Organizational Culture Framework for Mitigating Human Factors in Cybersecurity

Goleš Babić, Marko

Sveučilište u Zagrebu

Ekonomski fakultet

Managerial Informatics

ORGANIZATIONAL CULTURE FRAMEWORK FOR MITIGATING HUMAN FACTORS IN CYBERSECURITY

MASTER THESIS

Student: Marko Goleš Babić

JMBAG: 0067615102

Mentor: Prof. dr. sc. Mario Spremić

Zagreb, September 2020

Contents

1. Introduction 3
1.1 Topic and Goals of the Thesis 4
1.2 Explanation of methodology 4
1.3 Structure of the Thesis 4
2. Cybersecurity and social engineering 6
2.1 Cybersecurity overview 6
2.1.1 Definition and comparison with information security 8
2.2 Social Engineering Overview 8
3. Social Engineering Taxonomy 10
3.1 The Research Phase 12
3.2 The Exploitation Phase 13
3.2.1 Social engineering techniques 13
3.3 The Execution Phase 17
4. Cybersecurity Risk Factors and Mitigation 18
4.1 Human factor in cybersecurity 20
4.2 Impact of organizational culture on cybersecurity 23
4.3 Cybersecurity Awareness 27
5. Existing Culture Frameworks 29
5.1 ENISA Framework 29
5.2 Organizational Cybersecurity Culture Model 30
5.3 NIST Framework for Improving Critical Infrastructure in Cybersecurity 32
6. Proposed Culture Framework 36
7. Applying culture framework to a case study – Target data breach 43
7.1 Introduction of the case study and synopsis of the breach 43
7.2 Breach investigation overview 43
7.2.1 Events leading up to the breach 43
7.2.2 Breach investigation results 44
7.2.3. Aftermath 45
7.3 Target's culture of data protection 46
7.3.1 Target cybersecurity culture change 46
8. Conclusion 49
Literature 50
List of Tables 55
List of Figures 56

MARKO GOLES BABIĆ

Name and family name of student

STATEMENT ON ACADEMIC INTEGRITY

I hereby declare and confirm with my signature that the MASTER THESIS

(type of the paper)

is exclusively the result of my own autonomous work based on my research and literature published, which is seen in the notes and bibliography used.

I also declare that no part of the paper submitted has been made in an inappropriate way, whether by plagiarizing or infringing on any third person's copyright.

Finally, I declare that no part of the paper submitted has been used for any other paper in another higher education institution, research institution or educational institution.

In Zagreb, AUG 31, 2020

(date)

Student:

(signature)

1. Introduction

1.1 Topic and Goals of the Thesis

This thesis examines how knowledge from the field of organizational psychology can be utilized to mitigate cybersecurity risk for organizations, particularly when it comes to the liability that often stems from the human side of cybersecurity which is predisposed for being exploited by social engineering attacks.

The goal of the thesis is to introduce a framework for fostering an organizational cybersecurity culture. This framework must primarily ensure ease of application and adhere to most important protection measures in cyberspace.

1.2 Explanation of methodology

To confirm the prescribed objectives of the thesis the following methods were used: investigation of literature (primary and secondary data) and graphical and statistical methods for discussing the research results. A range of literature was available online, and certain academic sources were obtained from the author's personal educational experience throughout the years. The proposed framework is based on elements from existing cultural frameworks.

1.3 Structure of the Thesis

The thesis is structured in a manner that ensures that the topic is introduced to the reader before more complicated research and case studies are presented. The thesis consists of 5 large chapters: cybersecurity and social engineering, social engineering taxonomy, cybersecurity risk factors and mitigation, existing culture frameworks, and proposed culture framework. In the cybersecurity and social engineering chapter, a literature review on cybersecurity and social engineering is provided to the reader as if they have no prior knowledge of the topic. The social engineering taxonomy chapter explains the various stages in a typical social engineering attack and proposes a social engineering taxonomy based on existing research. The cybersecurity risk factors and mitigation chapter analyzes the human factor in cybersecurity, examines the impact organizational culture has on organizational cybersecurity, and introduces cybersecurity awareness as a potential method for mitigating human-enabled cybersecurity risk. The existing culture frameworks chapter will explain the basic methodology of existing cybersecurity culture frameworks, while the final large chapter will propose a framework for fostering organizational cybersecurity culture by detailing its basic principles, structure, and methods of implementation. In addition, the dangers and

consequences of a social engineering attack are presented through a real-life case study, and the proposed framework is utilized to provide a theoretical benchmark for implementing a healthy cybersecurity culture and mitigating the vulnerabilities identified in the case study.

The thesis concludes by examining the limitations of the methodologies and ethical and legal challenges of cyber risk assurance and suggests directions for further research to ensure that the proposed framework is fully applicable.

2. Cybersecurity and social engineering

This chapter will provide an overview of cybersecurity in terms of its' relation to information security and the cybersecurity risks associated with human, organizational, and technological factors.

2.1 Cybersecurity overview

Cybersecurity has been defined as the harmonization of capabilities in people, processes, and technologies to secure and monitor authorized and unauthorized access and safeguard computing systems along with the sensitive information they hold (Daniel Ani et al., 2016, p. 170). Historically, the term cybersecurity became prominent with the emergence of the cyber domain, which can be defined as a global domain of interconnected and interdependent networks of information that include computer systems, telecommunication networks, and the Internet. Before technological advancements provided the ability to interconnect devices and entire systems on a global scale, in the early 1990s cybersecurity was referred to as 'computer security', as there was only ever a need to safeguard a single computer. (Patterson, W., & Winston-Proctor, C.E., 2019, p. 3).

Patterson and Winston-Proctor (2019) identify three aspects of cybersecurity (p. 4):

- secrecy, which is the need to ensure that sensitive information is not disclosed to anyone who is not authorized to access it
- accuracy, which means that a system must not corrupt information or allow any unauthorized malicious or accidental changes to it
- availability, which means that the computer hardware and software need to work efficiently and be able to recover quickly and completely if compromised, as denial of service is sometimes as disruptive as actual information theft

As technology continues to advance at a rapid level, cyberspace continues to change, and it is consequently increasingly more complicated to adhere to the three aspects of cybersecurity. According to Dreibelbis et al. (2018), "the changes in cyberspace are driven by a unique interplay of technologies, companies, individual actors, governments, and academic institutions" (p. 347) and each of these factors are viable to be exploited in cybersecurity attacks. This threat is compounded by the fact that security concerns are often merely an afterthought when many of

the technologies are developed (Dreibelbis et al., 2018, p. 347). Additionally, the sheer pace of change in cyber domains makes it difficult to keep up with security considerations (Dreibelbis et al., 2018, p. 347), as a variety of independent factors (i.e. technology, people, digital transformation) potentially create vulnerabilities for an organization.

Spremic and Simunic (2018) point out that digital transformation has become a high priority among organizational leadership as recent research shows that close to 90% of business leaders in the U.S. and U.K. expect IT and digital technologies to make an increasing strategic contribution to overall business of their organization in the upcoming decade (p. 341). While digital transformation undoubtedly facilitates business processes, it also potentially exposes organizations to increased cybersecurity risks because the same technologies used to foster innovation can be utilized to create more externally oriented and sophisticated cybersecurity threats (Spremic & Simunic, 2018, p. 341). Moreover, Spremic and Simunic (2018) contend that, despite the significant impact cyberattacks can have on organizations, it appears that information security and underlying IT and digital technologies "are still mistakenly regarded as a separate organization of the business and thus a separate risk, control, and security environment" (p. 347). Some organizations simply are not aware of potential cybersecurity threats and vulnerabilities and the amount of damage these vulnerabilities can cause if exploited.

Since organizations increasingly rely on digital technologies to conduct everyday business and store sensitive information, the impact of cybersecurity incidents is often far greater than it would have been a decade ago. This is illustrated by the fact that, based on over 2,000 interviews across 254 organization in seven countries, the Ponemon institute determined that the average cost of cybercrime in 2017 was $11.7 million per organization (Van der Klei, R., & Leukfeldt, R., 2020, p. 16). Other examples of consequences of cybersecurity incidents include lost business opportunities, the loss of information assets, business disruption, and technological damage. With this taken into consideration, it can be concluded that the "main objective in managing cyber security is to carefully design and apply basic, sophisticated and smart, but effective and efficient security controls to address common, advanced and emerging threats to information stored in information systems supported by digital technologies" (Spremic & Simunic, 2018, p. 348).

2.1.1 Definition and comparison with information security

For the purpose of this work, it is necessary to define and compare the terms "cybersecurity" and "information security". According to Buchy (2016), cybersecurity is viewed as a subset of information security, as information security focuses on protecting information in both the physical and cyber environment, whereas cybersecurity concerns itself with protecting information in the cyber environment (Dreibelbis et al., 2018, p. 350). Spremic (2017) adds that information security offers a lower level of security as it concerns itself with safeguarding information, whereas the term cybersecurity involves mitigating and preventing the consequences of targeted and sophisticated cyberattacks in an organizational environment (p. 58). In other words, cybersecurity does not solely concern itself with protecting the cyberspace itself, but also focuses on protecting "those that function in cyberspace and any of their assets that can be reached via cyberspace" (Spremic, 2018, p. 342). Spremic and Simunic (2018) define the design and implementation of effective safeguards for protecting organizations and individuals from cyberattacks and breaches as the main focus of cybersecurity (p. 342).

It is important to note that cybersecurity also concerns itself with the physical environment but, unlike information security which fully incorporates the physical environment, only does so in situations in which the physical environment has an effect on security in the cyber domain. Another important distinction between the two terms is the fact that the foundation of cybersecurity is detecting problems and anticipating problems (Spremic, 2017, p. 48), whereas information security mainly focuses on reacting to and mitigating existing problems.

In the context of social engineering, information security and cybersecurity play an important role in mitigating risk, as social engineering attacks involve factors from both the physical and cyber domain.

2.2 Social Engineering Overview

Social engineering is defined as "…the use of manipulation, persuasion, and influence by an attacker to obtain sensitive information or access to restricted areas" (Hadlington, 2017, p. 3). In the context of cybersecurity, these psychological techniques are often used, along with technological tools, on individuals who are connected to the cyber domain, whether for personal reasons or as required by their profession. According to Lohani (2019), social engineering attackers prey on common aspects of human psychology such as curiosity, courtesy, empathy, and

gullibility to induce individuals into giving away information or carrying out specific tasks that can be of use to them (p. 385).

In most social engineering attacks, the victim does not realize an attack occurred until it is too late and, since social engineering attacks effectively exploit an individual's psychological makeup, technological safeguards are often not enough to prevent them. According to the United States Department of Justice (2017), social engineering attacks continue to be prevalent and pose a great threat, despite technological safeguards like antivirus software, firewalls, or intrusion detection systems (Aldawood & Skinner, 2020, p. 1). Another reason why security tools are often ineffective in preventing social engineering attacks is the fact that certain social engineering attacks occur strictly in the physical domain (e.g. stealing security credentials, devices, and sensitive files). Accordingly, Daniel Ani et al (2016) conclude that, in spite of the massive deployment of technology solutions to protect industry control systems, "human factors still play a very significant role towards the implementation of desirable cyber-secure ICS environment" (p. 171). Alternatively stated, organizational security could be completely undermined if employees fail to understand and uphold their roles in the security solution of an organization (Daniel Ani et al., 2016, p. 171).

