Haaga-Helia
University of Applied Sciences

The Human Element in IT Security

Leo Malinen

Bachelor's Thesis
Degree Programme in BITE
2021

Haaga-Helia
University of Applied Sciences

Abstract

2 May 2021

Author
Leo Mikael Malinen

Degree programme
Business Information Technology

Report/thesis title	**Number of pages and appendix pages**
The Human Element in IT Security	58 + 1

This research is focused on the topic of IT security from the perspective of the internal human element by examining employee's roles in organization's IT security. This is achieved by examining how big the role of the employees in the overall organization's IT security is and what measures can be taken to prepare for threats involving or originating from the internal human element.

The goal of the research is to give a clear overview of the aforementioned threats by categorizing them and examining real IT security incidents which have happened from said categories. The scope of this project is limited to IT security threats with direct involvement of the internal human element and hence excludes threats such as injections and software bugs.

This research is primarily based on qualitative data and was conducted between September 2020 and May 2021. The methods of acquiring the qualitative data in the research include referenced books, blogs, news articles and interviews on related topics.

The first part of the research goes over the practical aspects of this research after which it transitions into the theoretical background of the topics discussed later in the research. After the theoretical background, the research goes over the empirical part by examining real cases involving the internal human element and making observations based on interviews carried out during this research. The final parts go over the results and discussions of this research.

Results from this research include information on how factors such as solutions involving technology, organization sizes, risk assessments and psychology affect organizations capabilities to prepare for threats involving the internal human element.

The conclusion from this research is that employees play a large role in organizations IT security not only due to their direct actions but also based on their approach to the topic especially when considering IT security in organizations culture. This research also came to the conclusion that frameworks, especially the ISO 27001, are very beneficial for organizations when dealing with threats involving the internal human element.

Keywords
IT security, human element, social engineering, ISO 27001

Table of contents

1 Introduction

A screen with multiple windows open keeps opening more and more windows with an alarming number of beeps coming from the computer. The firewall has been breached. The IT security team is fighting hard against this threat by writing multiple lines of code in a matter of seconds. The battle continues as code is being written on both sides and the winner will be determined by their code. This is how IT security is often portrayed as in entertainment and even some forms of media. This perspective give the impression that IT security is all about coding and scripts. Whilst they do play an important role in IT security, one aspect not always immediately attributed to be part of it is the human element.

That is what why research examines the internal human element's role in organizations IT security. In this research this topic will be looked at from different angles with the main focus of giving the reader a comprehensive general idea of how employees in organizations affect their organizations IT security. The more people who are aware of their own actions having effects on IT security in their professional life, the stronger organizations IT security can be. That is why one aspect of this research is to try and introduce the topic to the reader in an understandable and a relatable way in hopes of the reader finding themselves thinking of their personal role in their organization's IT security in the future.

Chapter 1 of this thesis goes over the practical details of the research, explaining what the objective of the research is and what is within its scope. Chapter 1 also explains the structure of the research, key terminology and how the information was researched.

1.1 Objective

The main objective of this research is to *find how the internal human element of organizations, employees, play a role in IT security and how the threats to do with this source can be protected against efficiently.* Part of this objective is to categorize the origins of these threats so they can be recognized and remembered. Other objectives are finding cases where the internal human element has played a role in an IT security incident to give real examples of the possible threats to do with the internal human element and emphasize why it is an important element of IT security.

The focus of this this research is on gathering data on security incidents involving the internal human element and researching how organizations could prepare for them. The aim is to provide an efficient overview of how employees affect IT security in organizations of different sizes and what measures organizations can take against these threats. The outcome of this research is to try help both organizations and individuals be more aware

of how the human element plays a vital role in today's IT security. The benefit of this knowledge would hopefully strengthen organizations IT security resulting in fewer IT security incidents.

Main research question: *What are the threats within organizations involving the internal human element?*

Another research question: *How big of a role does the internal human element play in organizations IT security?*

Another research question: *How can these threats be categorized and prepared for?*

A research problem: *Finding examples of real-world IT security incidents where the internal human factor played a vital role.*

1.2 Scope

The scope of this research is examining IT security threats to do with the internal human element, employees, within organizations. This includes examining said scope from multiple different angels to get a better understanding of it. This research includes examining where these threats originate from, how these threats have changed over the years, how different factors play into these threats and how organizations are currently protecting against these threats.

This research is limited to examining these points from the perspective of the internal human elements role in these situations and has an emphasize on it. Problems originating from code or threats that only deal with malicious intent from outside the organization with no connection to the internal human element are not within the scope of this research.

1.3 Research methods

The main research method of this research is qualitative. The qualitative data is a collection of opinions and observations from professionals in the IT field and notable people who have worked on the human element in IT security, or who have otherwise contributed to this research. Some quantitative data is also present when examining statistics about IT security, but this is used as a tool to better understand and reflect on the qualitative data.

One method used to acquire information for this research is literature covering the topics discussed in the chapters. The literature consists of books on topics about the chapters,

existing guides created by organizations about IT security, and case studies conducted previously on cases relevant to this research.

Other methods of acquiring information for this research include using online websites for required purposes. This, depending on the chapter and topic, varies from official government websites to organizations own websites, news articles and other websites.

The final method of acquiring information for this research is conducting interviews with people who work in IT security in one form or another. The interviews are conducted towards the end of the research. The interviews include people specializing in IT security as their profession or IT security playing a key role in their jobs.

1.4 Structure of thesis

After this introductory chapter to the research, Chapter 1, the next chapter, Chapter 2, goes over theoretical background to better explain concepts and precautions currently used by organizations against threats examined in further parts of this research with focus being on the internal human element. Chapter 2 starts by going over how IT security has changed over the years and that transitions into how the human element plays a role in it, especially nowadays. After examining the human element's role, Chapter 2 goes over what solutions there are to counter these threats and examines the how to achieve the best results. In the last part of Chapter 2, it goes over how organizations evaluate the risks and how they are prepared for them currently.

The chapter after, Chapter 3, focuses on gathering examples of cases where the human element played a vital role in an IT security incident and analyses these cases. The cases are gathered from different sources. The first source used to gather the cases is case studies and literatures. This goes over cases that been documented well from multiple different perspectives and are well known in the field of IT security. The second source for cases is from news articles, this focuses on IT security cases that gathered interest from the public and were relatively big news articles in their time. The second source also contains cases from existing guides, which is followed by the third source of cases which are other sources that became apparent during this research. All these cases focus on IT security incidents and threats that deal with the human element playing a vital role.

Chapter 4 goes over the interviews conducted during this research, which were done by interviewing people who work in IT security, though their titles and job descriptions differ. The interviews go over their views on the human element in IT security in various aspects.

The next chapter, Chapter 5, goes over the results and conclusions of this research. Chapter 5 includes the final conclusions to the research, which includes answering the research problems from Chapter 1.1 and emphasizing key findings of this research.

The last chapter, Chapter 6, discusses the trustworthiness of this research and goes over what development ideas there are to do with it and how the reader can continue their research on the topic if they so choose. The last part of Chapter 6 focuses on evaluating the actual research process and the researchers own learning from it. At the end of the research are the references used in this research and the appendices.

There are some key terms used throughout this research that are explained here in order to make the text easier to follow. These terms are present throughout the various chapters and have been compiled here for easier understanding of the chapters in this research.

Internal human element: Refers to the employees working within the organization. Does not include external people such as organizations clients.

Malware: Software with malicious intent, created with the purpose to interfere with systems or to retrieve data that is not open to the public.

Social engineering: Social engineering involves attacks that rely on use of psychology to get people to perform tasks that are not in their best interest by tricking them. Various kinds of social engineer attacks are explained further in chapters covering them.

Framework: A predefined combination of procedures, rules and methods to deal with potential problems. Used to determine how to handle threats in advance or set a standard for handling certain issues.

Cybersecurity: Practice of ensuring data, data assets and networks are protected. Overlaps with IT security, the exact definitions vary depending on source.

2 Human element in IT security

This research theoretical background focuses on what role the human element plays in IT security and how it has changed with time. It also explores the different types of threats involving the internal human element and how organizations combat these security threats.

2.1 History

In order to understand the present and prepare for the future, understanding the past of human element in IT security plays a vital role, in the words of George Santayana “Those who cannot remember the past are condemned to repeat it”. This research was done to see how big of a role the internal human element has played in IT security incidents and what the trends involving them are.

