SOCIAL ENGINEERING INFOSEC POLICIES (SE-IPS)

Dalal Alharthi and Amelia Regan

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

ABSTRACT

The sudden increase in employees working primarily or even exclusively at home has generated unique societal and economic circumstances which makes the protection of information assets a major problem for organizations. 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, this paper develops a model of Social Engineering InfoSec Policies (SE-IPs) and investigates the incorporation of those SE-IPs in organizations. This paper proposes a customizable model of SE-IPs that can be adopted by a wide variety of organizations. The authors designed and distributed a survey to measure the incorporation level of formal SE-IPs in organizations. After collecting and analyzing the data which included over fifteen hundred responses, the authors found that on average, organizations incorporated just over fifty percent of the identified formal Social Engineering InfoSec Policies.

KEYWORDS

Cybersecurity, InfoSec, Security Policies, Social Engineering.

1. INTRODUCTION

Social engineering attacks have significant impacts on organizations. The damage can be devastating. Social engineers are looking for the easiest way into the organization systems, which is not to try and break the encryption on the organization database or type in every combination of characters to guess their employees' passwords. Often, the easiest way is to trick employees into giving them the keys. Hence, social engineers aim to exploit the weakest link in a security structure by manipulating individuals and organizations to divulge valuable and sensitive data [1]. 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) [2] [3]. According to [4], 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.

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 [5] [6]. Organizations must ensure that their employees understand the risks of social engineering and how to avoid becoming a victim. [7] emphasized

David C. Wyld et al. (Eds): AIAP, SIGML, CNSA, NIAI - 2021
pp. 57-74, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.110104

the need to adopt measures and tools, including policies and training programs, to mitigate the risk of social engineering attacks.

Additionally, recent security research [8] suggests that most organizations have unprotected data and poor social engineering cybersecurity policies in place, making them vulnerable to data loss. To successfully fight against social engineering attacks, it is imperative that organizations develop and adopt Information Security Policies (ISPs). [9] defined an information security policy (ISP) of an organization as a set of rules and policies related to employee access and use of organizational information assets. Unfortunately, the research lacks well designed formal Social Engineering InfoSec Policies (SE-IPs) that organizations can adopt to protect their assets in the cyber-world. To that end, the authors conducted a large-scale study to (1) develop a proposed customizable model of formal SE-IPs in organizations, and (2) investigate the incorporation level of those SE-IPs in organization.

To achieve (1) and (2), the authors designed, distributed, and analyzed a survey to investigate the incorporation level of SE-IPs in organizations. Then, considering the survey results as well previous work [2] [10], the paper developed a proposed model of SE-IPs that organizations can adopt. To summarize, the key contributions of this research are questionnaire to measure SE-IPs incorporation level in an organization, a customizable proposed model of formal SE-IPs that organizations can adopt, data analysis of 1523 responses from employees in various employment sectors, and available online dataset for researchers and practitioners in the field of cybersecurity to replicate or extend the work.

The remainder of this paper structured as follows. Section 2 provides the necessary background for this study as well as the related research efforts on social engineering security policies in organizations. Section 3 describes the research questions this paper tries to answer. Section 4 describes the methodology for surveying the employees and developing SE-IPs. Section 5 analyses the data collected and describes the results and the research achievements. Section 6 provides a proposed customizable model of formal SE-IPs. Section 7 calculates and describes formal SE-IPs incorporation level in organizations. Finally, the paper concludes with future work avenues in section 8.

2. RELATED WORK

This section discusses the related research efforts in light of the authors research, divided into two subsections as follows. Subsection 1 presents the authors previous work that provided a starting point for this study. Subsection 2 discusses the related work of other researchers.

2.1. Background

The authors earlier paper presented a taxonomy of the main target points of social engineers within organizations, which are people (employees), data, hardware, software, and networks [2]. The paper addressed the defense mechanisms for each of these target points as shown in Figure 1. For example, to defend employees against social engineering attacks, organizations must have an awareness training program, and it should be equipped with a technical staff that is knowledgeable about such attacks. To defend data, organizations must have some defense mechanisms related to backup and replication, least privileges determination and enforcement, and data sharing boundaries within and outside organizations. To defend the organization hardware and software, it is essential to have defense mechanisms related to management, work emails and accounts, authentication, and Bring Your Own Device (BYOD). Additionally, to defend the network, organizations should incorporate defense mechanisms related to internet

configuration as well as Remote Desktop Protocol (RDP) and Virtual Private Network (VPN). Employees and organizations should be aware of all these defense mechanisms to prevent social engineering attacks.

