Jouni Ali-Kovero

PROTECTING AGAINST SOCIAL ENGINEERING ATTACKS IN A CORPORATE ENVIRONMENT

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

ABSTRACT

Ali-Kovero, Jouni
Protecting against social engineering attacks in a corporate environment
Jyväskylä: University of Jyväskylä, 2020, 78 pp.
Information Systems, Master's Thesis
Supervisor: Siponen, Mikko

The purpose of this Master's thesis is to study the means of protecting against social engineering attacks in a corporate environment. The work is carried out by means of a literature review and a qualitative study, consisting of interviews with cybersecurity leaders in some of the biggest companies in Finland. The literature review part of this work discusses the phenomenon of Social Engineering (SE) from different viewpoints. At first, a definition for SE is formed. After that, an overview of different attack models and methods is discussed. Based on earlier research, a taxonomy of different attack methods is formed. Finally, protective measures against social engineering attacks are discussed. The literature review acts as a foundation for empirical research, which studies the actual protective measures organizations have implemented to protect themselves from social engineering attacks. Based on the conducted research, social engineering can be defined as the act of exploiting weaknesses in human psychology and thereby manipulating victims to either divulging or granting access to confidential information or data. Finnish organizations seem to have protected themselves against SE quite well, but there seems to be room for improvement especially in security training of personnel and physical security controls.

Keywords: Social engineering, security control, information security, security awareness

TIIVISTELMÄ

Ali-Kovero, Jouni
Käyttäjän manipuloinnilta suojautuminen organisaatioympäristössä
Jyväskylä: Jyväskylän yliopisto, 2020, 78 s.
Tietojärjestelmätiede, Pro gradu -tutkielma
Ohjaaja: Siponen, Mikko

Tämän Pro gradu –tutkielman tarkoitus on tutkia yritysten tapoja suojautua käyttäjän manipulointiin (eng. Social Engineering) pyrkiviltä hyökkäyksiltä. Tutkielma toteutettiin kirjallisuuskatsauksen ja haastatteluihin perustuvan kvalitatiivisen tutkimuksen keinoin. Tutkimuksen haastateltavat edustavat Suomen suurimpien yritysten tietoturvajohtoa. Työn kirjallisuuskatsaus tarkastelee käyttäjän manipulointia ilmiönä eri näkökulmista. Ensin määritellään käyttäjän manipulointi käsitteenä, minkä jälkeen tarkastellaan erilaisia käyttäjän manipulointiin tähtääviä hyökkäysmalleja ja metodeja. Hyökkäysmetodit luokitellaan taksonomisesti aiempaan kirjallisuuteen perustuen. Lopuksi tarkastellaan erilaisia keinoja suojautua käyttäjän manipulointiin tähtääviltä hyökkäyksiltä. Kirjallisuuskatsaus luo pohjan työn empiiriselle tutkimukselle, jossa tarkastellaan keinoja, joita yritykset ovat käyttöönottaneet sosiaaliselta manipuloinnilta suojautumiseen reaalimaailmassa. Tehdyn tutkimuksen perusteella käyttäjän manipulointi voidaan määritellä toiminnaksi, jossa ihmismielen heikkouksia hyväksikäyttämällä pyritään manipuloimaan uhria siten, että saataisiin tämä joko luovuttamaan arkaluontoista tietoa, tai sallimaan siihen pääsy. Tutkimuksen perusteella vaikuttaa siltä, että suomalaiset organisaatiot ovat suojautuneet käyttäjän manipuloinnilta melko hyvin. Kehityskohteita vaikuttaa kuitenkin olevan erityisesti käyttäjien koulutuksessa ja fyysisen turvallisuuden kontrolleissa.

Asiasanat: Käyttäjän manipulointi, tietoturvakontrolli, tietoturva, turvallisuustietotuus

FIGURES

TABLES

TABLE OF CONTENTS

1 Introduction

Publications addressing the topic of information security in a corporate context rarely fail to mention humans (and especially the organization's own employees) as the biggest security risk. The risks do not necessarily occur due to malicious activity, but rather because of poor understanding and negligence. For instance, EY's Global Information Security Survey (GISS) of 2018-2019 revealed that organizations see careless employees as the most probable vulnerability increasing their risk exposure (EY, 2018).

The aforementioned fallibility of human beings is what makes social engineering attacks possible. A cynical person might perceive social engineering as being nothing short of lying and deceiving and social engineers as con artists. In a sense, there would be some truth to this: social engineering (hereinafter also *SE*) is about creating deceptive pretexts. This is done by tricking the victims in various ways. In short, social engineering refers to the techniques used attackers to gain access to the desired information. This is done by exploiting the flaws in human logic (Luo, Brody, Seazzu, & Burd, 2011).

Since there is a human factor involved, social engineering is a problematic phenomenon from an organization's perspective. Even if companies can implement various security controls to protect themselves (e.g. multi-factor-authentication, firewalls and other forms of network segmentation, physical guards, server hardenings, etc.), it is unlikely they can ever completely mitigate the risk caused by a human factor. This is why humans have been, and most probably will continue being, one of the biggest vulnerabilities attackers seek to exploit. As ENISA (European Network and Information Security Agency) threat landscape report of 2018 states about the current threat landscape, "…there is a shift towards reducing the use of complex malicious software and infrastructures and going towards low profile social engineering attacks" (European Network and Information Security Agency, 2018, p. 7). PwC's Global State of Information Security –survey seems to point to the same direction: the majority of respondents (mostly CEO, CIO & CISO) say that their information security incidents occurred due to social engineering –related activities, such as phishing or employees and their social media being exploited. Still, only 52 % have an employee security training program in place (PwC, 2018).

The objective of this thesis is to gain a better understanding of the concept of social engineering and study the techniques used in social engineering attacks. Because of the writer's background in corporate security, it was chosen to study the phenomena in a corporate setting. In addition to gaining an understanding of the concept and techniques used, the goal is to shed light on the protective measures (e.g. policies, controls, procedures, and guidelines) organizations have implemented to protect themselves from such attacks.

1.1 Background

In one form or another, social engineering has existed as long as there has been life intelligent enough to deceive. The activity is prominent across the animal kingdom, but one species has developed particularly good at it: us, humans. It's been frowned upon throughout history and among different cultures. In fact, it has been so strongly disliked that in many cultures it has been considered a sin. It has been prohibited even in the ten commandments. Of course, social engineering is not only about deception, but the bottom line is that social engineering is about *influencing* other people. Sometimes the intentions are good, sometimes bad.

It could be argued that one of the most famous historical examples of social engineering is the story of Trojan Horse, told by Homer in his mythical book *Odyssey*. In the story, the army of Greeks seemingly decides to retreat after a long and wearing war against Trojans. As a gesture of humility, the Greeks leave a large wooden horse for the Trojans, who unsuspectingly accept this trophy of victory. The Trojans decide to bring the horse to their city for celebration. For this, they even have to tear down part of their city wall. What they do not realize, is that the horse is actually hollow and full of Greek soldiers. When the night falls, the Greeks break out from the horse and conquer the city of Troy. The rest is history, and nowadays Trojan Horse is a term used to describe a family of malware.

Of course, the term *social engineering* is of more recent origin. It was first coined as *sociale ingenieurs* by J.C Van Marken in an 1894 essay. Van Marken argued that in addition to traditional engineers dealing with machines and mechanics, organizations need social engineers - engineers to deal with human challenges (Van Marken, 1894). Since Van Marken's essay, the term has been used in various contexts and across different fields of study. Social engineering has also been addressed in both academic studies, as well as in books and other pop-culture productions intended for a wider audience. Majority of the research has been conducted in the field of humanistic sciences and in the field of information security.

One of the most cited publications on the topic, Social engineering: The art of human hacking (Hadnagy, 2010), is written from a security point of view. The book provides a thorough outlook in social engineering, by discussing the methods and tools a social engineer might use, as well as preventive measures that can be taken to protect oneself. It also includes case studies of Kevin Mitnick, one of the most well-known social engineers. A large part of the research on social engineering (SE) concentrates on different techniques and tactics of SE, and common attack models (e.g., Granger, 2006; Hinson, 2008; Luo et al., 2011; Krobmholz, Hobel, Huber and Weippl, 2014; Heartfield & Loukas, 2015) Another typical approach is to study methods and practices that should or could be used to protect from SE attacks. What seems to be missing, however, are studies of what organizations are actually doing in order to protect themselves.

1.2 Research problems

As mentioned in the first part of this chapter, it seems that social engineering attacks are likely to become even more common. The problem with social engineering is that stricter security controls might not work very well against it. What makes protecting against SE so difficult, is the fact that the victims rarely understand they are being attacked before it is too late (Hinson, 2008). Organizations are well aware of the phenomena. According to the 2018 survey conducted by Ernst & Young, global C-suite executives identify careless and unaware employees as the biggest vulnerability to increase their risk exposure (EY, 2018). In fact, this result has stayed the same for at least six consecutive years from 2013 onwards (EY, 2017). However, it still seems that not so many are acting on the knowledge. As the PwC's Global state of Information Security –survey of 2018 reported, globally only 52 % of companies have an employee security awareness training program in place. The number seems rather low, given that one common-sense approach for mitigating risks of SE could be raising employee awareness.

Naturally, most organizations have implemented some sort of protective measures, some stronger and some weaker. As mentioned in the previous section, a large part of the research on social engineering seems to concentrate either on different tactics, or preventive measures. Still, not a lot of research has been done about the actual preventive measures organizations have implemented to protect themselves from SE attacks. Building on top of the existing literature, this research will shed light on not only different attack techniques but also categorize the attacks in a taxonomy. Also, the best practices and corporate reality of present-day security measures will be studied by means of qualitative research based on 10 interviews with information security leaders from some of the biggest companies in Finland.

1.3 Research objectives

This research has two primary objectives. The first is to learn more about social engineering: What constitutes as such, what kind of techniques are used and why the techniques work. The concept of social engineering will be thoroughly studied by means of a literature review.

The second objective of the research is to study the means of protecting against social engineering attacks. Based on a literature review and a later qualitative study, the best practices and current security measures are explored.

1.4 Research questions

In order to comprehensively address the research problem and to attain the defined research objectives, three research questions are formed:

1. What is social engineering?
2. How can organizations protect themselves against social engineering attacks?
3. How are organizations currently protecting themselves against social engineering attacks?

2 Overview of research

This chapter provides an overview of the scope and research methods used in writing this thesis. Similarly, the basic concepts needed for understanding the work are described. The research consists of a Systematic Literature review and an interview-based qualitative study. Both concepts are discussed in sections 2.1 and 2.3. The research method for the empirical part of this study in described in detail in chapter 5.

2.1 Systematic literature review

The literature review part of this thesis is conducted by means of a systematic literature review. According to Armstrong, Hall, Doyle and Waters (2011), a systematic literature review is a method of collecting secondary data in a systematic manner. This data in then synthetized in either qualitative or quantitative manner and its quality, validity and relevance are assessed. Systematic literature reviews aim to utilize the best information available (Harris, Quatman, Manring, Siston, & Flanigan, 2007). In other words, the information used should be relevant, up-to-date, have support from the scientific community and if necessary, the results presented should be repeatable.

According to Harris et al. (2007), a systematic literature review consists of seven steps:

1. Forming the preliminary *research questions* and hence setting a scope of interest for the study.
2. Developing a *research protocol*, or in other words, determining the methods of finding, extracting and analyzing relevant information.
3. *Literature search*, referring to the keywords and databases used for finding relevant information.
4. *Data extraction*, or determining and extracting the information within the defined scope of interest.
5. *Quality appraisal*, or determining the quality of the used information. The researcher could, for instance, use a checklist for making sure a set of predefined quality requirements are fulfilled.
6. *Data analysis and results,* referring to the act of analyzing the collected information and deriving some sort of results based on that evidence.
7. *Interpretation of results,* or forming a conclusion based on the research conducted.

For this thesis, the research questions were formed early on in the research planning phase. The questions were formed so that they would address the recognized research problem as thoroughly as possible.

The research protocol for this literature review is simple: only sources found online are used. Potentially interesting sources are first skimmed through and if they contain information on the area of interest, they are then added to a list of "possibly used" references.

Literature is searched primarily through two different databases: Google Scholar and IEEE Xplore. These databased are chosen, because they are among the biggest in terms of volume and are praised in many online rankings ranking scholarly search engines. Keywords used during this phase include: *social engineering, social engineering attack, persuasion, social manipulation, security control, physical security* and *physical penetration testing.*

Data extraction during the review is rather simple. First, the literature deemed as "possibly used" is read through in a more systematic and thorough manner. The literature is then categorized by different topics and notes are taken about the main points discussed. The papers are then moved to corresponding folders created in a reference tool. For instance, papers discussing different methods of social engineering are organized in one folder.

Once data from the literature is extracted, its quality is checked against two criteria: The articles and literature used should be either published in a well-established and recognized scientific journal, or have a significant amount of citations. Finally, the collected data is analyzed and results are derived and concluded.

2.2 Scope

Defining a clear scope is very important in almost every kind of project – be it software development, IS implementation, system auditing or even planning construction. Similarly, a clear scope plays significant importance when planning research, not only by setting a clear set of outlines for the work but also by saving the writer from a lot of trouble. If the scope is poorly defined, there is a risk of scope creep – the research project might end up expanding too much and fail to meet its schedule and objectives (Cerpa & Verner, 2009).

In this research, social engineering is studied from an information security perspective. The emphasis is on social engineering attacks; the techniques used and the reasons why they work. In other words, the focus is on intentionally exploiting un-intentional vulnerabilities. Unintentional mistakes, such as losing one's smartphone, are left out of scope. Similarly, even if the distribution of malware might include a social engineering aspect, this study will not address the details on how malware work or how organizations can protect against them.
The research will focus on industry best practices and organizations' current security measures against social engineering attacks. Security measures against other types of threats are left out of scope. The sample of organizations included in the empirical study is not industry-specific. It consists of both globally operating and Finnish organizations. However, the possible effects of cultural and demographic factors on the risk of successful SE attacks are left out of scope.

2.3 Qualitative study

To comprehensively address the defined research questions, this thesis also consists of a qualitative study. Whereas the literature review provides insight on best practices in protecting against social engineering attacks, the qualitative study strives to shed light on current practices and controls organizations have implemented to protect themselves.

Qualitative and quantitative research are sometimes presented as two fundamentally different methods through which we study different phenomena. Whereas quantitative methods can be seen as striving to explain phenomena via statistics and numerical data (Mujs, 2004), qualitative research is seen as favoring humans and observation as the primary source of information. The traditional view of difference when comparing the two approaches is best crystallized by Myers (1997): "*The motivation for doing qualitative research, as opposed to quantitative research, comes from the observation that, if there is one thing which distinguishes humans from the natural world, it is our ability to talk*!" (p. 3).

In other words, the stereotypical view on the differences of these methods is that quantitative research is mostly concerned with numbers and statistics whereas qualitative research focuses on observation, interviews, and other data collection methods that might not be so straightforward to quantify. This view is sometimes supplemented with the notion that rather than testing or trying to validate a hypothesis, qualitative research seeks to create a comprehensive understanding of the studied topic (Hirsjärvi, Remes, & Salovaara, 2009). However, as discussed by Brannen (2007) and also Siponen & Klaavuniemi (2020), this whole view may be too simplistic. For instance, as argued by Siponen and Klaavuniemi (2020), qualitative methods, such as observation, can be used in validating hypotheses, for instance in the field of biology. Similarly, it may not be too uncommon to see quantitative elements, such as the number of respondents, in a research paper otherwise characterized as qualitative in nature. In fact, the same is true for the research conducted for this work. Even though the data collection was done through interviews and the research is qualitative in nature, some results are presented numerically. The rationale for choosing this particular method of study is further described in section 5.1.

As the study was being designed, a model proposed by Maxwell (2008) was used as a guiding principle. According to Maxwell, in order to design a coherent study, one has to consider the goals, conceptual framework, research questions, methods and validity of the research:

- *Goals* can most easily be defined by asking "Why is this study worth doing?" In this case, the goal of the study is to answer the research questions, which were formed based on the notion that social engineering attacks are A) a common problem for organizations and B) the current methods of protecting against the attacks have not been widely studied.
- *Conceptual framework* describes the beliefs and prior information the researcher has on the topic. In terms of this research, the background

information regarding social engineering and the organization's protective measures are influenced with both prior research and the researcher's observations in working with clients.

- *Research questions* help to crystallize what the researcher specifically wants to learn about the topic of interest. Research questions for this study were formed to address the identified research problem and research objectives.
- *Method* describes the means of collecting and analyzing data. In the qualitative part of this study, the data was collected by means of semi-structured interviews. The method will be described in more detail in chapter 5.
- *Validity* refers to the degree to which the chosen research method is actually useful in studying the topic of interest.

2.4 Basic concepts

There are several basic concepts discussed in this thesis. These include information security, social engineering, attacker and security control. In order to comprehensively understand this thesis, these basic concepts must be understood. In this section, a brief definition will be provided for each of the concepts.

2.4.1 Information security (definition)

Historically, many overlapping terms have been used to describe security in an information context. These include *computer security, IT security, network security, information systems security* and *cybersecurity* to name a few. Since the focus in this thesis is on the human element of security, it was seen appropriate to use a term that is neutral in terms of how information is being processed or stored. This is why we will use information security as the term of choice, instead of the ones mentioned above. Information security does not imply a need for a technology component, even though most information nowadays is processed with computers.

As in the ISO 27000 –standard, information security is often defined as the measures taken to protect *confidentiality, integrity, and availability* of information (ISO/IEC, 2018). The three concepts need to be defined to comprehensively address the topic of information security:

- Information has *Confidentiality* if it is protected from unauthorized access and disclosure. In other words, only authorized individuals should have access to confidential information.
- Information has *integrity* when it is not corrupted or otherwise altered in an unauthorized manner. In other words, the integrity of information can be threatened if there is a risk of alteration or corruption.