Over the years the method of attacks on organizations have changed but focusing on the methods that involve the human element can be used to quantify their role in IT security. In quarter 1 of 2017 Positive Technologies listed cybersecurity attack methods and their percentage of the cybersecurity attacks that year (Positive Technologies 2017) as follows:

- 36% Use of malware
- 23% Compromise of credentials
- 15% Software vulnerabilities exploitation
- 11% Web vulnerabilities exploitation
- 8% DDoS
- 6% Social engineering

Comparing the older data to newer data can be used to see patterns in IT security involving the human element. In quarter 2 of 2020 Positive technologies listed the same statistic about attack methods on organizations and their percentage of the cybersecurity attacks in 2020 (Positive Technologies 2020a) as follows:

- 62% Malware use
- 59% Social engineering
- 18% Hacking
- 15% Web attacks
- 5% Credential compromise
- 3% Other

The reason for the total being over 100% in quarter 2 of 2020 is that they likely started to list attacks having multiple sources. One trend that is immediately obvious from comparing the data from Q1 2017 to the data from Q2 2020 is the rise in social engineering being part of cybersecurity attacks. This is a type of attack that focuses on the internal human element in organizations, and it has become more popular over time. The internal human element’s role in cybersecurity incidents can be compared to other research to try and

verify Positive technologies statistics. In comparison, in the year 2020 Help Net Security referenced a Tessian report that up to 43% of US and UK employees had caused themselves or the company they work for cybersecurity repercussions (Help Net Security 2020).

In addition to this Positive Technologies has also been monitoring the attack targets of these cybersecurity incidents. In the two same reports they reported in 2017 that 19% of the attacks were targeted at the actual users instead of targets such as devices, terminals, web resources and infrastructure (Positive Technologies 2017). In 2020 they reported that 59% of cybersecurity attacks against organizations targeted people (Positive Technologies 2020a).

With these two metrics combined, percentage of social engineering attacks in cybersecurity incidents and users being the target of cybersecurity attacks, it is feasible to say the internal human element plays a bigger role in today's IT security than before. As shown in Figure 1 social engineering attacks and cybersecurity incidents being targeted at users have increased over time and both have trendlines continuing to climb.

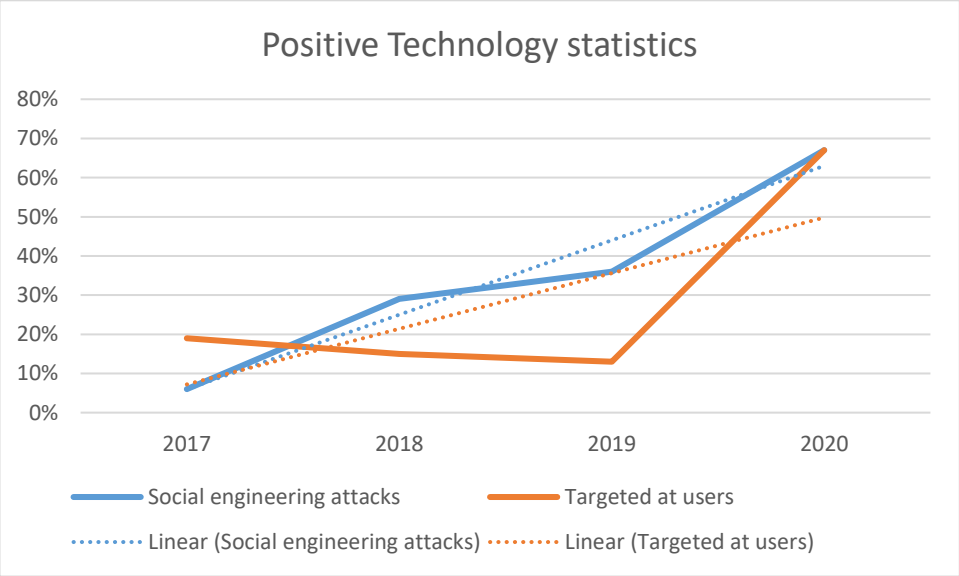

Figure 1. Collection of data from Positive Technologies (Positive Technologies 2020b)

The trend in growth of human element in IT security in recent years could be attributed to many factors, with the spike in 2020 being at least in part due to the pandemic, with more people working from home. Even before the pandemic the amount of social engineering attacks was on the rise. In order to get a better picture of how the human element has played a role over time and what the possible future of the human element in IT looks like, it is important to look a bit further back.

In the early 2000s IT security was focused heavily on protecting against malwares, which purpose was to disrupt users (Thales 2016). At this point, most IT security threats were to do with pieces of code targeting systems within organizations. Under 10 years later in 2009, one of the better known early social engineering experiments in IT security was performed (more about this in Chapter 3.1.2). In recent years IT security attacks aimed at the human element have increased in popularity as shown in previously in this chapter, discussed in the interviews in Chapter 4 and other sources such as universities like University of San Diego listing phishing and social engineering attacks as cybersecurity threats to be aware of (University of San Diego 2020).

In 20 years, the internal human element went from being a minor aspect of IT security to one of the biggest factors with already in 2017 Kaspersky in their official blog giving an estimate of 52% businesses thinking of employees as their biggest security risk (Kaspersky 2017). The reason the internal human element is being viewed by many businesses as their biggest security risk is not only due to the statistics about how many cybersecurity attacks are focused on them, but rather a combination of different threats involving them discussed in the next chapter.

2.2 Human elements

When examining internal human element security threats in this research it helps to categorize the risks into different subsections to easier keep track of said threats and understand the reasoning for them. This research goes over IT security threats discussed in later chapters by going over incidents where they have occurred before and discussing what protections can be used against them in the future. Figure 2 gives a visual demonstration of the sources of threats involving for the internal human element found in this research.

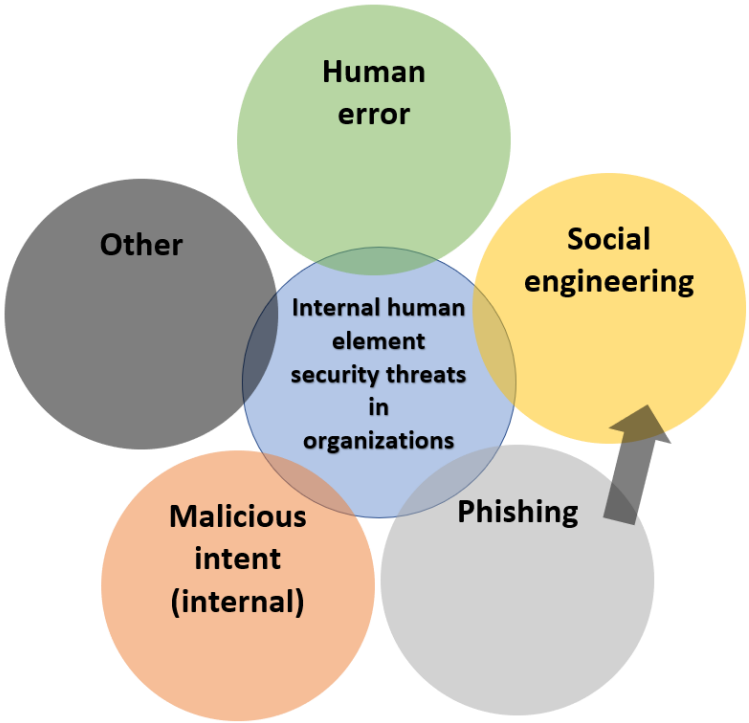

Figure 2. Sources of internal human element security threats based on this research

The first category of risks from the internal human element in organizations originates from **human errors** from employees. IBM in their “Cost of a Data Breach Report 2020”-report stated human error being the root cause for 23% of data breaches (IBM 2020, 30) and back in 2017 Kaspersky gave an estimate of 46% of cybersecurity incidents involving human error in the form of careless / uninformed staff (Kaspersky 2017). The metrics vary depending on source and as stated by John G. Voeller (Voeller 2014, 3) “Organizations currently face several problems related to the accuracy of measures. One problem is that measures are often defined imprecisely” but both reports indicate human error attributing heavily to cybersecurity incidents.

