnaire 2: Measuring SE-IPs Incorporation Level in Organizations

In this section, we analyze the data from our second questionnaire and illustrate the results. In light of that, we measure SE-IPs incorporation level in organizations.

5.1.1 Data Analysis and Results

The survey has a total of 30 questions. The average time to complete it was 6 minutes. 1523 employees responded to our calls and answered 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. We asked the participants about the department that they are working in. Only 30.62% of them work in IT department.

After distributing the survey, we collected the data and performed an analysis. This section sheds light on some of the interesting results and findings from the survey [9].

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 addressed that they do not have an assigned email to report phishing emails to.

In regards of the existence of a Data Protection Policy, we asked some questions about data backup policy, information sharing policy, as well as transmitting, storing, labeling, 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, labeling, 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 Removable Storage Policy. Only 42.49% of employees addressed that they have to have an approval prior to using any portable storage device on your work-computer (such as USB/external hard drive).

To summarize data protection related results addressed 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's data. Hence, employees can take their organization's data with them upon their departure, which raises the risk of data loss in organizations.

Other survey questions were asked regarding 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. We 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 password for their work related accounts as their personal online accounts. We asked some questions regarding 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 addressed 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 caf 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.

The participants were asked Who is responsible for cybersecurity in their organizations. While cybersecurity is a shared responsibility and it is everyone's job, less than 1% of them addressed that. The remaining stated that it is the IT, the SOC, and/or the Information Security Department's responsibility. It's critical that structures, guidelines and processes are in place to make employees care and be responsible to remain safe online while at work.

The last question of the survey asked participants to provide any additional comments, concerns and/or advises that they may have regarding cybersecurity in their organizations. Some responses illustrate the lack of cybersecurity implementation such as the following. (1)

"My organization does not have the minimum requirements for cybersecurity maturity.", (2) "There is a lack of cybersecurity awareness in my organization. Most employees think that they are not targeted in the cyber-world.", (3) "My organization have an awareness program, but it is not mandatory.", (4) "We have a mandatory cybersecurity awareness program, but it contains a lot of ambiguous information. Moreover, to report a cybersecurity incident, the process is not clear and it takes a very long time.", and (5) "When it comes to cybersecurity, my organization is reactive and not proactive.".

Other responses reflected the lack of employees awareness of social engineering such as the following "Cybersecurity slows our performance in my organization. We cannot download any software and we are required to change our passwords periodically. Requiring connecting to the VPN when accessing the organization's portal remotely makes things complicated.".

5.1.2 SE-IPs Incorporation Level in Organizations

To answer the second research question, we analyzed the data obtained from the survey to measure the current incorporation level of SE-IPs in organizations.

To that end, we grouped the survey's questions into different groups where each group measure the incorporation level of a SESP in Figure 5.3. As a result, Figure 5.1 depicts the correlation between questions from the survey to the social engineering security policies in SE-IPs taxonomy.

As shown in Figure 5.1, 50.75% of Employees Awareness SE-IPs, 37.73% of Data related SE-IPs, 62% of HW/SW related SE-IPs, and 54.25% of Network related SE-IPs are incorporated. Overall, the study shows that only 51.18% of SE-IPs are incorporated in organizations. Such a worrisome number calls for urgent actions to be taken from organizations to increase this percentage to mitigate the risk of social engineering attacks.

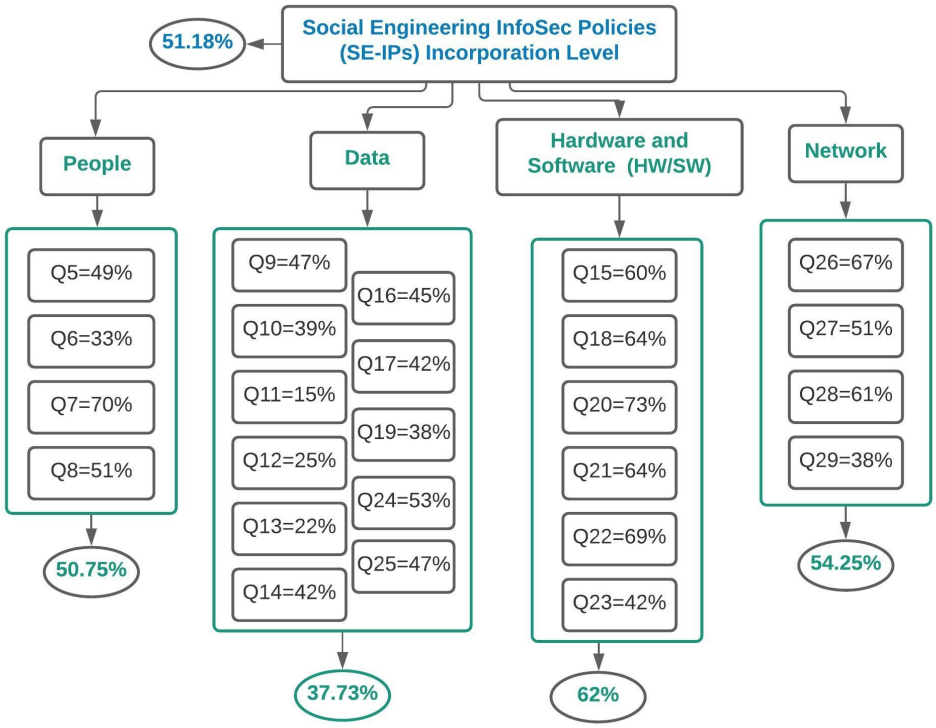

Figure 5.1: SE-IPs Incorporation Level in Organizations [9, 8]