In light of [2] the authors conducted an experimental study which involved 791 participants, to measure employees' awareness of social engineering defense mechanisms [10]. That study revealed that only 47.5% of participants are aware of such mechanisms. This implies that more than half of the employees are not aware of social engineering attacks and their defense mechanisms.

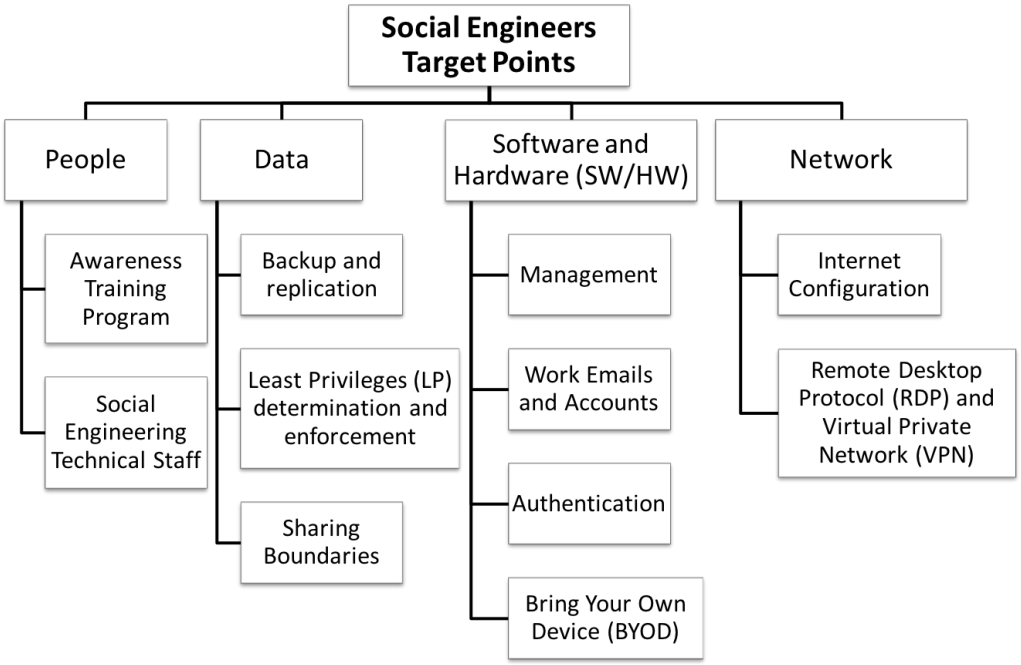

Fig. 1: Social Engineering Defense Mechanisms [2]

2.2. Related Work

Most of the proposed measures to mitigate cyber threats in the related research are focused on one element of cyber threats, namely, technical threats. Despite the importance and effectiveness of technical solutions, social engineers try to exploit the weakest link of an organization security, human vulnerabilities [11] [12]. Hence, the authors require solutions that understand and guard against human weaknesses. This subsection sheds light on related efforts to develop InfoSec policies to mitigate social engineering attacks.

Network administrators employ a variety of security policies to protect the organization data and services. [13] 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 cybersecurity program is having security controls and policies in place which are customized for their environment. [14] 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. [15] conducted an experimental study to assess end-user awareness of social engineering and phishing using a web-based survey, which presented a mix of 20 legitimate and illegitimate emails. The messages were categorized according to various characteristics of their appearance, all of which recipients may potentially use to aid their decision about whether to trust the content or not: identifiable recipient, identifiable sender, 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 [16], when employees are aware of their company information security policies and procedures, they are more competent to manage cybersecurity tasks than those who are not aware of their company policies. This result was based on a survey results from 579 business managers and professionals after employing Structural Equations Modeling (SEM) and ANOVA procedures on the results. In contrast, [12] 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) [17]. However, forcing individuals into the compliance might trigger undesired behaviours. [18] 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. [9] addressed the fact that social norms related to ISPs are the product of the principle ethical climate in an organization. The study explored the role of norms in employees' compliance with an organizational information security policy (ISP) and proposed a model to examine how ISP-related personal norms are developed and then activated to affect employee's ISP compliance behaviour. The results showed that ISP-related personal norms lead to ISP compliance behaviour, and the effect is strengthened by ISP-related ascription of personal responsibility. Social norms related to ISP (including descriptive, injunctive and subjective norms), awareness of consequences, and ascription of personal responsibility shape personal norms. Moreover, [19] explained the issue of employees' InfoSec noncompliance that causes the majority of organizational InfoSec breaches. When InfoSec policy (ISP) is implemented, it counteracts breaches and various approaches attempted to mitigate the phenomenon of ISP non-compliance. Yet, those approaches assume that employees will passively com- ply after they are enforced, and overlooked that human feelings, behaviour, and thoughts can affect the decision on whether to comply with the ISP. However, the ISP generates a new institutional logic featuring practices that collide with the existing institutional logic. This collision represented critical changes that are perceived as threats because the ISP values embedded in the practices are contrary to the employees' practices. These value changes significantly impact ISP non-compliance because the employees' values are misaligned with the ISP values.