An effective way to help employees understand their role in the overall security solution of an organization is to analyze social engineering attacks from the perspective of the attacker. In doing so, the average person who is not necessarily familiar with the threats of social engineering would be provided with a useful theoretical framework that is likely to increase their understanding and have a positive effect on their behavior. On that account, a social engineering taxonomy is proposed and expounded in the following chapter.

3. Social Engineering Taxonomy

Most cyber-attackers exploit certain vulnerabilities within a system or an organization. As cybersecurity awareness continues to rise, vulnerabilities are becoming increasingly harder to identify. Consequently, cyber-attacks are often preceded by a vulnerability analysis (sniffing), followed by an assessment of identified vulnerabilities (Spremic, M., 2018, p.). Conversely, the proliferation of technological innovations in today's digital economy often indirectly affects the cybersecurity of an organization. In terms of social engineering, innovative technology has facilitated the exploitation stage of social engineering attacks for hackers, as they are often able to obtain information, exploit it, and compromise the organization's system remotely without having to conduct an extensive research on their target.

According to Salahdine and Kabouch (2019), social engineering cyber-attacks typically have a common pattern that consists of the following stages: "(1) collect information about the target; (2) develop relationship with the target; (3) exploit the available information and execute the attack; and (4) exit with no traces" (p. 2). In literature, these four stages are also referred to as the research, hook, play, and exit phase, respectively (Breda et al., 2017, p. 2).

The most reliable sources for obtaining the most current information about an organization (i.e. upcoming events, organizational hierarchy, email, etc.) are the organization's websites and social media accounts. In some instances, attackers may also choose to target specific members of an organization, in which case employee social media may serve as an initial attack vector into the organization's system by providing the attackers with personal information necessary to answer private email security questions and potentially gain access to sensitive business material. Attackers may also take advantage of generally careless behavior displayed by members of an organization. Examples of such behavior include storing sensitive work files on a personal mobile device or computer, connecting to a public Wi-Fi, and writing down business passwords on post-it notes. Another method for acquiring information utilized by attackers is dumpster diving (i.e. searching through trash in hopes of coming upon sensitive information such as credit card and account numbers, passwords, and security codes).

From the hacker's point of view, the number of available attack vectors increased exponentially in the digitalized era. The scope of social engineering attacks has consequently significantly broadened over the past decade. When it comes to classifying such attacks, existing research offers a variety of approaches. From a broader perspective, social engineering attacks that require direct

contact between the hacker and the victim are classified as direct, whereas attacks that can be executed remotely are classified as indirect (Salahdine & Kabouch, 2019, p. 4). More specifically, since direct social engineering attacks require personalized interaction with a single target or a limited number of targets, they can also be classified as human-based attacks, while remote/indirect social engineering attacks with a wider reach can be classified as computer-based attacks (Salahdine & Kabouch, 2019, p. 3). Aldawood and Skinner (2020) take it a step further and classify each of the specific social engineering methods into its respective category, either human-based or technology-based (p. 3). However, it is important to note that certain social engineering methods such as spear phishing could be classified into either of these categories because they require personalized interaction with specific individuals through the use of technology. Salahdine and Kabouch (2019) classify these methods as 'social based' (p. 3).

The objective is to generate a novel taxonomy of social engineering attacks that can be utilized as a theoretical base for developing a psychological cybersecurity framework. The proposed taxonomy of social engineering attacks consists of three phases: the research phase, the exploitation phase, and the execution phase. Each phase contains subcategories identified from existing research and classified with the goal of creating a theoretical framework that would enable an objective breakdown of any real-life social engineering attack. Figure 1 represents an overview of the proposed taxonomy.

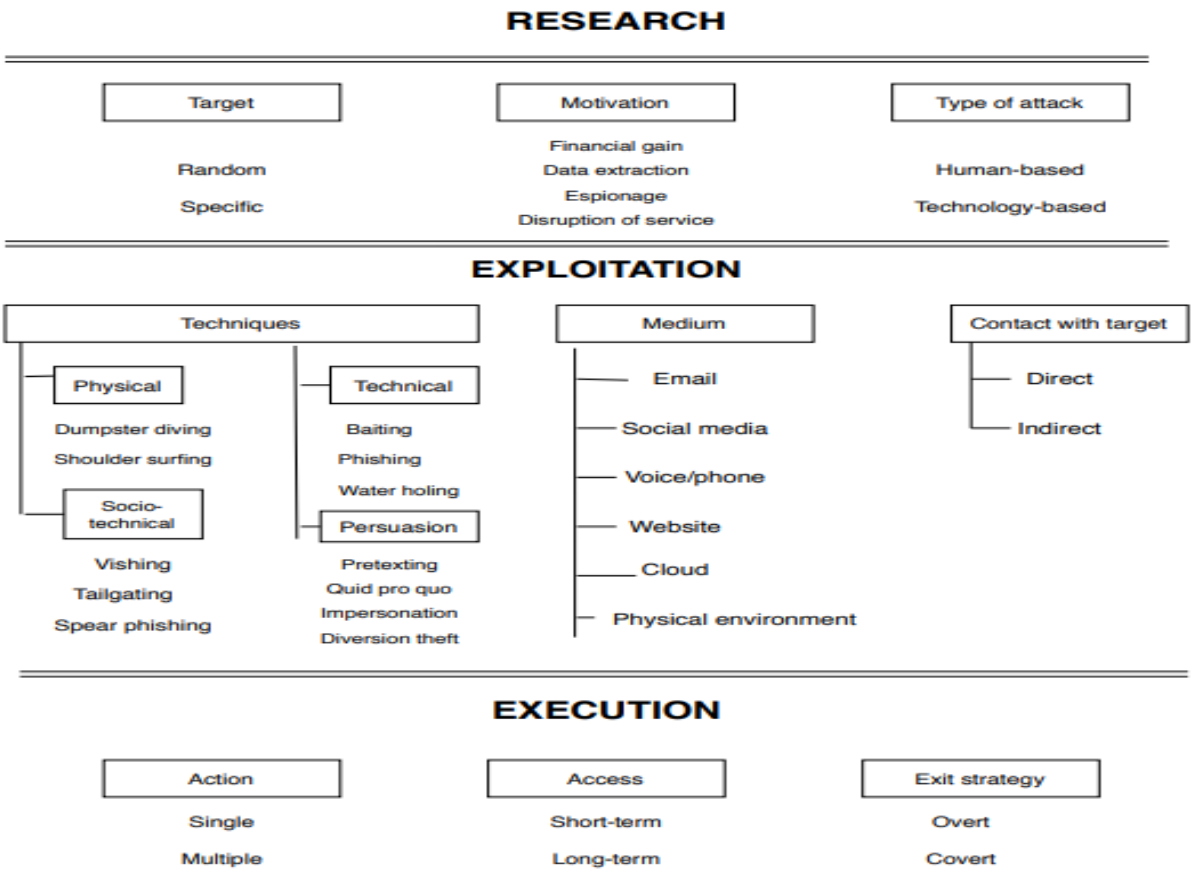

Figure 1 - Proposed Social Engineering Taxonomy

3.1 The Research Phase

In the taxonomy presented in figure 1, the research phase refers to the period during which attackers gather information about their targets. Subcategories in the research phase are classified from the perspective of the attacker.

Target

In terms of prospective targets, an attacker might choose to target a specific person and organization or decide to utilize social engineering techniques that target a broad spectrum of random victims. Target selection is likely to be influenced by the motivation behind the attack.

Motivation

Cyberattacks are often initiated for financial gain, to gain unauthorized access and extract sensitive and valuable information, or to cause a disruption of service.

Type of attack

Target selection and motivation behind the cyberattack determine whether every step of the cyberattack needs to be overseen by the attacker. Cyberattacks with a specific target typically

require human monitoring, whereas cyberattacks with random targets often call for the use of technological tools that allow many targets to be attacked simultaneously.

3.2 The Exploitation Phase

The exploitation phase refers to the period of a social engineering attack in which attackers exploit the vulnerabilities discovered during the research phase of the attack. Subcategories techniques, medium, and contact were classified as such in accordance with the factors identified as most common characteristics of a social engineering attack. The subcategory medium showcases the methods utilized by the hacker to initiate the social engineering attack. A social engineering attack can be initiated in the physical environment, over the phone, or electronically through a website, email, cloud service, or social media. It can therefore be inferred that, depending on the medium chosen for a social engineering attack, the third subcategory 'contact with the target' can either be direct or indirect. The classification of social engineering techniques will be explained in more detail in the following section.

3.2.1 Social engineering techniques

When conducting a social engineering attack, hackers utilize a variety of different techniques. As shown in Figure 1, social engineering techniques have been classified into physical, persuasion, technical, and socio-technical.

Physical social engineering techniques are types of techniques that require the hacker to perform some form of physical activity in the real world to secure an attack vector. Examples of physical techniques include dumpster diving and shoulder surfing.

Technical social engineering techniques rely primarily on technological tools to exploit vulnerabilities. Examples of such techniques are phishing, watering hole attacks, and baiting.

Persuasion techniques focus exclusively on exploiting the human factor in cybersecurity. More specifically, using a variety of psychological methods, hackers attempt to manipulate their target into inadvertently giving away sensitive information. Examples of persuasion techniques are pretexting, impersonation, quid pro quo, and diversion theft. In a diversion theft, attackers attempt to divert delivery packages to an address of their choosing. Quid pro quo refers to instances in which attackers impersonate technical support, contact multiple prospective targets, and claim to

be responding to a request for technical assistance until they reach someone who truly is expecting a callback.

Socio-technical techniques are those techniques in which both technical and persuasion elements need to be utilized by the attacker. Vishing, a form of phishing performed vocally, is an example of a socio-technical technique. In vishing, attackers often utilize caller ID spoofing and impersonate a reputable source (e.g. bank) to induce the target to reveal private information. Another example of a socio-technical technique is tailgating, during which the attacker physically follows a target into a secure area to gain access and extract the desired information. Spear phishing, a form of phishing that targets a specific target, is also classified into the socio-technical subcategory.

Phishing

According to Aldawood and Skinner (2020), "phishing is the practice of gathering personal or financial information by sending a message which looks like it is received from a trusted and legitimate source" (p. 5). A phishing email typically contains a malicious link which directs the victim to a fake website, designed to extract confidential information (Aldawood & Skinner, 2020, p. 5). It is currently estimated that more than 80% of organizations continue to experience phishing attacks (Thomas, 2018, p.1). The most dangerous characteristic of phishing is the fact that it often serves as an attack vector for greater cybercrimes, such as identity theft, malware attacks, and ransomware, which have the potential to cause damage in the excess of billions of dollars. Additionally, due to the technological advancements, the extent of the damage that could be caused by a phishing attack is becoming increasingly difficult to quantify. A cyber-attack classified as an advanced persistent threat (APT), for which phishing serves as an attack vector, is an example of one of the more prevalent cybersecurity threats today. In an APT cyber-attack, attackers gain access to a system or a network through an attack vector such as phishing, remain dormant within the system, and execute the attack at a time of their choosing to maximize the damage. The ability to retain unauthorized access to a system also often allows attackers to identify additional targets and spread the infection further (Thomas, 2018, p. 5).