- *Availability* of information ensures that authorized entities (be it computers or individuals) have access to information in a timely manner. In other words, the information should be available to those who need it when they need it.

These three concepts are often referred to as the CIA triad or C.I.A –triangle. The idea of *Confidentiality, integrity,* and *availability* of information has been the industry standard for decades. (Whitman & Mattord, 2011)

In addition to the three qualities of information mentioned above, Whitman and Mattord (2011) discuss three additional factors to be taken into account as well:

- Information has *Utility* if it can be used in a meaningful way. It other words, it has to be useful. If data is encrypted and the encryption key is lost, it can still retain its confidentiality, integrity, and availability, but is not of any use.
- *Possession* refers to the ownership of information. Information is said to be in one's possession if one obtains it. Possession is a different state from confidentiality because even if a breach of confidentiality always results in a breach of possession, the other way around is not necessarily true: One might *possess* encrypted data, but in absence of the encryption key, the data remains confidential.
- *Authenticity* refers to a quality of information of not being reproduced or fabricated. For instance, if this thesis was entirely plagiarized, but credited to Jouni Ali-Kovero, there would have been a breach of authenticity.

These six qualities of information are also referred to as the "Parkerian hexad" as they were introduced by Parker (1998).

2.4.2 Social engineering (definition)

As briefly discussed in the background section of this thesis, social engineering can mean different things in different contexts. Since this thesis focuses on security in a corporate setting, social engineering will be discussed in the context of security.

Since there is a lot of scientific literature about social engineering, the term has attracted many definitions. According to Luo et al. (2011), social engineering refers to the techniques used by attackers to gain access to desired information by exploiting flaws in human logic. Krombholz et al. (2014) state that social engineering is the act of "*manipulating a person into giving information to the social engineer*" (p. 1). It has also been called the "*'art' of influencing people to divulge sensitive information*" (Mouton, Malan, Leenen, & Venter, 2014, p. 1).

Hadnagy (2010), has a broader definition of social engineering. According to him, it is "*the act of manipulating a person to take an action that may or may not be in the "target's" best interest. This may include obtaining information, gaining access,* *or getting the target to take certain action*" (p. 32). For the purposes of this thesis, this definition will be used, because it takes into account the fact that social engineering might not always be malicious activity.

As Hadnagy's definition suggests, social engineering is a process encompassing several different steps. This is how it is also seen by Kevin Mitnick, one of the best known social engineers. According to Mitnick and Simon (2001), social engineering can be considered as a cyclical process consisting of four different phases. The process is depicted in Figure 1 below.

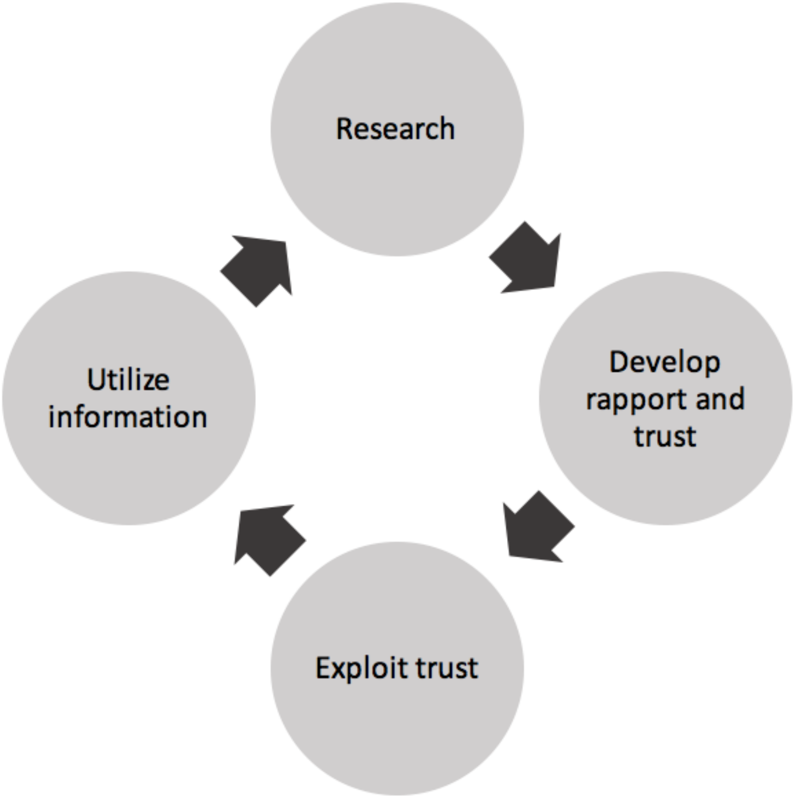

FIGURE 1. The four steps of a social engineering attack.

As Figure 1 depicts, the process of social engineering consists of *Research, Develop rapport and trust, Exploit trust and Utilize information* –phases. In the *research* –phase, the social engineer seeks to collect information about their target. This information could then be used to *develop rapport and trust* in their target. Once trust has been developed, it can be *exploited* in order to access information, which can then be later *utilized*. If needed, the accessed information can be utilized in further research as well.

There are several different techniques of SE that can be used in each of the discussed phases. Hence, social engineering can be seen as an umbrella term, encompassing a number of different techniques. These include, for instance, phishing, SMSishing, dumpster diving, shoulder surfing, watering hole, extortion and many more. Different techniques, as well theories on why social engineering works, will be discussed in detail in chapter 3. Also, a taxonomy for different social engineering attacks will be presented.

2.4.3 Attacker (definition)

Attacker (or hereinafter also *perpetrator* or *malicious actor*) is an individual with an intention to either cause harm to an organization or achieve some other goal by gaining unauthorized access to the organization's information assets. According to Pfleeger and Pfleeger (2012), an attacker must possess three qualities to ensure success: *Method, Motive, and Opportunity.*

- *Method* refers to the skill, tools, and techniques that are available to the attacker.
- *Motive* refers to the reasons for conducting an attack. These could include fame, financial gain, ideology, political gain, and terror. All attackers have some motives, since "attacking just for fun" is a motive as well.
- *Opportunity* refers to the possibilities (e.g. time, access, resources) for an attacker to conduct their attack.

If an attacker lacks any of these qualities, the attack will likely be unsuccessful or may not occur in the first place.

2.4.4 Security controls (definition)

According to Northcutt (2009), security controls are technical or administrative safeguards or countermeasures organizations implement to avoid, counteract or minimize loss or unavailability of information. Other definitions include: "*An action, device, procedure, or other measure that reduces risk by eliminating or preventing a security violation, by minimizing the harm it can cause, or by discovering and reporting it to enable corrective action*"(Stallings & Brown, 2015, p. 517).

To help organizations implement security controls, a number of control frameworks have been developed. These include, for instance, COBIT, NIST, COSO, ISO/IEC 27002 and ITIL. The controls in these frameworks are often based on industry-leading practices. According to Stallings and Brown (2015), controls can be classified in four classes:

- Management controls, addressing the issues relevant to an organization's management. These include controls related to policies, standards, and guidelines (PSGs). An example control could be, that an organization must have a security policy that is reviewed annually.
- Operational controls, which address the implementation of management controls. In other words, these controls are related to human work performed to implement management controls. An example of control could be that an organization has to have an incident response plan that is practiced annually.

- Technical controls address the correct use of hardware and software security capabilities. An example of control could be that the company passwords must be longer than 8 characters and contain numbers and special characters.

According to Northcutt (2009), controls can also be categorized by their nature in preventive, detective and corrective controls.

- **Preventive** controls seek to prevent a threat from realizing. For instance, a firewall can be considered as a preventive control.
- **Detective** controls seek to identify threats, should the preventive controls have failed. Examples of detective controls include intrusion detection systems and anti-virus software.
- **Corrective** controls seek to mitigate the damage, should a threat realize. A backup-scheme is an example of a corrective control.

Security control frameworks often contain dozens or even hundreds of different controls, addressing a wide array of security topics from physical security to the use of emerging technology. The controls are often divided into categories, such as *asset management, access control,* and *operations security.* Below, as an example, is a table listing the control categories and their objectives presented in ISO27002.

TABLE 1. ISO/IEC 27002 Security Control Objectives (Stallings & Brown, 2015).

Control Category	**Objective**
Security policies	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
Organization of Information Security	To establish a management framework to initiate and control the implementation and operation of information security within the organization, and to ensure the security of teleworking and use of mobile devices.
Human Resource Security	To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered, and to ensure that employees and contractors are aware of and fulfill their information security responsibilities, and to protect the organization's interests as part of the process of changing or terminating employment.

Asset Management	To identify organizational assets and define appropriate protection responsibilities, and to ensure that information receives an appropriate level of protection in accordance with its importance to the organization, and to prevent unauthorized disclosure, modification, removal or destruction of information stored on media.
Access Control	To limit access to information and information processing facilities, and to ensure authorized user access and to prevent unauthorized access to systems and services, and to make users accountable for safeguarding their authentication information, and to prevent unauthorized access to systems and applications.
Cryptography	To ensure proper and effective use of cryptography and to protect the confidentiality, authenticity and/or integrity of information.
Physical and Environmental Security	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities; to prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.
Operations Security	To ensure correct and secure operations of information processing facilities; to ensure that information and information processing facilities are protected against malware; to protect against loss of data; to record events and generate evidence; to ensure the integrity of operational systems and to prevent exploitation of technical vulnerabilities.
Communications Security	To ensure the protection of information in networks and its supporting information processing facilities; to maintain the security of information transferred within an

	organization and with an external entity.
System Acquisition, Development and Maintenance	To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks; to ensure that information security is designed and implemented within the development lifecycle of information systems; ensure the protection of data used for testing.
Supplier Relationships	To maintain an agreed level of information security and service delivery in line with supplier agreements.
Information Security Incident Management	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.
Information Security Continuity	To embed security in the organization's business continuity management systems; to ensure availability of information processing facilities.
Compliance	To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements; to ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

While control frameworks and different standards provide organizations with insight on the information security good practices, it should be noted that the frameworks too have their limitations. As discussed by Siponen (2006), an obvious limitation with security standards is that they often fail to provide detailed guidance on how the controls and best practices should be implemented and how the expressed security objectives can be achieved.

3 Social engineering

As discussed in the earlier sections of this thesis, social engineering can be defined as "*the act of manipulating a person to take an action that may or may not be in the "target's" best interest. This may include obtaining information, gaining access, or getting the target to take certain action*" (Hadnagy 2010, p. 32). In this chapter, the focus is on social engineering attacks, rather than terminology. Attack models, as well as different methods of attacks, will be discussed. Also, a taxonomy for different types of attacks is proposed.

3.1 Attack models

The basic elements of a social engineering attack constitute of research, developing rapport and trust, exploiting the trust and utilizing accessed information (Mitnick & Simon, 2001). This basic attack cycle was depicted earlier in Figure 1. Even though Mitnick and Simon's model is often mentioned in social engineering literature, the model is lacking detail in terms of different elements of an attack. Building on Mitnick and Simon's model, Mouton et al. (2014) have proposed a framework that takes into account different aspects related to each of the elements described in Mitnick and Simon's model. Figure 2 depicts this extended attack model.

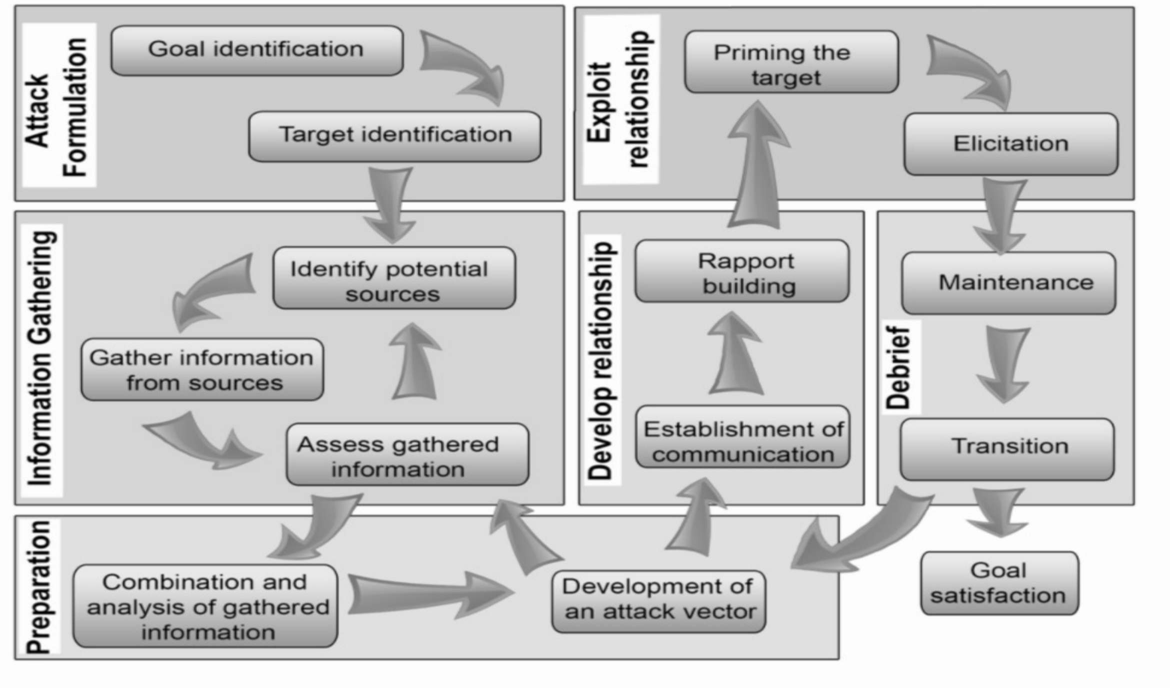

FIGURE 2. Social engineering attack framework (Mouton et al., 2014).

If compared to the Mitcnik and Simon model, the framework proposed by Mouton et al. expresses different elements of a social engineering attack in greater detail. The framework takes into account the fact that a target for an attack must be identified before any other measures can be taken. Also, Mouton et al. address the importance of finishing the attack in proper fashion – a matter not emphasized in Mitnick and Simon's model. The framework identifies six phases for a social engineering attack:

- **Attack formulation**. In this first step of the social engineering attack, the attacker must identify both the goal of his/her attack, as well as the target(s). In this planning phase, the attacker should consider questions such as *"What do I want to achieve with the attack*?" and *"Who should I target and why?"*.
- **Information gathering**. In the second phase of their attack, the social engineer will gather as much information as possible about their target, the attack circumstances and any other aspects relevant to their attack. At first, the attacker will identify potential sources of information. The sources can be either public (e.g. public websites, newspapers, social media, etc.) or private (e.g. sensitive documents thrown into the trash). Once the sources have been identified, the attacker will begin gathering information from these sources. The gathered information will be assessed in terms of validity, relevancy, and reliability. This phase will be repeated until the attacker is confident that he/she possesses enough information.
- **Preparation**. In the preparation phase, the attacker will combine all the gathered information in order to form a comprehensive understanding of their target. Once this understanding has been acquired, an attack vector will be developed. An attack vector is essentially the plan for the social engineering attack. It consists of the goal, target, method(s) and medium of the attack. In addition, a compliance principle has to be known. Compliance principle refers to *reasons* why the attack might succeed, such as the attacker trying to befriend their victim.
- **Develop relationship.** In this phase, the attacker will utilize all the gathered information to develop a relationship and establish trust with their victim. First, the attacker will establish communication with their victim. Various communication channels (e.g. email, phone call, SMS) can be used. Once the communication has been established, the attacker will build rapport with their victim. Rapport is built by forming a relationship. The relationships can vary in nature, examples including colleague-to-colleague –relationship and manager-to-employee –relationship.
- **Exploit relationship.** Once a relationship has been formed, the attacker will seek to exploit it by priming their target. Priming refers to an idea of bringing the victim to a desired state of mind, e.g. by creating a sense of urgency. Priming will lead to elicitation, meaning that the attacker will seek to obtain the required information from their target.
- **Debrief.** At the final stage, the attacker will first seek to return their victim in a normal state of mind (maintenance). This is done to mitigate the possibility of the victim getting suspicious. After maintenance, the attacker

has to decide whether their goals have been met or if they need more information.

Rather than a process, social engineering attacks can also be viewed in an ontological manner. Mouton et al. (2014) view attacks as something that "*employs either direct communication or indirect communication, and has a social engineer, a target, a medium, a goal, one or more compliance principles and one or more techniques*" (p. 2). Figure 3 depicts an ontological model of social engineering attacks.