When it comes to IT security, many risks and factors work in harmony to create threats. The keynote is that internal human error contributes a large portion of data security threats to organizations and human error naturally has been around for a long time in IT security. Human errors as category can also include many different types of errors such as bad decisions from IT security point of view, sharing classified documents by mistake, misconfigurations, or lack of knowledge leading to a security threat. The main point about human error in IT security is that it is caused by actions originating from the internal human element with no malicious intent.

The second source of risks from internal human elements in organizations are the threats originating from different types of **social engineering**. Social engineering can be explained as follows “Social engineering is a set of techniques that are widely being used in cyberattacks to orchestrate some of the most successful attacks. Social engineering uniquely targets a weak component in the cybersecurity chain—the user.” (Ozkaya 2018, 5).

Social engineering can be further described as acts that influence people to take actions that may not be in their best interest (Hadnagy & Wozniak 2018, 1). This is achieved by taking advantage of human behaviour patterns in which malicious attacker take advantage of people’s emotions, trust, human psychology to trick other people. Social engineering itself consist of multiple different attack methods, the target however is the internal human element, when targeting organizations. As discussed in Chapter 2.1, the use of social engineering as a cyberattack method has been on the rise over the years. In further chapters this research goes over different social engineering attacks with examples that have occurred.

Social engineering attacks have a certain method in them referred to as **phishing**. Whilst phishing is a type of social engineering attack, the methodology, age of attack, frequency and other key pieces of information qualify it to be its own category when discussing threats of internal human element in this research. Where social engineering can refer to a broader context such as dressing up a certain way, usually as an IT/construction worker, or other methods of misdirection, phishing is a more standard form of social engineering taking shape online, whereas other methods of social engineering can take place in person.

National Cyber Security Centre describes phishing as follows “Phishing is when attackers attempt to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware, or direct them to a dodgy website.” (National Cyber Security Centre 2018). Phishing itself also has more categories within it but phishing usually refers to the email version of trying to get users to perform actions. National Cyber Security Centre also explains the dangers of phishing emails as follows: “Phishing emails can reach millions of users directly and hide amongst the huge number of benign emails that busy users receive. Attacks can install malware (such as ransomware), sabotage systems, or steal intellectual property and money.” (National Cyber Security Centre 2018).

Phishing attacks can be done in two ways, one is relying on numbers and sending an email to more people with less personal information and relying on people clicking the link

or attachment in the email out of curiosity or by accident. This could something as simple as an email titled “Restore your account” where the email states an account for a service has been locked and the user must follow the link to regain access to the account. This email can be targeted at basically anyone within an organization in the hopes that someone opens the email and gets their hardware infected or log in details stolen. More targeted attacks take into account the user’s personal life and can include information gathered from social media such as the date for when they were part of a biking event and use that information in the email to lure to user to click links or download attachments by promising things such as monetary reward for being in the competition (Conheady 23 November 2010).

Organizations internal human elements also cause security threats by being targeted with other types of phishing. Where phishing took the form of tricking employees over email, vishing takes place over the telephone, an example of vishing is creating an interactive voice response (IVR) and getting employees to call the number and give their details (Ozkaya 2018, 420). The more common version of vishing nowadays is smishing, which tries to achieve the same results as phishing and vishing but smishing is done over SMS. Each of these methods are targeted at the internal human element at organizations and without proper protection against, can cause serious IT security threats.

The next type of security threat related to internal human element is an internal one. The previous attacks relied on the internal human element to fall for the attack or threats were caused by human error. Sometimes the origin of the threat can be internal in the form of **malicious intent** from employees. The Australian Cyber Security Centre lists the possibilities for malicious insiders as follows “There are many reasons an insider can be or become malicious including revenge, coercion, ideology, ego, or seeking financial gain through intellectual property theft or espionage” (Australian Cyber Security Centre 2020). Employees have varying access to credentials, information, and systems within organizations and when misused can create big cybersecurity threats.

Whereas the previous four categories: human error, social engineering, phishing, malicious intent (internal), cover the majority of risks from the internal human element in organizations, there are other risks associated with the internal human element. The last category, **other**, covers origins of other threats discussed in this research. An example of other threats was discovered in this research during the interviews. This threat was to do with the attitude towards IT security from management or even an individual employee. If management does not incorporate IT security into the organizations culture well enough,

then threats such as inefficient resources or negligence in regard to IT security may occur. This is discussed further in Chapter 4.7.

2.3 Solutions involving technology

The next important factor to look at is how organizations can prepare for cybersecurity threats involving the internal human element. The human element in IT security requires constant training and repetition in order to be effective. Having policies in organizations that are not reinforced well or are just in handbooks handed out to new employees is not enough to train employees for cybersecurity. The human element training requires the employees to understand everyone is part of the IT security and everyone plays a vital role in it. Potential threats and mistakes should ideally always be reported without fear of having done something wrong. It is better to know a potential threat as soon as possible rather than later even if it originated internally.

When accessing solutions for IT security threats involving the internal human element, a common method is to emphasize teaching employees on how to handle risk situations such as potential malware emails. A lot of IT security revolves around the human element and many training programs focus on this aspect for a reason. Organizations such as “Globalquest Solutions – Professional IT services” have articles surrounding this issue. Globalquest published an article called “Employee awareness training – Your first line of defense against cyber threats.” (Globalquest Solutions 2018).

News sources also writes articles on the matter such as Training Journals news article in 2020 titled “A human firewall: The first line of defence”, which discussed the human element in companies when defending against cybersecurity threats (Training Journal 2020). Human element in cybersecurity defence plays a vital role but articles, trainings and other sources might give readers an unbalanced view on how to better secure organizations against cybersecurity threats, emphasizing too much on the human element for the solution.

Training employees on basic IT security standards alone is not enough to protect the frontline of IT security. Even in the Training Journals news article they mention “However, for organizations looking to better defend themselves, a combined human and technology-driven approach is essential.” (Training Journal 2020).

The role of integration of technology to better secure organizations, even in the front line where human elements such as employees interact with emails is an important topic. Dr. Andrea Little Limbago, Chief Social Scientist from Virtu, has talked about human element

not going away from cybersecurity but instead we should focus on technology that takes the human behavioural element into account and work together with it to improve front line cyber defences (Limbago 14 November 2018). She also has stated that blaming the human element for frontline vulnerabilities and not the technology is a cop out, we should instead have the two, human element and technology, work together to strengthen the cybersecurity. She has made the argument “If a defense is don’t click on that link, that’s really not a terribly creative defense” (Limbago 14 November 2018), which summarizes well the need for IT solutions on all levels of IT security and not just employee training.

Large organizations have already implemented this into their IT security and are constantly working on improving it. An example of this would be IBM, according to Forbes the 51st largest public company (Forbes 2020), who is working on AI for cybersecurity to improve the interaction between the human element and technology solutions (IBM 2020). Kevin Skapinetz, IBM Security vice president, explained their use of AI for cybersecurity as a tool used together with the human element to strengthen both the human element and technology side. The analogy he used to describe the human element and technology in cybersecurity was to compare it to a police officer, who has his own training, experience, and intuition (the human element in cybersecurity in this analogy) and a canine, who has heighted senses for certain threats (the technology solution in this analogy) (IBM 2020). The canine can inform the police officer of potential threats and they work best together.

These are the reasons for trying to implement beneficial technology solutions for IT security threats even when the origin of threat might be the internal human element. The technological solution to IT threats in systems should also be considered if possible, when building the application/software rather than as an afterthought and this is currently taken more into consideration in IT security according to John G. Voeller (Voeller 2014, 41). Training of employees plays a vital role and using efficient tools in addition to this creates a better safety net for organizations. In this research, when possible, technological solutions are suggested as tools to counter mentioned threats to increase security.

2.4 Organization sizes

As discussed previously, the internal human element in IT security needs to be kept up to date on the cybersecurity threats present and educated on their role of IT security within the organizations, the size of the organization has a correlation with how well this task is usually performed, as explained in this chapter. Size of companies can drastically affect their IT security plans, IT security department sizes and resources. In order to know which companies and organizations benefit most from which IT security plans it is important to

know the differences in company sizes and how it affects the IT tools they use on a day-to-day basis.