Employees in the private sector are more aware of social engineering attacks than employees in the public sector [7]. Moreover, this paper indicates that the incorporation level of SE-IPs in private organizations is more that it is in public organizations as shown in Figure 5.2 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.

5.2 Formal SE-IPs Proposed Model

In light of our second survey's results, this section aims to answer the third research question, What are the SE-IPs that should be incorporated in organizations?, by defining the security

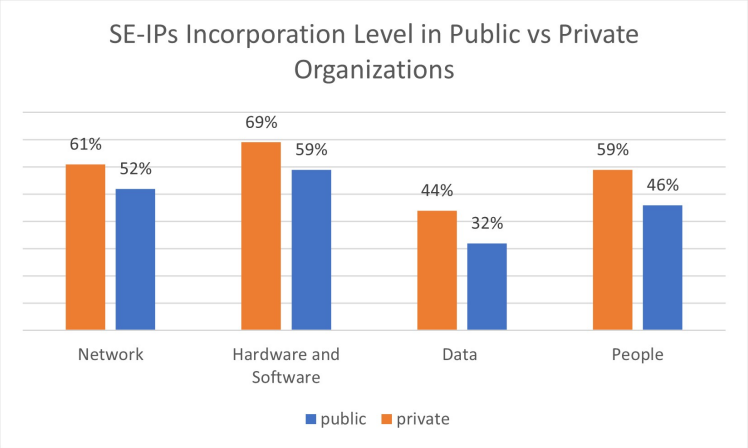

Figure 5.2: SE-IPs Incorporation Level in Public vs Private Organizations [9, 8]

requirements for the proper and secure use of the Information Technology services in organizations. Employees should be aware of these requirements to mitigate the risk of social engineering attacks and protect the Confidentiality, Integrity, and Availability (CIA) of the organization's data, as well as the organization's reputation and business outcomes. According to [57], Confidentiality refers to the protection of sensitive information from unauthorized disclosure, Integrity is defined as the accuracy, completeness, and validity of information in accordance with 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, we suggest incorporating 18 Social Engineering InfoSec Policies (SE-IPs) shown in figure 5.3. Table 2 briefly describes the policies and their short descriptions [9][8].

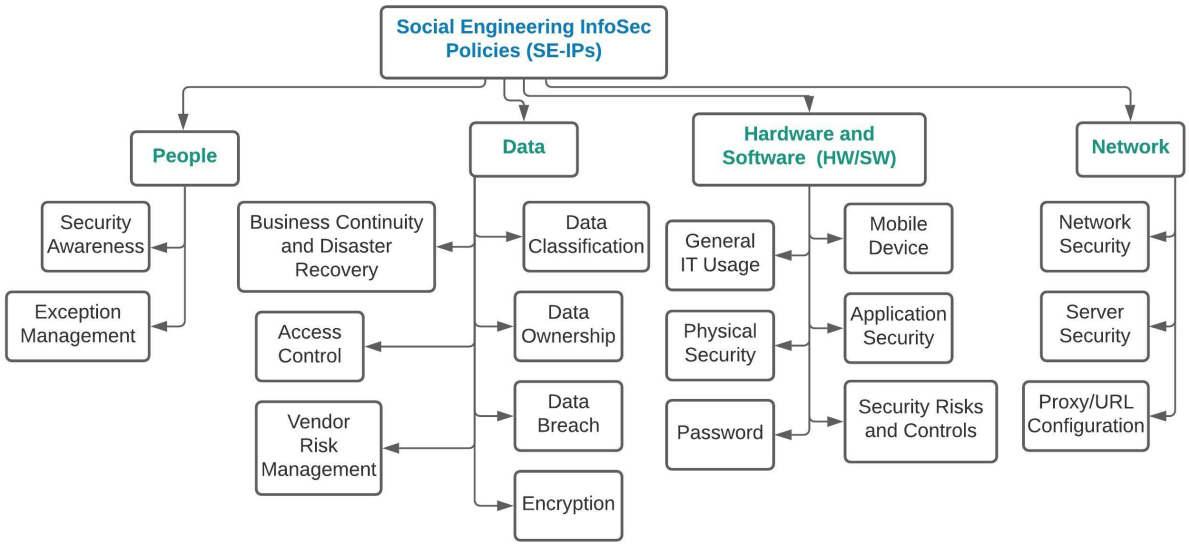

Figure 5.3: Proposed Social Engineering InfoSec Policies (SE-IPs) [9, 8]

Social Engineering InfoSec Policy	Brief Description
Exception Management Policy	To address the required approvals for any exceptions to the organizations policies and procedures.
Data Classification Policy	To cover the different types of data classifications and how each should be handled based on the level of confidentiality required.
Data Ownership Policy	To outline the details regarding data ownership, including creation, responsibilities, and control over the data.
Data Breach Policy	To outline the procedures required for reporting a data security breach.
Encryption Policy	To covers the requirements for encryption technologies used to secure their data.