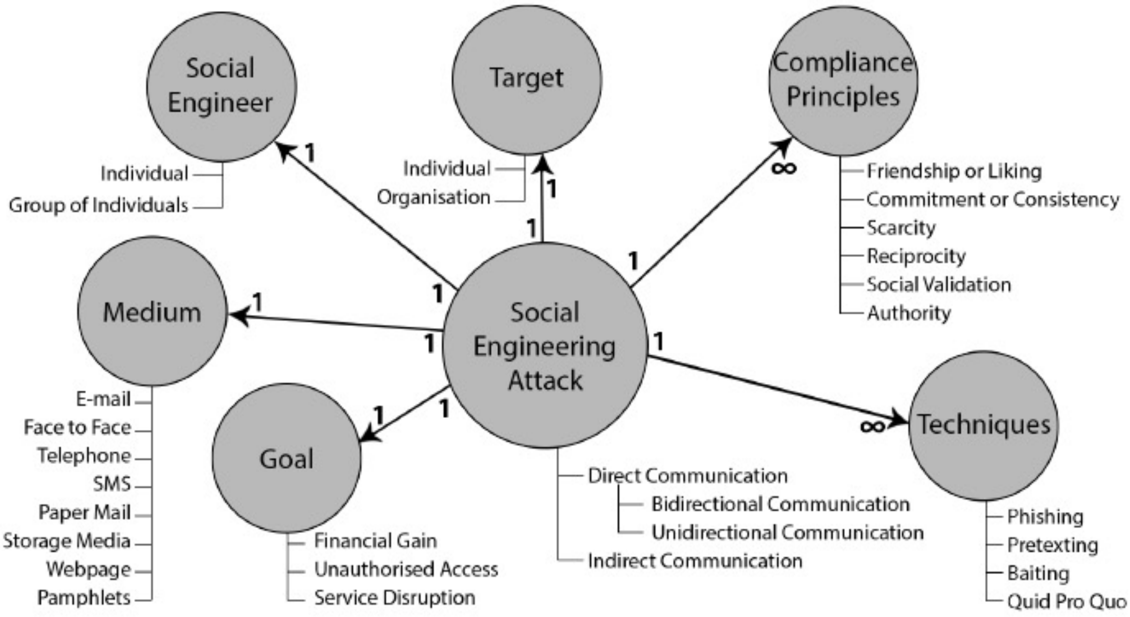

FIGURE 3. An Ontological Model of a Social Engineering attack (Mouton et al., 2014).

As the model suggests, there are many different aspects related to a social engineering attack. First of all, a *Social engineer* (or the attacker) has to exist. The social engineer can be either an individual or a group of individuals. The attack also needs a *target*. Likewise, the target can be either an individual or an organization, depending on the attacker's goals. In order to succeed, the attack has to involve one or more *compliance principles.* Essentially, compliance principles mean the reasons why a victim might comply with the social engineer's requests. The social engineer could, for instance, establish a sense of superior authority over their victim and this way strike a sense of urgency. The compliance principles are established with different *techniques*. These include e.g. phishing, pretexting and SMSishing. The techniques are executed via a *medium* of the attackers choosing. Potential media include email, telephone, SMS, and webpages. The chosen media are used to communicate with the victim. Depending on the chosen medium, communication can be either direct (e.g. a phone call to the victim) or indirect (e.g. a webpage to which the victim is lured to browse). All the different elements of an attack serve a common goal. The goals can vary widely, from financial gain to hacktivism and from espionage to cyber terrorism.

3.2 Attack methods

As suggested in the earlier sections, social engineering attacks can take many forms. Depending on their goals, the attackers may use a variety of different techniques and methods. In this section, an overview of different attack methods will be provided.

3.2.1 Phishing

When it comes to social engineering attack methods, Phishing is probably something most people have heard of. Phishing is an attack method in which the attacker attempts to acquire sensitive information by impersonating a trustworthy party, such as IT-support, work colleague or even the company CEO (Jagatic, Johnson, Jakbsson & Menczer, 2005;Hadnagy, 2010;Hong, 2012). Most often phishing is done via email and the sender's address is spoofed, meaning that the attacker fakes the sender's address. These emails typically contain a malicious link, of which the victim is lured to click. This link then leads to, for instance, a fraudulent website on which the victim is asked to insert his/her login credentials. Often these credentials are then stolen and later sold or used for malicious purposes.

3.2.2 Spear-phishing

Whereas phishing emails are often sent to a large audience and not targeted to any individual in particular, Spear-phishing refers to a type of phishing, in which relevant contextual information is used to trick the victim (Hadnagy, 2010;Hong, 2012). Spear-phishing attacks are more complex in nature, and they involve a personalized element (such as mentioning familiar names) to increase their credibility (Halevi, Memon, & Nov, 2015). Before sending the spear-phishing mail, the attacker takes some time to collect information about their victim. They could, for instance, browse through the victim's social media profiles in order to pick information about familiar names, places, and events. This information can then be used to build trust and increase credibility.

3.2.3 SMSishing & Vishing

Since phishing and Spear-phishing are often seen as mostly email-related attack methods, SMSishing and Vishing should be considered separately. According to Yeboah-Boateng and Amanor (2014), SMSishing refers to a type of phishing done via SMS messages, whereas Vishing (Voice-phishing), refers to phishing done via phone calls. Both of these methods often aim to lure the victim to visit a malicious website.

3.2.4 Pretexting

Pretexting is a method often used in combination with other methods. It means that the social engineer collects information relevant to their target, such as names, emails, phone numbers, events, etc., and then uses this information in order to build trust (Allsopp, 2009; Hadnagy, 2010). For instance, namedropping and knowing the corporate-specific lingo is likely to increase the odds for a successful attack (Mitnick & Simon, 2001).

3.2.5 Watering hole

Whereas the previously mentioned methods require active effort from the social engineer, watering hole is passive in nature. Watering hole refers to a technique, in which the attacker first compromises a website likely to be in the target's interest and then waits until the target visits that website (Mitnick, 2001; Krombholz et al., 2014). The website could be e.g., infected with a piece of malware. Watering hole is more often aimed at a larger target group, such as a company or an organization.

3.2.6 Reverse social engineering

This attack method seeks to reverse the direction of communication: instead of the attacker asking for information or help from the victim, the attacker tries to create a situation in which the victim requires help (Krombholz et al., 2014, Mouton, Leenen & Venter, 2016). Once the situation has been created, the attacker then presents him/herself as someone trustworthy and able to help. An example of reverse social engineering would be a situation in which the attacker first convinces their victim to believe their computer has been infected with malware and then asks the victim to type certain commands in their command line. These commands would then be malicious in nature, creating e.g., a backdoor or other forms of unauthorized access for the attacker. Reverse social engineering can be used together with *baiting.*

3.2.7 Baiting

As Conteh and Schmick (2016) argue, baiting can be considered somewhat similar to phishing. As the name suggests, this attack method involves setting up a bait. This bait is used to lure the victim to express certain behavior or perform a certain type of action (Hadnagy, 2010). An example of baiting could be that the attacker leaves a USB-drive on a parking lot, say, next to their victim's car. The goal is to get the victim to insert this drive in their computer. Various exploits, such as key loggers or reverse connections could then be executed by the attacker.

3.2.8 Dumpster diving

As the term suggests, dumpster diving refers to a technique in which the attacker searches trough their victim's trash in order to find sensitive or otherwise valuable information (Krombholz et al., 2014). At first thought this method might sound strange, but according to Long, Pinzon, Wiles and Mitnick (2008), it is rather common that organizations throw away sensitive documents, such as insurance bills. Examples of sensitive information being handled inappropriately include a case of sensitive patient data having being thrown away to a dumpster of an apartment building (HS, 2016).

3.2.9 Shoulder surfing

To put frankly, shoulder surfing refers to an activity where an attacker observes on their victim's actions, typically looking over their shoulder (Krombholz et al., 2014). Hence the term shoulder surfing. The method can be used for various information gathering purposes, such as spying on passwords or other sensitive data. According to Long et al. (2008), an abundance of information can be gathered just by looking at the victim's screen. A desktop view of one's screen could give away information on things such as: OS, version of OS, programs used and names of potentially sensitive files. In addition, even more sensitive information could be extracted from barcodes often found on corporate laptops' screens. What makes shoulder surfing especially effective, is the fact that with modern cameras, an attacker can record their victim's actions even from a distance.

3.2.10 Tailgating

According to Long et al. (2008), tailgating "*simply means following an authorized person into a building – basically, riding on their coattails*" (p. 14). Tailgating is used in gaining access to a building, to which access would otherwise be restricted. Long et al. argue that is one the best methods to gain access to a secured facility.

Tailgating exploits a very common weakness in humans: common courtesy. People are often willing to, for instance, hold doors open to other people walking after them. To increase their odds of successful tailgating, an attacker can dress appropriately. For instance, in an office environment wearing a suit could increase their odds, whereas in a warehouse or factory a safety vest and a helmet would be better choices.

3.3 Proposed taxonomy of social engineering attacks

As implied in the previous sections, social engineering attacks can take many forms and a multitude of different attack methods, or as sometimes called, *attack vectors* exist. Even though the attacks are different in many ways, the share a lot of common characteristics. In this section, a taxonomy of different attacks is proposed to help to categorize different attacks. The taxonomy builds upon the work of Krombholz et al. (2014) by extending it to cover more methods of social engineering attacks.

In their 2014 paper, Krombholz et al. discuss a taxonomy categorizing social engineering attacks in different **types**, **operators** and **channels**. **Type** refers to the most prominent approaches present in the attacks. They identify four attack types: social, socio-technical, technical and physical.

- *Social* approaches involve mostly a social element, such as face-to-face human contact.
- *Socio-technical* approaches involve a technical aspect (such as email) in addition to the above.
- *Technical* attacks are mostly carried over the internet.
- *Physical* approaches involve some physical aspect to them, such as visiting a venue in real life.

Operator is the origin from which the attack comes from. Operators can be either human or software. Finally, the **channel** refers to the medium used for the attack. Channels include, for instance: email, cloud, telephone, SMS and websites.

However, it can be argued that Krombholz et al. include somewhat unnecessary elements in their taxonomy. For instance, they have included *technical* attack approaches as a distinguished type, even though it could be argued that all social engineering attacks include some sort of social aspect by definition. Therefore, the type *socio-technical* covers all relevant situations. This is why the new proposed taxonomy does not discuss purely technical types of attacks. Furthermore, the concept of *operator* can be debated as well. Krombholz et. al argue that software can be seen as the operator, because some social engineering attacks can be automated (e.g. by using Social Engineering Toolkit –tool found in Kali Linux). However, even behind automated attacks, there is always a human initiation involved. In other words, very rarely would software perpetrate attacks by themselves. Rather, humans use different software as *tools* for their attacks. This would be the case even with attacks carried out by an advanced AI: at some point of time has a human developed the algorithm, or *set of rules*, according to which the AI behaves.

The proposed taxonomy builds upon that of Krombholz et al. by simplifying it in two ways. Firstly, due to the reasons specified above, attacks are no longer seen as only technical. Secondly, the origin of the attack, or *the operator,* is removed, because as argued above, there are reasons to believe it is always human. Furthermore, a more comprehensive set of attack methods, as well as corresponding common attack channels are presented in the new taxonomy, which is depicted below in Figure 4.

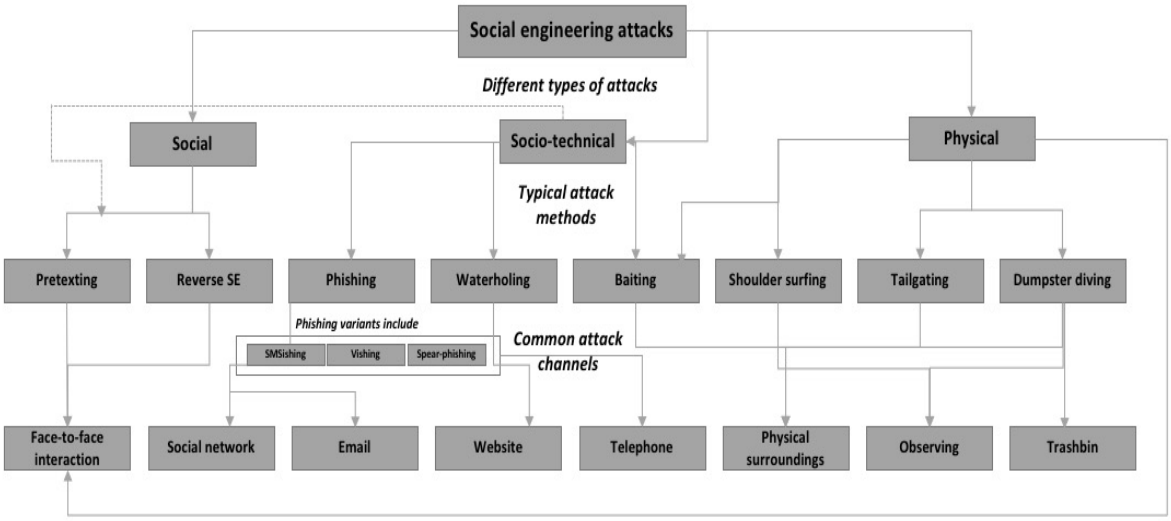

FIGURE 4. A taxonomy for social engineering attacks.

The taxonomy divides social engineering attack approaches into three types: Social, Socio-technical and Physical. *Social approaches* can be best characterized by the fact that they involve a human element, but do not necessarily require any technological means. Pretexting and reverse social engineering can be seen as typical attack methods for social approaches, even though they can, and often are, present in socio-technical approaches as well. This relationship is depicted with a dotted line. Social approaches mostly involve face-to-face contact as an attack channel. Because of this, they also involve a physical aspect.

Socio-technical approaches are the most common approaches for a social engineering attack. The attack methods involve both a technological and a social component. Take phishing for example: it involves email as a technical component and a persuasive message as social component. Common attack channels for socio-technical approaches include social networks, email, different websites and telephone (be it smart or not).

Physical approaches involve a physical aspect to them. Typically, the attacker would, for instance, visit their victim's workplace or other venues of importance. Methods of physical approaches include shoulder surfing, tailgating and dumpster diving. Typical attack channels for physical approaches are physical surroundings, observing the victim, as well as trash bins or other venues containing potentially important information.

3.4 Social engineering and human psychology

While in the previous sections different social engineering attacks, attack models and techniques have been discussed, one fundamental question has remained unanswered: Why and how does social engineering work? The answer, at least in part, can be found in the human mind - or rather its flaws and built-in limitations. This subsection describes ideas and theories that help explain how and why social engineering works.

3.4.1 Selective attention and other human tendencies

According to Wiles, Gudaitis, Jabbusch, Rogers and Lowther (2012), three main aspects of the human psyche make social engineering attack possible: *Selective attention*, *propensity to distraction* and *tendency to trust.*

The first aspect, selective attention, can be best described with the famous "invisible gorilla" –test. In the test, conducted by Simons and Chabris (1999), a video of people passing around a basketball was shown to a test group. The test subjects were asked to count how many times the ball gets passed during the video. What they were not told, is that a person wearing a gorilla suit would appear in the video as well. After watching the video, the test group was asked whether they saw something unusual. Most people did not report seeing a gorilla. Simons and Chabris call the phenomenon "sustained inattentional blindness". If our attention is locked to one thing or event, we have a tendency of disregarding other things that our mind deems irrelevant in that given moment. This human tendency can be exploited, for instance, in reverse social engineering attacks. When a social engineer creates a sense of urgency to their victim, the victim might not understand that their actions are against the interests of themselves and their organization.

The propensity to distraction is strongly linked to selective attention. Wiles et al. (2012) compare successful distraction to good magic: even if their audience know that they are watching a magic trick, they are still most likely to miss how the trick is actually done. In terms of social engineering, the goal is to not let the audience know they are tricked in the first place.

Humans have an inherent tendency to trust. According to Kramer (2009), trust is built in our biology – it makes evolutionary sense. Because people are likely to assume other people have good intentions, social engineers can do what they do. The inherent tendency to trust can be exploited in various ways as Mitnick (2001) demonstrates. For instance, lying is often very effective, because people will assume you are speaking the truth.

3.4.2 Persuasion

Social engineering is, to a large extent, an art of persuasion – getting people to do what you want them to do. Cialdini (2001) has identified six principles of human nature that make us susceptible to persuasion. The principles are *liking, reciprocity, social proof, consistency, authority, and scarcity.*

- **Liking** refers to our tendency to like people who like us.
- **Reciprocity** refers to our tendency to repay kindness.
- **Social proof** refers to our tendency to follow the example of others.
- **Consistency** refers to our tendency to align with people that seem committed to their cause.
- **Authority** refers to our tendency to trust, listen and obey those that we perceive as experts.
- **Scarcity** refers to our tendency to want what is scarce.

In his book of 2018, Hadnagy (2018) extends Cialdini's list of principles with *Obligation* and *Concession.*

- **Obligation,** closely related to reciprocity, refers to our tendency to feel obliged to do something in certain situations
- **Concession** refers to our tendency to concede after initial resistance has been overcome

Social engineers exploit these tendencies in various ways. For instance, spearfishing attacks often utilize the principle of authority: When an email seems to be coming from a trusted and authoritative source, the victim is more likely to click it. Similarly, reciprocity could be used in gaining access by tailgating: When entering a building, a social engineer could hold the outermost door open to an actual employee. The employee is then likely to repay this kindness by holding another door open for the social engineer. This second door could well be something that usually requires a keycard.

3.4.3 Theory of planned behavior

Human behavior in a social engineering context can be studied trough behavioral theories as well. The theory of planned behavior (TPB) is a well-established theory in social psychology (Flores, 2016). It is often used to predict customer behavior, but according to Sommestad, Karlzén and Hallberg (2015), it has proved useful in predicting information security related behavior as well. While TBT may not provide a comprehensive explanation of why SE works, it is useful in discussing different factors of human behavior and what kind of effect a social engineer may have on those factors.

The TPB, as introduced by Ajzen (1991), is an extension to the theory of reasoned action by Fishbein (1980). According to the TPB, human intention to engage in a certain behavior is influenced by their attitude towards that behavior, perceived subjective and social norms and perceived control over one's behavior (Ajzen, 1991). Should the intention be strong enough, humans are likely to engage in that planned behavior. Figure 5 depicts the relationships between different concepts of the TPB.