The definition for small, medium and large companies varies depending on source, market, location and multiple other factors but the general premise is usually the same. The size of organizations also affects what potential threats the internal human element may cause, best ways to prepare for these threats, and the organizations capability to take these preventive measures. In order to better understand what this research means when referring to organizations of certain sizes later on, this chapter contains definitions for small, medium and enterprise level organizations and businesses.

Small businesses have under 100 employees (Sangoma 2019). When it comes to IT in small businesses, usually the tools are very minimal and there might not be a person who is focusing purely on the IT aspect of the business. Some small businesses can have IT staff and use a lot of programs or technology in their work, such as small programming companies but usually small companies are independently owned and where one individual, the owner, makes majority of the decisions.

Medium sized businesses vary from 100 to 999 employees and have an annual revenue of $5-$10million. These businesses generally have one or few people working specifically in IT staff (Sangoma 2019). The amount of people working specifically in IT staff has a drastic effect on the IT security, explained further in this chapter later on.

Large enterprises are different from medium enterprises in the sense that they have over 1000 employees, operate globally, and have an annual revenue of over $1 billion (Sangoma 2019). The key thing about their IT staff that differentiates them is that they have full time IT staff which include multiple specialists from different aspects of IT (Sangoma 2019).

The amount of people actively working in the IT staff has a drastic effect on the strength of the organization's IT security. If there are not enough people to have at least one person dedicated to IT security alone, but rather someone doing it along with their other tasks, then it stands to reason that there may be gaps in their IT security plans. IT security is something that requires constant effort to keep up with, in the words of Patricia Titus, former CISO (chief information security officer) at transportation security for the Department of Homeland Security USA as reported by Baseline, "Cyber-threats constantly change, so companies have to constantly change too" (Baseline 2012). Having people dedicated to monitoring and adapting to current IT security threats is crucial for a good IT security plan.

Generally, in small businesses the amount of people specialised with technology used is quite small and users are taught by user to user instead of creating big IT plans that affect multiple people. In small businesses there might not even be a person knowledgeable enough in IT to implement certain IT security plans safely and the work could backfire. Something such as encoding hard drives, which generally is a good procedure, could cause data loss if the encoder is unaware of how to do it properly, this is discussed further in Chapter 3.3.1.

Medium sized businesses and enterprises however have personal dedicated to IT and IT security, meaning they can apply IT solutions properly. The number of staff overall also raises at these points, so more automated solutions should be applied so everything does not have to be made for each individual and general security threats can be reduced more efficiently. The larger the business or enterprise also gets, generally the more IT products and services they use. Larger companies can also start implementing more complex solutions to IT security threats, such as the ones discussed in the next chapter.

2.5 Risk management

When preparing organizations for threats involving the internal human element and seeing how these threats can be countered, it is possible to first see how other IT security threats are handled in organizations. One key component when organizations handle any IT security threats is the risk assessment and this is key to prepare appropriate security controls with cost-benefit analysis (ISG 2019).

A common method in the IT security field to assess various threats is to use a type of a risk scale chart. With this, threats both impact and likelihood are taken into account and threats beyond certain thresholds require actions from the IT security team. Figure 3 is an example of a simplified risk assessment chart where both impact and likelihood range from 1 to 5. Within the chart is colour coding that represents the severity of the threat, green means low severity and generally does not warrant actions, yellow means medium severity and requires some action, orange means high severity and requires proper action from IT security team, red means very high severity and must always be considered in the IT security plan and always be well prepared for.

Very High	5	6	7	8	9	10
High	4	5	6	7	8	9
Medium	3	4	5	6	7	8
Low	2	3	4	5	6	7
Very Low	1	2	3	4	5	6
	Impact	1	2	3	4	5
	Likelihood	Very Low	Low	Medium	High	Very High

Figure 3. Risk assessment chart

Organizations can use these charts to determine the risks from the internal human element to categorize threats better and make sure required precautions are taken. According to CIISec report in 2020 of 445 IT security professionals, the resources given to IT security professionals were often times not enough for the rising threat levels (Chartered Institute of Information Security 2020). This is where charts such as this help organizations prioritize certain threats also involving the internal human factor and optimize resource usage.

Examples of how charts like this can be utilized by organizations to help protect against threats involving the internal human element can examined by looking at a couple threats and how charts like this help categorize and prepare for them. Example cases:

- Phishing email sent to CFO (Chief Finance Officer) about swapping bank account for a deal that was made with another organization
- Employee forgetting to lock computer when going for lunch
- Employee accidentally deleting stored data from server

The first case about phishing is highly likely to happen, there are news reports about security incidents involving phishing (examined more in Chapter 3.2.2) and a targeted attack at CFO could cause severe financial and reputational loss if the attack were to succeed, hence it placed in the very high severity in the chart. The second case about an employee not locking their workstation as they go to eat has a medium chance of happening and the impact of this threat is medium if proper security is in place for who have access to workstations. This is a medium severity threat and requires some action for example in the form of setting group policies to lock sessions after a certain amount of time being inactive (Microsoft 2018a). The last case about data being deleted by accident is very likely to happen over time and depending on lost data, it can have medium to very high consequences. This places it high on the risk assessment chart and resources have to put into IT security to counter this from occurring, an example of a preventative measure against this is creating backups of data handled by users. This solution requires a lot of resources

but since the threat is high, it can be justified. This is demonstrated in Figure 4 where the example cases are visualized on the chart.

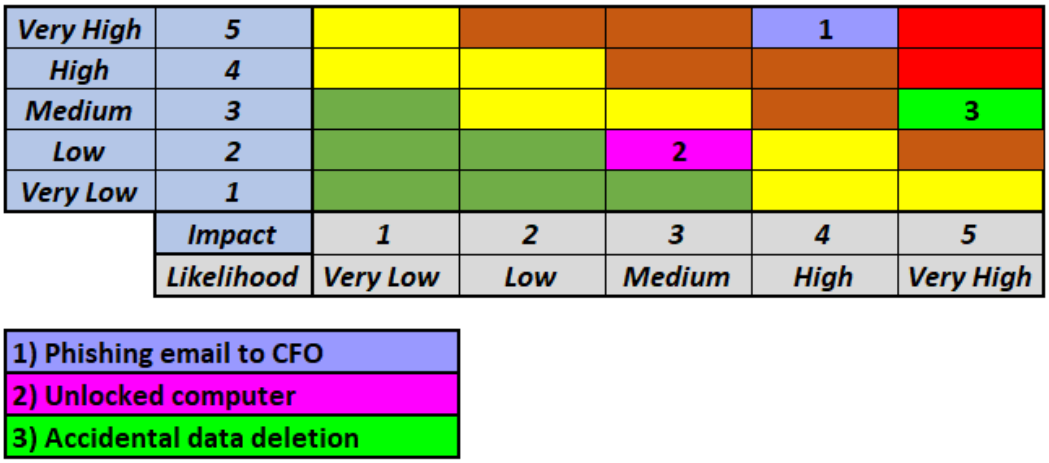

Figure 4. Risk assessment chart with examples

With processes like these organizations can more easily manage resources required to combat IT security threats involving internal human element and make sure the distribution of resources meets the threat level. In addition to knowing how likely a threat is and what the impact it has if it were to occur, organizations should also use other tools to prepare for IT security threats involving the human element.

Another tool used in IT security is security frameworks surrounding the process of how IT security threats are handled. These frameworks aim to reduce the risks of IT security threats impacting organizations (Dawson 27 June 2019). This is achieved by setting certain standards, best practices, and guidelines to manage risks involved with IT security (Poggi 9 November 2020). One of the more common frameworks in this industry is the NIST CSF (National Institute of Standards and Technology Cybersecurity Framework), which was originally developed in response to an Executive Order signed by President Obama to improve critical infrastructure cybersecurity signed in 2013 (Obama White House 2014) and private organizations also use it as a part of their IT security (Mutune 18 September 2019). Even though NIST CSF primarily focuses on infrastructure, it also includes elements to do with the human element (National Institute of Standards and Technology 2018, 35).

The NIST Cybersecurity Framework has five core functions within it; Identify, Protect, Detect, Respond, Recover and these cores are not a process that goes from start to end but rather five activities that when used together and concurrently can combat IT security

threats (National Institute of Standards and Technology 2018, 7). These five core functions are shown in Figure 5. The National Institute of Standards and Technology explains the five core functions as follows (National Institute of Standards and Technology 2018, 7-8):

- Identify, develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- Protect, develop and implement appropriate safeguards to ensure delivery of critical services.
- Detect, develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- Respond, develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- Recover, develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due toa cybersecurity incident.