Social Engineering InfoSec Policy	Brief Description
Business Continuity and Disaster Recovery Policy	To define the required controls around reducing vulnerabilities/single points of failure and testing contingency plans.
Access Control Policy	To cover the requirements for proper and secure control of access to IT services and infrastructure in the organization.
Vendor Risk Management Policy	To outline the requirements for assessing third-party vendor security risks.
Mobile Device Policy	To address the policy that should be applied to any mobile device issued by the organization or used for conducting business (e.g. BYOD Bring Your Own Device) which transmits or stores organizations data.
Application Security Policy	To cover secure coding practices, assessments, and remediation for any applications being developed or integrated with the organizations environment.
Security Risks and Controls	To outline security control requirements that must be in place to minimize and manage the organizations IT risks.
General IT Usage Policy	To outline the acceptable use of computer equipment in the organization.
Physical Security Policy	To outline the requirements for physically securing the organizations assets.
Password Policy	To address the requirements around password creation, password change, and password protection.
Network Security Policy	To cover standards for maintaining a secure network infrastructure to protect the integrity of organizations data and mitigate risk of a security incident.

Social Engineering InfoSec Policy	Brief Description
Server Security Policy	To establish standards for the base configuration of internal server equipment that is owned and/or operated by the organization.
Proxy/URL Configuration Policy	To outline the baseline of websites which should be blocked or permitted at the web proxy.

The following subsections from 5.2.1 to 5.2.8 explain in more depth our suggested Formal SE-IPs Model.

5.2.1 Security Awareness Policy:

To outline the requirements for security awareness and training. In order to protect organization's 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.

5.2.2 Exception Management Policy:

Organizations must incorporate and enforce a policy that addresses the required approvals for any exceptions to the organization's policies and procedures.

5.2.3 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 organization's data.

5.2.4 Data Ownership Policy:

Organizations must incorporate and enforce a policy that outlines the details regarding data ownership, including creation, responsibilities, and control over the data. Identifying the data owner should be performed by taking into account several factors such as: the primary user of the data, the creator of the data, and responsible party for that data, from a business, technical, legal, or regulatory standpoint.

5.2.5 Data Breach Policy:

Data breach can lead into severe operational, financial, reputational, and legal impacts in organizations[49]. 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's employees, partners and stakeholders from illegal or damaging actions by individuals, either knowingly or unknowingly.

5.2.6 Encryption Policy:

Organizations must incorporate and enforce a policy that covers the requirements for encryption technologies used to secure their data. The use of encryption should be restricted

to algorithms that have been proven to work effectively at securing organizational data both in transit and at rest. Additionally, all encryption keys must be protected to prevent their unauthorized disclosure and subsequent fraudulent use.

5.2.7 Business Continuity and Disaster Recovery Policy:

Most organization are equipped with the latest technological fronts but lacks disaster recovery plan management which may often lead to crisis [68]. The IT Business Continuity (BC) and Disaster Recovery (DR) standards provide requirements to manage business continuity related risks and effectively address crisis situations. The standards define the required controls around reducing vulnerabilities/single points of failure and testing contingency plans so that business processes and operations are adequately protected from interruption or data loss.

5.2.8 Access Control Policy:

This policy should cover the requirements for proper and secure control of access to IT services and infrastructure in the organization.

5.2.9 Vendor Risk Management Policy:

This Policy should outline the requirements for assessing third-party vendor security risks.

5.2.10 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 (e.g. BYOD Bring Your Own Device) which transmits or stores organization's data.

5.2.11 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 [19], SQL injection attack and Denial-of-service (DOS) attack are two most important security threads found in the web applications. SQL injection is a one of the web application security vulnerability in which SQL statements are altered by attackers which is executed by the web application and submitted to the database server. DOS attack is an attack which makes network resources unavailable to its intended users.

5.2.12 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.

5.2.13 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.

5.2.14 Physical Security Policy:

For any security-conscious business, a strong physical security must be enforced throughout the organization, without exception [60]. Hence, it is significant to incorporate and 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.