Research also suggests that, over the past decade, the target range of phishing scams narrowed. While phishing in the past consisted of sending out mass emails without a specific target in mind, phishing emails have become more selective and their content more suited towards a specific target

(Bullee et al., 2017, p. 595). Social engineering methods that emerged from the shift in focus include spear phishing, whaling, and clone phishing. Whaling is a social engineering method in which high-profile members of an organizations are targeted through spear phishing in an attempt to manufacture a relationship and extract sensitive information from the victim, whereas clone phishing involves copying a legitimate email, equipping it with malicious attachments, and sending it to the victim under the guise of the original sender. According to the proposed social engineering taxonomy, whaling would be classified as a socio-technical engineering technique.

Spear Phishing

According to Thomas (2018), "spear phishing is a targeted form of phishing, typically an email attack that utilizes specialized social engineering methods to attempt to influence users to expose sensitive account, personal, and business information, or to enable intrusion into the computing infrastructure (p. 3). Human resource departments are common targets for spear phishing because of their access to sensitive employee data, such as W-2 forms and social security numbers (Thomas, 2018, p. 4).

During the research stage of their spear phishing attack, hackers gather information about the target in order to create a personalized message that would entice the target to believe the legitimacy of the email. Examples of personalized messages include impersonating the victim's superior and drafting a fake invitation for a cause the victim is passionate about. The assumption is that the target is more likely to find the message authentic if it comes from a seemingly reliable source, as opposed to the generic message sent in regular phishing attempts. A spear phishing study across 5 organizations in Sweden supported this assumption as results showed that employees who received a personalized spear phishing email were 5.3 times more likely to click the link in the email (Bullee et al, 2017, p. 596). Additionally, a survey with more than 19,000 respondents found that only 3% of respondents were able to successfully identify a phishing email (Thomas, 2018, p. 4).

Watering hole attack

A watering hole attack is a social engineering method often utilized as an attack vector for an APT attack. During the research stage of a watering hole attack, attackers select several websites frequently visited by members of an organization and compromise them with malware to create an opportunity to gain unauthorized access into the organization's system. Watering hole targets are much more likely to unknowingly infect their work devices with malware as they move through

the websites because they are used to visiting them on a daily basis. Once downloaded, the malware collects sensitive information and spreads through the organization's network, setting up an APT attack.

Watering hole attacks are increasingly difficult to detect due to the sheer number of online traffic an organization generates through the year. The fact that an organization was found to have visited more than 120,000 sites at least 10 times within a period of 8 months suggests that daily malware monitoring simply would not be feasible (Alrwais et al, 2016, p. 2). To avoid detection, attackers can strategically compromise any number of websites and utilize spoofing to retain the impression of legitimacy. Furthermore, the variety of ways in which a watering hole attack can be executed has resulted in the absence of real-world watering hole attack data, as only 29 cases were documented by 2017 (Alrwais et al, 2016, p. 2).

Baiting

Baiting is a social engineering attack that utilizes baiting techniques and offers designed to trick the target into falling victim to the attack. Baiting is commonly done through emails and ads, through which the target is promised a reward (e.g. free music, free phone) in return for sharing their personal information. Another example of baiting includes leaving an USB drive infected with malware in a public place or workplace, 'baiting' those who find it to insert the drive into their device and automatically infect it with malware. Studies have shown that "…the attack would be effective against most users and that the average person does not understand the danger of connecting an unknown peripheral to their computer" (Tischer et al, 2016, p. 1).

Pharming

Pharming is a technology-based social engineering attack that involves infecting the domain name system (DNS) server in order to direct any incoming traffic from a specific website towards a newly created fake website infected with malware (Alawood & Skinner, 2020, p. 6). In other words, anyone visiting the original website will automatically get redirected to the infected fraudulent site. The fact that the fraudulent website is indistinguishable from the original website makes pharming a particularly effective social engineering tool. According to the proposed social engineering taxonomy presented in figure 1, pharming would be classified as a technical social engineering technique.

Pretexting

In a pretexting attack, the attacker invents a fake scenario designed to manipulate the target into cooperating and revealing sensitive information. Targets can be contacted by email, in-person, or over the phone. Impersonating a bank representative and requesting credit card information due to an issue with a bank account is an example of a pretexting social engineering attack.

3.3 The Execution Phase

When it comes to the execution phase of social engineering attacks, the proposed taxonomy considers several factors. Namely, the motivation behind the cyberattack dictates whether one or multiple actions need to be taken for the attack to be successful. For instance, if the motivation behind the attack is data extraction, the act of utilizing technological tools to extract data needs to follow the action of securing an attack vector, and the cyberattack would be classified as a multi-step attack. Conversely, since it only requires an attack vector, a ransomware attack can be classified as a single-step attack. The proposed taxonomy also considers whether the cyberattack requires long-term or short-term access to the target's system. An example of cyberattacks that requires long term-access is an APT attack. The last factor considered in the taxonomy is the exit strategy of the cyberattack. For example, ransomware attacks necessitate an overt exit strategy, whereas repeated attacks such as APT attacks need to remain covert.

4. Cybersecurity Risk Factors and Mitigation

While the proposed social engineering taxonomy provides a useful theoretical framework for social engineering attacks, it does not offer a solution. According to Dreibelbis et al. (2018), "the exponential growth of the various types of threats that occur from multiple sources (e.g., malware, physical information loss, network threats) has resulted in an increased need to evaluate such dangers from perspectives beyond computers and security" (p. 348). To construct a viable risk mitigation framework, it is therefore important to address social engineering from an organizational perspective. From an organizational standpoint, with the increasingly connected workplace, where a greater portion of work necessitates relying on interface with the Internet, Dreibelbis et al. (2018) contend that "it is important to not only consider changes to the organization with the onboarding of more cybersecurity professionals, but also the changes necessary to ensure cybersecurity with all end-users" (p. 359). Dreibelbis et al. (2018) assert that this can be done with the help of industrial and organizational (I-O) psychologists, namely through job analysis and incorporating cybersecurity compliance tasks into job analyses for any roles that are connected and pose a cybersecurity risk (p. 359). The following table displays areas of cybersecurity that I-O psychologists can contribute to (Dreibelbis et al., 2018, p. 360):

	Practice in these areas	Practice should facilitate research in these areas
Job and work analysis	• Consider appropriate job analysis techniques to account for the changing nature of cyber jobs. • Incorporate cybersecurity policy and responsibilities into end user job requirements according to organizational policies.	• Expand and refine existing frameworks for cyber jobs. • Investigate the utility of strategic and cognitively oriented job analysis techniques for cyber related work roles.
Cyber selection	• Select for specific cyber skills, knowledge, motivation, and fit. • Understand the ethical motivations behind hackers and cyber professionals. during the hiring process. • Consider nontraditional sources for recruitment and selection.	• Investigate the antecedents, particularly personality and motivation, of cybersecurity performance for cyber professionals and end-users. • Model the effects of cybersecurity selection and training on individual- and organizational-level outcomes.
Cybersecurity obligations	• Increase awareness of the risks to electronically stored data. • Ensure that sensitive data is secured and compliant with EU data regulations.	• Develop methods of assessment and data analysis techniques that can minimize the necessity for personally identifiable data.
Counteracting IP loss	• Make sure Internet selection tests are properly proctored and secured. • Closely monitor web traffic and the Internet for signs of breaches or stolen material. • Ensure that there is response protocol, should intellectual property be stolen.	• Assess the damage that intellectual property theft can have on an organization's reputation. • Develop effective responses to breaches in terms of public response and outreach after a breach.
Insider threat	• Select for individuals who are less likely to pose a threat. • Develop training programs to reduce insider threats.	• Examine the potential antecedents for each malicious and nonmalicious insider threats.

	Practice in these areas	Practice should facilitate research in these areas
Growing a cybersecurity culture	• Consider methods for identifying individuals who need targeted cybersecurity training. • Work toward integrating the acceptance of cyber safe behaviors in the workplace at all management levels. • Build an internal security climate/culture.	• Determine the utility of different selection tools. and/or interventions for reducing insider threat. • Further explore the antecedents and consequences of organizational cyber culture. • Develop psychometrically sound measures for assessing cyber culture, exploring possible facets of cyber culture.
Organizational adaptation	• Create organizational policies, norms, and standards for employee responses to cybersecurity threats and breaches. • Build and select for agile cyber teams.	• Investigate the factors that promote and inhibit successful cyber team performance. • Explore the relationship between cyber selection, training, and culture on organizational level outcomes, such as organizational adaptiveness to cyber threat.

Figure 2 - Areas of Contributions for I/O Psychologists

While these potential contributions of I-O psychologists appear to be useful, to be able to effectively contribute to any of these areas, it is important to take a more detailed look at one of the most prominent risk factors in cybersecurity; the human factor.

4.1 Human factor in cybersecurity

Current research identifies human factors as the weakest link in cybersecurity. Even the most sophisticated cyberattacks are often made possible by human vulnerabilities (Corradini & Nardelli, 2019, p. 193) and most cybersecurity experts concur that the greatest challenge to effective security is not the strength of a technical solution, but the weakness in human behavior which often compromises technical safeguards that were put in place (Patterson, Winston & Fleming, 2016, p. 254). Various types of employee behavior may put the organization at risk. Examples include leaving the workstation unattended, writing logon credentials on post-it notes, storing sensitive

documents in unsecured areas or on personal devices, disclosing internal information on publicly accessible mediums such as social media, and accessing work material on open wireless networks. Email links and attachments, web-based download, and application vulnerability have been identified as the top three threat vectors for compromising security credentials (Nobles, 2018, p. 73).

Hadlington (2017) proposes an interesting analogy for human-enabled cybersecurity risk in organizations by equating it to seat belts in automobiles (p. 14). Namely, the idea is that seat belts give drivers a false sense of security and indirectly cause them to take more risk on the road. Similarly, many organizations implement technological countermeasures against security breaches, thereby giving employees a false sense of protection in the workplace and making them more inclined to "take more risks, circumvent accepted protocols, and engage in poorer information security behaviors (Hadlington, 2017, p. 14). The seat belt analogy aligns with existing research, which suggest that the majority of such breaches occur due to human lack of awareness and accidental oversight. Conversely, research (Crossler et al., 2013) also shows that, when surveyed, most individuals tend to express concern about cybersecurity (as cited in Shappie et al, 2019, p. 1). According to Shappie et al. (2019), it can be assumed that most individuals have every intention of complying with cybersecurity policies, which makes it "counterintuitive how people simultaneously engage in actions that violate policies and put their own and other people's sensitive data at risk" (p. 1).

In general, most human-enabled cybersecurity vulnerabilities can be ascribed to poor safeguarding measures against potential attacks. From an organizational perspective, examples of poor information safeguarding include failure to withdraw IT clearances from former employees, lack of official procedure for granting authorization to IT systems and failure to segment access to systems according to employee job description. The 2015 IBM Cyber Security Intelligence Index revealed that 9 out of 10 information security incidents that year were caused by a form of human error (Glaspie & Karwowski, 2017, p. 269). Furthermore, PWC's Information Security Breaches Survey determined that unintentional human error caused 50% of the worst security breaches in 2015 (Evans et al., 2016, p. 4668). The following year, human-enabled errors accounted for 80-90% of security breaches in the United States and the United Kingdom (Nobles, 2018, p. 74) and

three out of the top five cybersecurity threats (ENISA, 2017, p. 29). These statistics show that an effective approach to cybersecurity cannot overlook the importance of the human factor.