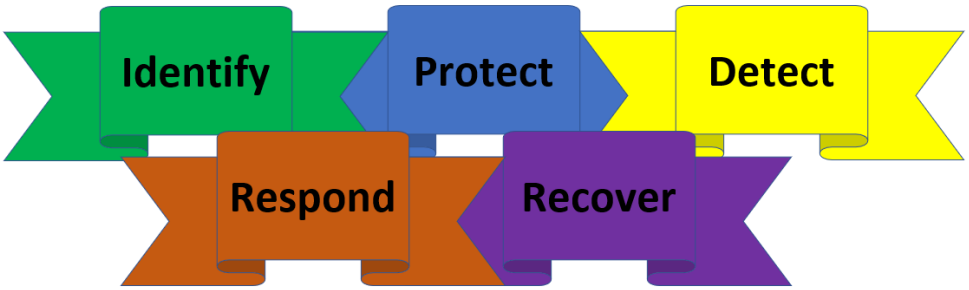

Figure 5. NIST CSF five core functions visualized

NIST CSF gives a good overview of cybersecurity frameworks function within organizations and what the objective for increasing security is from them. Even though NIST CSF focuses primarily on infrastructure, even it includes cores linked to the internal human element. In the function “Identify” when analysing risks, risks to people within the organization are also considered as stated above. Another crucial aspect to do with the internal human element comes from the function “Protect” where NIST explains as one of the outcome categories to be “Empowering staff within the organization through Awareness and Training including role based and privileged user training” (NIST 2018). This training and raising awareness of staff is something that many cybersecurity frameworks include independent of what security aspect the framework is designed more to protect.

One framework that is also well known that takes the internal human element more into consideration is the ISO 27001 (full name is ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements) (Advisera 2020). The ISO 27001 was published by two well-known organizations that develop international standards: International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). The ISO 27001 has controls (safeguards) as a part of its framework that focus on the human element in cybersecurity.

The structure of the ISO 27001 is relatively complex, for this research Annex can be interpreted as “chapter” and control can be interpreted as “guideline within that chapter”. ISMS online has explanations used for the Annexes and controls in the ISO 27001 talked about in this research (ISMS online 2021).

Examples of ISO 27001 Annex A Controls include Annex A.6: Organisation of Information Security, which goes over the information security of the organization internally. This includes a control for defining security responsibilities within the organization and making sure the responsibilities are handled (A.6.11) and another control is the segregation of duties for conflicting areas of responsibilities or interests in order to protect against the internal human element (A.6.1.2).

The framework includes an Annex focused on the human element titled “Annex A.7 – Human resource security” which objective is to make sure employees suit their roles within the organization and comprehend their responsibilities. This Annex goes over screening employees for their tasks (A.7.1.1) and making sure employees are aware of their responsibilities in regard to IT security (A.7.1.2). Other controls, such as disciplinary processes (A.7.2.3) and management responsibilities (A.7.2.1) are also determined in this Annex.

As a part of the Annex A.7: Human Resource Security, it contains the same idea of educating and making sure the staff is aware of their role in IT security as discussed in NIST CSF in the form of a control named “Information Security Awareness, Education & Training” (A.7.2.2). The role of this control is to ensure employees are able to perform their tasks securely whilst minimizing IT security risks affiliated with those tasks by giving employees education and awareness to the IT security threats present.

The ISO 27001 has multiple other Annexes and controls involving the internal human element such as limiting access to information from employees based on needs (Annex A.9: Access Control) and even limiting access to physical locations based on security threats (Annex A.11: Physical & Environmental Security).

Frameworks in combination with risk assessment charts can be used in organizations to manage risks and threats related to the internal human element within organizations. Good frameworks such as the ISO 27001 exists to help organizations prepare better threats discussed in Chapter 2.2.

3 Examples of human element related IT security incidents

To properly list IT security threats that originate from or involve the internal human element in organizations this research gathered known incidents from different sources and compiled important ones in order to give examples of real cybersecurity incidents involving the internal human element. In each of the methods used to gather data, this research will justify the methods for using those channels for data and examine which category of threats they belong to.

3.1 Case studies and literature

Cybersecurity is taken very seriously through different great powers, such as the EU. When cybersecurity is breached, the organizations can't withhold the information in order to save public relations but must report the situation as stated by the European Union Agency for Cybersecurity "A cornerstone of European Union cybersecurity legislation (mandatory) is cybersecurity breach reporting. Cybersecurity breach reporting is important not only for the public but also to help national authorities with their supervision tasks, to understand cybersecurity trends, cross-cutting issues, weaknesses in the sector, etc., without having to rely on just media reports, which may not always give a balanced view." (European Union Agency for Cybersecurity 2020).

The first source of examples of cybersecurity incidents involving the human element are from case studies and other sources of literature. These example incidents focus on incidents which are fairly well known in IT security. The benefit of examining incidents which have either case studies on them or are part of literature is that they are well recorded.

3.1.1 Malicious intent

A case study by Lorenzo Carrazana titled "The Economics of Cybersecurity and Cyberwarfare: A Case Study" discusses a massive cyberattack called notPetya (Carrazana 2018, 3). The cyberattack was made possible due to the internal human element, discussed later in this chapter, but first it is important what the attack was and what it affected. In the case study Lorenzo goes on to explain that notPetya was a cyberattack originating from Russia which aimed at harming the Ukrainian infrastructure. The attack itself took place in June 2017 and is categorized as an cyberattack directly aimed at a country. Whilst cyberattacks by and against countries do occur, they are rarer due to the severity of the attacks. Even in these cases, much can be learned by organizations on how to defend themselves against threats involving the human element by examining what happened, and how it was preventable.

The cyberattack was aimed at Ukraine and Lorenzo's case study explains the aftermath as follows "Ukraine, however, was devastated by the virus. In a matter of hours, an estimated 10% of all computers in the country were destroyed. The attack affected several hospitals, banks, airports, and credit card payment systems all throughout the nation." (Carrazana, 4). To take a deeper look at how this affected single organizations, Lorenzo examines Maersk, a shipping and logistics organization. When examining how much this cyber-attack cost the single organization, multiple sources such as Wired (Greenberg 2018) and Data Insider (Lord 2020) report the cost of damages to around 300 million US dollars for Maersk. The total cost of damages resulting from notPetya is uncertain due to large amount of parties affected and not all parties disclosing data. Maersk has been very open about the cyberattack to the public hence examining it from their perspective gives a good view into the situation from a single organizations point of view.

One year after the cyberattack occurred Maersk hired a new Chief Information Security Officer called Andy Powell (Schwartz 2019) and he has done public talks discussing the matter of Maersk and notPetya. In one of his talks, he discusses the origins of notPetya and how it affected so many organizations and computers (Powell 5 December 2019). The malware (wiper, not ransomware as it did not offer decryption services in exchange for monetary value), affected the computers and servers that it did by travelling in a Ukrainian tax program, M.E.Doc, that was mandatory for organizations working in Ukraine. The malware was able to spread by an update the tax program and permanently encrypted the infected hardware's.

Andy Powell publicly stated on December 5th, 2019, in black hat Europe 2019 panel how the malware was able to travel through M.E.Doc by saying "It was through the M.E.Docs application that notPetya was spread. Basically, an individual within the company, who provided the software, was we believed coerced or blackmailed, sorry, or bribed, some months before to provide the credentials to enable a third party to insert the malware into the next upgrade into M.E.Docs and it was that upload that then caused what happened. But anybody who thinks it was some smart front door methodology to get it in, it wasn't. As we understand it, it was coercion or bribery through an individual user." (Powell 5 December 2019).

This is where the internal human element of organizations in IT security can be noticed and threats like this need to be prepared for. This massive cyberattack was a result of malicious intent from an individual human within the organization, whether he was blackmailed or bribed is uncertain but the cyberattack was only able to happen due to actions

of the organization's internal human element. Protecting against malicious internal actions is extremely hard but there are solutions to try to cover these threats and prevent similar events from happening in the future to other organizations.