5.2.15 Password Policy:

In todays world of increasing dependence on computers and computer systems, it is imperative that we be able to rely on secure and confidential connections to the computers. Traditionally, this has been by authentication with usernames and passwords. According to [58], most employees had insecure passwords. Many of them create inherently weak usernames and passwords, while many others write their passwords down. The survey results were based on responses from 3000 IT professionals Organizations must incorporate and

enforce a password policy that covers the requirements for passwords to secure systems and accounts. Any system that handles valuable information must be protected with a password-based access control system. Password Policy must address three key policies, which are (1) Password Creation Policy, (2) Password Change Policy, and (3) Password Protection Policy.

5.2.16 Network Security Policy:

To cover standards for maintaining a secure network infrastructure to protect the integrity of organization's data and mitigate risk of a security incident.

5.2.17 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 organization's proprietary information and technology. [21] conducted a study about firewall informed by web server security policy. It illustrated how the firewall may intercept the content request, and receive information from the client device identifying which browser process initiated the content request. Before passing the content request to the appropriate web content server, the firewall may request and download a security policy from a security policy server. The security policy may notify the firewall which hosts are authorized/unauthorized for use with a particular domain, and which file types from each of these hosts are authorized/unauthorized for use with the particular domain. The firewall may then filter content related to the identified browser process based on the security policy.

5.2.18 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. The definition of any new website fitting the categories is done automatically by the tool via subscription. Subscription updates are based on the same approach virus definition updates are obtained.

Chapter 6

Conclusion and Future Research

This chapter summarizes our key contributions and findings, and shed some light on our plan to extend this research project in the future.

6.1 Conclusion

Social engineering, due in part to the increasing popularity and advancements in information technology and ubiquity of devices, has emerged as one of the most challenging cybersecurity threats in the contemporary age. In the context of cybersecurity, social engineering is the practice of taking advantage of human weaknesses through manipulation to accomplish a malicious goal. To mitigate the risk of social engineering attacks, organizations must raise employees awareness level of social engineering defense mechanisms and incorporate formal Social Engineering Security Policies (SE-IPs).

After investigating the current level of employees awareness of such attacks and the SE-IPs incorporation in organizations, the paper found that only 47.5% of employees are aware of social engineering tactics and their defense mechanisms and only 51.18% of SE-IPs are incor-

porated. To help raising these percentages, we developed a taxonomy of social engineering defense mechanisms and proposed a customizable model of SE-IPs that organizations can adopt, which consists of 18 SE-IPs categorized in 4 main categories.

In summary, this dissertation makes the following key contributions:

Taxonomy of Social Engineering Defense Mechanisms: we developed a comprehensive taxonomy of the five main target points of social engineers and the SE defense mechanisms. The five main target points are: people, data, hardware, software, and network.

Questionnaires: we designed two survey instruments. The first survey can be used to measure employees awareness level of social engineering defense mechanisms. The second survey can be used to measure the formal SE-IPs incorporation level in an organization.

Formal SE-IPs Model: we developed a customizable proposed model of SE-IPs that organizations can adopt.

Data Analysis: we surveyed 2314 employees in the two survey instruments in various employment sectors in Saudi Arabia, then analyzed the results and reported them.

The Data-set: we made the data available online for researchers and practitioners in the field of cybersecurity to replicate or extend the work.

6.2 Future Research

After developing well-designed SE-IPs, the next step is to provide some recommendations regarding enforcing those written policies by translating them to technical processes within the organization systems and develop an awareness training session for organizations to educate their employees about SE-IPs to mitigate the risk of social engineering attacks.

Moreover, because defending against social engineering involves understanding the attack tactics that are particularly effective today, we are planning to investigate how to assess an organization readiness for social engineering attacks by simulating phishing attacks after receiving a written permission from the organization.

As other venues of future directions, we are planning to replicate the research in the US and compare the results, and examine the data-sets we have using Structural Equation Modeling (SEM), which is a framework of a number of different multivariate techniques/methods that includes measurement theory (psychology), path analysis (epidemiology and biology), correlation/Regression (statistics), simultaneous equations (econometrics), and factor analysis (psychology and statistics).

Bibliography

[1] V. 2018. 2018 data breach investigations report, 2018.

[2] T. Ahmad. Corona virus (covid-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity. *Available at SSRN 3568830*, 2020.

[3] H. Aldawood and 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*, pages 110–115. ACM, 2019.

[4] H. Aldawood and G. Skinner. Contemporary cyber security social engineering solutions, measures, policies, tools and applications: A critical appraisal. *International Journal of Security (IJS)*, 10(1):1, 2019.

[5] H. Aldawood and G. Skinner. Reviewing cyber security social engineering training and awareness programspitfalls and ongoing issues. *Future Internet*, 11(3):73, 2019.

[6] D. N. Alharthi, M. M. Hammad, and A. C. Regan. A taxonomy of social engineering defense mechanisms. pages 27–41, 2020.

[7] D. N. Alharthi and A. C. Regan. Social engineering defense mechanisms: A taxonomy and a survey of employees awareness level. pages 521–541, 2020.