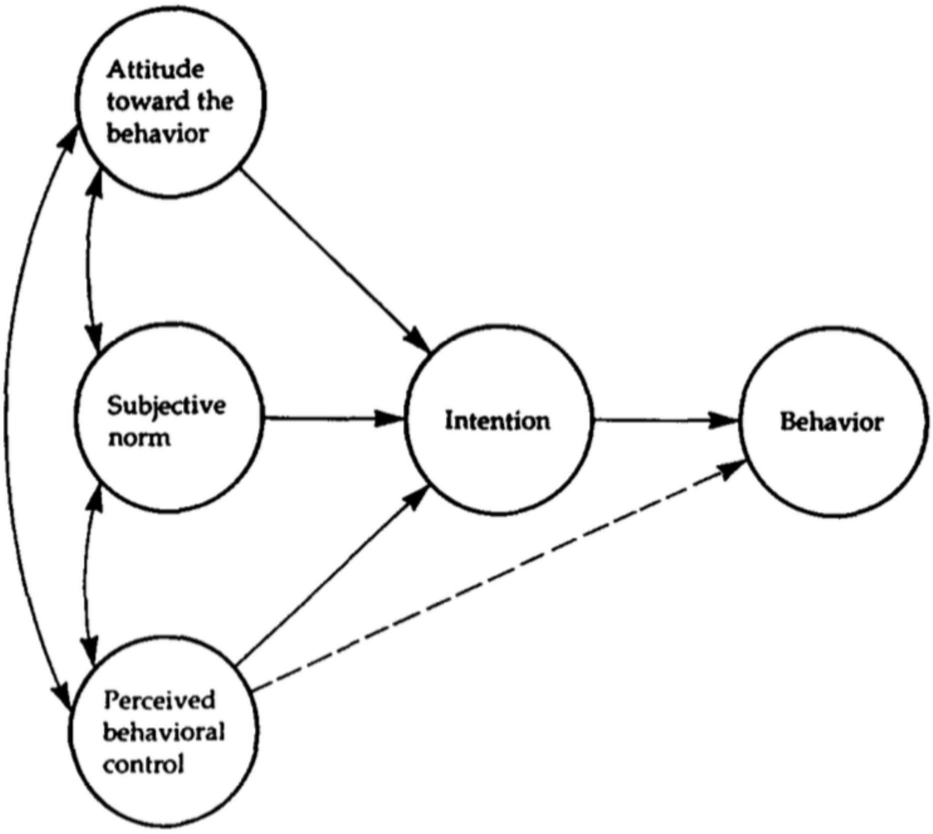

FIGURE 5. The theory of planned behavior (Ajzen, 1991).

Being aware of the concepts affecting human behavior can help social engineers to conduct their attack successfully. Similarly, awareness of what influences our behavior can help us protect against SE attacks. To put the TBT in a SE context, let us first discuss a fictitious attack scenario:

An attacker wants to gain access to an organization's sensitive information by having access to their employee's computer. For this purpose, they construct a scheme involving spear-phishing, vishing and reverse social engineering. At the first part of the attack, the attacker calls to their target company's service desk. The service desk agent answers with their full name "Hello, this John Doe from XYZ-corp service desk, how can help you?". At this point, having learnt one service desk agent's name, the attacker hangs up the call. Once a name of an employee is known, the attacker uses a web search to look for the company's syntax in email-addresses.

After having learned, that John Doe's email address is john.doe@xyz-corp.com, the attacker constructs a spear-phishing email, claiming that they are from the company's IT department and that John's computer has been compromised. In order for the IT department to solve this issue, John has to change their password temporarily to "passwd123", so that the IT department can take necessary actions. They also reassure John by claiming that many of the employees' computers have been compromised lately and that it will only take them 30 minutes to fix the issue. After this, the attacker sends the email to John and calls the service desk again. If it is John answering again, the attacker will claim that they are calling from the IT-department and urge John to check his email. In a more preferred *scenario, the second call is answered by some of John's colleagues. The attacker could then namedrop John's name and request the colleague to urge John to check his email.*

In the above scenario, there are several different ways in which the attacker tries to affect John's behavior. First of all, they try to affect John's attitude by creating a sense of urgency. If the spear-phishing email just asked John to change his password without providing any reasons for it, the attack would not be as likely to succeed. Secondly, by reassuring John that many others in the same company have had their computers compromised, the attacker tries affect John's normative beliefs. The goal is the reassure John, that this nothing out of ordinary. Finally, the attacker tries to overcome John's perceived behavioral control or *difficulty of engagement* by reassuring him that the problem will be fixed quickly. Should all these efforts to affect be successful, John's intention to engage in changing his password would likely be strengthened.

3.4.4 Effect of personality traits

As Hadnagy (2018) stresses in his book, an important factor for successful social engineering is the engineers' ability to profile their victims. This way, the attacker can try to identify which vulnerabilities of the human mind to exploit and which principles of persuasion to adopt.

Uebelacker and Quiel (2014) discuss the principles of persuasion in the context of the Five-Factor-Model (FFM), also known as the Big Five of personality traits. The Five-Factor-Model suggests a taxonomy of human personality traits and proposes dimensions that make up human personality and psyche. According to Mcrae and John (1992), FFM consist of *Openness to experience, conscientiousness, extroversion, agreeableness and neuroticism.*

- **Openness to experience** refers to the degree an individual is willing to try new things and overall curiousness
- **Conscientiousness** refers to the tendency of an individual to display self-discipline
- **Extraversion** refers to the degree an individual enjoys interaction with external world and other people
- **Agreeableness** refers to the degree an individual seeks for social harmony and good relations with other people
- **Neuroticism** refers to the degree in which an individual tends to experience negative emotions

As McCrae and John (1992) point out, the FFM is not an exhaustive model for explaining everything in human personality, but it can be still used as a foundation and core knowledge of human personality psychology. An interesting application of FFM is that of Uebelacker and Quiel (2014), in which they studied how different tendencies related to the big five personality traits can be used by social engineers. For instance, people that express high tendency of agreeableness may be more susceptible to phishing attacks. Similarly, extroversion may increase the risk of an individual not following security policies.

Based on a literature review study, Uebelacker and Quiel (2014) propose a framework mapping the different personality traits of FFM with Cialdini's principles of persuasion. Figure 6 depicts the framework:

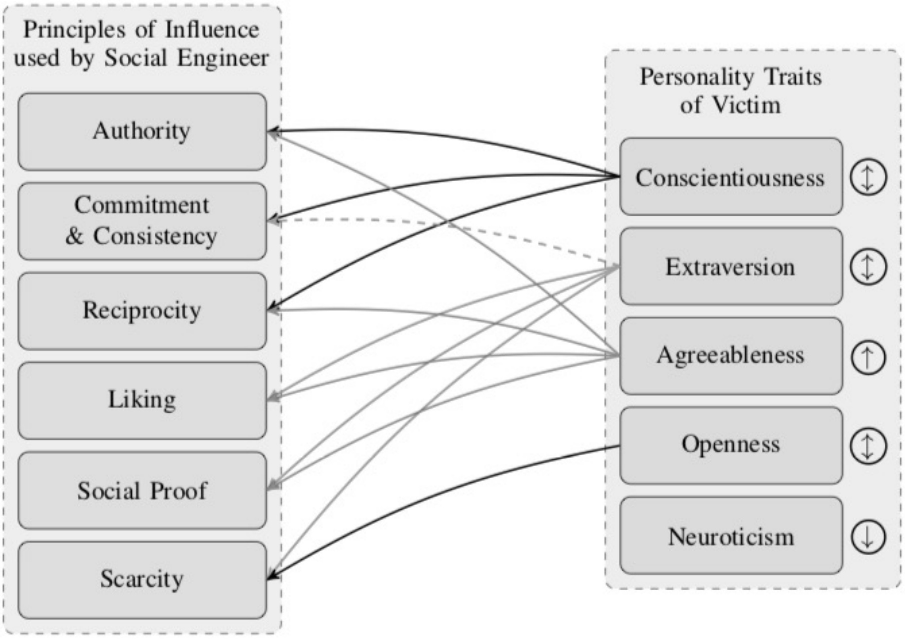

FIGURE 6. Social engineering personality framework (Uebelacker & Quiel, 2014)

As the framework suggests, certain personality traits are more susceptible to certain principles of influence. For instance, the principle of commitment and consistency may be more efficient when directed toward individuals expressing high degree of conscientiousness if compared to individuals expressing high degree of extraversion. In contrast, the principles of Liking and Social proof might resonate better with extraverted people. Even though the framework remains to be validated, it still provides insight on how different personalities might respond differently to SE attacks.

4 Protecting against social engineering attacks

In the previous chapter, models, tools, methods, as well as the psychological constructs behind social engineering, were discussed. In this chapter, an overview of generally recognized protective measures is presented.

4.1 Security policy

A large body of literature on SE countermeasures recognize the importance of security policies in protecting against social engineering attacks (see e.g Mitnick & Simon, 2001; Luo et al., 2011; Conteh & Schmick, 2016; Mouton et al., 2016). Fundamentally, a security policy is a written document outlining how the organization and its assets should be protected against different threats. Identifying the organization's most important assets and recognizing threats to those assets are key steps in defining a policy. Hence, security policies are organization-specific documents.

According to Conteh and Schmick (2016), a well-written security policy should include both technical and non-technical approaches that can then be driven down in the organization by means of different procedures and guidelines. The policy should be written in a clear, understandable and concise manner, and be distributed so that every person in the organization can easily access it (Mitnick, 2001). In addition, it should be made clear to the employees, what is expected of them in terms of information security behavior (Luo et al., 2011). According to Luo et al. (2011), a good and well-communicated security policy decreases the risk of employees being affected by social engineering attacks.

Since security policies are company-specific, there is no simple right answer on how to create a good security policy. However, organizations like ISO, NIST, ISACA and SANS have developed guidelines on what a good security policy should include. An important factor of a good policy, as pointed out by Siponen (2000), is to consider the justification of the policy. In other words, organizations should not just create a policy and force the employees to comply with it, but instead, reason why complying with the policy is important. Otherwise, the employees may find it difficult to be motivated to comply with the policy.

4.2 Security awareness program

Another generally recognized countermeasure against SE attacks is company-wide information security awareness program (see e.g Mitnick & Simon, 2001; Mann, 2008; Luo et al., 2011; Mouton et al., 2016). Such a program often includes training, e.g. on topics like code of conduct, secure behavior models, employee's responsibilities, resources for security, security and incident response procedures and role-specific security matters. Since everyone in the company is susceptible to SE attacks, all employees should participate in security awareness training (Mitnick, 2001). According to Conteh and Schmick (2016), security awareness training should also include recurring refresher training so that the company can respond to changing threat landscape.

According to Whitman and Mattord (2008) (as cited by Luo et al., 2011), there are multiple benefits for information security awareness training: It helps to tackle human error, improves employee security behavior, informs members of the organization on where to report security incidents and enables companies to hold employees accountable for their action.

In terms of SE –specific security training, Mitnick (2001) discusses a number of aspects that should be addressed during the training. Some of the key issues include:

- A description of how social engineering skills are used to deceive people
- The methods used by social engineers
- How to recognize a possible social engineering attack
- How to handle a suspicious request
- Where to report attempted or successful attacks
- The correct means to disclose sensitive information

However, a security awareness program can consist of many other things than training. According to Mann (2008), companies can arrange face-to-face briefings, email bulletins, intranet postings, interactive online training, login screen messages, security posters on walls, awareness through testing and even nominate "local champions" of security, say, on monthly basis.

What should be taken into account in all security awareness activities, is that security awareness needs and priorities vary between different employee roles. An employee with no access to company sensitive information does not need as much training as a system administrator (Mann, 2008). A proposed simple framework for determining the training needs of employees is presented in Table 2.

TABLE 2. Framework for determining employee security training needs. (Extends that of Mann, 2008).

Employee's potential impact on security	**Examples of employees**	**Training and awareness needs**	**Access to critical systems and data**
High	System administrators, security personnel, internal auditors	Regular, targeted and specific in terms of countermeasures and incident response	Direct admin access to critical data/systems

Medium	Managers, developers, IT-support personnel	Induction training and ongoing updates. Training somewhat tailored to position.	Potential or limited access to critical systems and data
Low	Employees with limited access to company systems outside their competency (e.g. graphical designers)	General security training. Role specific instructions.	No access to critical systems or data

In addition to analyzing the training needs, organizations should also focus on other internal factors important to the success of their awareness efforts. For instance, as identified by Puhakainen and Siponen (2010), the top management's visible support for information security is necessary for getting the employees to comply with security policies. In their study, Puhakainen and Siponen (2010, p. 775) identified seven success factors for a security awareness program:

1. *"Use a systematic training program when designing and implementing IS security training programs.*
2. *When providing IS security training, use learning tasks that are of personal relevance to the learners, so there are visible consequences for the self and others.*
3. *Use IS security policy compliance training methods and ideas that enable learners' systematic cognitive processing of information.*
4. *When designing IS security policy compliance training, practitioners should take into account the learners' previous knowledge regarding IS security policy compliance.*
5. *Integrate IS security training with normal business communication efforts in order to eliminate employees' perceptions of IS security as a separate issue from business function and employees' work tasks.*
6. *To ensure that users comply with IS security policies, visible support of IS security by top management is necessary.*
7. *Improve IS security by activating employees to discuss security through educational sessions."*

4.3 Security controls

Sometimes security policies and employee training fail to prevent a social engineer from committing their attack. Security controls provide another layer of security for safeguarding the company's assets and mitigating the possible damage. As presented in Table 1, there are a number of different controls organizations can implement.

In terms of protecting from SE attacks, some of the most important security controls are different forms of access controls (Mann, 2008; Mitnick, 2001). Access controls can be implemented to protect the organization from both physical attacks, as well as those done via the internet. An example of physical access control is an employee-specific security key tag, which has to be used on each entrance to the facility. Ideally, entries with the tag are logged. Examples of computer access controls include two-factor authentication when accessing company sensitive information. To help organizations implement security controls, a number of control frameworks have been developed. These include, for instance, COBIT, NIST, COSO, ISO/IEC 27002 and ITIL.

Security controls can be implemented to address all the methods of SE attacks identified in chapter 3. Table 3 maps the identified methods with corresponding examples of controls.

TABLE 3. SE attack methods and corresponding security controls.

SE attack method	**Examples of security controls**
Phishing (and variants)	Security awareness training, security guidelines, email whitelisting, email blacklisting, traffic flow control, Data Loss Prevention (DLP)–solution, Multi-Factor Authentication (MFA)
Pretexting	Security awareness training, security guidelines, code of conduct, acceptable use policy
Watering hole	Security awareness training, web traffic filtering, anti-virus software, patch management process, hardening of endpoint devices
Reverse SE	Security awareness training, code of conduct, acceptable use policy, policy of least privilege, hardening of endpoint devices
Baiting	Security awareness training, acceptable use policy, anti-virus software, hardening of endpoint devices
Dumpster diving	Security awareness training, security guidelines, acceptable use policy, document shredding procedure
Shoulder surfing	Security awareness training, acceptable use policy, screen privacy filter
Tailgating	Security awareness training, policy of always wearing a visible photo-id, physical segmentation of premises

4.4 Examples

Unfortunately, attackers might not resort to only one type of SE attack. More advanced attacks are likely to combine multiple methods of social engineering in order to increase the likelihood of a successful attack. Therefore, it is not enough to be able to protect oneself from just one or two types of common attacks. Organizations should, instead, try to identify possible attack scenarios and implement needed systemic improvements accordingly. Among the best practices is an approach often referred to as *Defense in Depth (DiD).* The approach suggests that organizations should implement security controls in a layered fashion: if one control fails, there are still additional safeguards available (NSA, 2010). Even if DiD might not guarantee security, as illustrated by Kewley and Lowry already (2001), it is still better than nothing.

According to NSA (2010), an important principle of the Defense in Depth model is that it requires a balanced focus on three primary elements: *People, Technology* and *Operation*s. Security controls should be implemented on all these three fronts:

- **People** related controls refer to those having direct impact on people and their work. The controls include segregation of duties, security awareness & training and ownership of assets
- **Technology** related controls refer to those implemented on the organization's network and assets. Examples of technology controls include network segmentation, Intrusion Detection Systems and multifactor authentication
- **Operations** related controls refer to those ensuring security on the organization's day-to-day work. The controls include security policies, patch management procedures and recurring security assessments or audits

This section illustrates the importance of Defense in Depth approach by first presenting an example of a SE attack utilizing several attack methods. Then, protective measures and corresponding security controls are discussed. Finally, a model for identifying social engineering attacks is presented.

4.4.1 Gaining access to an organization's network and bypassing multi-factor authentication

In this attack scenario, the goal is to gain access to an organization's network. Like any other attacks, the attacker first gathers as much information on the organization and its employees as possible (e.g., names, phone numbers, email addresses, job titles, social media accounts, positions within the organization, etc.) Once enough information is gathered, the attacker utilizes this information for developing a phishing email. In the email, the attacker claims to represent the organization's helpdesk and urges the employees to click a link included in the email. The pretext for the email could be, for example, critical *security updates, fixing erroneous configurations or security testing. The effect of the email can be reinforced with a phone call to the employee. As the employee clicks the link in the email, he/she is presented with a page appearing similar to the company's intranet. The employee is asked to login in the page with his/her credentials. In reality, this page is only used for stealing the employee's credentials.*

Once the credentials have been stolen, the attacker can seize any communication with the first victim. At this point, the attacker will conduct what is called a sim port attack. Pretending to be an employee, the attacker calls the organization's cellular service provider. Claiming to have lost his/her phone, the attacker asks the customer service to port the target-employee's phone number on another sim-card. Once the sim-swap is successful, the attacker tries to connect to the organization's network via a Virtual Private Network (VPN). Even if the organization has SMS -based multi-factor authentication in place, the attacker can now bypass it as the victim's mobile subscription has been compromised and the MFA messages will be sent directly to the attacker.