In the context of enforcing an ISP, [20] suggested a simple enforcement system using a Software Defined Network (SDN) controller to block the malicious and restrict the anonymous users in the

organization network. They presented a fully configurable system for an institution using POX which is a famous SDN controller. A security policy can be enforced, accessed, and controlled through it. So that a single change in policy will be reflected in all the OpenFlow switches attached to the SDN resulting in reduced cost and time, as compared to the conventional networks where each switch is managed individually.

To ensure the implementation of the organization InfoSec policies, penetration testing is required. [21] 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 [22]. [23] suggested engaging the public in planning for disaster recovery, which will lead to increased stakeholder awareness of risk, available resources, and support for policies that build resilience.

3. RESEARCH QUESTION

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 [24]. Most cyber-criminals consider it much easier to abuse a person's 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 today workplace, it is vital to incorporate and enforce security policies in organizations to keep organization's networks safe from such attacks. To that end, this section presents the research questions this study tries to answer two questions, which are (RQ1) what are the formal SE-IPs that should be incorporated in organizations? And (RQ2) what is the current level of formal SE-IPs incorporation in organizations?

4. RESEARCH METHODOLOGY

This section describes the research methodology that the authors followed to develop a proposed SE-IPs model and to measure the level of SE-IPs incorporation in organizations.

4.1. Measuring the Incorporation of Formal SE-IPs

To measure the level of SE-IPs incorporation, the authors carefully designed a survey instrument. To build the survey, the authors relied on the taxonomy of social engineering defense mechanisms [2] and the resulting survey consisted of 30 questions 9. The survey was distributed

using SurveyMonkey [25], an online cloud-based service, to publish and distribute the survey. 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 participating 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 questionnaire can also be used by organizations to measure their incorporation level of SE-IPs. The average time to complete the survey was 6 minutes.

4.2. Developing a Formal SE-IPs Model

To develop the SE-IPs, the authors relied on the Taxonomy of Social Engineering Defense Mechanisms [2] as well as the results of the survey. Additionally, the authors developed a Systematic Literature Review of recent studies published on the subject. The literature review examined recent journals and conferences papers that contained "Social Engineering", "Cyber Attacks/Threats", and/or "Information Security Policies" in their titles. The authors then extracted Social Engineering InfoSec Policies (SE-IPs) from each paper.

4.3. Surveyed Employees

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

4.4. Selected Country

As a case study, this research focuses on public, private, and non-profit organizations in Saudi Arabia. According to the Saudi General Authority for Statistics, the Saudi population was 34.2 million in 2020 [26]. And according to The Statista Portal [27], the number of Internet users in Saudi Arabia is increasing rapidly, reaching about 89% of the population in 2020, which increases the need for enhanced cybersecurity awareness to defend sensitive information in the cyberspace. The authors selected Saudi Arabia as a country of this study for the following reasons:

- Saudi Arabia is the most targeted country in the Middle East and North Africa (MENA) region. For example, in 2012, over 35,000 of Aramco computers were infected by a virus called Shamoon, which operated like a time bomb (logic bomb malware). These devices were partially wiped or totally destroyed [28], [29], [30].

- Saudi Arabia designed and sponsored many governmental programs to prevent cybersecurity attacks as well as to increase the awareness level of its employees regarding cybersecurity. According to the Global Cybersecurity Index (GCI) created by the UN International Telecommunication Union (ITU) [31], Saudi Arabia achieved ranking first at the Arab level and 13 at the global level out of 175 countries for its commitment to cybersecurity.

- This paper is an extension of the research work in [2] and [10], which used the same sample for a related survey but had a lower response rate.

5. RESEARCH ACHIEVEMENTS

The survey has a total of 30 questions. The average time to complete it was 6 minutes. 1523 employees responded to the survey. The sample represented a wide range of ages. Approximately 1% of the participants are less than 20 years old, 16% are from 20-29, 40% are from 30-39, 26% are from 40-49, 14% are from 50-59, and 3% of the participants are 60 and above years old. 60.44% of the participants work for the government, 36.29% of them work in the private sector, and 3.27% work in the non-profit sector. The authors asked the participants about the department that they are working in. Only 30.62% of them work in IT department. After distributing the survey, the authors collected the data and performed an analysis. This section sheds light on some of the interesting results and findings from the survey.