[8] D. N. Alharthi and A. C. Regan. A literature survey and analysis on social engineering defense mechanisms and infosec policies. pages 41–61, 2021.

[9] D. N. Alharthi and A. C. Regan. Social engineering infosec policies (se-ips). pages 57–74, 2021.

[10] A. Alzahrani. Coronavirus social engineering attacks: Issues and recommendations. *Int. J. Adv. Comput. Sci. Appl.*, 11(5):154–161, 2020.

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

[12] N. A. G. Arachchilage and S. Love. Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38:304–312, 2014.

[13] A. J. Aviv, K. L. Gibson, E. Mossop, M. Blaze, and J. M. Smith. Smudge attacks on smartphone touch screens. *Woot*, 10:1–7, 2010.

[14] T. Bakhshi, M. Papadaki, and S. Furnell. A practical assessment of social engineering vulnerabilities. In *HAISA*, pages 12–23, 2008.

[15] S. S. Basamh, H. Qudaih, and J. B. Ibrahim. An overview on cyber security awareness in muslim countries. *International Journal of Information and Communication Technology Research*, 2014.

[16] F. Bélanger, S. Collignon, K. Enget, and E. Negangard. Determinants of early conformance with information security policies. *Information & Management*, 54(7):887–901, 2017.

[17] A. Berg. Cracking a social engineer,[online]. lan times, 1995.

[18] R. Beuran, K.-i. Chinen, Y. Tan, and Y. Shinoda. Towards effective cybersecurity education and training. 2016.

[19] 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)*, pages 1–6. IEEE, 2016.

[20] C. Bronk and E. Tikk-Ringas. The cyber attack on saudi aramco. *Survival*, 55(2):81–96, 2013.

[21] H. V. Carames. Firewall informed by web server security policy, July 2 2020. US Patent App. 16/697,082.

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

[23] D. D. Cheong. Cyberattacks in the gulf: lessons for active defence. 2012.

[24] A. Chitrey, D. Singh, and V. Singh. A comprehensive study of social engineering based attacks in india to develop a conceptual model. *International Journal of Information and Network Security*, 1(2):45, 2012.

[25] M. Choi, Y. Levy, and A. Hovav. The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse. In *Proceedings of the Pre-International Conference of Information Systems (ICIS) SIGSEC–Workshop on Information Security and Privacy (WISP)*, 2013.

[26] N. Y. Conteh and P. J. Schmick. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, 6(23):31, 2016.

[27] T. Dimkov, A. Van Cleeff, W. Pieters, and P. Hartel. Two methodologies for physical penetration testing using social engineering. In *Proceedings of the 26th annual computer security applications conference*, pages 399–408, 2010.

[28] B. M. E. Elnaim and H. A. S. W. Al-Lami. The current state of phishing attacks against saudi arabia university students.

[29] Z. Fu, S. F. Wu, H. Huang, K. Loh, F. Gong, I. Baldine, and C. Xu. Ipsec/vpn security policy: Correctness, conflict detection, and resolution. In *International Workshop on Policies for Distributed Systems and Networks*, pages 39–56. Springer, 2001.

[30] A. B. Garba, J. Armarego, D. Murray, and W. Kenworthy. Review of the information security and privacy challenges in bring your own device (byod) environments. *Journal of Information privacy and security*, 11(1):38–54, 2015.

[31] I. Ghafir, V. Prenosil, A. Alhejailan, and M. Hammoudeh. Social engineering attack strategies and defence approaches. In *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, pages 145–149. IEEE, 2016.

[32] S. Granger. Social engineering fundamentals, part i: hacker tactics. *Security Focus, December*, 18, 2001.

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

[34] M. Gupta and R. Sharman. Social network theoretic framework for organizational social engineering susceptibility index. *AMCIS 2006 Proceedings*, page 408, 2006.

[35] 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)*, pages 489–494. IEEE, 2018.

[36] C. Hadnagy. *Social engineering: The art of human hacking*. John Wiley & Sons, 2010.

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

[38] R. Heartfield and G. Loukas. A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys (CSUR)*, 48(3):37, 2016.

[39] T. Herath and H. R. Rao. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2):154–165, 2009.

[40] 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*, 17:33–37, 2016.

[41] S. Inc. Surveymonkey, Accessed 2019.

[42] ITU. Committed to connecting the world, Accessed 2019.

[43] R. Kalniņš, J. Puriņš, and G. Alksnis. Security evaluation of wireless network access points. *Applied Computer Systems*, 21(1):38–45, 2017.

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

[45] K. J. Knapp, R. F. Morris Jr, T. E. Marshall, and T. A. Byrd. Information security policy: An organizational-level process model. *Computers & Security*, 28(7):493–508, 2009.

[46] K. Krombholz, H. Hobel, M. Huber, and E. Weippl. Advanced social engineering attacks. *Journal of Information Security and applications*, 22:113–122, 2015.

[47] 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*, 45:13–24, 2019.

[48] K. Manske. An introduction to social engineering. *Information systems security*, 9(5):1–7, 2000.