The importance of the human factor is compounded by the fact that employees often place their organization at risk and effectively negate any technological countermeasures that the organization put in place by behaving in a careless matter and not following security protocols (Hadlington, 2017, p. 2). Research also suggests that most organizations are aware of security concerns and implement available technological tools to eliminate security threats yet continue to overlook the human factor. Nobles (2018) contends that "even with the influx of technological capabilities coupled with operational, administrative, and technical countermeasures; there is a continuity of failure to address human factors concerns in information security" (p. 74). The Health Information Trust Alliance (2014) also states that 'cybersecurity does not address non-malicious human threat actors, such as a well-meaning but misguided employee' (Evans et al., 2016, p. 4667). Compared to the investment in cybersecurity tools and systems, organizational investment in human factors of cybersecurity appears trivial (Glaspie & Karwowski, 2017, p. 269).

Literature proposes several theories as to why the human factor has been continuously ignored. Namely, a lack of sufficient knowledge about the human factor in cybersecurity, combined with organizational oversight of threat warnings and countermeasures, can be summarized as a lack of self-preservation instinct (Wisniewska et al, 2020, p. 40). When buying expensive cybersecurity software, organizations often "…fail to notice the terrifying reality that it is not attacks from the outside, but those from the inside that pose the most serious threat" (Wisniewska et al., 2020, p. 40). More specifically, although authorized network users pose a more probable and more dangerous threat to organizational cybersecurity, large organizations hold on to the belief that they are more susceptible to outside threats and consequently place too much emphasis on sophisticated security tools while neglecting liabilities from within (Wisniewska et al, 2020, p. 39). Technological determinism is another theory cited in current literature that could help explain why the human factor remains an issue in cybersecurity. According to Nobles (2015), technological determinism is a theory based on constant integration of new technologies with the goal of simplifying processes and improving the quality of work without any concern for societal, cultural, and organizational implications of such an integration (Nobles, 2018, p. 79).

In terms of cybersecurity, Nobles (2018) claims that the unbalanced focus on automated technology has had an unwanted side-effect of minimizing the role of cybersecurity professionals (Nobles, 2018). This notion was affirmed in 2015 when the U.S. National Security Agency characterized the absence of human factor experts to assess human performance and behavior in real situations as “an egregious oversight in cybersecurity” (Nobles, 2018, p. 75). According to Cobb (2016) it can be argued that the shortage of trained cybersecurity professionals compels organizations to invest further in automated cybersecurity technologies (Nobles, 2018, p. 79), thereby creating a disconcerting paradox in which organizational over-investment in technology creates the shortage of cybersecurity experts and the shortage subsequently causes even more over-investment in technology.

The fact that the human factor continues to be underemphasized illustrates the clear gap between the findings of theoretical research and organizational procedures that are in place in most organizations (National Science and Technology Council, 2016). To date, the implementation of cybersecurity tools has not been able to diminish the negative impacts of the human factor in cybersecurity, as “ignoring human factors in the development and deployment of cybersecurity policies and processes predestines these activities to failure” (ENISA, 2017, p. 30). It can therefore be inferred that a change in organizational approach is necessary to successfully safeguard against human-enabled errors. To do so, the impact of organizational culture on organizational cybersecurity needs to be analyzed.

4.2 Impact of organizational culture on cybersecurity

In the field of cybersecurity, the importance of organizational culture has been identified in research. According to Glaspie and Karwowski, “prevalent research highlights that a positive information security culture can increase security policy compliance, strengthen the overall information security posture, and reduce the financial loss due to security breaches” (Glaspie & Karwowski, 2017, p. 270). Hadlington (2017 adds that “human factors initiatives can be solidified through organizational culture by implementing practices and processes to increase awareness of human performance and decision-making” (Nobles, 2018, p. 76). Furthermore, a survey regarding risk perception in a multinational company from the financial sector highlighted the need for a strong organizational risk culture (Corradini & Nardelli, 2019, p. 193).

In the context of cybersecurity, culture can be a significant factor in predicting attitude to privacy and affect decision making relative to cybersecurity risks (Corradini, 2020, p. 64). Organizational culture is typically defined by academics (Denison, 1990; Schein, 1992; Cameron & Quinn, 1999) as "a set of shared values, beliefs, assumptions and practices that shape and direct members attitude and behavior in the organizations" (as cited by Lim et al, 2009, p. 88). According to De Long & Fahey (2000), culture can be observed on multiple levels in an organization (p. 115). Namely, in an organization, a culture consists of (De Long & Fahey, 2000):

- Values defined as implicit preferences about what the organization strives to accomplish and how it goes about accomplishing it. For example, if an organization places value on quality of service, members of the organization are much more likely to do everything in their power to ensure customer satisfaction.
- Norms, which are products of values and are generally more explicit. For instance, in an organization that values quality of service, employee advancement might be contingent upon good customer service ratings.
- And practices, shaped by norms and defined as "any widely understood set of repetitive behaviors" (p. 115). Examples include monthly staff meetings, weekly reports, and other procedural activities performed on a regular basis.

While each of these levels influence employee behaviour in their own respective way, they all need to be appropriately aligned for employees to behave in accordance with organizational values (Connolly, Lang, & Tygar, 2014, p. 427). In terms of cybersecurity, research suggests that employee behaviour does not always reflect organizational values. A recent study surveyed information security officers from seven U.S. based organizations and revealed that, despite the fact that most organizations listed information security as one of their core values, information security rules were being circumvented by some of the employees (Connolly et al, 2014). Connolly et al (2014) identified conflicting values, practices (e.g. lack of education) and norms (e.g. casual information safeguarding, lack of security policy) as catalysts for such behaviour (p. 427). Similarly, Hedström et al. (2011) argue that non-compliance with information security policies "may be a result of competing values between policies and the values that employees emphasize in conducting work" (Reegard & Blackett, 2019, p. 4038). More specifically, employee non-compliance may be due to (Connolly et al, 2014, p. 428):

- A conflict between values, norms, and practices.
- Conflicting organizational values in the form of encouraging employees to take risks while simultaneously emphasizing procedural adherence. Values promoted by upper management may differ from the values of lower management, thereby indirectly stifling innovation.
- Conflicting individual and organizational values. Individuals may have conflicting values due to age, gender, and educational background.

When practices and norms are aligned and everyone is adhering to organizational values, the organizations are set up to thrive (Corradini, 2020, p. 65). It is therefore valuable to try to identify the factors that foster conflicting values, norms, and practices. Veiga and Martins (2017) contend that, in most organizations, an organizational culture consists of a dominant culture and subcultures (p. 73). De Long and Fahey (2000) define subcultures as "distinct sets of values, norms, and practices exhibited by specific groups or units in an organization" (p. 117). In an organizational subculture, employees have different values compared to the dominant culture and these values can be influenced by the work environment, job description, geographical location, and their respective backgrounds (Veiga & Martins, 2017, p. 73). In the context of cybersecurity, several cybersecurity subcultures could be present in an organization, each differing from the dominant cybersecurity culture. For instance, employees in the human resource department are required to place much more value on information security compared to sales representatives, who would likely prioritize their sales numbers. Furthermore, if subcultures exist in an organization, instilling appropriate values throughout the organizational hierarchy would be difficult even if cybersecurity already is one of top management's core values.

In cybersecurity, besides the 3 factors identified in De Long and Fahey's culture framework (2000), some research adds a fourth factor of knowledge and argues that knowledge influences assumptions, values, and behaviors (ENISA 2017; Van Niekerk & von Solms, 2010, as cited in Reegard & Blackett, 2019, p. 4038). From a cybersecurity perspective, it would be erroneous to disregard the importance of knowledge in organizational cybersecurity. As previously stated, the advance of cybertechnology and the significant threat of the human factor continue to pose significant threats for organizations. As a result, cybersecurity requirements continue to evolve, thereby mandating cybersecurity knowledge to be regularly updated. This paper will therefore

regard knowledge as a fourth factor of culture in cybersecurity. While knowledge does influence assumptions, values, and behaviors, this influence can often be hindered by the effect culture has on the perception of knowledge. According to De Long and Fahey (2000), cultures and subcultures "heavily influence what is perceived as useful, important, or valid knowledge in an organization (p. 116). Put differently, culture shapes what type of knowledge will be perceived as relevant and dictates what type of knowledge will be focused on (De Long & Fahey, 2000, p. 116). This is particularly relevant for the field of cybersecurity and social engineering, as most research identifies lack of awareness, disinterest, and carelessness as common factors in human-enabled security breaches. It is therefore necessary to identify cultural deficiencies before cybersecurity protocols are fully adhered to and cybersecurity experts can make any meaningful contributions to organizational cybersecurity. A healthy attitude towards knowledge appears to be a crucial factor for implementing a viable cybersecurity culture.

Figure 2 proposes a framework for (sub)cultures in cybersecurity derived from existing research.

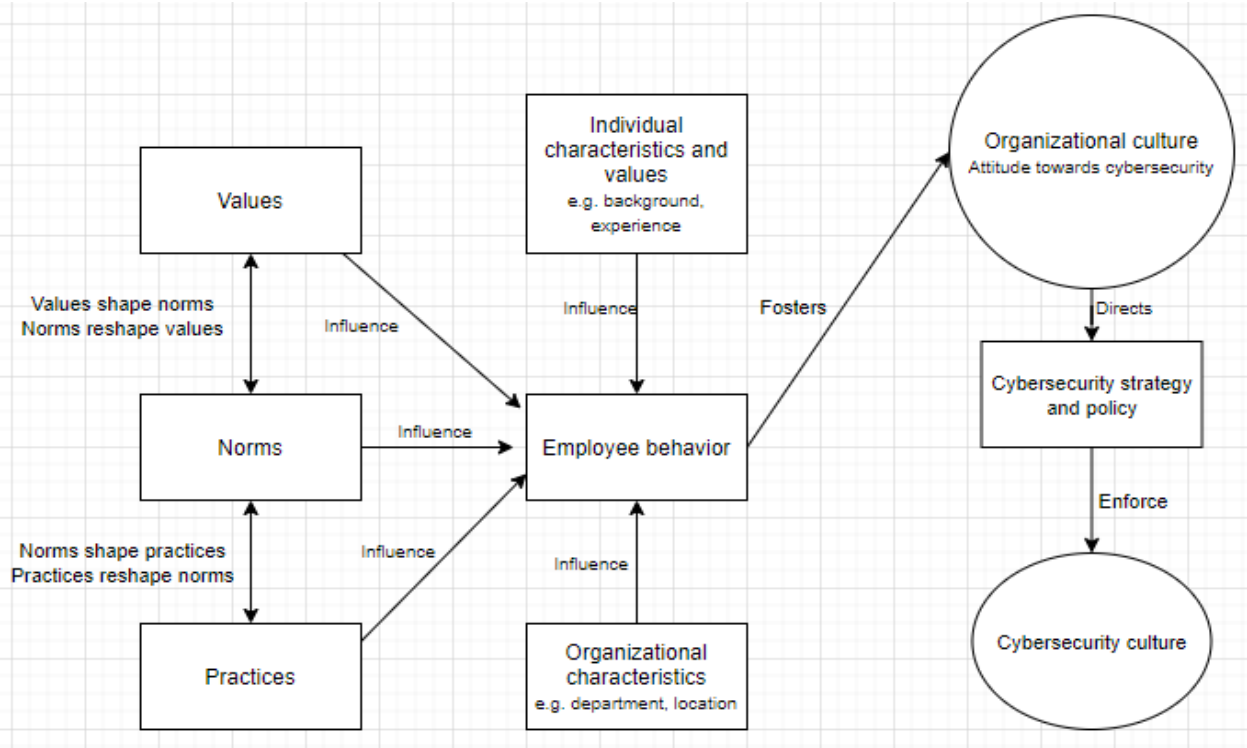

Figure 3 - Proposed Organizational Culture Taxonomy

From an organizational standpoint, it does not seem feasible to mitigate risky human behavior by focusing on distinct traits and psychological characteristics of each individual employee. As shown

in figure 2, other than individual characteristics and values, organizational values, practices, and norms also influence employee behavior. Therefore, a more effective approach for human risk mitigation for organizations would be working towards fostering a healthy organizational cybersecurity culture (Corradini & Nardelli, 2019), as the development of a cybersecurity culture plays an important role in managing risk of the human factor, while enabling the adoption and utilization of new technologies by organizations (ENISA, 2017, p. 30). According to Corradini (2020), to foster an effective cybersecurity culture, it is essential to develop appropriate cybersecurity awareness programs (p. 101).