One of these methods to prepare for malicious intent and to also reduce human error is the four eyes principle. The four eyes principle can be explained by having more than one person being accountable for certain decisions or changes for example, this is done to increase probability of catching errors and making important decisions not be based on an individual employee (Weatherill 2017).

3.1.2 Social engineering

As discussed in Chapter 2.1 social engineering attacks on organizations have grown in popularity over the years. The book by Gawin Watson, Andrew Mason, and Richard Ackroyd "Social Engineering Penetration Testing" lists multiple techniques of manipulation in social engineering such as impersonation, baiting, gaining credibility, emotional states, and body language to name a few (Watson, Mason & Ackroyd 2014, 39). These techniques have been used in multiple social engineering attacks over time.

Social engineering attacks can happen in a multitude of ways, of which the most common is phishing (example of this in Chapter 3.2.2) where, for example, someone pretends to be someone else over email as an attempt to gain access or information that is not open to the public. Social engineering attacks however also have more techniques which will be discussed with examples in this chapter.

The technique of impersonation has been used in more elaborate ways in the past to gain classified knowledge. This technique is explained by Watson as follows "The vast majority of social engineering pretexts will involve an element of impersonation. As previously mentioned, this impersonation need not be of a real individual, instead it will likely be a character specifically designed for the pretext." (Watson & al. 2014, 42).

A social engineering experiment done by Thomas Ryan (white hat hacker) from Provide Security already in 2009 used this method of impersonation and creating a fictional character as a method to gather intel (Ryan 2010, 3). He created a social network presence for the fake character Robin Sage with the title Cyber Threat Analyst and befriended security experts to increase Robin's credibility according to Ryan (Ryan 2010, 4). After having expanded Robins social network connections Ryan used the fake account to gather information that was not open to the public.

According to Washington Times in 2009 he was also able to cover military information regarding the location of troops on patrol in Afghanistan with embedded data sent to Robin in a photo from a soldier (Waterman 2010) and sensitive information such as this gathered through social engineering can cause immense security threats. These type of highly thought out, customized, and well executed social engineering attacks can be targeted at organizations and the internal human element is the target of these attacks.

This shows that social engineering attacks have been around for a long time and can be more complex than just an individual email. Some social engineering attacks have multiple phases and are not always even only limited to technology but can happen in person. When it comes to defending against such attacks, multiple methods should be used to increase cybersecurity. One of the methods that can help protect against social engineering attacks is use of MFA (multi-factor authentication) (Whitney 2020). This means that even if account information is leaked outside of the organization, the malicious attacker still cannot access sensitive information without the MFA tool from the employee. Whilst this does not always prevent account information from potentially being leaked, it gives the organization time to react to the leak and increases chance to prevent it from happening. With MFA being the technological solution the IT threat the other method of protection is informing the internal human element that everyone plays a vital role in the organizations security and proper training as discussed in Chapter 2.3.

3.2 News and existing guides

Even though case studies and literature give good examples of security breaches with analysis on the incidents, other sources also offer valuable information when planning defence strategies. One source which also covers a lot of security breaches is the news. News can give important information about the trends happening in IT. Hence it is important to examine which news articles involving the internal human element have happened either recently or when they happened, gathered a great deal of interest from the public.

3.2.1 Human error

Individual employees in organizations are prone to mistakes and sometimes the consequences of these mistakes can be quite severe. This is visible when examining news even from recent times such as BBC's article from September 2020 "Coronavirus: 18,000 test results published by mistake" (BBC 2020). In the article BBC states, "The health body said the data of 18,015 Welsh residents was viewable online for 20 hours on 30 August." and

goes further to explain that information leaked by accident included things such as “initials, date of birth, geographical area and sex” (BBC 2020). Whilst these pieces of information alone might not be enough to identify each of the over 18 000 people, this is still highly confidential information that should not have been accessible to the public.

In the article BBC also explain how the error occurred by stating “The incident was the result of ‘individual human error’ when information was uploaded to a public server searchable by anyone using the site.” (BBC 2020). In this case the internal human element (employee) caused a data breach by accident, but this breach could have been avoided with more preparation from IT security department. Fail-safes for human error in IT systems are a good line of defence, they can automate certain aspects of IT security and this is an example of where it would have proved greatly useful. When handling sensitive data such as ones listed by the European Commission “genetic data, biometric data processed solely to identify a human being, health-related data” (European Commission 2019), the method of processing and storing the data at any given point must be well defined.

An example of how this breach could have been better prepared for is using stricter policies in Windows server environments with File Serve Resource Manager (FSRM). Microsoft explains file classification in the FSRM as follows “File Classification Infrastructure provides insight into your data by automating classification processes so that you can manage your data more effectively. You can classify files and apply policies based on this classification. Example policies include dynamic access control for restricting access to files, file encryption, and file expiration. Files can be classified automatically by using file classification rules or manually by modifying the properties of a selected file or folder” (Microsoft 2018b). With these policies the files could be protected more with encryption and restricted access to the files. In this case had the file been encrypted, even if the file had been published the encryption would have kept it from being viewed. More methods to protect against such cases where someone accidentally leaks classified information are discussed in Chapter 4.7.

3.2.2 Phishing

One news subject regarding internal human element and data security within organizations that has been around for a long time is the subject of phishing attacks. “Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the

freezing of the system as part of a ransomware attack or the revealing of sensitive information."(Imperva 2020). The origin of this data breach is external but what causes actual harm is the actions of the internal human element by ways of granting access or downloading something malicious with no intent of doing so.

In March 2016 Trend Micro published an article called "Spear Phishing Attack Exposes Tax Information of 3,000 Community College Employees", which goes over an incident where a single employee fell for a phishing attack which resulted in over 3000 employee's personal information being compromised (Trend Micro 2016). The article explains the chain of events for the data breach as follows "an email was sent by an employee to an unknown recipient that seemed to have come from a legitimate TCC account. It was then identified that the request was a ruse and that the file containing the employee tax information was sent to a cybercriminal-controlled account—a classic spear-phishing attack tactic."(Trend Micro 2016).

In this news article the phishing attack originated from an email which seemed to come from within the organization. In order to protect against this the IT security department could set up DMARC which creates policies in the DNS (Domain Name System) that prevent people from spoofing your domain in an email. DMARC's website explains it as follows "DMARC, which stands for 'Domain-based Message Authentication, Reporting & Conformance', is an email authentication, policy, and reporting protocol. It builds on the widely deployed SPF and DKIM protocols, adding linkage to the author ('From:') domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, to improve and monitor protection of the domain from fraudulent email."(DMARC s.a.). National Cyber Security Centre, NCSC, also recommends organizations take a multi-layered approach to the defend against phishing consisting of four steps (National Cybersecurity Centre 2018):

1. Make it difficult for attackers to reach your users
2. Help users identify and report suspected phishing emails
3. Protect your organisation from the effects of undetected phishing emails
4. Respond quickly to incidents

The combination of National Cyber Security Centres steps, recommendation of setting up DMARC and relying more on technical measures as stated in their guide, "Typical defences against phishing often rely exclusively on users being able to spot phishing emails. This approach will only have limited success. Instead, you should widen your defences to include more technical measures." (National Cybersecurity Centre 2018) will provide organizations with a greater defense against phishing attacks.

3.2.3 Environmental security

A lot of IT security guides and handbooks already exist which compile many of the most prominent IT security risks. These are created by professionals in the field and provide good examples of threats involving the internal human element. These guides warn about physical security breaches that employees can also cause with their actions, an example of this would be piggybacking (also called tailgating). This is explained in the 2006 “Information Security Management Handbook” edited by Harold F. Tipton and Micki Krause as follows “Physical piggybacking is a method for gaining access to controlled access areas when control in accomplished by electronically or mechanically locked doors. Typically, an individual carrying computer-related objects (e.g., tape reels) stands by the locked door. When an authorized individual arrives and opens the door, the intruder goes in a well.” (Tipton & Krause 2006). In other terms the person without access to areas, tricks employees to hold the door for them so they can access restricted areas.

This is a type of social engineering, tricking employees to allow potential threats to secured areas. With this method unauthorized people can gain access to for example server rooms, which can cause massive security threats. The reason employees hold the door open even to people they do not personally know is out of courtesy, in the words of Jean-Jacques Rousseau “Man is naturally good”, since the person holding the door open has no ill intent, they expect the person following them to also have none. This is something criminals and people with ill intent are aware off and take advantage off.