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

[50] B. D. Medlin, J. A. Cazier, and D. P. Foulk. Analyzing the vulnerability of us hospitals to social engineering attacks: how many of your employees would share their password? *International Journal of Information Security and Privacy (IJISP)*, 2(3):71–83, 2008.

[51] F. Mouton, L. Leenen, and H. S. Venter. Social engineering attack examples, templates and scenarios. *Computers & Security*, 59:186–209, 2016.

[52] F. Mouton, M. M. Malan, L. Leenen, and H. S. Venter. Social engineering attack framework. In *2014 Information Security for South Africa*, pages 1–9. IEEE, 2014.

[53] NCSC. National cybersecurity center, Accessed 2019.

[54] C. Okoli and K. Schabram. A guide to conducting a systematic literature review of information systems research. 2010.

[55] G. L. Orgill, G. W. Romney, M. G. Bailey, and 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*, pages 177–181. ACM, 2004.

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

[57] T. R. Peltier. *Information security fundamentals*. CRC press, 2013.

[58] L. Rosencrance. Survey: Insecure passwords can be costly for companies. *Computer-World. August*, 8:2003, 2003.

[59] F. Salahdine and N. Kaabouch. Social engineering attacks: A survey. *Future Internet*, 11(4):89, 2019.

[60] J. Saleem and M. Hammoudeh. Defense methods against social engineering attacks. In *Computer and network security essentials*, pages 603–618. Springer, 2018.

[61] N. Sarginson. Securing your remote workforce against new phishing attacks. *Computer Fraud & Security*, 2020(9):9–12, 2020.

[62] 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*, 9(9):1460, 2020.

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

[64] S. Shane and M. S. Schmidt. Hillary clinton emails take long path to controversy. *The New York Times*, 2015.

[65] H. Siadati, T. Nguyen, P. Gupta, M. Jakobsson, and N. Memon. Mind your smses: Mitigating social engineering in second factor authentication. *Computers & Security*, 65:14–28, 2017.

[66] M. Siponen and J. Iivari. Is security design theory framework and six approaches to the application of isps and guidelines. *Journal of the Association for Information Systems*, 7(7):445–472, 2006.

[67] M. Siponen, M. A. Mahmood, and S. Pahnila. Employees adherence to information security policies: An exploratory field study. *Information & management*, 51(2):217–224, 2014.

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

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

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

[71] A. Thapar. Social engineering: An attack vector most intricate to tackle. *CISSP: Infosec Writers*, 2007.

[72] K. Thomas, F. Li, A. Zand, J. Barrett, J. Ranieri, L. Invernizzi, Y. Markov, O. Comanescu, V. Eranti, A. Moscicki, et al. Data breaches, phishing, or malware?: Understanding the risks of stolen credentials. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1421–1434. ACM, 2017.

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

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

Appendix I

A questionnaire to measure employees awareness level of social engineering defense mechanisms

Q#	The Question	The answers
Q#1	Age	○ Less than 20 ○ 20-29 ○ 30-39 ○ 40-49 ○ 50-59 ○ 60 or more
Q#2	Gender	○ Male ○ Female
Q#3	What is the highest degree or level of school you have completed?	○ Less than a High School Diploma ○ High School or equivalent ○ Community College ○ University ○ Advanced Degree
Q#4	Do you have any qualification/degree in an IT field?	○ Yes, I have a Diploma in an IT field. ○ Yes, I have a Bachelor degree in an IT field. ○ Yes, I have a Master degree in an IT field. ○ Yes, I have a PhD degree in an IT field. ○ No, I have no qualification/degree in an IT field.
Q#5	How often do you use the Internet every day?	○ Less than one hour ○ One-two hours ○ Two-three hours ○ More than three hours
Q#6	Where do you work?	○ Public organization ○ Private organization ○ Non-profit organization
Q#7	What is your job? (This is an optional question)	.....
Q#8	Does your organization have an Information Technology (IT) department?	○ Yes ○ No ○ I do not know
Q#9	If yes, does the IT department have a cybersecurity team?	○ Yes ○ No ○ I do not know
Q#10	My computer has no value to hackers, they do not target me.	○ True ○ False
Q#11	How secure do you feel your work computer is?	○ Very secure ○ Somewhat Secure ○ Not secure
Q#12	Do you know how to tell if your work computer is hacked or infected?	○ Yes, I know what to look for to see if my work computer is hacked or infected. ○ No, I do not know what to look for to see if my work computer is hacked or infected.