4.3 Cybersecurity Awareness

Security awareness is defined as essential security education of employees that can be immediately and practically applied to the workplace and beyond (Yildrim, 2016, p. 213). Yildrim (2016) asserts that essential security education entails "an awareness of possible risk, danger, or real threats to life, safety, or valued assets that will be translated into action or behaviors that address those risks and threats" (p. 213). In the field of cybersecurity, the need for increased cybersecurity awareness among individuals has been identified throughout existing research. Namely, a recent study by Corradini and Nardelli (2020), involving 212 employees from two organizations, showed that those employees who had already participated in cybersecurity awareness training sessions had a better comprehension of potential cybersecurity threats related to digital technology. Considering the results of the study, the authors classify the lack of security awareness as a vulnerability for every organization because it facilitates social engineering attacks (Corradini & Nardelli, 2020, p. 64). Another survey among employees in the United Kingdom revealed that 98% of those questioned delegated responsibility for organizational cybersecurity to management, while 58% possessed knowledge necessary to protect the organization from cybercrime (Hadlington, 2017, p. 12). Hadlington (2017) contends that individuals who are dismissive or lack necessary knowledge of cybersecurity threats are more likely to engage in risky behavior and consequently identifies instilling good security-based behavior "as being of paramount importance for all organizations, irrespective of their size and complexity" (p. 12).

It is important to note that the act of informing people of potential cybersecurity risks needs to be regarded as merely the first step in the awareness building process, as cybersecurity awareness programs need to focus on awareness, training, and education as three key areas necessary for

positively affecting employee behavior (Corradini, 2020, p. 103). The following figure provides definitions for each of the key areas (Corradini, 2020, p. 103):

Awareness	Training	Education
Having knowledge of a certain situation and behaving consequently. Awareness is not just having information, but developing sensitivity to important issues in an area and act accordingly	An active and a more or less formal process to teach specific skills, i.e. the "know how" knowledge allowing people to solve operational problems in a known context	The process of providing integrated knowledge and skills within a theoretical framework, which allows learners to use them to face future or unknown situations

Figure 4 - Key Areas that Affect Employee Behavior

In the context of organizational culture, for a cybersecurity awareness program to have a positive effect, the value of cybersecurity needs to be shared throughout the organizational hierarchy. Designing a good awareness program should reflect human psychology, cognitive abilities, social attitudes, and modern work environments (ENISA, 2017, p. 38). Top management ought to know and understand which element of organizational culture influences employee motivation and behavior (Yusof et al., 2016, p. 53) and implement effective programs designed to afford employees autonomy and ownership, and align individual security goals with organizational values (ENISA, 2017, p. 39). Put differently, employee motivation to actively participate in cybersecurity training and education is most effectively influenced through a cultural change on the organizational level that would allow them to actively contribute to the development of cybersecurity policies. It can therefore be concluded that cybersecurity awareness tools, while beneficial, are best utilized as supplements to a comprehensive cybersecurity culture framework.

5. Existing Culture Frameworks

Several culture frameworks can be identified in existing literature and will be presented in the following section.

5.1 ENISA Framework

The European Union Agency for Network and Information Security suggests a theoretical framework for establishing and fostering a cybersecurity culture. According to ENISA (2017), a successful strategy should reinforce strong governance attitudes and actions, be aligned with other business functions to ease acceptance, be built around an adaptable framework to facilitate long-term use, and be measurable to demonstrate success (p. 31). The following step-by-step guide, based on existing literature, is proposed (ENISA, 2018, p. 40):

1. **Top management commitment** – the first step in implementing any form of cultural change entails upper management commitment. Namely, upper management identifies the need for a cultural change in terms of security, sets the new direction of security culture, and reinforces the change through security policies.
2. **Define problem in business context** – to accurately assess the current state of the organization in terms of employee attitude and behavior, upper management needs to:
    a. Assess the current state by examining existing (1) values, policies, and procedures, (2) practices, (3) assumptions and beliefs, and (4) knowledge
    b. Define the ideal state of the organization along the same 4 lines with a specific and measurable goal in mind.
    c. Clearly define the specific steps needed to move from the current state to the ideal state. A security policy can be used to shape future goals, processes, and employee education.
3. **Educate the employees** – an educational program should be designed to ensure that the employees are aware of the need to change the existing security culture and adequately educated on their expected behavior to foster this change
4. **Define culture change metrics** – metrics should be used to measure the development of CSC and offer continuous feedback to employees and management.
5. **Feedback, rewards, and punishments** – Continuous feedback, based on performance metrics, should be offered to employees by management.

6. **Review and refinement** – the initially set goals may require revising if they are impossible to achieve or unacceptable to employees. In some cases, the final culture being strived for can be strengthened through renegotiation.

5.2 Organizational Cybersecurity Culture Model

Huang and Pearlson (2019) propose an organizational cybersecurity culture framework that managers can utilize to build a culture of cybersecurity and evaluate if their current culture drives cyber secure behaviors (p. 6406). The framework identifies two types of employee behavior that play a role in creating or reducing cybersecurity vulnerabilities: (p. 6400)

- In-role cybersecurity behaviors, which encompass actions and activities employees take as required by the nature of their job
- Extra-role cybersecurity behaviors, which refer to activities of employees that are not part of their job description (e.g. stating their opinion about cybersecurity)

The proposed framework also acknowledges three organizational levels of cybersecurity culture (Huang & Pearlson, 2019, p. 6400):

- Leadership level – assessed through three constructs:
    - Top management's priorities, which assesses whether management prioritizes cybersecurity-related activities
    - Top management's participation, which refers to the extent of the management's direct involvement in cybersecurity-related activities
    - Top management's knowledge, which refers to the extent of the cybersecurity knowledge and experience leaders possess
- Group level, summarized by three constructs:
    - Community norms and beliefs about cybersecurity
    - Teamwork perception, which refers to the ways in which teams within the organization work together to be more secure
    - Inter-department collaboration, which refers to the extent of the collaboration between different departments of the organization
- Individual level, involving three constructs:

- Employee's self-efficacy – the level of the individual's awareness of their ability to execute cybersecurity-related activities
- Cybersecurity awareness – the individual's knowledge of what cybersecurity behaviors are encouraged by the organization
- General cyber threat awareness – the individual's comprehension of potential cybersecurity threats and vulnerabilities

According to the framework, employee behavior is influenced by beliefs, values, and attitudes on all three organizational levels which are influenced by organizational mechanisms or methods leaders use to influence the cybersecurity culture. These methods include cybersecurity culture leadership (i.e. appointing an individual or team to build a cybersecurity culture), performance evaluations, rewards and punishments, cybersecurity training, and communication (p. 6402). Beliefs, values, and attitudes are also influenced by external influences such as the type of culture of the society in which the organization is located, external rules and regulations, and peer institutions (p. 6403). The full comprehensive framework can be seen in Figure 3 (Huang & Pearlson, 2019, p. 6404).

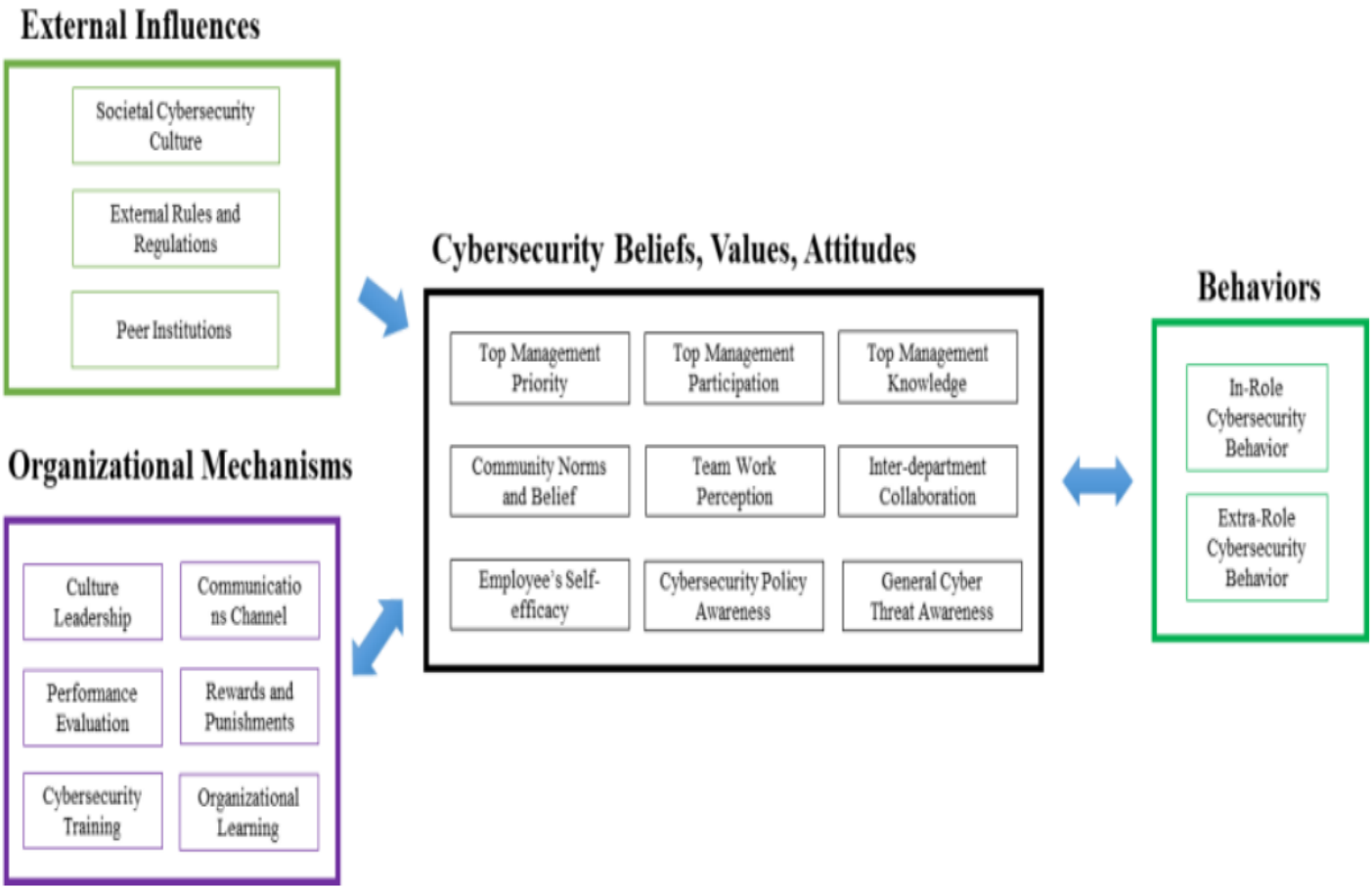

Figure 5 - Organizational Cybersecurity Culture Model

5.3 NIST Framework for Improving Critical Infrastructure in Cybersecurity

The existing NIST Framework for Improving Critical Infrastructure in Cybersecurity was published on April 14th, 2018 (NIST, 2018). Despite its name, there are a variety of uses for the NIST framework, as the decision about its implementation is left to the implementing organization. While the framework is primarily designed for improving infrastructure, its theoretical constitution is applicable to existing cybersecurity culture frameworks as a complement for risk management processes and cybersecurity programs. The framework can be utilized to help develop, foster, and communicate an understanding of cybersecurity risk management, aligned with industry practices, throughout the organizational hierarchy. The framework consists of three parts:

1. Framework Core – the Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes throughout the organizational hierarchy, and is comprised of five concurrent and continuous functions:

   a. Identify – asset management, business environment; governance; risk assessment; and risk management strategy,
   b. Protect – develop and implement appropriate safeguards through identity management and access control, awareness and training, data security, information protection processes and procedures, maintenance, and protective technology,
   c. Detect – timely discovery of cybersecurity anomalies and events through security continuous monitoring and detection processes,
   d. Respond – Develop and implement appropriate activities when a cybersecurity incident is detected. Activities include response planning, communications, analysis, mitigation, and improvements,
   e. Recover – recovery planning, improvements, and communications.
2. Framework Implementation Tiers – meant to support organizational decision making about how to manage cybersecurity risk. Organizations are able to determine the desired tier based on identified organizational cybersecurity needs. The following 4 tiers (described from lowest to highest) provide context on how an organization views and manages cybersecurity risk:
   a. Tier 1 (partial) – organizations partially manage cybersecurity risk in an ad hoc and sometimes reactive manner,
   b. Tier 2 (risk informed) – limited awareness of cybersecurity risk on an organizational level,
   c. Tier 3 (repeatable) – risk management practices are approved by management and expressed as an organizational policy,
   d. Tier 4 (adaptive) – cybersecurity practices are adapted based on previous and current cybersecurity activities.
3. Framework Profile – can be used to determine both the current (Current Profile) and the desired state of cybersecurity in an organization (Target Profile). The target profile indicates the outcomes necessary for successfully attaining the desired state of cybersecurity risk management in an organization.

The framework also describes the common flow of information throughout the organizational hierarchy, as seen in Figure 4. Namely, the executive level of the organization identifies and communicates priorities, available resources, and overall risk tolerance to the mid-level of the

organization (i.e. the business/process level) which uses the information as input into the risk management process and works with the implementation/operations level of the organization on developing and implementing the Target Profile. Subsequently, the implementation/operations level updates the business/process level on the progress of the target profile, while the business/process level reports to management on the current state of the risk management process and the level of awareness throughout the organization.

Figure 6 - NIST Framework Information Flow

Steps for establishing or improving a cybersecurity program are also included in the framework:

1. Determine priorities and scope of the program,
2. Identify current assets, regulatory requirements, and existing vulnerabilities,
3. Create a Current Profile,
4. Conduct a risk assessment,
5. Create a Target Profile,
6. Determine, analyze, and prioritize gaps between current and target profile,
7. Implement action plan.

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.04162018

Figure 7 - NIST Framework

6. Proposed Culture Framework

In the following section, elements from existing frameworks and research will be combined to create a cybersecurity culture framework designed to minimize the threat of social engineering and mitigate the vulnerabilities caused by the human factor. The organizational culture taxonomy proposed in Figure 2 serves as a theoretical basis for determining aspects of the proposed framework and is supplemented by elements from each of the frameworks described in the previous section. The following steps illustrate the methods for establishing or improving a cybersecurity culture that comprise the framework:

1. **Conduct information classification and identify priority level**

   While mitigating the threat of the human factor should be a priority for any organization, the scarcity of resources often necessitates prioritization of cybersecurity methods. As a first step in identifying its priorities, it is important for an organization to assess the data it holds and the level of protection it should be given. Information classification is an important factor in cybersecurity because it gives organizations an idea of the type of information they hold and how attractive that information may be to potential attackers, thereby facilitating decision-making when it comes to extent of organizational resource allocation towards cybersecurity. Information can be classified on three levels, as shown in Table 1. As digital transformation becomes increasingly prominent worldwide, the amount of moderate and high impact information organizations possess continues to increase. Large organizations in the public, service, and retail sector are likely to hold a significant amount of high impact information that can be targeted through social engineering attacks and should consequently view the mitigation of the human threat as a high priority. In other words, depending on the structure of the organization (i.e. if it is digitally transformed), its resources, and the type of information it holds, the level of priority given to this aspect of cybersecurity will vary. Prioritization is not required in instances in which a human-enabled cybersecurity attack already occurred, thereby highlighting the inadequacy of the current cybersecurity culture.

Low Impact Information	Moderate Impact Information	High Impact Information
The unauthorized disclosure of this information could have a ***limited*** adverse effect on the organization and its clients. Low impact information includes public information that can be openly accessed, shared, and discussed, as well as internal information such as employee handbooks, memos, and general policies.	The unauthorized disclosure of this information could have a ***significant*** adverse effect on the organization and its clients. Moderate impact information includes confidential information such as business strategies, upcoming projects, and resource allocation.	The unauthorized disclosure of this information could have a ***catastrophic*** adverse effect on the organization and its clients. Examples include highly sensitive information such as trade secrets and personally identifiable information (e.g. social security numbers, mailing or email addresses, credit card information).

Table 1 - Information classification

2. **Top management commitment**

   In accordance the ENISA framework (2017), a crucial step in implementing any form of cultural change entails upper management commitment. After cybersecurity becomes a top management priority, leaders are encouraged to have increased cybersecurity knowledge to better understand what type of behavior and technological liabilities (e.g. out of date software) leave attack vectors for hackers. If top management possesses substandard cybersecurity knowledge, creating new leadership positions for cybersecurity culture to be filled by cybersecurity professionals is a viable option. Additionally, to reinforce the importance of cybersecurity throughout the organization, employees need to be made aware of how important cybersecurity is to upper management. This can be done through memos, videos, blog posts, and weekly cybersecurity updates. By placing high value on cybersecurity, top management is more likely to have subsequent cybersecurity measures more readily accepted throughout the organization.

3. **Assess the current state of the organization**

   To identify existing cybersecurity liabilities, upper management needs to assess several factors. Namely, since the effectiveness of cybersecurity strategy and policies depends on the existing overall attitude towards cybersecurity within the organization (Figure 2) which is indirectly influenced by existing values, norms, practices, and individual characteristics of employees. upper management should:

a) ***Examine existing organizational values, norms, and practices,***

Organizational values, norms, and practices can be inferred by conducting interviews with employees individually, or as members of their respective departments. Values are often difficult to effectively measure, but gauging employee perception of current organizational values typically provides the most valuable insight.

b) ***Examine employee behavior and attitude towards cybersecurity***

Observing employee behavior on a long-term basis provides valuable insight into cybersecurity attitudes withing the organization. Certain cybersecurity software tools can be used to collect data on the number of successful and prevented attacks on the organization's network, as well as the time it took to identify them (ENISA, 2017, p. 41). In addition, fake phishing attacks and their effectiveness showcase the extent of the cybersecurity liability that stems from the human factor.

c) ***Examine employee cybersecurity knowledge and awareness***

Once upper management has a better understanding of employee behavior, motivating factors behind the behavior should be identified. Questionnaires and in-person interviews should be conducted to determine whether substandard behavior exhibited by employees occurs due to negligence or subpar knowledge and lack of cybersecurity awareness.

To account for the possibility of subcultures existing within the organization, these factors should be examined on both the group and individual levels, as classified by Huang and Pearlman (2019).

4. **Mitigate identified vulnerabilities by modifying contributing factors**

Keeping in mind the organizational culture taxonomy (Figure 2), members of the organization should collectively work on modifying the factors that foster the existing cybersecurity culture. This can be done by:

a) ***Implementing incentives to promote cybersecurity culture and behavior***. Cybersecurity education should be a priority for all members of the organization and the employees that exhibit substandard cybersecurity behavior should be subjected to additional, more extensive cybersecurity training and awareness

programs. Individual performance evaluations are another useful tool to incentivize employee behavior. Employees should be made aware that their cybersecurity efforts will be reflected in their performance evaluations. Instances of substandard cybersecurity behavior and concerted efforts to create a stronger cybersecurity culture are examples of activities that would negatively and positively affect employee performance evaluations, respectively.

b) ***Developing cybersecurity training and awareness programs***. Awareness can be increased by creating an organizational cybersecurity policy designed to clarify the intention of upper management and illustrate the cybersecurity changes the organization hopes to achieve. Cybersecurity training and awareness programs should be administered on a regular basis, as people change their behavior when they are supported by a continuous cycle of training and information activities (Corradini, 2020, p. 131). As previously mentioned, cybersecurity training has a better chance of having a lasting and positive effect on an organization once the value of cybersecurity is shared throughout the organizational hierarchy.

c) ***Modifying organizational norms and practices***. As previously mentioned, cybersecurity training has a better chance of having a lasting and positive effect on an organization once the value of cybersecurity is shared throughout the organizational hierarchy. Organizational norms and practices should be modified to appropriately reflect the value of cybersecurity. Examples include mandating employees to clear desks of any confidential documents at the end of the day, log-off their desktops when not in their office and follow reporting procedure for suspicious cyber activities (ENISA, 2017, p. 22).

5. **Monitor progress through predetermined metrics**

It is important for organizations to be able to evaluate the effectiveness of each implemented cybersecurity measure over time, as self-assessment and measurement improves decision making about investment priorities (NIST, 2018, p. 20). According to the NIST framework, to examine the effectiveness of each implemented measure, “an organization must first have a clear understanding of its organizational objectives, the relationship between those objectives and supportive cybersecurity outcomes, and how those discrete cybersecurity outcomes are

implemented and managed" (p. 20). The preceding steps in the proposed framework, along with the proposed organizational culture taxonomy (figure 2), allow the organization to have a clear understanding of the relationship between all the elements that comprise an organizational cybersecurity culture.

In the digital era in which the human workforce has become a prime vector and target of cyberattacks, understanding the cybersecurity knowledge and the capabilities of employees is key to developing a more effective and skilled workforce (Daniel Ani et al., 2016, p. 180). An effective metric for evaluating the impact of implemented measures on employee attitude toward cybersecurity and, by extension, organizational cybersecurity culture are attitude scales. According to Hadlington (2017), given the capacity for attitudes to change over time, attitude scales provide a "good metric to examine if interventions have served to alter knowledge and perceptions" (p. 12). A positive change in employee attitude towards cybersecurity over time can be viewed as an indicator that the implemented measures for improving cybersecurity culture likely have a positive effect on employees.