Regarding the participants' cybersecurity knowledge and behaviour, one of every two employees mistakenly believes they are not a target for cyberattackers. The result showed that only 49.17% of participants think that their work computer would be valuable for hackers/social engineers. Additionally, only 33.42% of organizations have a cybersecurity awareness training program for their employees. Moreover, when suspecting that a theft, breach, or exposure of organizations protected data has occurred, only 70.31% of employees feel comfortable notifying the appropriate team in their organizations. However, 48.03% of them responded that they do not have an email address specifically assigned for reporting phishing emails.

In regards of the existence of a Data Protection Policy, the authors asked some questions about a data backup policy, an information sharing policy, and transmitting, storing, labelling, and handling sensitive information. The results illustrated that only 47.70% of computerized systems save backups of the employees' work. 60.11% of employees do backup their work using USB and/or cloud storage periodically, and 84.66% of them do not encrypt their work-related files. Moreover, only 25.75% of the participants addressed that their organizations have policies regarding what not to discuss over phone calls with your colleagues (i.e., organization information that is too sensitive to be discussed over phone). Additionally, only 21.88% of organizations have policies regarding verifying who is on the other end of the phone call. The survey showed also that only 42.23% of organization have policies regarding transmitting, storing, labelling, and handling sensitive information within/outside the organization. After that, a question was asked about having policies regarding transferring organizations data to a personal email account, i.e., sending a work-related email to a personal email account. Only 38.56% of organizations have those policies. Additionally, a question was asked regarding a Removable Storage Policy. Only 42.49% of employees addressed that they must have an approval prior to using any portable storage device on your work-computer (such as USB/external hard drive).

To summarize data protection related results discussed above, 60.11% of employees do backup their data, 38.56% forward work emails to their personal emails, and 42.49% of them use external storage devices to store organization data. Hence, employees can take their organization data with them upon their departure, which raises the risk of data loss in organizations.

Other survey questions were asked regarding hardware/software (HW/SW) protection policies. 60.31% of employees addressed that their work-computer is current with virus protection and software patches. Moreover, the survey showed that only 55.17% of organizations grant the access to IT services and infrastructure under the principle of least privilege. The authors also asked employees if they are required to request an approval prior to installing software to their work-computer. Only 64.38% of organizations have policies regarding that, which means that 35.62% of organizations are susceptible to downloading copyrighted software, offensive material, or files that are infected with harmful computer viruses.

Regarding Password Policies, 73.58% of organizations have password creation requirements/guidelines, and 65.18% of them enforce employees to change their passwords periodically. 31.02% of employees addressed that they use the same pass- word for their work-related accounts as their personal online accounts. The survey asked some questions regarding a Mobile Device Policy. Only 42.29% of organizations have a Bring Your Own Device (BYOD) Policy, while 46.50% of them allow their employees to store work-related data via mobile device such as iOS and/or Android. However, 52.91 % of employees reported that they do not regularly patch their phones OS within 90 days of the new OS release, which can lead to cyberattacks.

Regarding Internet Usage and Social Media Policies. Only 66.91% of organizations block access to some internet websites and services when using work-computer, the rest allow their employees to have an unlimited access to internet websites including websites that may be harmful and dangerous. Additionally, 66.31% of organizations do not have a Proxy/URL Configuration Policy, and employees in those organizations can access social media without applying for proxy exception. 38.96% of employees have logged in their work-related accounts using public WiFi, such as from a cafe shop or a hotel lobby. Using public WiFi can lead to cyber-risks such as Man-in-the-Middle, malware distribution, snooping and sniffing. While using VPN services can help establish secure and encrypted connections, only 38.23% of participants addressed that they use it when transmitting organizations data or accessing organizations resources remotely.

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 responsibility. It is 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 (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 an exceptionally 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 "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 portal remotely makes things complicated.".

6. PROPOSED MODEL OF FORMAL SE-IPS

This section aims to answer the first research question, RQ1 (What are the formal SE-IPs that should be incorporated in organizations?) by defining the security 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 data, as well as the organization reputation and business outcomes. According to [32], 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 and to protect its CIA, this paper suggested incorporating 18 formal Social Engineering InfoSec Policies (SE-IPs) shown in Figure 2.