Q#	The Question	The answers
Q#13	Have you ever found a virus on your work computer?	○ Yes ○ No ○ I am not sure if my work computer has been infected before or not. ○ I do not know what a virus is
Q#14	Has any of your accounts been hacked or stolen? (Check all that apply)	○ Yes, a work-related account has been hacked or stolen. ○ Yes, a personal account has been hacked or stolen. ○ Yes, both a personal and a work-related accounts have been hacked or stolen. ○ No, none of my accounts has been hacked or stolen. ○ I am not sure.
Q#15	If yes, can you please write about that incident(s) in which your account has been hacked or stolen? I.e. how the hacker got your account password? (This is an optional question)	.....
Q#16	Have you ever received a phone call requesting personal information from someone you do not know?	○ Yes ○ No ○ Uncertain
Q#17	Have you ever received an email requesting personal information from someone you do not know?	○ Yes ○ No ○ Uncertain
Q#18	Do you know what a phishing attack is?	○ Yes ○ No
Q#19	Do you know what a scam email is and how to identify it?	○ Yes ○ No ○ I am aware of some scams, but probably not all of them.
Q#20	Have you ever been asked about your password by a co-worker?	○ Yes ○ No
Q#21	Have you ever given your work-related account password to someone else?	○ Yes ○ No
Q#22	Do you have an anti-virus tool that is up-to-date and enabled in your work computer?	○ Yes, I have an up-to-date and enabled antivirus in my work computer ○ I have an outdated antivirus in my work computer ○ No, I do not have an anti-virus in my work computer ○ I do not know if the antivirus is up-to-date or not ○ I do not know what an anti-virus is

Q#	The Question	The answers
Q#23	Is the firewall enabled in your work computer?	○ Yes, it is enabled. ○ No, it is not enabled. ○ I do not know if I have a firewall or not. ○ I do not know what a firewall is.
Q#24	Is your work computer configured to be automatically updated?	○ Yes ○ No ○ I do not know.
Q#25	Do you store your personal data such as your bank's credit card and bank numbers on your computer?	○ Yes ○ No
Q#26	Do you only access secure websites (HTTPS), and make sure there is a letter S before signing in to a sensitive website such as the bank's website?	○ Yes ○ No ○ Sometimes
Q#27	Have you ever clicked on a link, which led you to download a potentially dangerous file?	○ Yes ○ No ○ I am not sure. ○ I do not know how to tell if the file is dangerous or not.
Q#28	How careful are you when you open an attachment in your email?	○ I always make sure it is from a person I know and I am expecting an attachment. ○ As long as I know the person or the organization that sent me the email, I open it. ○ I always open attachments because my work computer is already secured.
Q#29	How often do you read or open spam emails?	○ Often ○ Rarely ○ Not at all ○ I do not know what SPAM is.
Q#30	If you receive an unusual request from your boss or a co-worker via email, such as sending some of organizations information to an unknown email, what do you do?	○ Send it right away. ○ Reply to the sender via email to verify his/her request. ○ Call the sender by phone to verify his/her request. ○ I would not send my organizations information to an unknown email.
Q#31	Do you use the same password for all of your work accounts?	○ Yes ○ No
Q#32	Do you use the same password for your work accounts as you do for your personal accounts, such as Facebook, Twitter or your personal email accounts?	○ Yes ○ No

Q#	The Question	The answers
Q#33	Have you downloaded and installed software on your work computer?	○ Yes ○ No ○ I cannot do it on my work computer since software installations are only done by IT.
Q#34	Can you use your own personal devices, such as your mobile phone or laptop, to store or transfer confidential organizations information?	○ Yes ○ No ○ I do not know
Q#35	How often do you take information from the office and use your personal computer to work on it?	○ Almost every day. ○ At least once a week. ○ At least once a month. ○ Very rare ○ Never
Q#36	Have you logged into work accounts using public computers, such as from a library, a cafe shop, a hotel lobby, etc.?	○ Yes ○ No
Q#37	If yes, do you use Virtual Private Network (VPN) to log remotely to your work accounts?	○ Yes ○ No
Q#38	At work, do you have policies on which websites you can visit?	○ Yes, there are policies which I fully understand. ○ Yes, there are policies limiting what websites I can and cannot visit while at work, but I do not know the policies. ○ No, there are no policies, I can visit whatever websites I want while at work. ○ I am not sure if we have policies for that.
Q#39	Do you login social media sites, such as Twitter and Facebook, using your work computer?	○ Yes ○ No
Q#40	Do you have policies on what you can and cannot use your work email for?	○ Yes, there are policies which I fully understand. ○ Yes, there are policies limiting what emails I can and cannot send while at work, but I do not know the policies. ○ No, there are no policies, I can send whatever emails I want to whomever I want. ○ I am not sure if we have policies for that.
Q#41	Do you know who to contact in case your work computer is hacked or infected?	○ Yes ○ No ○ I do not know