4.4.2 Protecting from the example attack

In the example described above, the attacker utilizes several methods of SE (phishing/spear-phishing & vishing, pretexting, reverse social engineering and baiting). To protect from such attacks, organizations should have implemented a number of security controls and protective measures.

The first line of defense for such a scenario is a strong set of PSGs and a comprehensive security awareness program. The organization should have clear rules and guidelines on the acceptable use of social media and sharing organization related information online. Similarly, the employees should be made aware of common social engineering techniques and they should be equipped with knowledge on how to recognize an attack. The organization could, for instance, require every employee to go through training related to the topic.

The second line of defense is technical measures on the organization's network. The measures include firewalls, email whitelisting/blacklisting, spam-filtering, and other anti-phishing tools. If the organization has such measures in place, the likelihood of the attacker's phishing email coming through decreases significantly. Similarly, organizations should also control outbound traffic. They could, for example, block any connections to the internet that are not within a list of trusted sites or that are hosted by parties with a bad reputation. If configured properly, the solution would block any attempts to visit malicious sites even if the victim were to click the malicious link discussed in the above example.

In this case, the third line of defense could be a more secure way of implementing MFA. Instead of using SMS-based authentication, the organizations could use either physical tokens or authenticator apps tied to a certain mobile device. With this approach, the attacker could not utilize the victim's credentials even after gaining access to their mobile subscription. Similarly, the organization could monitor connections established remotely and conduct recurring user access reviews to remove any access that is not necessary.

Fourth and fifth line of defense refer to the controls that would mitigate the damage the attacker could cause, even if they did reach the organization’s network. The controls include, e.g., Backups, Antivirus systems, DLP-solutions, monitoring and data encryption.

Figure 7 illustrates an example of Defense-in-Depth approach. The security measures mentioned above are mapped to their corresponding layers in the Defense-in-depth model.

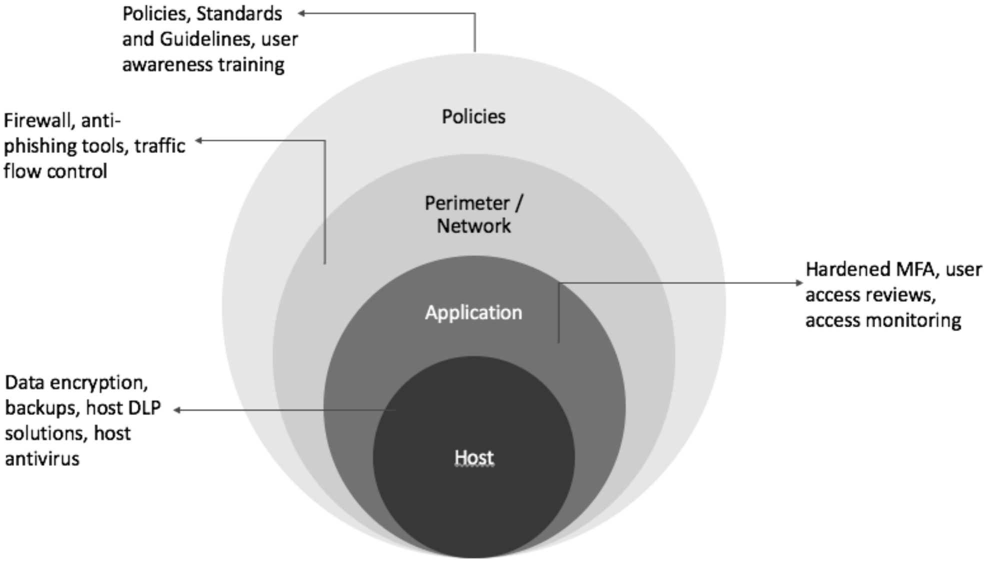
Policies, Standards and Guidelines, user awareness training
Policies
Firewall, anti-phishing tools, traffic flow control
Perimeter / Network
Hardened MFA, user access reviews, access monitoring
Application
Data encryption, backups, host DLP solutions, host antivirus
Host

FIGURE 7. Defense-in-Depth –model. Modified from that of InfoSec Institute (2015)

There have also been attempts to create a model for recognizing SE attacks. Probably the most cited is the Social Engineering Attack Detection Model (SEADM), introduced by Mouton, Leenen and Venter (2011, 2016). As the name suggests, the model was created for detecting SE attacks. As it is a somewhat complex flow-chart type diagram, its use cases in real-time human interaction are limited. However, it provides the necessary mental tools for detecting an attack and can be used as basis for developing more secure processes for, e.g., information and data requests. Similarly, the model can be used as a supporting resource in designing employee training against SE attacks. Figure 8 illustrates the SEADM-model.

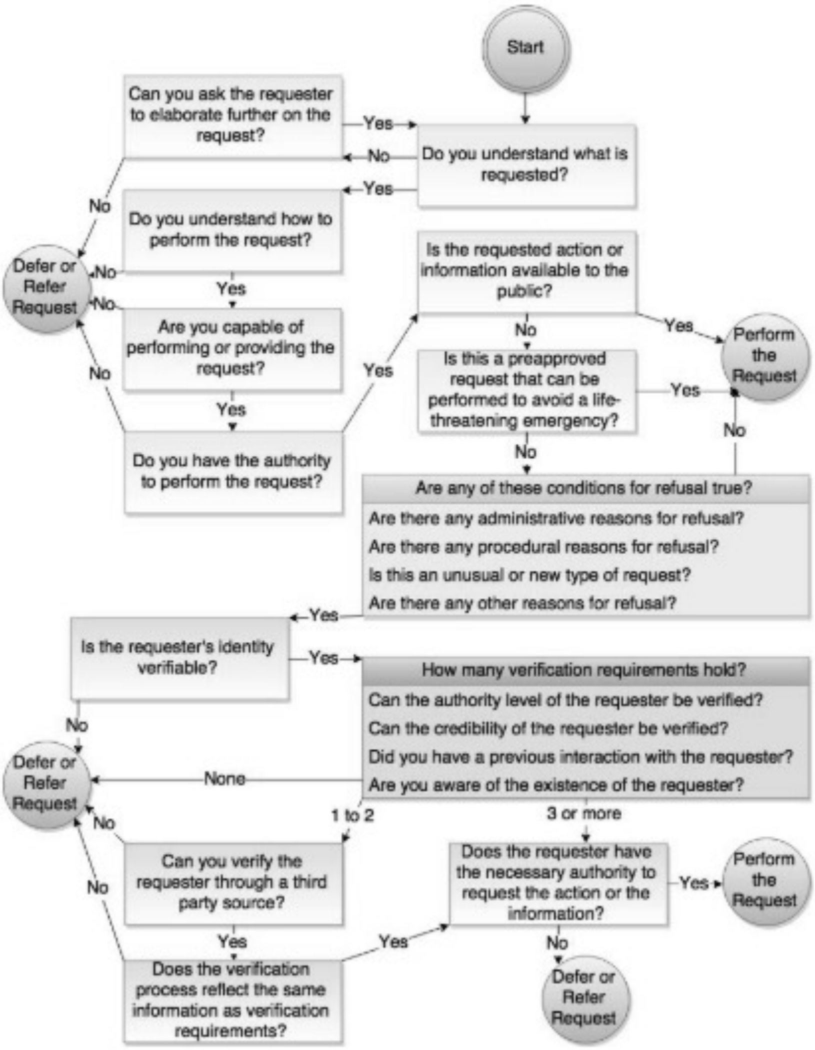
Start
Can you ask the requester to elaborate further on the request?
Yes
No
Do you understand what is requested?
Yes
No
Do you understand how to perform the request?
Defer or Refer Request
No
No
Yes
Are you capable of performing or providing the request?
No
Yes
Do you have the authority to perform the request?
Yes
Is the requested action or information available to the public?
Yes
Perform the Request
No
Is this a preapproved request that can be performed to avoid a life-threatening emergency?
Yes
No
No
Are any of these conditions for refusal true?
Are there any administrative reasons for refusal?
Are there any procedural reasons for refusal?
Is this an unusual or new type of request?
Are there any other reasons for refusal?
Yes
Is the requester's identity verifiable?
Yes
How many verification requirements hold?
Can the authority level of the requester be verified?
Can the credibility of the requester be verified?
Did you have a previous interaction with the requester?
Are you aware of the existence of the requester?
No
Defer or Refer Request
None
1 to 2
3 or more
No
Can you verify the requester through a third party source?
No
Yes
Does the verification process reflect the same information as verification requirements?
Yes
Does the requester have the necessary authority to request the action or the information?
Yes
Perform the Request
No
Defer or Refer Request

FIGURE 8. Social Engineering Attack Detection Model (Mouton et al., 2016)

If such a model was followed, attacks such as the one described in 4.4.1, would be more difficult to execute, as the victim would strive to verify the requester's identity. Unfortunately, in a real-life scenario, this level of verification can be difficult to achieve.

5 Research method

As mentioned in the introductory part of the thesis, the objective of this work is to gain a better understanding of the concept of social engineering, study the techniques used in social engineering attacks and shed light on the protective measures organizations have implemented. As the literature review part of this work focuses on the two first research questions:

1. *What is social engineering?*

and

2. *How can organizations protect themselves against social engineering attacks?*

the empirical part of the study focuses on the third question:

3. *How are organizations currently protecting themselves against social engineering attacks?*

As the theoretical background for SE attacks, attack methods and protective measures have been established, the reality of the corporate world can be studied. The goal of the empirical part of the study is to understand what kind of protective measures (such policies, technologies, procedures, and guidelines) organizations have implemented to protect themselves from social engineering attacks. This chapter describes how the study was conducted: the chosen research method, methods of data collection and analysis.

5.1 Method of study

Traditionally, the research within the field of Information Systems and IT has utilized quantitative methods. However, as the field is in a constant state of change and involves both human and technology, it often requires more flexible methods of study than the quantitative methods can provide (Kaplan & Duchon, 1988). For instance, as there are dozens of different security vendors and technologies, as well as ways of implementing those technologies, it could be difficult to capture a sufficient amount of detail in a quantitative survey-based study.

Similarly, an interview-based data collection allows the researcher to ask clarifying questions, whereas a written survey might not be able to catch interesting or unexpected notions. According to Rubin and Rubin (2011), interviews allow the researcher to discover counterintuitive matters, ideas or findings that may not have been discovered through other means of research. As put by Schultze and Avital (2011), the goal of an interview is to connect with the interviewee through discussion and gain first-hand information in this manner. According to Bhattacherjee (2012), a face-to-face interview is the most suitable method for research, in which the target is a person.

As mentioned in section 2.3, this study was conducted by using qualitative research methods. Such methods were chosen after comparing qualitative and quantitative methods and their strengths and weaknesses. The rationale behind the decision is largely based on the notion that it was seen important to be able to ask clarifying questions and understand the context in which the sample organizations had made their decisions regarding security measures. Similarly, since the data collection for the research was conducted via interviews, qualitative methods were seen as a better fit for this study. However, as discussed in 2.3, even though the study is qualitative in nature, some results are summarized and reported in a quantitative manner.

5.2 Data collection

Data collection for this work was conducted during late 2019 and early 2020 – from September to January. The collection was carried out with semi-constructed interviews, both in-person and via telephone. All interviews were held in Finnish language.

An invite to the interview was sent to 40 people in charge of their organization's cybersecurity. Out of the 40 invitees, 3 people declined, 25 people did not reply, 2 people initially agreed but later stopped responding and 10 people agreed and were interviewed. In other words, 25% of the invitees were interviewed. The most common title for the interviewees was Chief Information Security Officer (CISO).

The data collection process consisted of preparing a framework for the interviews, selecting a suitable sample and conducting the interviews. Next, these phases are discussed in detail.

As mentioned, the interviews were carried out with a semi-constructed approach, meaning that rather than asking all the interviewees the same questions, the interviews were divided into different topics/themes, leaving the researcher room for adapting and asking clarifying questions. According to Myers and Newman (2007), an unstructured interview allows the interviewer to improvise if needed. The themes for the interview framework were based on the defense-in-depth model discussed in the literature review part of this work. In other words, the ways in which organizations protect themselves against social engineering attacks were observed through the lens of the defense-in-depth approach. As put by Schultze and Avital (2011), an interview based on a set framework makes interviews more efficient by guiding the interviewee throughout the discussion. The framework used in this research can be found in Appendix 1. Protective measures for all layers of the defense-in-depth, (policy, perimeter, application & host) were discussed in all interviews. The themes in the interviews were:

- Background information on the interviewee and their role in the organization
- The degree to which the organization has experienced social engineering attacks and the types of the attacks
- The degree to which social engineering is on the organization's risk agenda
- Different controls implemented to protect from the attacks (awareness, policies, technical controls, physical security controls)
- Perceived strengths and weaknesses in the information security posture

The background information was asked to reduce the artificial feeling of the situation – essentially to start with easy questions and gradually advancing to more complex matters. The role of the interviewee is important to know for the interviewer so that the questions can be adjusted accordingly. For instance, if the interviewee stated that physical security matters are not within their responsibility, nor do they have very much knowledge on the topic, it is not meaningful to spend too much time discussing physical security. Similarly, if the interviewee discloses having contributed significantly to the development of the organization's security training and awareness materials, it is worthwhile to spend some time on the topic.

The degree to which the organizations had experienced social engineering attacks is important for mainly two reasons. First, it allows the researcher to gain insight into the degree of commonality of social engineering attacks and attack methods. Secondly, the gathered information can be combined with information from the next theme to assess, whether there is a connection between attack exposure and the perceived risk associated with social engineering attacks.

The degree to which SE is on the organization's risk agenda was asked to clarify how much risk organizations associate with SE attacks. The goal was to find out whether the organizations conduct cybersecurity risk assessments and if so, the degree to which SE is seen as a risk.

Different controls to protect from attacks were discussed to gather information on the main topic of this thesis: what kind of measures organizations have implemented to protect themselves from SE attacks. As discussed, this theme of the interview was constructed around the defense-in-depth model.

Perceived strengths and weaknesses in information security posture allow later comparison between the organizations and highlight the perceived issues and strengths in the security posture of organizations operating in Finland.

The sample of the study was determined on a discretionary basis. To ensure comparability between the results, each of the organizations can be considered "a large organization" by Finnish standards, meaning that each of them had revenue of over 50 million euros annually. In fact, the smallest organizations by revenue in this research still amount to 200-500 million euros annually. The sample was chosen on a discretionary basis also because smaller organizations often do not have a dedicated CISO role or similar.

As mentioned earlier, the universe of the sample consisted of people perceived by the researcher to be in charge of information security matters in their respective organizations. Such a universe was determined to be the best source of information on the protective measures organizations have implemented to protect from SE attacks. This type of discretionary sampling is common in qualitative research (Hirsjärvi, Remes, & Salovaara, 2009). Similarly, the discretionary sample is more likely to produce more generalizable results, as the interviewees are roughly in the same rank and are likely to have similar visibility on information security matters in their respective organizations.

The interview candidates were approached in LinkedIn and via email. To increase the likelihood of accepted invites, the interviewee candidates were promised to receive the final work as its finished, as well as an "executive summary" report prepared exclusively for the interviewees. The benefit of participating in the study was further underlined by the fact that the results received from the research could possibly be used as a benchmark in strengthening the organization's cybersecurity posture.

The interviewees were given the option for having the interview either in-person in the greater Helsinki area, or remotely. Six of the interviews were held in person and four via telephone or Skype. All of the interviews were recorded with the interviewees' permission for further analysis. The recording was conducted with two separate devices to decrease the risk of losing valuable data. Notes were taken in each of the interviews. The interviews followed a loosely defined framework, which was sent to the interviewees for review prior to the interviews. The framework was used to facilitate an open discussion on each of the themes at hand. In addition to the pre-identified themes, clarifying questions were asked when deemed necessary. The length of the interviews averaged to approximately 50 minutes, ranging from 45 to 60 minutes. All of the interviews followed the same framework, but there was variance in the clarifying questions asked.

5.3 Method of analysis

As described in the previous sections, qualitative methods were chosen for this research. The analysis of gathered data was conducted in the following phases: interview transcription, reading the transcriptions, labeling and coding different sections of the interview, searching for differences, similarities and relevant findings and finally reporting the results.

In the first phase, the interviews were transcribed based on the recordings and written notes. An edited transcription method was chosen, meaning that the researcher would listen through the interviews and supplement the taken notes with transcriptions from the interview recordings.

Next, each of the transcriptions was read through. At this point, the researcher would already try to identify differences, similarities and relevant findings from the data. As the transcripts were read through, the researcher would already identify different themes and codes related to the data.

The data was coded by identifying themes and findings relevant to the topic of the research. These themes were identified based on the information analyzed during the literature review. A theme could be, for instance, “Organization’s experiences of social engineering attacks”. This theme would then be divided into more specific topics, such as “SE attack methods used against the organization”.

Once the codes had been identified, the data were analyzed in a spreadsheet format. Different codes would be assigned to the relevant data from each of the interviews. For instance, if the topic of interest was security awareness training and a code was “The extent of security awareness training”, identified data point could be:

“We have different web-based learning for white- and blue collar workers. The training for white-collars is more focused on privacy and information security related topics, whereas the training for blue collars focuses more on safety in the production facility.”

As the analysis proceeded, more and more specific topics were analyzed. For instance, when discussing the technical security controls used within the organization, the code could be “use of MFA” and a data point could be:

“Currently we’re in the process of implementing MFA for all employees. Right now only the privileged access [e.g application & network admins] is behind MFA.”

The research would also try to find elements that initially were not discussed in the source literature. For instance, the issue with physical security was prevalent with many of the organizations having functions in several countries:

“We don’t have very good visibility to the physical security in remote locations. I’m afraid there might also be cultural differences on how seriously the matters are taken.”