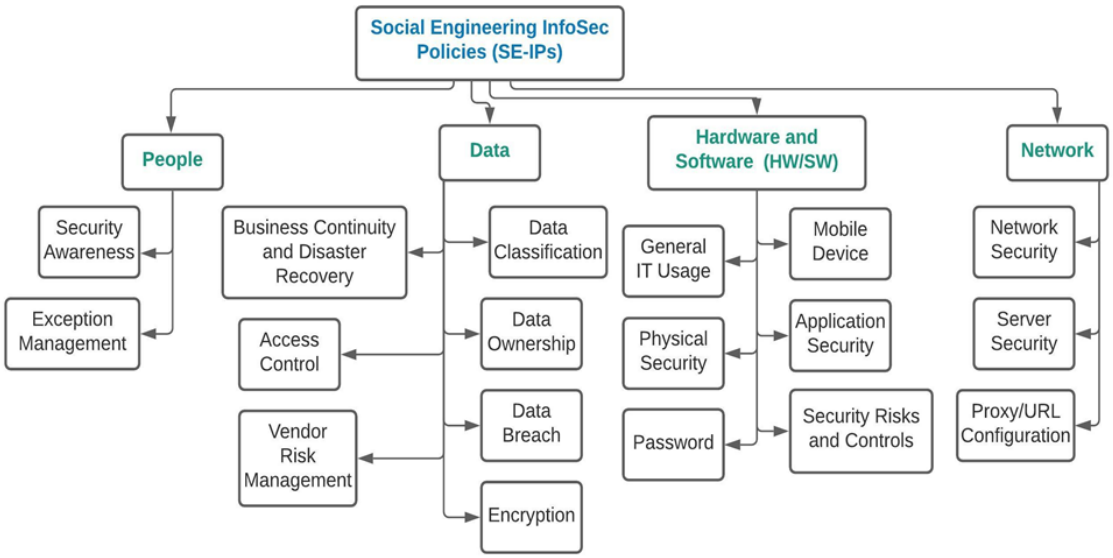

Fig. 2: Proposed Formal Social Engineering InfoSec Policies (SE-IPs)

Below are the policies and their short descriptions.

1. **Security Awareness Policy:** To outline the requirements for security awareness and training. To protect organization assets, all employees need to defend the integrity and confidentiality of the organization resources. One of the best ways to achieve a significant and lasting improvement in information security practice is through raising awareness of everyone who interacts with information assets.
2. **Exception Management Policy:** To address the required approvals for any exceptions to the organization policies and procedures.
3. **Data Classification Policy:** To cover the different types of data classifications and how each should be handled based on the level of confidentiality required. Different levels of data classifications exist, ranging from public to highly confidential, and specific levels of security are required for storing and transmitting organization's data.
4. **Data Ownership Policy:** To outline the details regarding data ownership, including creation, responsibilities, and control over the data.
5. **Data Breach Policy:** Data breach can lead into severe operational, financial, reputational, and legal impacts in organizations [33]. Hence, it is vital to incorporate/enforce a Data Breach Policy to outline the procedures required for reporting a data security breach. This will help protecting the organization employees, partners and stakeholders from illegal or damaging actions by individuals, either knowingly or unknowingly.
6. **Encryption Policy:** To cover the requirements for encryption technologies used to secure organization's data.
7. **Business Continuity and Disaster Recovery Policy**: Most organization are equipped with the latest technological fronts but lacks disaster recovery plan management which may often lead to crisis [22]. 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.

8. **Access Control Policy:** To cover the requirements for proper and secure control of access to IT services and infrastructure in the organization.
9. **Vendor Risk Management Policy:** This Policy should outline the requirements for assessing third-party vendor security risks.
10. **Mobile Device Policy:** Mobile devices create added risk and potential targets for data loss. Usage of such devices must be in alignment with appropriate standards and encryption technology must be used. This policy should be applied to any mobile device issued by the organization or used for conducting business (i.e., BYOD Bring Your Own Device) which transmits or stores organization's data.
11. **Application Security Policy:** To cover secure coding practices, assessments, and remediation for any applications being developed or integrated with the organizations environment. Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities be remediated prior to production deployment. Additionally, organizations must be aware of web application threats. According to [34], 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.
12. **Security Risks and Controls:** The Consolidated IT Controls Catalog (CITCC), known as the Blue Book, is a baseline of IT security controls intended to provide IT Management, information custodians, and staff with a set of consolidated control requirements that must be in place to minimize and manage the organizations IT risks. The controls outlined are mandatory requirements based on the applicability to specific IT environments and follow the premise of, implement once, satisfy many requirements.
13. **General IT Usage Policy:** To outline the acceptable use of computer equipment in the organization. It should cover general IT usage of the organization's resources including, but not limited to: Acceptable Use, Internet Usage, Electronic Mail, Wireless Connections Remote Access, Workstation Security, Removable Storage Media, Software Installation, and Social Media.
14. **Physical Security Policy**: For any security-conscious business, a strong physical security must be enforced throughout the organization, without exception [35]. Hence, it is significant to incorporate/enforce a policy that outlines the requirements for physically securing the organization's assets, including but not limited to computer hardware, workstations, servers, printers, and building/room access.
15. **Password Policy:** To cover the requirements for passwords that secure systems and accounts. Any system that handles valuable information must be protected with a password-based access control system. Password Policy must address Password Creation Policy, Password Change Policy, and Password Protection Policy.
16. **Network Security Policy:** To cover standards for maintaining a secure net- work infrastructure to protect the integrity of organization data and mitigate risk of a security incident.
17. **Server Security Policy:** To establish standards for the base configuration of internal server equipment that is owned and/or operated by the organization. Effective implementation of this policy will reduce the risk of unauthorized access to the organization proprietary information and technology. [36] 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.