However, when it comes to evaluating the effectiveness of implemented measures in terms of cybersecurity risk, it is important to separate what employees have learned attending cybersecurity training and awareness programs and what knowledge they actually transfer into their workplace behavior (Corradini, 2020, p. 132). A healthy attitude towards cybersecurity is of little worth for an organization's cybersecurity if employees do not behave in a safe manner. It is therefore vital to effectively evaluate the impact of implemented measures on employee behavior. Table 2 offers a checklist for predetermined metrics for mitigating social engineering risk on an organizational level.

METRIC
Specialized cybersecurity training experts with extensive knowledge of preventive measures for mitigating vulnerabilities caused by a lack of cybersecurity awareness have been hired
Training coordinators and instructors stay updated and regularly attend the latest cybersecurity conferences to ensure up-to-date training

Employees have been tested to determine current vulnerabilities *Employee susceptibility to social engineering attacks can be measured through assessment tests and fake phishing attacks.*
Cybersecurity training sessions have been designed to prioritize helping high-risk individuals *Employees lacking knowledge and exhibiting high-risk behavior should attend extended cybersecurity training sessions. Since low-risk individuals attend shorter cybersecurity training sessions, the ability to allocate its scarce resources to high-risk individuals creates a budgetary benefit for an organization.*
Cybersecurity training and awareness programs have been appropriately developed *It is necessary to determine who will oversee educating employees on cybersecurity and the way the education will be conducted.*
Cybersecurity training and awareness programs are effective and up to date *Cybersecurity programs are aligned with industry standards and satisfy all legal requirements.*
Cybersecurity awareness programs have been adjusted based on organizational hierarchy *Employee social engineering education should be adjusted based on the nature of respective occupations.*
Role-specific interventions for identified weak points have been designed at each level of organizational hierarchy *Identified vulnerabilities are addressed based on the employee's position within the organizational hierarchy and interventions are adjusted to best accommodate the nature of their occupation.*
Threat response policy has been established along with the individuals responsible for overseeing it *Employees have been informed on who handles what aspect of threat response and mitigation.*
Incident response and incident recovery processes have been developed *Steps that should be taken in response to cybersecurity incidents have been outlined and employees responsible for overseeing the process have been named.*
Important data sets have been categorized and safety measures for data storage have been put into motion *Information classification has been conducted and technological measures for safeguarding the information have been implemented.*
Clear security guidelines have been established and are easily understandable to members of the organization *Organizational security policy is clearly defined and readily available to members of the organization*

A job analysis has been conducted *A job analysis should be conducted to identify specific job requirements*. and appropriately implement segmented access to systems according to identified requirements
Employees are granted segmented access to systems *Employees should only be authorized access to parts of the system that are pertinent to their job requirements.*

Table 2 - Organizational Cybersecurity Metrics

6. Ensure adaptability to fluid environments

The environment in which the organization operates is susceptible to change over time. Employee turnover, expansion, new partnership agreements, and external rules and regulations are examples of contingencies that may affect an existing organizational cybersecurity culture. To adapt to these contingencies, organizations should continually assess the current cybersecurity culture and, if the situation calls for it, be prepared to modify the metrics and measures used to foster it.

7. Applying culture framework to a case study – Target data breach

7.1 Introduction of the case study and synopsis of the breach

In December of 2013, Target, an American retail corporation, fell victim to a cybersecurity breach. It is unclear how many customers were affected by the cyberattack, but some reports suggest that sensitive personal and financial information of more than 70 million customers was compromised during the attack (Plachkinova & Maurer, 2018, p. 12). The stolen data included encrypted debit card PIN numbers of Target customers, as well as their personal information such as names, addresses, phone numbers, and email addresses (Plachkinova & Maurer, 2018, p. 13). According to reports, attackers were able to collect 11 GB of data on a server in Russia between November and December of 2013 and the data was subsequently offered for sale on black market forums (Shu et al, 2017, p. 3). As a result, Target lost the trust of its customers and investors, saw its profit for the holiday quarter decrease by 46% compared to the previous year's quarter and, at the end of 2015, disclosed that costs related to the breach had reached $290 million (Manworren et al., 2016, p. 1, 3)

Customer data was accessed through a vulnerability in one of Target's contractors, Fazio Mechanical Services, which served as an attack vector into Target's systems. Investigation after the fact determined that phishing served as the initial vector into Fazio Mechanical Services, thereby making the Target attack a real-life example of the significant damage a social engineering attack can cause to an organization.

7.2 Breach investigation overview

The following subchapters will provide a summary of the events leading up to the breach, an overview of the breach investigation and its results, and a comprehensive discussion of the implications of the breach through the lens of organizational psychology.

7.2.1 Events leading up to the breach

Leading up to the breach, Target appeared to have implemented appropriate safeguards to protect its sensitive data. According to Plachkinova and Maurer (2018), in 2013, Target had implemented a $1.6 million worth malware detection tool and passed a compliance audit for the Payment Card Industry Data Security Standard (PCI-DSS) which involves "…a review of critical security controls and systems configurations to verify that best practices for protecting payment card information on computer systems are maintained" (p. 12). Target also monitored cybersecurity

threats on its network from security operations centres in Minnesota and India on a round-the-clock basis (Plachkinova & Maurer, 2018, p. 13).

Despite seemingly up-to-date cybersecurity practices, the human factor can be identified as a liability leading up to December's cyberattack. Investigation has revealed that Target's security tools detected malware on several occasions and issued multiple warnings that went unaddressed. More specifically, on November 30th, security personnel in India was alerted about potential malicious activity by their malware detection software and shared the alert with the security operations center in Minnesota, but no preventive actions were taken (Plachkinova & Maurer, 2018, p. 13). As the attackers began extracting sensitive information from the system, security personnel received multiple warnings once again but took no action (Manworren et al, 2016, p. 3). In addition, a few months before the breach, Fazio Mechanical Services victim to a phishing attack and had its systems infected by malware designed to steal security credentials. It is unclear whether the organization was aware of the breach prior to the Target attack, but research suggests that the compromised credentials served as a vector into Target's systems.

7.2.2 Breach investigation results

The Target attack has subsequently been categorized into 5 phases: the initial phase, PoS infection, data collection, data exfiltration, and monetization (Shu et al, 2017, p. 2). A brief description of each respective phase is provided below.

1. The initial phase of the attack refers to the phishing attack on Fazio Mechanical Services. As a supplier of Target, Fazio was given access credentials to the Target's billing system, which were stolen during the phishing attack.
2. Target's network was not appropriately segmented, which meant that the attackers could utilize Fazio's compromised access credential to gain access to the entire network and infect point-of-sale (PoS) terminals (Shu et al, 2017, p. 3).
3. The malware installed by the attackers copied customer data directly from the memory storage of the PoS system (Manworren et al, 2016, p. 2).
4. The collected credit card information was subsequently encrypted, forwarded to infected File Transfer Protocol (FTP) servers, and relayed to drop sites in Miami and Brazil (Shu et al, 2017. p. 3).
5. The monetization phase involved selling customer information on black market forums.

7.2.3. Aftermath

To this day, it has not disclosed what exact changes the organization made in response to the breach. According to Target communications representative Molly Snyder, the retailer brought in new senior leadership and joined two cybersecurity threat-sharing initiatives: namely the Financial Services Information Sharing Analysis Center (ISAC) and the Retail Cyber Intelligence Sharing Center (Gagliordi, N., 2015).

Breach investigation determined that, at the time of the breach, Target was operating with a flat network, in which traffic was not segmented and data was consequently less secure. In response, a Target corporate webpage outlines a number of technical changes that were made to correct the error (Gagliordi, N., 2015). The organization has improved network segmentation, developed point-of-sale management tools, and created a comprehensive firewall governance process. Additional security improvements were made, including the monitoring and logging of system activity; the installation of application whitelisting on POS systems and POS management tools; limited or disabled network access for vendors; expanded use of two-factor authentication and password vaults; and disabled, reset, or reduced privileges on over 445,000 Target personnel and contractor accounts (Gagliordi, N., 2015).

However, it does not appear that there were any attempts made to directly address the human factor that played a crucial role in the breach. Cybersecurity experts have attributed the organization's failure to react to repeated security alerts to the overwhelming number of alerts that were being received on the daily basis (Finkle & Heavy, 2014). It was later revealed that Target did not begin investigating the alerts until the U.S. Justice Department notified the organization on suspicious activity within its systems (Finkle & Heavy, 2014). As stated by Target Chief Financial Officer John Mulligan: "Through our investigation, we learned that after these criminals entered our network, a small amount of their activity was logged and surfaced to our team. That activity was evaluated and acted upon. Based on their interpretation and evaluation of that activity, the team determined that it did not warrant immediate follow up" (Finkle & Heavy, 2014).

The initial entry vector achieved via a phishing attack served as an impetus for raising awareness among cybersecurity experts on the importance of ensuring that an organization grants third party access strictly to those parts of the organization's system that are pertinent to the business

relationship between the organization and the third party. Cybersecurity expert Stephen Cobb contends that the Target breach marked the beginning of a broader awareness of the supply chain threat vector (Myers, L., 2018). Accordingly, in recent years there has been a greater understanding for network segmentation and more robust authentication options that would have made stolen credentials less useful to attackers.

However, the phishing attack that enabled the breach points to a need for a better employee education on social engineering threats, as cybersecurity expert Stephen Cobb adds: “if the C-suite is not making security a priority for all departments and all employees, you are at higher risk than your competitors that do prioritize security” (Myers, L., 2018).

7.3 Target’s culture of data protection

While Target implemented several highly effective countermeasures in response to the breach, available information does not suggest any attempts were made to make cybersecurity a priority in all departments and among all employees. Target’s cybersecurity countermeasures, network structure, and employee behaviour prior to and during the breach point to a lack of cybersecurity awareness throughout the organization. The fact that the organization implemented a $1.6 million worth malware detection tool and passed a compliance audit for the PCI-DSS further illustrates that technological countermeasures alone cannot account for the threat posed by the human factor in cybersecurity. As stated by cybersecurity expert Cameron Camp: ”Target came to understand that it’s not enough to just have fire-and-forget, very expensive tech to detect ‘bad things’; that correct configuration and tuning are of the essence”. (Myers, L., 2018). For an organization the size of Target, ‘correct configuration and tuning’ entails mitigating the risk posed by its employees and business partners or, in other words, fostering a healthier cybersecurity culture.

7.3.1 Target cybersecurity culture change

In Table 3, the proposed cybersecurity culture framework will be applied to the Target data breach to provide a theoretical benchmark for fostering a healthy cybersecurity culture in large organizations.

Conduct information classification and identify priority level

Given the nature of its business, Target holds large amounts of personally identifiable customer data that would be classified as high impact information because, as illustrated by the breach, the disclosure of this information can have a catastrophic effect on the organization. This classification would confirm the need to foster a healthy cybersecurity culture throughout the organizational hierarchy.

Top management commitment

In the aftermath of the breach, Target upper management demonstrated a willingness to commit to organizational cybersecurity by hiring cybersecurity professionals (creating new cybersecurity leadership positions) and implementing various technological safeguards to mitigate vulnerabilities exposed by the breach. This culture framework can be utilized as an additional supplement, particularly for raising employee awareness to mitigate human vulnerabilities. In addition to steps it already took, upper management should work towards emphasizing the value of cybersecurity on all organizational levels. The most effective way to do that is for cybersecurity professionals to inform employees of new cybersecurity priorities through mandatory staff meetings for all organizational departments.