As the analysis was conducted, the results were reported based on the identified codes and findings. The results of this research are presented in the next chapter.

6 Results

In this chapter, the results of the conducted research are reported. First, the background information of the interviewees is presented. Then, the sample organizations' experiences regarding SE attacks are reported from multiple points of view. Thirdly, the organizations' perceptions regarding risk related to SE are reported in detail. Finally, the implemented protective measures, as well as organizations' perceptions regarding their security posture are described.

6.1 Background information

This section presents the background information of the interviewees. The sample of the research consisted of 10 people discretionarily chosen amongst cybersecurity leaders in organizations operating in Finland. The most prevalent title amongst the interviewees was Chief Information Security Officer (CISO), amounting to 50% of the interviewees. Other titles included "Head of Information Security" or similar. The interviewees represented different industries and each of them worked in Finland. The majority of the organizations were publicly listed and all of them can be considered "large organizations" by Finnish standards. The interviewees and details of their respective organizations are described in Table 4.

TABLE 4. The interviewees by industry and company revenue.

Interviewee	Industry*	Revenue €*
Interviewee 1	Manufacturing, industrial products	5-10 billion
Interviewee 2	Manufacturing, consumer products	1-5 billion
Interviewee 3	ICT	1-5 billion
Interviewee 4	Retail	< 1 billion
Interviewee 5	Manufacturing, consumer products	1-5 billion
Interviewee 6	Manufacturing, industrial products	< 1 billion
Interviewee 7	Banking, finance and insurance	N/A
Interviewee 8	Industrial services	< 1 billion
Interviewee 9	Banking, finance and insurance	N/A
Interviewee 10	Retail	> 10 billion

* To protect the anonymity of the interviewees, the industries and revenues are only presented in a high level.

6.2 Experiences of social engineering attacks

This section describes the degree to which organizations have experienced social engineering. The prevalence of attacks, different attack methods, degree of successful attacks and perceived maturity in identifying an attack are reported in detail.

6.2.1 Prevalence of attacks

Each of the organizations (100% of interviewees) said they had experienced at least one form of social engineering attack in the organization they are currently working for. Email-based phishing was by far the most common type of attack, and similarly, 100% of the interviewees declared that their organization receives phishing emails at least on a weekly basis. The interviewees also perceived that phishing is a very common issue across all industries:

"Well, I guess all organizations are targeted with phishing emails. For us though, the role is twofold: We get it as a firm, but also our customers receive phishing emails where the attacker claims to represent us" – Interviewee 9.

Some of the interviewees had also statistics on the number of emails coming in vs. how many of them filtered as spam/junk/phishing. Due to differences in filtering tools, methods, and configurations, the numbers cannot be compared, but still paint a rough idea on the volume of un-wanted email traffic:

"There are quite a lot them [phishing emails] coming through... this is even if 94-95 %of incoming email traffic are currently filtered... or at least over 90 %, the figure is – Interviewee 6.

"We used to have around 90 % of our email traffic filtered away... well, it's hard to say what is the initial amount of traffic due to various layers of filtering, trust-services and such... but right now around 60 % of the emails are clean, according to the statistics of our email service" – Interviewee 7.

The majority of the received phishing was not targeted to specific individuals or groups, meaning that it was produced in bulk. However, all organizations had also experienced more targeted attacks:

"Phishing...we've had some more targeted phishing cases and then those where they've just sent it [phishing emails] in bulk to our employees" – Interviewee 3

"Yeah, it involves targeted [phishing] as well, and clearly they [the attackers] have studied our organizational structure" – Interviewee 6.

> *"Well, most of it [social engineering attacks] is of phishing-type, but then there are also clearly things like business email compromise, CEO fraud and fake invoicing" – Interviewee 10.*

Many organizations had also experienced other types of social engineering, such as physical intrusion, voice phishing and CEO fraud. The methods of attacks the organizations had experienced are described in the next subsection.

6.2.2 Attack methods

This subsection describes the findings regarding the different attack methods experienced by organizations. The results are summarized in Table 5 below. Next, the results are discussed in more detail.

TABLE 5. Identified attack methods.

Method of attack	Prevalence (%)	Prevalence (n)
Phishing (email)	100 %	10
Spear phishing	100 %	10
Voice phishing (Vishing)	70 %	7
Phishing (social media)	30 %	3
Pretexting	30 %	3
CEO fraud	50 %	5
Fake invoicing	30 %	3
Physical intrusion	20 %	2
Business email compromise	10 %	1
Typo squatting domains	10 %	1

As mentioned in the previous subsection, by far the most common attack method seems to be phishing, and more specifically, phishing emails sent in bulk. All organizations had experienced phishing. However, there was variance in the degree of sophistication related to these attacks. For instance, seven out of the ten said they have received voice-based phishing, or *vishing,* as well:

> *"Yes, we've had some sketchy requests as well...are they all for fraudulent purposes... well it's hard to say… there is sometimes a fine line between social engineering and a good sales technique"* – Interviewee 1

> *"There's been phone-based [phishing] from prepaid-numbers… seemed professional"* – Interviewee 2

Some of the organizations also remarked that the phone-based phishing was supplemented with text-messages:

"We've had cases of voice phishing, and they [the attackers] have tried to make it more effective by following up with messages on WhatsApp" – Interviewee 6

Also, there was one instance of a fraudulent voice-message being received:

"There was this one case where a colleague received a [WhatsApp] voice message supposedly from the CEO… it was however quite simple in nature… like: "I need your help in this important project and whatnot" … not very sophisticated. However, what was interesting was that it came from the CEO's personal phone number" – Interviewee 1

Sometimes the purpose of the fraudulent phone calls was to pretext and to build rapport and supplement other types of attack methods, such as spear-phishing. Three of the interviewees said that they had received phone calls either prior to, or after a spear-phishing email:

"… [the attackers] try to create this sense of familiarity, like "can I send you this attachment via email" … with the goal of getting the victim to click on the attachment... this is what I receive personally and I'm aware of others getting it too" – Interviewee 9

Interestingly, phishing and more targeted spear-phishing both seem to occur also on social media. Three of the interviewees mentioned having received these types of messages in either WhatsApp, LinkedIn or both:

"a newer [type of phishing attacks] occurs through social media… LinkedIn and WhatsApp… if you count them as social media… mainly its phishing for access credentials in these channels" – Interviewee 10

Phishing for information might not occur only in the digital world. Three of the interviewees thought there are probably phishing attempts occurring in face-to-face situations as well:

"and of course if there is some sort of an event and somebody starts asking questions…these [type of incidents] have not been brought to my attention though" – Interviewee 1

"I can imagine there are different kinds of instances where there is an attempt to phish information by means of conversation… but we don't have reported cases of this happening" – Interviewee 7

"then there is influencing in one's social circles…we don't have reports on those, but we've covered the topic in our awareness material, like" note that somebody might come asking for things by the football field. It happens in many channels"" – Interviewee 9

After different types of phishing, the second most common types of attacks were different types of fraud aiming for financial benefit. Among the most common was CEO fraud, reported by five organizations:

"as the names of the management are public, there are these cases that they [the attackers] try to manipulate people by pretending they are the CEO or CFO..." – Interviewee 6

"and then there is the CEO fraud… they are very common. We get it all the way to the top management and the goal is mostly to either phish information for getting access to our systems or to gain financial benefit" – Interviewee 7

In addition to the CEO-fraud, receiving fake invoices is not too uncommon. Three organizations reported having received one or more fake invoices:

"there's been fake invoices and also the payment process… [they] have tried to exploit the payment process" – Interviewee 1

One organization also mentioned, that attackers have tried to scam third parties by pretending to represent their organization:

"and it's not only phishing, [the attackers] have also pretended to represent us in the field of our business, even though in reality we have had nothing to do with that. [They] have tried to gain financial benefit and information by doing this…it's been conducted via telephone and they have also set up a fake website" – Interviewee 2

The third most common type of social engineering attacks were attempts of physical intrusion. However, only two interviewees mentioned having reported cases of such attempts:

"There have been cases of activists trying to come visit us uninvited" – Interviewee 2

"We had this case where there was somebody hiding behind the reception desk… There have also been cases in which someone has managed to slip to our offices. I think it's been more about theft" – Interviewee 3

It seems that the motive for these attacks has been more on activism or simple theft of physical property, rather than attacks on confidentiality, integrity or availability of information. The rest of the organizations either had not had any similar incidents, or were not aware of them happening.

In addition to the methods described above, there were two separate instances of social engineering, that were not discussed in the source literature. One organization reported business email compromise being a growing issue, and increasingly often emails are received from legitimate email addresses, that have been hacked:

"We're seeing more and more these [type of emails] coming from cracked legitimate addresses… this is among the biggest issues needing fixing" – Interviewee 10

Typo squatting on domains was also mentioned in one interview:

"We've had one case of the attacker registering [companyname.com with one letter changed]. We have a procedure for following these though" – Interviewee 1

6.2.3 Degree of success on attacks

This subsection describes the degree to which organizations have experienced SE attacks that were at least somewhat successful from the attacker's perspective. In other words, the cases in which companies have either lost credentials or their data have been under a threat, are discussed.

Four out of the ten interviewees, or 40 %, reported having had a SE related security incident. One company stated that employee data was almost lost, but the organization's security team was able to prevent the incident.

In all of the four cases, the interviewees reported that a phishing/spear-phishing email had resulted in the attacker successfully gaining access to employee credentials. Due to credentials being lost, the organizations had had to reset employee credentials:

"We investigate logins that they [the employees] don't recognize on a weekly basis. There've been cases that we have had to reset their passwords and O365 accounts" - Interviewee 10.

Even though only four organizations reported having experienced such incident, it is possible that the number is actually higher and interviewees chose not to disclose this information:

"There have been indications, that passwords have been leaked to wrong places… In fact, I find it hard to think of an organization that could say this issue does not touch them…" – Interviewee 5

6.2.4 Perceived maturity in identifying an attack

Each of the interviewees were asked to describe their organization's perceived maturity in identifying and protecting from social engineering attack. The maturity was asked to be estimated against their peers. This subsection describes how the sample organizations perceive their maturity.

Of the ten interviewees, six thought their maturity is higher than their peers', one estimated to be on the same level, two somewhat behind on certain aspects and one could not tell. Some of the interviewees estimating their maturity to be higher than their peers had data to support their view:

"Well in fact I have quantitative data for that. We did this test with a simulation system in which the goal was to check the state of awareness and the result was a positive surprise…Even though we hadn't done any similar simulations before, the results was significantly better than the average" – Interviewee 8

Another interviewee shared similar insight:

"We've had this training platform for a year now, and during this time our maturity has grown significantly. We get benchmark data from the service provider and we rank substantially better in identifying attacks than the benchmark" – Interviewee 9

The interviewees who estimated their maturity to be lower on certain aspects, also identified that they are behind their peers in technical capabilities rather than in the awareness of their people:

"I'd say the awareness among our middle- and top management is high… surprisingly high in fact. Difficult to say how we compare to our peers though. The focus has been in the awareness and I think we're slightly behind in terms of technical capabilities" – Interviewee 4

Another interviewee mentioned differences among different units of the organization:

"Well, there are two dimensions to this. In our factory floors things are good according to the last audits, but in our offices we are a little behind" – Interviewee 5

Altogether it seems that most organizations think the level of their employees' awareness is good. However, the interviewees also seem to recognize that there is variance among the employees, with some being more alert than others:

"There are several thousand people using [the Company]'s credentials and you can fit the entire spectrum of society in that. Others might be alert and some not so much. Of course there might also be cultural differences to this" – Interviewee 5.

Interviewees also noted that even with high employee awareness, there is still a risk of an attacker succeeding:

"Our employees are reasonably good [in identifying attacks]. However, I'd say that anyone can be fooled if just put enough effort to it. Our goal is that most people don't fall for the easiest ones [referring to SE attack attempts]" – Interviewee 3

All in all, the organizations seem to estimate their maturity to be better than their peers. The next section describes the degree to which organizations see social engineering as risk to their information security or business in general.

6.3 Social engineering on risk agenda

This section describes the degree to which organizations see social engineering as a risk. The employees were asked whether they conduct a formal risk assessment of information security risk and if SE is seen as a risk, and whether they have conducted any SE related testing. There seems to be a lot of variance among organizations in this topic. The results are reported in detail in subsections 6.3.1 and 6.3.2.

6.3.1 Risk assessments

90 % of the interviewees reported that their organization conducts risk assessments of information security risks. However, there seems to be variance on the degree to which organizations see SE as a risk to their information security or business in general. The results are summarized in Table 6 below:

TABLE 6. Risk assessment and perceived risk in social engineering

Finding	Prevalence (%)	Prevalence (n)
Conducts risk assessments on information security risks	90 %	9
SE is a recognized risk on the risk map	40 %	4
SE is a recognized risk only through phishing	20 %	2
SE is not recognized as a risk on the risk map	20%	2
Does not conduct risk assessment on information security risks	10 %	1

Even though most organizations conduct risk assessments on information security risks, not all view SE the same way. Of the nine organizations conducting risk assessments, 44 % (n = 4) said they have recognized social engineering as a risk on their information security risk map.

> *"Yes we've done them [information security risk assessments] and social engineering has been identified as a risk. That [information security risk map] is the only map we have it on though"* – Interviewee 2

Some interviewees stressed that not only is SE recognized on their risk map, it is also seen among the biggest risks:

"We do information security risk assessments yearly as per our year clock. Social engineering is identified and I see it as a big risk" – Interviewee 6

"Frequently we do this [information security risk assessments]. The assessments are done at least yearly, and then there is a mid-year review every six months. Social engineering is on the map and I think of it as one of the biggest risks to the entire organization" – Interviewee 8

Two of the interviewees said they have not identified social engineering as a risk in itself, but different types of phishing have been identified an addressed in their risk map:

"Well, it [identification of SE as a risk] comes through email –based phishing. We recognize email as the easiest and most common way for attackers to gain access to firms and this is what we strive to protect from. In other aspects, it's not too big of a priority" – Interviewee 3

"We've had phishing on the risk map, but not social engineering in its entirety" – Interviewee 7

Two of the interviewees, or 22 % conducting information security risk assessments in general, reported not having formally recognized social engineering as a risk to the information security of their organization:

"It's not there [on the risk map]. Should it be? Well that's a good point. It's been identified yes, but not formally listed"- Interviewee 1

"Social engineering in itself is not on the risk map. Rather, it is its possible consequences… So it is not a risk theme, but has to do [the identified risks] more on the availability and privacy of information" – Interviewee 4

The organization not conducting risk assessments on information security risks still reported thinking of social engineering as one of the most important risks to their information security.

The next subsection describes the degree to which organizations have conducted any social engineering –related testing or audits to test and verify their capabilities in protecting from attack attempts.

6.3.2 Testing and audits

The organizations were asked to describe whether they conduct or have conducted any testing or audits related to social engineering attacks. Most organizations did either physical intrusion tests, red-teaming tests, different kinds of security audits or a combination of all. The results are summarized below in Table 7.

TABLE 7. Testing and audits related to social engineering

Finding	Prevalence (%)	Prevalence (n)
Audits on information security	100 %	10
Phishing simulation	70 %	7
Physical intrusion testing	40 %	4
Other (e.g red-teaming, unspecified details)	30 %	3

When asked to describe the types of testing and audits they conduct, all organizations mentioned having some sort of audits. Many of the interviewees chose not to specify the details of these audits, but they were often done as part of financial audits, as part of the internal audit, or by an external auditor. Typically, the topic in these audits would be the security of certain services or systems, identity and access management, or third-party risk management.

Most organizations had either conducted or were continuously conducting phishing simulation tests. These types of tests are conducted by sending simulated phishing emails to organization's employees to test whether the employees are able to identify the phishing. 70 % of the organizations reported having conducted these tests, and interestingly all but two had utilized the same service provider for conducting the tests.

"We've had this phishing simulation platform for a year and a half now. Currently it's implemented on voluntary basis. It's a good way of keeping people alert" – Interviewee 3

Four of the organizations reported having conducted also physical intrusion tests. For some the tests were conducted on a periodic basis, whereas others would conduct the tests ad-hoc.

"We did an experiment… can you follow a person to the offices… Whether people would hold a door open for you if you have a cup of coffee in your hand. The person was identified and escorted out of the premises, but got to move around in the offices for a while" – Interviewee 1

"We've done physical pen-tests and found some areas of development. We do these tests every now and then, especially if there are physical changes in the facility" – Interviewee 7

30 % of the interviewees said they conduct red- or purple teaming exercises with various scopes. The exercises could be directed towards management, staff or both. In fact, one of the interviewees mentioned their organization being in the middle of a red-teaming exercise in the time of the interview:

"We actually have one [red-teaming] exercise ongoing. It is quite independent, so even I don't know the exact date when it starts…" "…I've given a them [the red-team] a list of management personnel towards whom the attack will be conducted "– Interviewee 8

6.4 Protective measures

This section describes the protective measures organizations have implemented to protect themselves from social engineering attacks. The interviewees were asked to describe their security & awareness training, technical controls, policy framework and physical controls. The results are reported in detail in subsections 6.4.1, 6.4.2, 6.4.3 and 6.4.4.

6.4.1 Training and awareness

100 % (n = 10) of the organizations reported having at least some sort of information security training or awareness materials available or were about to launch such. However, there was variance in the degree to which the training was mandatory, the depth and breadth of the training, training frequency, the degree to which the organizations were able to monitor the training and awareness coverage, and whether the training addressed the topic of social engineering. In this subsection, the results regarding training and awareness activities in the sample organizations are reported. The results are summarized in Table 8 below.