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.

7. FORMAL SE-IPS INCORPORATION LEVEL

To answer the second research question, RQ2 (What is the current level of formal SE-IPs incorporation in organizations?), the authors analyzed the data obtained from the survey, to measure the current incorporation level of SE-IPs in organizations. To that end the survey questions were grouped so that each group measures the incorporation level of an SE-IP shown in Figure 2. As a result, Figure 3 depicts the correlation between questions from the survey to the social engineering security policies in the SE-IPs taxonomy.

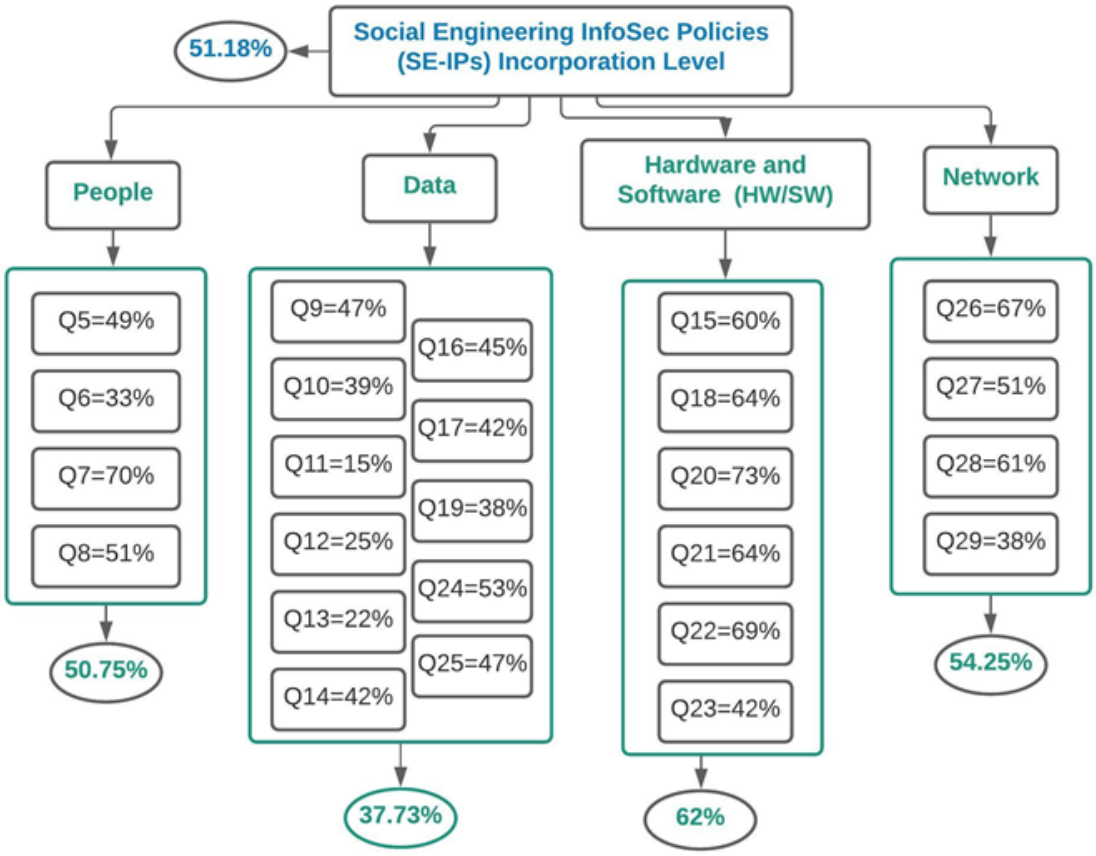

Fig. 3: Formal SE-IP Incorporation at the Organizational Level

For example, to measure the incorporation level of formal SE-IPs related to protecting the organization Hardware and Software, the authors analyzed the results from six survey questions as shown in Figure 3 and addressed in Table 1. Using the same methodology, the paper correlated between the questions from the survey to a Social Engineering InfoSec Policy (SE-IP) and found the following. 50.75% of Employees have Awareness regarding SE-IPs, 37.73% are aware of Data related SE-IPs, 62% of HW/SW related SE-IPs and 54.25% of Network related SE-IPs. Note that the numbers provided at the bottom are averages within each SE-IP category and the number at the top is the average across all SE-IP categories. 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.