Q#	The Question	The answers
Q#42	Do you know what types of information you are allowed to exchange with your co-workers from a different departments in your organization?	○ Yes, I follow my organizations policy regarding this issue. ○ No, I just follow my instincts. ○ I am not sure if we have policies for that.
Q#43	Do you know what types of information you are allowed to exchange with other employees from a different organization?	○ Yes, I follow my organizations policy regarding this issue. ○ No, I just follow my instincts. ○ I am not sure if we have policies for that.
Q#44	Do you know what types of information you are allowed to exchange with the public?	○ Yes, I follow my organizations policy regarding this issue. ○ No, I just follow my instincts. ○ I am not sure if we have policies for that.
Q#45	Do you think that the contracts in your organization clearly oblige the contracting party to comply with the cybersecurity policies?	○ Yes ○ No ○ I do not know
Q#46	Do you think cybersecurity policies are clear and accessible to everyone in your organization?	○ Yes ○ No ○ I do not know
Q#47	Does your organization offer training sessions regarding social engineering security polices?	○ Yes and the attendance is mandatory. ○ Yes but the attendance is optional. ○ No, they do not. ○ I am not sure if there are such training sessions.
Q#48	Do you have any information you would like to share regarding this study? (This is an optional question)	.....

Appendix II

A questionnaire to measure the incorporation level of Social Engineering InfoSec Policies (SE-IPs)

Q#	The Question	The Answers
Q#1	Age	.....
Q#2	Where do you work?	○ Public Organization ○ Private Organization ○ Non-Profit Organization
Q#3	Do you work in the IT department?	○ Yes ○ No
Q#4	Do you think your work-computer would be of any interest or value to hackers or social engineers?	○ Yes ○ No ○ Uncertain
Q#5	Does your organization have a mandatory cybersecurity awareness training upon beginning employment and annually?	○ Yes ○ No
Q#6	When suspecting that a theft, breach, or exposure of organizations protected data has occurred, do you feel comfortable notifying the appropriate team in your organization?	○ Yes ○ No ○ Uncertain ○ I dont know whom to report such incidents to
Q#7	Does your organization have a mailbox or a designated contact to report any suspected phishing email?	○ Yes ○ No ○ Uncertain
Q#8	Does the computerized system in your organization save backups of your work?	○ Yes ○ No ○ Uncertain
Q#9	Do you backup your work yourself (such as by copying it on an USB/external hard drive or uploading it to a cloud storage) at the end of your working day?	○ Yes ○ No
Q#10	If yes, do you encrypt your files that contain your work (whether they are on USB/external hard drive or on a cloud/remote server)?	○ Yes ○ No

Q#	The Question	The Answers
Q#11	Does your organization 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)?	○ Yes ○ No ○ Uncertain
Q#12	Does your organization have policies regarding verifying who is on the other end of the phone call?	○ Yes ○ No ○ Uncertain
Q#13	Do you need to request an approval prior to use any portable storage device on your work-computer (such as USB/external hard drive)?	○ Yes ○ No ○ Uncertain
Q#14	Is your work-computer current with virus protection and software patches?	○ Yes ○ No ○ Uncertain
Q#15	Does your organization grant the access to IT services and infrastructure under the principle of least privilege, i.e. each user shall receive the minimum rights and access to resources needed for them to be able to perform their job responsibilities?	○ Yes ○ No ○ Uncertain
Q#16	Does your organization have policies regarding transmitting, storing, labeling, and handling sensitive information within/outside the organization?	○ Yes ○ No ○ Uncertain
Q#17	Do you need to request approval prior to installing software to your work-computer?	○ Yes ○ No ○ Uncertain
Q#18	Does your organization have policies regarding transferring organizations data to a personal email account? For example, sending a work-related email to a personal email account i.e. Google, Yahoo, Hotmail.	○ Yes ○ No ○ Uncertain

Q#	The Question	The Answers
Q#19	Does your organization have password creation requirements/guidelines such as minimum number of characters or including at least 1 symbol?	○ Yes ○ No ○ Uncertain
Q#20	Are you required to change your work-related password periodically?	○ Yes ○ No ○ Uncertain
Q#21	Do you use the same password for your work-related accounts as your personal online accounts?	○ Yes ○ No
Q#22	Do you need approval prior to using your own personal device to work on organizations documents and/or to login to your work-related accounts/emails?	○ Yes ○ No ○ Uncertain
Q#23	Do you transmit or store any work-related data via mobile device such as iOS or Android?	○ Yes ○ No
Q#24	If yes, do you regularly patch your mobile device operation within 90 days of the new OS release?	○ Yes ○ No ○ Uncertain
Q#25	Do you have an unlimited access to internet websites and services when using your work -computer?	○ Yes ○ No ○ Uncertain
Q#26	Can you access social media on your work computer without applying for a proxy exception?	○ Yes ○ No ○ Uncertain
Q#27	Have you logged in your work-related accounts using public WiFi, such as from a caf shop or a hotel lobby?	○ Yes ○ No ○ Uncertain
Q#28	Are you required to use a secure connection (i.e. VPN) when transmitting organizations data or accessing organizations resources?	○ Yes ○ No ○ Uncertain
Q#29	. Who is responsible for cybersecurity in organizations in general? (Optional)	.....
Q#30	. Please, provide any additional comments, concerns and/or advice that you may have regarding cybersecurity in your organization. (Optional)	.....