TABLE 8. Findings regarding training and awareness

Finding	Prevalence (%)	Prevalence (n)
Provides information security training	100 %	10
Training is mandatory	90 %	9
Is able to monitor training coverage within organization	70 %	7
Has tailored training for different roles	40 %	4
Training covers social engineering or phishing at least to some extent	80 %	8

90 % of the organizations reported that they have information security training, that is mandatory. Most often the training was offered as part of new employee onboarding, but many organizations had also introduced mandatory refresher training. Often the refreshers were due every year:

"We have a mandatory basic security training yearly and then there is an induction training for all newcomers" – Interviewee 3

Most organizations offered their information security training as web-based learning. This allowed them also to monitor the degree to which their employees have taken the training. 70 % said they are able to monitor the coverage of their information security training within the organization.

When asked about the degree to which there are different trainings for different roles in the organization, most organizations reported having the same trainings for everyone. 40% of the interviewees said they offer tailored training for, e.g., blue collars, management, IT personnel and developers.

"…and then as we have this information security management system, there is a dedicated, more specific [training] for the IT people" – Interviewee 8

"[referring to the scope of training] so there are the whole personnel, then there is the management, RD, testers and this sort of 'train the trainers' for more technical teams" – Interviewee 9

Many interviewees stated that they think role-based training would be beneficial, but did not yet provide such training:

"It [role-based training] would be good to have, but it's difficult to get there as there is shortage of awareness resources" – Interviewee 3

"Right now there is no [role based training]. The direction though is that it would be nice to have dedicated training for, say, the payroll" – Interviewee 5

The contents of the security training also yielded more variance. Even though 80 % of the interviewees reported that their training covers social engineering at least to some extent, the degree and depth in which the topic was addressed proved to set the organizations apart. Table 9 summarizes the findings of social engineering –related training reported by the interviewees:

TABLE 9. Aspects of social engineering related training [of those providing SE training]

Finding	**Prevalence (%)**	**Prevalence (n)**
Training provides tools to recognize phishing	88 %	7
Training includes SE case examples	63%	5
Training covers other methods of SE than phishing	38%	3

When asked about the degree to which their organization's security training covers social engineering, most interviewees described the topic being touched on a *general* level. The most common type of SE covered in the training was phishing. Phishing was commonly addressed by teaching how to recognize phishing emails.

Many organizations had also included SE case examples to their training. Again, the most common case was a real phishing email, which was used to demonstrate the "students" with common indicators of phishing.

> *"The training includes case examples… so there is this message [imitates] "would you say this is real". The aim is to provide awareness on how to recognize phishing "-* Interviewee 6

There were also examples of cases other than phishing:

> *"There are these videos with cases of phishing and suspicious phone calls… It's an imaginary company that the videos are set in. Goes through humor, it seems to sink in well"* – Interviewee 5

> *"There's also a video-case of physical intrusion"* – Interviewee 6

6.4.2 Technical controls

In terms of different solution implementations, there seems to be a rather little variance in the technical controls organizations have implemented to protect themselves from social engineering attacks. However, the degree and coverage within the solutions, e.g., coverage of MFA, seems to yield more variance. Findings regarding the technical controls identified in the interviews are summarized in Table 9 and reported in more detail below.

TABLE 9. Findings regarding technical controls

Finding	Prevalence (%)	Prevalence (n)
Multi-factor authentication		
MFA is implemented for internal and external users, in office network and remote connections	30 %	3
MFA is implemented for internal and external users, but for remote connections only	40 %	4
MFA not yet in widespread use or implementation is still in progress	30 %	3
Host antivirus		

Host antivirus and/or firewall	100 %	10
IDS / IPS		
IDS/IPS capabilities have been implemented	80 %	8
Email filtering		
Basic spam-filtering as part of email service	100 %	10
More advanced filtering capabilities purchased separately	70 %	7
Security Operations Center (SOC)		
A SOC is monitoring logs, at least partly	70 %	7
Data Loss Prevention (DLP)		
A DLP system has been implemented	30 %	3
Network protection and segmentation		
At least basic capabilities (e.g Firewall on perimeter)	100 %	10
At least intermediate segmentation capabilities (e.g., dedicated server networks, different locations in own segments)	20 %	2
Also more advanced segmentation (workstations in microsegments, own segments for different business processes)	30 %	3

70% of the organizations reported having Multi-Factor Authentication in place when connecting to their network. However, there was variance in the degree to which the solution was implemented. For instance, three of the interviewees reported having implemented MFA for both remote connections and within the company network, whereas four of the interviewees for remote connections only. Some had also implemented MFA for all remote connections, and administrative access within the company network.

There was also variance in the means of implementing the MFA. Some of the organizations were using a mobile application as an authenticator, whereas others had chosen a SMS-based authentication. Many organizations chose not to disclose their solution, but the ratio seemed to be roughly 50/50.

Three of the interviewees said that they either do not have MFA in widespread use, or are currently implementing it:

"We have it [MFA] coming across the entire organization, it's not that widely used yet" – Interviewee 2

Host-based antivirus solutions yielded less variance. All of the interviewees reported having a host antivirus solution in place. Most common scenario was, that the organization's workstations are installed from an image, consisting, among other things, the antivirus solution.

Different IDS/IPS solutions also proved surprisingly common. 80 % of the interviewees reported having such solutions in place either on the edge of their network, or even between different network segments. However, there is variance in the degree of sophistication in these solutions. For instance, some of the interviewees reporting having AI and Machine learning based IDS/IPS between different segments of their network.

"We have plenty of [IDS/IPS solutions] in place. We have, for instance, capabilities to identify anomalies in the traffic between different segments of our network… It's done with... well it is a buzzword but it's done by machine learning" – Interviewee 9

More common approach was to base the solutions on different rules and domain reputation:

"On the edge of our network there are IDS/IPS capabilities, like detecting IPs and domains related to malicious activity and blocking the traffic" – Interviewee 1

"*There are certain categories we've chosen… so those are blocked… I don't have the specs on those… and then there are the general reputation services that we use*" – Interviewee 6

Most companies with such solutions were also able to block potentially harmful outbound traffic, such as an employee clicking malicious email:

"…yes and the outbound [traffic] too, we have a [firewall vendor]'s next generation firewall and it has this capability. Of course it only works within our company network though" – Interviewee 5

Email/spam filtering was also widely adopted. All of the interviewees said they have at least basic spam filtering capabilities. Most often the solution was offered by their service provider, and it was based on domain reputation and blacklisting.

70 % of the interviewees also reported having purchased more advanced email-filtering capabilities, such DMARK, DKIM, and SPF-based filtering, as well as different ATP solutions, such as those offered by Microsoft:

"We have Microsoft's APT plans 1 & 2 in use with our email. It monitors the links within received emails and… so if it detects a malicious link, that email will be deleted" – Interviewee 5

"We have different tools for this [email/spam filtering] offered by Microsoft… Like their APT-plan… We're trying to get rid of whitelisting" – Interviewee 10

Similarly, 70 % of the interviewees reported having a dedicated Security Operations Center (SOC) monitoring their logs at least to certain extent. Many of the interviewees chose not to disclose the coverage or details regarding their SOC monitoring, but many reported that various logs are collected and stored in a centralized fashion. Most often, the SOC was purchased as a service.

"We have a SOC and they're monitoring the logs 24/7" – Interviewee 9

Even though most interviewees reported having capabilities to monitor and filter their outbound internet traffic, only 30 % had implemented a Data Loss Prevention (DLP) system. Some of the interviewees said they are currently in the process of assessing whether such system would be suitable for their environment and needs:

"It [DLP implementation] is the theme of this year… starting from classification of information, deploying new [data governance] models, introducing them to the organization… It will be implemented this year – Interviewee 5

It also seems that organizations may not always see the benefits of such system:

"At this time, we do not have it [a DLP system] in use. They are quite expensive and I would question the value they actually bring… Also the legality remains a question mark, it's hard to get a clear statement from Traficom [Finnish Transport and Communications Agency]" – Interviewee 3

When asked about the degree to which organizations have segmented their networks, there seems to be some variance in the level of sophistication in the segmentation effort. All of the interviewees reported having at least a basic firewall between their company network and the Internet. However, many said they have identified points of improvement in this area:

"There is certain segmentation [in the network] … this is where we have identified needs for improvement … It is somewhat challenging though, thinking of how companies built their networks 10 years ago vs. how they should be built now" – Interviewee 1

"It [network segmentation] is a big project for next year…Currently our network is quite mesh, so it allows lateral movement in the network" – Interviewee 4

"Well there is lot of variance… Our legacy is that there are several countries with all having their own implementation… the architecture is quite complicated. We're working on this site by site. The environments are so complex, that maybe it's complicated for the attacker as well" – Interviewee 2

Two interviewees described their segmentation effort as being on a more intermediate level, with some segmentation effort being implemented:

"Well the factory networks are of course separated, and the office networks are their own physical networks from dedicated address spaces… there are still things to be done on this front" – Interviewee 5

"…there are firewalls on sites and the workstations and servers are in their dedicated segments" – Interviewee 6

Rest of the interviewees reported segmentation effort that can be considered somewhat advanced, in relation to the effort reported by most:

"Well, let's put it this way that in our network the workstations cannot see each other" – Interviewee 7

"To some extent there is too much of that [segmentation]. The basic principle is that there is no traffic going from segment to another if not separately allowed… You can't even ping" – Interviewee 9

"Within the network, certain business processes have been segmented… there is, e.g., the office network, OT network, building automation network and so on…" – Interviewee 10

6.4.3 Policies

When asked about the different policies, standards and guidelines (PSGs) organizations have implemented to protect themselves, there seems to some variance especially in the domain of physical security. In this subsection, the findings regarding PSGs are reported.

Even though all of the interviewees reported having published an information security policy, one said their current policy is not up to date:

"Drafting and publishing a new information security policy is Q1 activities this year. At that front [policies in general] there are things to be done. We have published an information security policy, but it's not updated" – Interviewee 5

All organizations reported having implemented a clean-desk policy if applicable. An identification badge was also mandatory in most locations:

"Clean desk policy, badges, locking your screen… we have all these basic things" – Interviewee 9

"Where I sit there is a clean desk policy… it's an open office… but we have also locations where employees have their own offices, there it's different" – Interviewee 5

However, the clean-desk policy may not always be enforced:

"We have a clean desk policy, but not in the strictest fashion, or forced that much really… and of course there are differences in different locations" – Interviewee 1

Similarly, it may not be very strictly followed:

"There is a clean desk policy, but it might not actualize that well… it's followed only partly" – Interviewee 2

Surprisingly, 40 % of the interviewees reported not having a physical security policy or standard in place, or it only existed as a draft. Often the physical security matters were not on the interviewees' responsibility, but rather on either the risk management organization, corporate security or facilities organization. Some interviewees also reported, that they only have a physical security policy for their factory floors, not for the office premises.

A common approach was also to leave the physical security aspects to be determined by individual sites. Some interviewees reported having organized their physical security in this manner:

"We don't have a physical security policy… but it [physical security] is considered in the information security policy. There are separate [physical security] guidelines for sites, but there are some differences in the ways sites do it" – Interviewee 1

"There is no physical security policy. Instead, every location makes their own guidelines. I think it's a bit of a problem" – Interviewee 8

In addition to information- and physical security related policies, many interviewees also reported having policies and guidelines for privacy and data governance. A common theme for PSGs was that many of the interviewees reported difficulties in deploying the PSGs within their respective organizations:

"The policies are being implemented little by little in different locations… The guidelines and policies exists, but the deployment is still ongoing" – Interviewee 2

"Well we go through these [PSGs] with the new-joiners, but other than that its somewhat difficult [to deploy the PSGs]. It's a little like 'doesn't' matter what we publish here, not all will still receive it'. We have identified this issue" – Interviewee 5

6.4.4 Physical security

The physical security controls implemented by organizations yielded some variance in the degree to which the controls had been implemented. All interviewees reported their organization having at least CCTV surveillance and a manned reception in place, at least in their headquarters:

"In the HQ there is always a person in the reception, we have access controls on all floors of the facility… so there are cameras and there is access control" – Interviewee 2

"Cameras, fences, guards… all of these we have at the HQ" – Interviewee 8

Similarly, most organization had implemented at least some sort of physical segmentation. The most common approach was a keycard, that only allowed access to certain areas within a facility. However, many organizations with multiple locations reported difference in practices between their sites:

"It [the implemented physical security measures] varies by site… the storage facilities are best protected" – Interviewee 4

"There might not be a reception in the smaller locations… Although there is still access control" – Interviewee 6

"In the smaller offices there aren't any specific guidelines, so they might not be that secure… there is quite a lot of variance" – Interviewee 8

Similarly, the organizations with operational sites (e.g., manufacturing or similar) reported having a stricter approach for their OT environments compared to their offices. However, the OT security measures might not always reflect the requirements of information security:

"On the physical side… I think the mindset is in different kind of threat… maybe information security is not that much considered. I don't think we've prepared for somebody to come and 'burn' their face in gathering information on site – Interviewee 1

6.5 Perceived strengths and areas of improvement

The interviewees were also asked to share their perspective on both the strengths, and areas of improvement with regards to protecting from social engineering attacks. Findings regarding the strengths and improvement areas are summarized in Table 10 and reported in more detail below.

TABLE 10. Summary of perceived strengths and areas of improvement.

Finding	Prevalence (%)	Prevalence (n)
Perceived strengths in protecting from SE attacks		
Technical controls	60 %	6
Training and awareness	20 %	2
Policies and guidelines	10 %	1
Physical security	10 %	1
Perceived areas of improvement in protecting from SE attacks		
Training and awareness	50 %	5
Physical security	30 %	3
Policies and guidelines deployment	20 %	2
Technical controls	10 %	1
Visibility in information security practices of other locations	10 %	1

When asked about their view on the strengths their respective organization has in protecting from SE attacks, majority of the interviewees mentioned technical controls and capabilities as their biggest strength. The results align with the notion that all organizations reported having at least basic technical capabilities in place to protect from social engineering attacks, as described in subsection 6.4.2. Other aspects of protection, such as training and awareness, or physical security, were not mentioned that often.

Interestingly, training and awareness was most commonly mentioned as the single biggest area of improvement in protecting from social engineering attacks:

> *"The training side is the most difficult…how to organize continuous training to thousands of people. The training should be timely…It's difficult because of other hurries"* – Interviewee 3

> *"Training related to user's work profile and responsibilities… We need more training in that area. Targeted training…"* – Interviewee 5

> *"Awareness is most behind. It's a lot of work translating the material to all the local languages"* – Interviewee 10

Physical security matters also stood out as the more commonly mentioned areas of improvement:

> *"[areas of improvement] In some countries and certain aspects of physical security…Maybe I won't go any deeper to that"* – Interviewee 2

> *"Physical security is the weakest link for us"* – Interviewee 8

In terms of policies and guidelines, both findings relate to the deployment of the documentation. The interviewees reported having difficulties in deploying the PSGs in their respective organization. The issues were related to translating the documentation and effectively communicating it to the personnel.

> *"Training and deployment [of PSGs] are the topics with most need for development…Just by publishing something in the intranet you don't get that far. On this front we need to keep putting more effort to it"* – Interviewee 9

Technical controls were mentioned as the biggest area of improvement in only one occasion. This notion is in line with the finding that most organizations seem to perceive their technical capabilities as their biggest strength in protecting from SE attacks.

All in all, it seems that organizations have the most confidence with regards to their technical capabilities in protecting from SE attacks, and the least confidence in their capabilities regarding training and awareness. The finding is significant, given that all organizations have been targeted with at least some form of social engineering attack, and as SE attacks are by definition targeting people – the same people that ought to be trained to identify and protect from such attacks. In the next section, the results of the study are discussed and concluded.

7 Discussion and conclusion

In this section, the results of the study are discussed and compared with earlier research. Similarly, the results are concluded in order to answer the research questions identified previously in this work. Finally, the limitations of this study, as well as suggestions for future research are discussed.

7.1 Discussion

It seems that SE attack attempts were somewhat more prevalent amongst the sample organizations if compared to their peers internationally. For instance, UK officials reported that 80 % of businesses in the UK have experienced phishing or other fraudulent emails (Department for Digital, Culture, Media & Sport, 2019). The corresponding number amongst Finnish organizations was 100 %. This difference is likely due to the fact that the sample in the UK survey consisted of both small and large organizations, whereas the Finnish respondents represented only large organizations.

Attackers seem to be a little less successful against Finnish organizations than their foreign counterparts. In the United Kingdom, 49 % of security breaches were due to phishing or other fraudulent emails (Department for Digital, Culture, Media & Sport, 2019). In Finland, the number stands a little lower at 40 %. However, it is still possible that the actual number is higher in Finland. As indicated by some of the interviewees, organizations may not always have a clear view of the root cause of security incidents. Hence, they might be unaware of whether a breach was caused by a SE attack, malware or something else.

Interestingly, seven out of ten interviewees perceived their organization's maturity in identifying an SE attack either similar to or higher than their peers. Only two thought they are somewhat behind. This result is somewhat contradictory to the finding that many organizations reported their security training and awareness programs as having most room for improvement. It seems that organizations trust their employees having common sense when it comes to dealing with suspicious communication attempts, such as email, calls or text messages. When compared to earlier studies, the notion of high maturity is somewhat contradictory. For instance, according to EY's Global Information Security Survey (EY, 2018), 60 % of information security leaders perceive careless or unaware employees as the top cause increasing their risk exposure.