Table 1. The incorporation level of Data-related SE-IPs

Q#	**The Question**	**The Answer**
Q#15	Does your organization grant the ac- cess to IT services and infrastructure under the principle of least privilege, i.e., each user shall receive the mini- mum rights and access to resources needed for them to be able to perform their job responsibilities?	o Yes o No o 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.	o Yes o No o Uncertain
Q#20	Are you required to change your work-related password periodically?	o Yes o No o Uncertain
Q#21	Do you use the same password for your work-related accounts as your personal online accounts?	o Yes o 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?	o Yes o No o Uncertain
Q#23	Do you transmit or store any work- related data via mobile device such as iOS or Android?	o Yes o No

Employees in the private sector are more aware of social engineering attacks than employees in the public sector [10]. 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 4 that compares SE-IPs incorporation level in public, depicted in blue bars, and private, depicted in orange bars, organizations. The figure indicates that 58.25% of SE-IPs are incorporated in private organizations, comparing to 47.25% of them in public organizations.

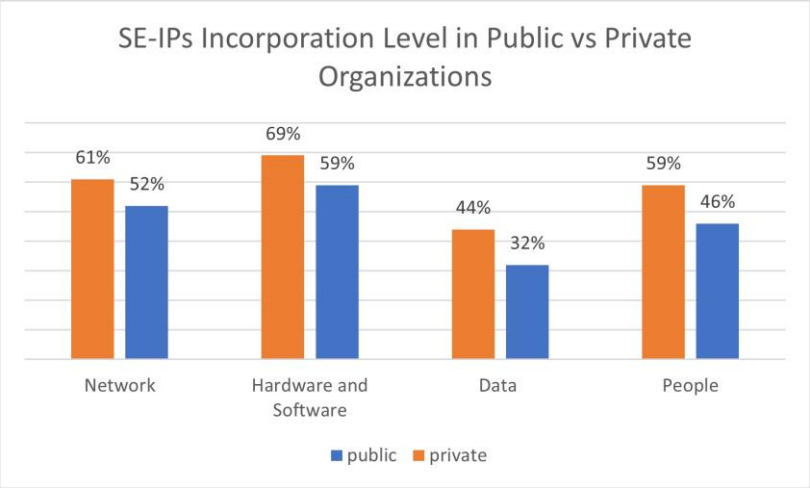

Fig. 4: Formal SE-IPs Incorporation Level in Public vs Private Organizations

8. CONCLUSIONS

Social engineering 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 incorporate Social Engineering InfoSec Policies (SE-IPs). After surveying 1523 employees in various employment sectors to investigate the current level of formal SE-IPs incorporation in organizations, the paper found that only 51.18% of formal SE-IPs are incorporated. To help raising this percentage, the authors proposed a customizable model of SE-IPs that consists of 18 SE-IPs categorized in 4 main categories. In summary, the key contributions of this research are a survey instrument that can be used to measure SE-IPs incorporation level in an organization, a customizable proposed model of formal SE-IPs that organizations can adopt, and an available online dataset for researchers and practitioners in the field of cybersecurity to replicate or extend the work.

The authors 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 developed questionnaire questions were designed carefully to match recent and real social engineering-based attacks on organizations.

After developing well-designed SE-IPs, the next step is to provide some recommendations regarding enforcing those written policies and translating them to technical processes within organizations system. Moreover, as another venue of future directions, the authors are planning to develop an awareness training session for organizations to educate their employees about mitigating the risks of social engineering security attacks.

ACKNOWLEDGMENTS

The first author was supported by a generous fellowship from Shaqra University. All errors and omissions are the responsibility of the authors alone.

Additionally, the authors gratefully acknowledge and appreciate the significant contributions from managers in the Saudi public and private organizations, whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication.

REFERENCES

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

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

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

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

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

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

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

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

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

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

[11] N. Y. Conteh and P. J. Schmick, "Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks," *International Journal of Advanced Computer Research*, vol. 6, no. 23, p. 31, 2016.

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

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

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

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

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

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

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

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

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

[21] 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*, 2010, pp.399–408.