Assess the current state of the organization

- *Examine existing organizational values, norms, and practices,*
  Conduct employee interviews to gauge employee perception on their respective departments and organization as a whole.
- *Examine employee behavior and attitude towards cybersecurity*
  Collect data on the number of successful and prevented attacks on the organization's network, deploy fake phishing attacks, and utilize attitude scales
- *Examine employee cybersecurity knowledge and awareness*
  Questionnaires and in-person interviews should be conducted to determine whether substandard behavior exhibited by employees occurs due to negligence or subpar knowledge and lack of cybersecurity awareness

Judging by the vulnerabilities identified by the breach investigation, had Target assessed the current state prior to the attack, it would have undoubtedly revealed the need for improvement.

Mitigate identified vulnerabilities by modifying contributing factors

- *Implement incentives to promote cybersecurity culture and behavior*
  Mandatory cybersecurity training attendance and cybersecurity performance evaluations
- *Develop cybersecurity training and awareness programs*
- *Modify organizational norms and practices*
  An effective modification to organizational norms and practices would be adjusting the company's hiring strategy to place a higher value on candidate's self-efficacy and cybersecurity awareness

Monitor progress through predetermined metrics

Since the organization's resources allow the organization to hire experienced cybersecurity professionals, this step can be left to their discretion.

Ensure adaptability to fluid environments
This is a particularly important step for organizations the size of Target, as its business environment exhibits continuous changes. Previous steps should therefore be repeated on a regular basis.

Table 3 – Applying Culture Framework to Target Case Study

8. Conclusion

Digital transformation and the advancement of technological tools have vastly changed cyberspace and provide organizations with more efficient ways to store information and run their business operations. However, technology alone has not been able to address the weakest link in cybersecurity – the human factor. Social engineering continues to be a prominent method of attack and is capable of inflicting significant damage on organizations. To effectively combat human-enabled cybersecurity threats, it is important to address them from an organizational perspective. Organizational culture has a strong impact on an organization's cybersecurity, as it influences employee behavior and attitudes. To ensure a healthy organizational culture, organizations can rely on a variety of cybersecurity culture frameworks such as the ENISA framework, the NIST framework, and the Organizational Cybersecurity Culture Model. This thesis proposes a cybersecurity culture framework that is based on existing frameworks and designed to serve as a theoretical benchmark for implementing and fostering a healthy cybersecurity culture. Taxonomies for organizational culture and social engineering attacks are proposed to ensure a clearer understanding of all the factors that need to be taken into account when strengthening the cybersecurity of an organization. One of the most notable limitations of both the existing and proposed frameworks is the fact that they do not offer specific metrics for assessing the level of risk on an organizational level. Further research may consider devising risk assessment methods that can be used to supplement existing cultural frameworks by facilitating the process of prioritizing the need to eliminate identified vulnerabilities within an organization.

Literature

1. Aldawood, H., & Skinner, G. (2020). An Advanced Taxonomy for Social Engineering Attacks. *International Journal of Computer Applications*, *177*(30), 1–11. doi: 10.5120/ijca2020919744
2. Alrwais, S.A., Yuan, K., Alowaisheq, E., Liao, X., Oprea, A., Wang, X., & Li, Z. (2016). Catching predators at watering holes: finding and understanding strategically compromised websites. *Proceedings of the 32nd Annual Conference on Computer Security Applications*.
3. Breda, F., Barbosa, H., & Morais, T. (2017). Social engineering and cyber security. *Proceedings of the International Conference on Technology, Education and Development*., Valencia, Spain
4. Bullee, J.-W., Montoya, L., Junger, M., & Hartel, P. (2017). Spear phishing in organisations explained. *Information and Computer Security*, *25*(5), 593–613. doi: 10.1108/ics-03-2017-0009
5. Connolly, L., Lang, M., & Tygar, D. (2014). Managing Employee Security Behaviour in Organisations: The Role of Cultural Factors and Individual Values. *ICT Systems Security and Privacy Protection IFIP Advances in Information and Communication Technology*, 417–430. doi: 10.1007/978-3-642-55415-5_35
6. Corradini I., Nardelli E. (2019) Building Organizational Risk Culture in Cyber Security: The Role of Human Factors. In: Ahram T., Nicholson D. (eds) Advances in Human Factors in Cybersecurity. AHFE 2018. Advances in Intelligent Systems and Computing, vol 782. Springer, Cham. https://doi.org/10.1007/978-3-319-94782-2_19
7. Corradini, I. (2020). Building a cybersecurity culture in organizations. Springer International Publishing, vol 284.
8. Corradini I., Nardelli E. (2020) Social Engineering and the Value of Data: The Need of Specific Awareness Programs. In: Ahram T., Karwowski W. (eds) Advances in Human Factors in Cybersecurity. AHFE 2019. Advances in Intelligent Systems and Computing, vol 960. Springer, Cham. https://doi.org/10.1007/978-3-030-20488-4_6
9. Daniel Ani, U.P., He, H.M., Tiwari, A. (2016). Human Capability Evaluation Approach for Cyber Security in Critical Industrial Infrastructure. *Advances in Human*

Factors in Cybersecurity. Advances in Intelligent Systems and Computing, 169-183. https://doi.org/10.1007/978-3-319-41932-9_14

10. De Long, D.W., & Fahey, L. (2000). Diagnosing Cultural Barriers to Knowledge Management. *Academy of Management Executive*, 14, 113-127. https://doi.org/10.5465/ame.2000.3979820
11. Dreibelbis, R. C., Martin, J., Coovert, M. D., & Dorsey, D. W. (2018). The looming cybersecurity crisis and what it means for the practice of industrial and organizational psychology. *Industrial and Organizational Psychology: Perspectives on Science and Practice, 11*(2), 346–365. https://doi.org/10.1017/iop.2018.3
12. European Union Agency for Network and Information Security (2017). *Cybersecurity Culture in Organizations* [PDF]. Available at: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations
13. Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks*, 9(17), 4667–4679. doi: 10.1002/sec.1657
14. Finkle, J., Heavey, S. (2014). Target says it declined to act on early alert of cyber breach. Retrieved from https://www.reuters.com/article/us-target-breach/target-says-it-declined-to-act-on-early-alert-of-cyber-breach-idUSBREA2C14F20140313
15. Gagliordi, N. (2015). The Target breach, two years later. Retrieved from https://www.zdnet.com/article/the-target-breach-two-years-later/
16. Glaspie, H. W., & Karwowski, W. (2017). Human Factors in Information Security Culture: A Literature Review. *Advances in Intelligent Systems and Computing Advances in Human Factors in Cybersecurity*, 269–280. doi: 10.1007/978-3-319-60585-2_25
17. Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7). doi:10.1016/j.heliyon.2017.e00346
18. Huang, K., & Pearlson, K. (2019). For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture. *Hawaii International Conference on System Sciences*. p. 6398-6407

19. Lim, J.S., Chang, S., Maynard, S. and Ahmad, A. (2009) "Exploring the relationships between organizational culture and information security culture". *Proceedings of the 7th Australian Information Security Management Conference*. 88-97
20. Lohani, S. (2019). Social Engineering: Hacking into Humans. *International Journal of Advanced Studies of Scientific Research*, *4*(1), 385-393. Available at SSRN: https://ssrn.com/abstract=3329391
21. Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons, 59,* 257-266. doi:10.1016/J.BUSHOR.2016.01.002
22. Myers, L. 2018. Target targeted: five years on from a breach that shook the cybersecurity industry. Retrieved from https://www.welivesecurity.com/2018/12/18/target-targeted-five-years-breach-shook-cybersecurity/
23. National Institute of Standards and Technology (2018). *Framework for Improving Critical Infrastructure Cybersecurity* [PDF]. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
24. Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. *HOLISTICA – Journal of Business and Public Administration*, *9*(3), 71–88. doi: 10.2478/hjbpa-2018-0024
25. Patterson, W., Winston, C., & Fleming, L. (2016). Behavioral Cybersecurity: Human Factors in the Cybersecurity Curriculum. *Advances in Intelligent Systems and Computing Advances in Human Factors in Cybersecurity*, 253–266. doi: 10.1007/978-3-319-41932-9_21
26. Patterson, W., & Winston-Proctor, C. E. (2019). *Behavioral cybersecurity: Applications of personality psychology and computer science*. Boca Raton (Fla.): CRC Press Taylor & Francis Group. https://doi.org/10.1201/9780429461484
27. Plachkinova, M. & Maurer, C. (2018). Teaching Case: Security Breach at Target. *Journal of Information Systems Education*, 29(1), 11-20.
28. Reegård, K., Blackett, C., & Katta, V. (2019). The Concept of Cybersecurity Culture. *29th European Safety and Reliability Conference,* 4036-4043. doi:10.3850/978-981-11-2724-3_0761-cd
29. Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet, 11,* 89.

30. Shappie, A.T., Dawson, C. A., & Debb, S. M. (2019). Personality as a Predictor of Cybersecurity Behavior. *Psychology of Popular Media Culture.* Advance online publication
31. Shu, X., Tian, K., Ciambrone, A., & Yao, D. (2017). Breaking the Target: An Analysis of Target Data Breach and Lessons Learned. *ArXiv, abs/1701.04940*
32. Spremić, M., Šimunic, A. (2018): Cyber security challenges in digital economy, *Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering WCE 2018*, pp. 341-347, IAENG, Hong Kong
33. Spremić, M. (2017): Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, sveučilišni udžbenik, Ekonomski fakultet Zagreb
34. Thomas, J. E. (2018). Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks. *International Journal of Business and Management, 13*(6), 1. doi: 10.5539/ijbm.v13n6p1
35. Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E., & Bailey, M. (2016). Users Really Do Plug in USB Drives They Find. *2016 IEEE Symposium on Security and Privacy (SP)*. doi: 10.1109/sp.2016.26
36. Van der Kleij, R., & Leukfeldt, R. (2020) Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security. *Advances in Human Factors in Cybersecurity. 960*. 16-27. AHFE 2019. https://doi.org/10.1007/978-3-030-20488-4_2
37. Veiga, A. D., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, *70*, 72–94. doi: 10.1016/j.cose.2017.05.002
38. Wisniewska M., Wisniewski Z., Szaniawska K., Lehmann M. (2020) The Human Factor in Managing the Security of Information. *Advances in Human Factors in Cybersecurity*. *960*. 38-47. AHFE 2019. https://doi.org/10.1007/978-3-030-20488-4_4
39. Yildirim, E. (2016). The Importance of Information Security Awareness for the Success of Business Enterprises. *Advances in Intelligent Systems and Computing Advances in Human Factors in Cybersecurity*, 211–222. doi: 10.1007/978-3-319-41932-9_17

40. Yusof, H.S., Said, N.S., & Ali, S.R. (2016). A Study of Organizational Culture and Employee Motivation in Private Sector Company. *Journal of Applied Environmental and Biological Sciences, 6*(3), 50-54.

List of Tables

Table 1 - Information classification 37
Table 2 - Organizational Cybersecurity Metrics 42
Table 3 – Applying Culture Framework to Target Case Study 48

List of Figures

Figure 1 - Proposed Social Engineering Taxonomy 12
Figure 2 - Areas of Contributions for I/O Psychologists 20
Figure 3 - Proposed Organizational Culture Taxonomy 26
Figure 4 - Key Areas that Affect Employee Behavior 28
Figure 5 - Organizational Cybersecurity Culture Model 32
Figure 6 - NIST Framework Information Flow 34
Figure 7 - NIST Framework 35