When it comes to assessing cybersecurity risks, it seems that the Finnish organizations are far better off than their global counterparts. 90 % of the interviewees reported their organization conducting risk assessments for cybersecurity risks. In the UK, only 31 % of the respondents reported having conducted risk assessments on cybersecurity risks according to the Department for Digital, Culture, Media & Sport survey of 2019. According to a global survey conducted by Marsh & Mclellan (2018) in cooperation with Microsoft, 34 % of organizations do not assess cybersecurity risks. This significant difference between Finnish organizations and companies abroad is again likely explained by the sample of the research; both the UK study and the Marsh & Mclellan study had a significant proportion of small organizations in their sample. Comparison in security testing and audits yields similar findings in favor of the Finnish organizations.

Also, the findings related to security training seem to favor the Finnish organizations over their global counterparts. In the UK, only 27 % of the organizations overall have had their employees attend an information security training. The number is significantly higher among large organizations (73 %) but still lags behind the Finnish number of 100 %. When it comes to SE and phishing related training, the Finnish still stand strong; 80 % of the interviewees reported their organization's training program covering SE-related topics. The similar number globally is 55 % according to Marsh & Mclellan (2018).

When it comes to technical controls and protective measures, there is some variance between Finnish organizations and their global counterparts. The Finnish are ahead in some aspects and behind in others. Table 10 summarizes a comparison between Finnish organizations and companies globally, as reported in various publications:

TABLE 11. Findings of technical controls compared with earlier research.

	Ali-Kovero (2020)	Cyberedge group (2019)	UK DDCMS (2019)	Marsh & Mclellan 2018	SANS (2019)*
Finding					
MFA implemented at least for remote connections	70 %	54 %	N/A	40 %	N /A
Host antivirus in place	100 %	66 %	90 %	N /A	53 %
IDS / IPS capabilities	80 %	59 %	N/A	N/A	76 %
Email filtering / secure email gateway	100 %	58 %	N /A	N /A	N/A
Security Operations Center or other activity monitoring	70 %	N /A	57 %	N /A	25 %
Data Loss Prevention System (DLP) implemented	30 %	57 %	N / A	35 %	23 %

At least basic Network security capabilities, such as firewall on perimeter	100 %	N /A	89 %	N /A	N / A

*SANS-survey (Filkins, Wylie, & Dely, 2019) results reflect ICS/OT environments

As summarized above, it seems that the Finnish organizations are better off in terms of technical security controls compared to their global counterparts. However, it seems that a DLP-system is not as common in Finland as it is in other parts of the world. This finding might be due to the fact that the samples in the reference studies consist of organizations around the world, and they might not be subjected to as strict privacy and other data protection laws as Finland (and other EU countries). This notion is further supported by the comments made by some of the interviewees regarding the unclear legal status of DLPs in Finland.

In terms of cybersecurity policies, the Finnish organizations seem to be once again ahead of their peers. In Finland, all of the organizations reported having a cybersecurity policy in place, even though in one case it was outdated. In the UK, the same number is 74 % for large companies.

When it comes to physical security controls, Finnish organizations seem to have implemented many of the best practices (such CCTVs, fences, guards, access controls, etc.) as described in the source literature, (e.g., Baker & Wallace, 2007; Hutter, 2016). However, as mentioned by a number of interviewees, physical security matters do not fall under their responsibility. Hence, there is a risk of physical security measures not reflecting the needs of information security as discussed with one of the interviewees.

For the perceived strengths and areas of improvement, a notable finding was that many organizations reported needs for improvement in their training & awareness capabilities. The finding is interesting, given that all organizations had a training program in place, the training was mandatory in most cases and the majority of organizations had the capability to monitor the execution rate of the training. In light of these notions, the maturity of organizations' training and awareness capabilities seems quite high. It is possible, that the lack of dedicated and role-based training contributed to this view among the interviewees. Also, a notable finding was that most training programs seem to lack detail when it comes to SE related training. Given that most organizations had experienced SE attacks, the finding is rather surprising.

All in all, the Finnish organizations seem to be quite mature when it comes to protective measures against SE attacks. The organizations have implemented many of the best practices in protective measures as described in information security literature. Compared to their counterparts globally, the Finnish organizations seem to perform better in most aspects. However, it needs to be noted that the sample of this study consisted of some of the largest organizations in Finland, and often larger organizations have also the ability to dedicate bigger resources for information security efforts. Similarly, as one of the interviewees pointed out, it might be that this type of study attracts interviewees with more confidence in their security posture, whereas less confident organizations might refuse to participate in such study.

7.2 Conclusion

In this work, we studied the phenomenon of social engineering from different viewpoints. At first, the different theoretical concepts of SE were examined through means of a literature review. The literature review part of this work sheds light on the two first research questions:

1. What is social engineering?
2. How can organizations protect themselves against social engineering attacks?

Based on the conducted research, social engineering can be defined as the act of exploiting weaknesses in human psychology and thereby manipulating victims to either divulging or granting access to confidential information or data. As an umbrella term, social engineering covers a wide array of different techniques ranging from fraudulent email-messages to physical intrusion attempts.

When it comes to protecting from SE attacks, it seems that the best approach for organizations is to adopt the doctrine of defense in depth. In other words, organizations should implement various protective measures on several different fronts, including people, processes and technology. These measures include, for instance, training, audits, policies, guidelines, access controls, and network security controls.

The empirical part of this work focused on the reality of protective measures organizations have actually implemented to protect themselves from SE attacks. The empirical research sheds light on the third research question:

3. How are organizations currently protecting themselves against social engineering attacks?

As the conducted research suggests, SE attacks, and phishing in particular, are very common problems for organizations in their current operating environment. Still, many organizations do not formally recognize SE as an information security risk, even though most of the interviewees personally recognized it as such. This lack of formal recognition is somewhat surprising, given that in many of the most famous cyberattacks, such as *Stuxnet* and *attacks on the Ukrainian power grid*, the initial access was gained through SE.

At their current state, organizations seem to have adopted the approach of defense in depth – at least in part. However, there seem to be improvement needs especially in their efforts regarding training and awareness and physical security. The training often lacks detailed guidance on how to protect from SE attacks and has not been tailored to suit the needs of different organizational roles. Similarly, the organization’s physical security measures might not always reflect the perspectives of information security.

7.3 Research limitations, success and impact

Like all academic research, this study also has its limitations. The noted limitations center around the data collection, both in terms of literature review and empirical research.

As it turns out, Social Engineering as a concept and phenomenon has been studied quite widely. However, the body of research on protective measures against SE attacks is much lighter. This research often seems to be somewhat high-level, providing advice such as “implement access controls” without specifying what those controls could or should be. Therefore, it proved quite laborious to extract information on the best practices of protecting against SE.

The other observed limitation has to do with the generalizability of the research results. Even though qualitative research may not strive for statistical generalizability, the limitations of this research should still be noted. As discussed, the sample of interviewees for the research was chosen on a discretionary basis and the interviewees represent some of the biggest companies in Finland. Therefore, the results should be considered in the context of big organizations and should not be directly viewed as applicable to smaller organizations.

When it comes to the success factors of this work, the study was successful in terms of practical execution. The study was planned as an empirical, qualitative study to be conducted through semi-structured interviews by interviewing information security leaders in Finland. All interviews were carried out successfully, allowing for a large collection of data to be analyzed for this work. The analysis and results, as reported in chapter six, proved sufficient in answering the research questions formed for this work.

As far as the researcher is concerned, this is the first time in Finland the actual protective measures organizations have implemented against SE attacks are studied to this extent. Therefore, this work’s impact is not only in providing detailed information on the current state of companies in Finland but also provides a benchmark and best practices for organizations to use in strengthening their overall information security posture.

7.4 Suggestions for future research

As implied in the previous section, not too much research has been conducted on the protective measures against SE attacks. Therefore, this work leaves room for studying the phenomena in different contexts; be it smaller organizations, companies in other countries, third sector organizations, or even individual people.

Similarly, there is room for research regarding the effectiveness of different controls. Such research would help companies to strengthen their security posture, as it would provide the means for prioritizing their security needs and efforts.

Future research could also shed light on whether there are different security needs for smaller companies compared to larger ones when it comes to protecting from SE attacks. As the small and medium-size companies make up the biggest majority in Finland by far, it would be valuable to study their security needs and requirements in terms of SE. As smaller organizations have often limited resources, such a study could provide helpful insight for assessing the ways the smaller organizations should allocate their resources.

REFERENCES

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Process*, *50*(2), 179–211.

Allsopp, W. (2009). *Unauthorized access - Physical penetration testing for IT security teams*.

Armstrong, R., Hall, B. J., Doyle, J., & Waters, E. (2011). "Scoping the scope" of a cochrane review. *Journal of Public Health*, *33*(1), 147–150.

Baker, W. H., & Wallace, L. (2007). Is Information Security Under Control? *IEEE Security and Privacy*.

Bhattacherjee, A. (2012). *Social Science Research: Principles, Methods, and Practices*.

Brannen, J. (2007). Mixing Methods: The Entry of Qualitative and Quantitative Approaches into the Research Process Julia. *International Journal of Social Research Methodology*, *8*(3), 173–184.

Cerpa, N., & Verner, J. M. (2009). Why did your project fail? *Communications of the ACM*, *52*(12), 130.

Cialdini, R. B. (2001). Harnessing the Science of Persuasion October 2001. *Business*, (March).

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23), 31–38.

Department for Digital, Culture, M. & S. (2019). *Cyber Security Breaches Survey*.

European Union Agency for Network and Information Security. (2018). *ENISA threat landscape report 2017 - 15 Top Cyber-Threats and Trends*.

EY. (2017). Cybersecurity regained: preparing to face cyber attacks. *20th Global Information Security Survey 2017-18*, 30.

EY. (2018). Is cybersecurity about more than protection? *Ey Global Information Security Survey 2018-2019*.

Filkins, B., Wylie, D., & Dely, A. J. (2019). SANS 2019 State of OT / ICS Cybersecurity Survey. *SANS Technology Institute*, (June).

Flores, W. R. (2016). *Shaping Information Security Behaviors Related to Social Engineering Attacks. PhD Thesis*.

Granger, S. (2006). Social Engineering Fundamentals , Part I : Hacker Tactics Social Engineering Fundamentals , Part I : Hacker Tactics. *Most*, *1527*.

Hadnagy, C. (2010). *Social Engineering - The art of Human Hacking*.

Hadnagy, C. (2018). *Social Engineering - The Science of Human Hacking*.

Halevi, T., Memon, N., & Nov, O. (2015). Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks. *SSRN*.

Harris, J. D., Quatman, C. E., Manring, M. M., Siston, R. A., & Flanigan, D. C. (2007). How to write a systematic review. *American Journal of Sports Medicine*, *42*(11), 2761–2768.

Heartfield, R., & Loukas, G. (2015). A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. *ACM Computing Surveys*, *48*(3), 1–39.

Hinson, G. (2008). Social Engineering Techniques, Risks, and Controls. *Edpacs*, *37*(4–5), 32–46.

Hirsjärvi, S., Remes, P., & Salovaara, P. (2009). *Tutki ja kirjoita*. Tammi.

Hong, J. (2012). The State of Phishing Attacks. *Communications of the ACM*, *55*(1),

HS. (2016). Husin potilaspapereita löytyi kerrostalon pihalta Vantaalla – ”27 yrs of basic healthy woman, behind two alatiesynnytystä”. *Helsingin Sanomat*.

Hutter, D. (2016). Physical Security and Why It Is Important. *SANS Technology Institute*.

InfoSec Institute. (2015). Defense in depth is dead; Long live defense in depth!

ISO/IEC. (2018). INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Overview and vocabulary, *2018*, 38.

Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2005). Social Phishing. *Communications of the ACM*, *2005*, 1–10.

Kaplan, B., & Duchon, D. (1988). Combining Qualitative and Quantitative Methods in Information Systems : A Case Study. *MIS Quarterly*, *12*(4), 571–586.

Kewley, D. L., & Lowry, J. (2001). Observations on the effects of defense in depth on adversary behavior in cyber warfare. *Proceedings of the IEEE SMC Information Assurance Workshop*, 1–8.

Kramer, R. (2009). Rethinking trust. *Harvard Business Review*, (June).

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2014). Advanced Social Engineering Attacks. *Journal of Information Security and Applications*, 1–11.

Long, J., Pinzon, S., Wiles, J., & Mitnick, K. (2008). *No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing*.

Luo, R., Brody, R., Seazzu, A., & Burd, S. (2011). Social engineering. *Information Resources Management Journal*, *24*(1), 1–8.

Marsh, & Mclellan. (2018). *By the Numbers : Global Cyber Risk Perception Survey*.

Maxwell, J. A. (2008). *Designing a Qualitative Study*.

Mcrae, R., & John, O. (1992). An Introduction to the Five-Factor Model and Its Applications. *Journal of Personality*, *60*(2), 175–215.

Mitnick, K., & Simon, W. (2001). *THE ART OF DECEPTION - Controlling the Human Element of Security*.

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social Engineering Attack Detection Model: SEADMv2. *Proceedings - 2015 International Conference on Cyberworlds, CW 2015*, (October), 216–223.

Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014). Social engineering attack framework. *2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference*, (August).

Mujs, D. (2004). *Doing Quantitative Research in Education*.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*, *17*(1), 2–26.

Northcutt, S. (2009). Security controls. Retrieved from https://www.sans.edu/cyber-research/security-laboratory/article/security-controls

NSA. (2010). Defense in Depth - A practical strategy for achieving Information Assurance in today’s highly networked environments. *National Security Agency*.

Parker, D. (1998). FIGHTING COMPUTER CRIME: A NEW FRAMEWORK FOR PROTECTING INFORMATION. *Wiley*, 506.

Pfleeger, C. P., & Pfleeger, S. L. (2012). *Analyzing Computer Security*.

Puhakainen, P., & Siponen, M. (2010). IMPROVING EMPLOYEES' COMPLIANCE THROUGH INFORMATION SYSTEMS SECURITY TRAINING: AN ACTION RESEARCH STUDY. *MIS Quarterly*, *34*(4), 757–778.

PwC. (2018). The Global State of Information Security Survey 2018, (January).

Rubin, H. J., & Rubin, I. S. (2011). *Qualitative interviewing: The art of hearing data*.

Schultze, U., & Avital, M. (2011). Information and Organization Designing interviews to generate rich data for information systems research. *Information and Organization*, *21*(1), 1–16.

Simons, D. J., & Chabris, C. F. (1999). Simons and Chabris (1999). *Perception*, *28*, 1059–1074.

Siponen, M. (2006). Information Security Standards Focus on the Existence of Process, Not Its Content. *Communications of the ACM*, *49*(8), 97–100.

Siponen, M., & Klaavuniemi, T. (2020). Demystifying beliefs about the natural sciences in information system. *Journal of Information Technology*, *00*(0), 1–13.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*, 31–41.

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information and Computer Security*, *23*(2), 200–217.

Stallings, W., & Brown, L. (2015). *Computer Security - Principles and Practice*.

Uebelacker, S., & Quiel, S. (2014). The Social Engineering Personality Framework. *Workshop on Socio-Technical Aspects in Security and Trust. IEEE*, 24–30.

Whitman, M. E., & Mattord, H. J. (2011). Principles of Information Security Fourth Edition. *Learning*, 269, 289.

Wiles, J., Gudaitis, T., Jabbusch, J., Rogers, R., & Lowther, S. (2012). *Low tech hacking: street smarts for security professionals*. *Low Tech Hacking: Street Smarts for Security Professionalsen*. Elsevier Inc.

Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing , SMiShing & Vishing : An Assessment of Threats against Mobile Devices. *Journal of Emerging Trends in Computing and Information Sciences*, *5*(4), 297–307.

APPENDIX 1: THE INTERVIEW FRAMEWORK

Esittely, tutkimuksen tausta ja tavoitteet

Haastateltavan rooli yrityksessä ja vastuualueet lyhyesti

Taustatiedot:
Kartoitetaan haastateltavan näkemyksiä ja kokemuksia social engineering hyökkäyksistä:

- Haastateltavan mahdolliset kokemukset social engineering -hyökkäyksistä
- Yleisnäkemys oman yrityksen kyvykkyyksistä hyökkäyksiltä suojautumiseen

Agenda:
Kartoitetaan, missä laajuudessa social engineering -hyökkäysten uhka on yrityksen riskiagendalla:

- Tehdyt riskikartoitukset ja social engineeringin tunnistaminen riskiksi
- [Yleisellä tasolla] Suunnitellut / tehdyt toimenpiteet riskien minimoimiseksi
- Mahdollisesti aiemmin tehdyt auditoinnit/testaukset ja havainnot niiden perusteella

Kontrollit:
Kartoitetaan, minkälaisia kontrolleja ja tapoja yrityksellä on social engineering -hyökkäyksiltä suojautumiseen ja toisaalta riskien minimoimiseen.

- Työntekijöiden saama tietoturvakoulutus
    - Koulutuksen laajuus ja kohderyhmät
    - Koulutuksen sisältö, kattavuus ja suorituksen seuraaminen
    - Koulutuksen SE näkökulma

- Implementoidut tekniset kontrollit/turvamekanismit, esim:
    - MFA (implementoinnin laajuus)
    - Sähköpostifiltterit
    - Anti-phishing tools
    - Päätelaiteturvallisuus
    - Biometriikka IAM:issa
    - IDS/IPS
    - Whitelistaukset
    - Verkkoturvallisuus

  - DLP
  - Muuta?

- Politiikka -tason kontrollit

  - Tietoturvapolitiikka ja sen sisältö
  - Ohjeet
  - Prosessit
  - Muuta?

- Fyysinen turvallisuus

  - Vartiointi ja valvonta
  - Pääsyrajoitukset
  - Muuta?

Koetut vahvuudet ja heikkoudet:
Kartoitetaan, millä suojautumisen osa-alueilla organisaatiot kokevat olevansa vahvimpia ja missä puolestaan on eniten kehitettävää.