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

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

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

[25] S. Inc., "SurveyMonkey," Accessed 2020. [Online]. Available: https://www.surveymonkey.com/

[26] Stats, "Saudi general authority for statistics," Accessed 2020. [Online]. Available: https://www.stats.gov.sa/
[27] Statista, "Statista," Accessed 2020. [Online]. Available: https://www.statista.com/
[28] C. Bronk and E. Tikk-Ringas, "The cyber-attack on Saudi Aramco," *Survival*, vol. 55, no. 2, pp. 81–96, 2013.
[29] D. D. Cheong, "Cyberattacks in the gulf: lessons for active defence," 2012.
[30] S. S. Basamh, H. Qudaih, and J. B. Ibrahim, "An overview on cybersecurity awareness in Muslim countries," *International Journal of Information and Communication Technology Research*, 2014.
[31] ITU, "Committed to connecting the world," Accessed 2020. [Online]. Available: https://www.itu.int/en/Pages/default.aspx
[32] T. R. Peltier, *Information security fundamentals*. CRC press, 2013.
[33] T. McClelland, "The insider's view of a data breach-how policy, forensics, and attribution apply in the real world," 2018.
[34] R. Bhor and H. Khanuja, "Analysis of web application security mechanism and attack detection using vulnerability injection technique," in *2016 International Conference on Computing Communication Control and automation (ICCUBEA)*. IEEE, 2016, pp. 1–6.
[35] J. Saleem and M. Hammoudeh, "Defense methods against social engineering attacks," in *Computer and network security essentials*. Springer, 2018, pp. 603–618.
[36] H. V. Carames, "Firewall informed by web server security policy," Jul. 22020, uS Patent App. 16/697,082.

AUTHORS

Dalal Alharthi Alharthi received a B.S in Computer Science, a M.P.A in Public Administration, and a M.S in Computer. She is a Ph.D. Candidate in Computer Science at University of California, Irvine. She is also a Resident Engineer at Palo Alto Networks. She is equipped with 12+ years of work experience between academia and industry. Her research interests are in the field of Cybersecurity; Network Security; Cloud Security; Privacy; Human-Computer Interaction; and Artificial Intelligence.

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

APPENDIX: A QUESTIONNAIRE TO MEASURE THE INCORPORATION LEVEL OF SOCIAL ENGINEERING INFOSEC POLICIES (SE-IPS)

Q#	The Question	The Answer
Q#1	Age	.....
Q#2	Where do you work?	o Public Organization o Private Organization o Non-Profit Organization
Q#3	Do you work in the IT department?	o Yes o No
Q#4	Do you think your work-computer would be of any interest or value to hackers or social engineers?	o Yes o No o Uncertain
Q#5	Does your organization have a mandatory cybersecurity awareness training upon beginning employment and annually?	o Yes o 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?	o Yes o No o Uncertain o I do not 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?	o Yes o No o Uncertain
Q#8	Does the computerized system in your organization save backups of your work?	o Yes o No o Uncertain
Q#9	Do you backup your work yourself (such as by copying it on an USB/ex- ternal hard drive or uploading it to a cloud storage) at the end of your working day?	o Yes o 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)?	o Yes o No
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)?	o Yes o No o Uncertain
Q#12	Does your organization have policies regarding verifying who is on the other end of the phone call?	o Yes o No o Uncertain
Q#13	Do you need to request an approval prior to use any portable storage de- vice on your work-computer (such as USB/external hard drive)?	o Yes o No o Uncertain

Q#	The Question	The Answer
Q#14	Is your work-computer current with virus protection and software patches?	o Yes o No o Uncertain
Q#15	Does your organization grant the ac- cess to IT services and infrastructure under the principle of least privilege, i.e., each user shall receive the mini- mum rights and access to resources needed for them to be able to perform their job responsibilities?	o Yes o No o Uncertain
Q#16	Does your organization have policies regarding transmitting, storing, labeling, and handling sensitive information within/outside the organization?	o Yes o No o Uncertain
Q#17	Do you need to request approval prior to installing software to your work-computer?	o Yes o No o 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.	o Yes o No o Uncertain
Q#19	Does your organization have pass- word creation requirements/guide- lines such as minimum number of characters or including at least 1 symbol?	o Yes o No o Uncertain
Q#20	Are you required to change your work-related password periodically?	o Yes o No o Uncertain
Q#21	Do you use the same password for your work-related accounts as your personal online accounts?	o Yes o 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?	o Yes o No o Uncertain
Q#23	Do you transmit or store any work- related data via mobile device such as iOS or Android?	o Yes o No
Q#24	If yes, do you regularly patch your mobile device operation within 90 days of the new OS release?	o Yes o No o Uncertain
Q#25	Do you have an unlimited access to internet websites and services when using your work - computer?	o Yes o No o Uncertain
Q#26	Can you access social media on your work computer without applying for a proxy exception?	o Yes o No o Uncertain
Q#27	Have you logged in your work-related accounts using public WiFi, such as from a café' shop or a hotel lobby?	o Yes o No o Uncertain

Q#	The Question	The Answer
Q#28	Are you required to use a secure connection (i.e., VPN) when transmit- ting organizations data or accessing organizations resources?	o Yes o No o 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)	.....