Many IT security organizations realize this threat and are aware it is hard to counter fully hence incorporate it into IT security training. F-secure for example has used this method to test organizations IT security and has gained access to restricted areas. They have openly talked about it on their podcast as follows “We also did an exercise where we were tailgating people, having somebody open a door for us and walking in after them, and when somebody did that and didn’t challenge us, we’d give them a flier, like ‘*Here’s a flier, check it out when you have time*,’ and the flier was like ‘*You just got tailgated, and this is how that happens, and don’t let it happen again*.’”(Michael 2019).

There are multiple methods organizations tackle the security threats of physical tailgating, ranging from educating employees about the risks of it, using photo IDs, hiring security guards to monitor entrances, video surveillance, etc. The most effective combination would be to implement many failsafe’s and to educate the personal on the reasoning for the security. Having more checkpoints at a workplace can be inconvenient but increases

security. One of most effective tools against tailgating are physical checkpoints, usually at entrances, that limit access to one person per valid access code (for example ID card).

3.3 Other cases

The previous sources of IT security threats discussed more noticeable topics in IT security, hence the topics have had news articles, case studies and existing guides to cover them but there are also other security threats which can still have impacts on organizations IT security. This chapter focuses on other threats involving the internal human element.

3.3.1 Lack of training

Encryption for example can used as tool to store confidential data, by requiring a key to access said data. When done intentionally, correctly, and with no ill will, it can provide a significant security benefit to organizations data. An example of encryption being used in a harmful way is ransomware, which is described by Cybersecurity & Infrastructure security agency as “Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.” (Cybersecurity & Infrastructure security agency 2021).

Sometimes encryption can also cause problems, even when the person doing the encrypting has no ill intent. This can happen in organizations when an employee handles important data on their work computer, for example on a laptop, and wants to ensure that the data does not get into the wrong hands. The employee might take the security risk into their own hands and decide to encrypt their work computer by themselves. This creates several problems, the most noticeable being that if they forget the key to access the computer, none of the locally stored data is accessible.

Another problem is that if something happens to the employee, for example an unexpected tragic coma, then the organization has no way to retrieve the local data for his replacement. This can also happen if the person in charge of IT security implements security solutions without proper training. If the employee in charge on encrypting organizations computers does not standardize how it is performed, then the same threats may come to fruition as when the individual employee performs it.

The way this issue can be combated within organizations is with proper communication and training towards the potential security risk and structured solutions towards IT security

threats. The IT department can offer or force encryption of work computers when handing out computers to employees and explain the security benefits for both the user and organization. This requires the IT department has a proper plan and methodology to implement security features such as these (such as use of frameworks). When the encryption is handled by a well-trained IT department, then it is more organized and standardized and prevents accidental loose of data on work computers due to lack of training.

Other technological solutions can be used to tackle these sorts of issues. In this example, the organization computers could only work as way to connect to instances on servers, where all the data is stored. This way if something happens to the physical computer, the data can still be accessed by another computer with correct credentials and said data is encrypted on the servers.

3.3.2 Human psychology

Humans' moods are affected by a magnitude of different factors and employee's mood can affect how they handle potential security threats. If an employee is stressed or tired, they may be more likely to click a phishing email than if they were well rested and happy (University of Central Lancashire 2020). Preparing for situations like these require different approaches to the IT security threats. Examples can be automating certain aspects such as discussed with phishing and training employees well enough on the importance of IT security so that even in moments when they are in an optimal mood, they still have the idea of IT security in the back of their mind.

One potential problem with the employees' moods is also in regard to how the employees handle problematic situations. If for example a file is not opening on the employee's computer this can cause frustration. If the employee is already tired and overworked, the potential IT security threat could arise from the employee not handling the situation via the correct channels but rather trying to fix problem themselves or not reporting the issue at all. If the file or program the employee is trying to access is critical for their, or potentially also others, work tasks and tries different solutions to quickly fix the situation instead of going through the proper channels then there is the potential of loss of data, depending on what the employee attempts and how it turns out.

Even if employees actions either by accident or due to their actions whilst frustrated result in loss of data, there should be proper counters for these situations from the organization. These can include alternative methods to access programs or backups of important data that even if an IT security incident involving loss of data occurs, the data can still be retrieved from another source or recovered after.

In certain cases, technological solutions can be used as tools to even relieve stress from the employees or lessen their workload when implemented correctly which in return can result in heightened IT security from the employee as discussed before. Solutions such as these could be automated systems automatically removing some portion of phishing emails, reducing the time the employee has to spent on emails or providing knowledge that their data is safely secured with backups possibly resulting in reduced stress from the employee. The solutions cannot counter all IT security threats so the internal human element still plays a vital role but examples such as these show how they can work better together.

4 Interviews on the human element in IT security

This segment of the research first goes over who were interviewed, the reasoning for choosing these professionals, how the interviews were conducted, the structure of the interviews and questions used in the interviews. After this, the topics discussed in the interviews are broken into smaller chapters, examining the professional's opinions on the topics.

4.1 Information about interviews

Interviews in this research were conducted after other research methods used previously had been completed. The purpose of the interviews was to gain an additional perspective on the matter of internal human element in IT security and to see how people working in the field of IT security comment on matters discussed so far in the research. Four people were interviewed as a part of this research and the people were chosen based on their current roles in IT security. The job titles in this research are also written in Finnish to avoid any translation errors, since the official titles the interviewed have are in Finnish. The four peoples job titles and industries they worked in were as follows:

- **Chief Information Security Officer (**Tietoturvapäällikkö) in an organization specializing in information management, information security, and data protection. Works in IT industry.
- **Director of Development** (Kehityspäällikkö) who handles information security and data protection in a Finnish IT service company. Works in IT industry.
- **Information Security Specialist** (Tietoturva-asiantuntija) in a University of Applied Sciences. Works in education industry, performing IT tasks.
- **CEO** (Toimitusjohtaja), safety device installer (turvalaiteasentaja) in a smaller company providing on location security such as surveillance and alarm systems. Also works as Senior System Specialist in an organization providing ICT-solutions. Works in security industry and also performs tasks from IT industry.

The intention with these interviews was to have people working in different aspects of IT security to better cover IT security as a whole. Two of the interviewed are in organizations in the IT industry and their jobs focus on IT security, this was to make sure IT security professionals' opinions were included as a part of the interview segment in this research. One interviewed was contacted by emailing a Helpdesk in a University of Applied Sciences in order to try and compare with the organizations working in the IT field previously mentioned. The fourth interviewed was chosen based on the research done so far and the importance of physical and environmental safety in IT security. These four people were chosen for the interviews in order to gain answers and opinions on the subjects discussed from different perspectives to form a more comprehensive picture.

The interviews were all held on week 11 of 2021 and were done over Microsoft Teams. The structure of the interviews was semi-structed, which can be explained as allowing more conversation on topics based on the interviewees wants when compared to a structured interview (Brinkmann 2013, 21), this also allowed the interviewer to ask clarifications on certain answers. The interviews were one on one between the researcher and the person being interviewed and durations ranged from around 35 minutes to about 60 minutes, depending on interview. The interviews were recorded, with permission from people being interviewed, in order to listen back to interviews later to more accurately quote and phrase answers discussed in this chapter.

The interviews were conducted in Finnish and the questions asked are listed in this research's appendices as "Appendix 1. Interview questions". The interviews did not always proceed in the same order as in the appendix as the questions sometimes opened good discussions that lead to other questions in the appendix and follow up questions were asked then. Despite the structure being more open than a list to go through, all people interviewed were asked about opinions on matters discussed in the questions list.

The classification of the interviews was chosen to be individual interviews due to benefits it provided this research. The benefits individual interviews provide are that it allows the interviewer to keep the conversation to subjects relevant to the research and allows more confidentiality when studying sensitive subjects (Brinkmann 2013, 27). When dealing with IT security, conversations may come close to sensitive information and semi-structured individual interviews allow interceptions and comments at those points, so no party feels uncertain of what is allowed to be used in the research. Since the scope of the topic is the internal human element in IT security, individual interviews also help keep the conversation on said topic. The styles of the interviews were receptive interviewing, this can be explained as the interviewee being asked relatively few, open ended questions that they are free to answer in the way they see best fit (Brinkmann 2013, 31).

The reason the interviews were limited to four people rather than a large group of people is to do with the nature of the interviews as discussed above, the thematic analysis of the semi-structured individual interviews would be more accurate if it focused on finding common themes and opinions from professionals directly involved with IT security in their professional life's rather than increasing the quantity of interviews but losing the expertise opinions on the topics.

4.2 The internal human element

When asked what the most important aspects and elements of IT security as a whole were from the people being interviewed a key element that was repeated in the answers was proper preparation and planning of IT security. A common theme in the answers was that it is not just a requirement for software, but rather structured planning and that it needs to be integrated into the organizations culture. The aspect of IT security being part of an organizations culture for IT security to be more effective was a theme that occurred in several of the questions throughout the interview, especially from the two interviewed working with IT security in the IT field.

Overall, all interviewed stated human element playing a role in IT security at some point in the interview. An example of elements in IT security was offered by one person in the form of layers. The lowest layer consisted of technology and systems, the next layer consisted of administrative processes (how devices maintenance and life span is taken into account for example), the last layers were to do with how management interacts with IT security and what should be in done in regard to IT security in the future of the organizations (for example a half year and two-year plan).

Already in these answers the human element played a role within organizations IT security in the form of organization culture, management decisions regarding IT security, and one person saying the human element being up to half of information security.

Next the interviewed were asked specifically about the human element in IT security and how big of a role it plays in the organization's IT security in their opinion. All interviewed answered human element playing a large role in IT security with two directly saying that is also the one of the most vulnerable parts of it. The two who said it was one of the most vulnerable parts, said it was usually the easiest way for attackers to get classified information from organizations via for example phishing.

Overall, from the discussions the role of the internal human element in IT security seemed to play an important role. One of the ways it plays an important role was through the leadership within the organization and how management handles IT security within the organization. This was an aspect not heavily discussed so far in this research and the importance of managements perspective on IT security within the organization, whether it is something that is included in all aspects of operations or more of an afterthought was clearly an important factor in IT security.

4.3 Different threats

Next the threats involving the internal human element from Chapter 2.2 were discussed. There was a lot of common consensus for the threats regarding the likelihood and impact of them from all interviewed. The order the threats were discussed varied depending on the conversations in the interviews but in this research the answers and opinions about the threats are gone over in the following order: human error, social engineering, phishing, malicious intent, and other.

With regards to the human error from employees in IT security, the threats revolving these were considered highly likely to happen and depending on incident, able to cause considerable damage. Since this is the case in the field of IT security and this threat seemed to be well known, many methods to counter these are already in place to mitigate damage from these threats. These methods range from IT solutions such as programs limiting access to certain files even if a link is provided, for example if the link were to try and be opened by someone outside of the organization (based on for example IP or user ID for log in session), to solutions involving how different processes are handled.

The methods of how processes are handled, such as change management, involved precautions such as having more than one person work on changes and having predefined procedures in place for more risk associated tasks. This is done to mitigate risks from human error but has the downside of increasing the workload of certain tasks. One interviewee connected this back to the culture of IT security in organizations and how organizations and employees are more willing to spent additional resources on tasks such as these when IT security is part of the culture within the organization.

The threat of social engineering, in this case more focused on physical and environmental security, with the example of someone being dressed as a maintenance worker and trying to get access to workstations or server room was discussed with the interviewed. The focus was on how the internal human element, employees, would react in situations regarding environmental security. Overall, the opinions of the interviewed were that the likelihood of a threat where someone dresses up a certain way to try and gain access from the employee to restricted areas, was not as likely to happen as the other threats discussed in the interviews.

This topic was heavily discussed with the safety device installer, due to his connection to the topic. The onsite safety and how well employees personally look after securing their workstations might not always be linked to the industry they work in, however places such

as datacentres are highly unlikely to fall for these type of security incidents. Based on the interviews, it did not seem too uncommon for employees to keeps doors open for strangers out of politeness if the person following them exhibited polite signs such as smiling. Throughout the interviews other factors were discussed in regard to what factors into the employees on whether they for example keep doors open to people they do not personally know. A link between how often employees interact and are reminded of IT security in the organization was discussed as a potential factor on how they handle situations such as these, again coming back to the culture of IT security within organizations.

On the topic of phishing, it was obvious from the answers provided by the interviewed that phishing plays a large role in IT security, especially these days. All of the interviewed placed phishing as one of, if not most, common security threats within organizations and emphasized it happening all the time. One of the interviewed mentioned that it is not a case of if organizations get phishing attacks but rather a question of when, and for many the case is that they have already encountered such attacks and incidents.

A key fact many of the interviewed presented was that phishing attacks nowadays are more sophisticated and harder to spot. They gave examples of old email phishing attacks where an email written in poor English with a dodgy link to a site that seemed off was provided and compared it to the phishing attacks organizations deal with currently. Currently the phishing attacks can consist of well written, very specific emails, seeming to originate from trusted sources with links to real looking websites that sometimes even update their visuals via help of bots almost in real time compared to the websites they are trying to imitate. The current level of phishing attacks can be very hard to spot and can be targeted at almost anybody, increasing the risk that someone will fall for it. In the interviews they also said that technology cannot prevent all the phishing attacks and the internal human element will face these threats.

The general opinion from the interviews seemed to be that awareness and training on the matter of phishing attacks is crucial to help prevent incidents from happening since the likelihood for these attacks is extremely high. There were also opinions that employees are relatively familiar with the concept of phishing attacks already due to the popularity of the attack, which helps reduce incidents from them.

Malicious intent from employees was not considered very likely to happen based on the interviews and the reasoning for this seemed to be how recruitment is done in organizations and the overall aspect of human nature. Two of the interviewed specified that background checks when hiring and safety procedures such as deactivating credentials when

someone's employment ends, further help reduce the risk from malicious intent. One comment suggested higher risk of malicious intent in industries where the rate of change for employees is higher but overall malicious intent did not seem to be very likely according to the people interviewed. This said, they opinionated that just because it is not likely to happen, it is still something that must be prepared for. The methods for these ranged from recruiting and termination procedures listed above, to proper logging of user activity and one interviewed used the risk assessment chart where he gave an example of probability to happen being 1/5 and risk being for example 5/5 to be used to determine what resources are spent on the threat.

When asking about other threats involving the internal human element, two new threats became apparent that had not been heavily examined in this research prior to interviews. The first of these threats is the potential lack of managements and partly employee's role of integrating IT security into the organizational culture. When IT security is not considered when making decisions, this can lead to more threats, not just ones to do with human error, but also resource allocation and how small day-to-day tasks are performed. The second threat is employees' actions outside of their work life, what they share on social media, how they act on the internet, and things such as using same passwords for personal accounts as work related accounts.

4.4 Organizations perspective on human element

Based on the interviews done for this research, organizations do not generally take the internal human element factor into consideration enough in regard to IT security. Many of the interviewed responded as this being something many organizations could improve on and one said that in their opinion it is getting better over time but there is still a lot to improve on a general level. One point of topic that was uncovered was the fact that it is not always tied to the industry the organization works in. In some cases, organizations working in the IT field fail to include the human element in their IT security adequately whereas organizations working in other industries/fields might be taking it into consideration very well. It is way more dependent on the organization itself, rather than the industry it works in.

Another key opinion that was brought forth via the interviews was on how the organization size affects how well they take the internal human element into consideration. Points were made for both benefits and hardships of larger organizations. Generally, the people interviewed viewed that larger organizations have better resources to train and raise of awareness of employees, with people or teams dedicated to the tasks. However there are also

problems with having many employees at different locations which makes the logistics of raising awareness and training harder.

Another opinion stated in the interviews was that unfortunately some organizations still view IT security as something related to IT solutions primarily, such as having up to date firewalls. A point of concern from two of the interviewed was that even when organizations consider the human element of IT security, they do not reinforce it enough. Based on discussions IT security for employees would ideally start as soon as someone starts working in an organization by being part of the briefing and being built on over time with reminders, more awareness, training and overall being integrated into the work culture, instead of there for example being one general meeting about it per year by the organization.

4.5 Employee's awareness and role

Organizations generally not taking the internal human element enough into consideration in their IT security seemed to directly reflect onto how employees view their role in it and how aware they are of it. The interviewed viewed that employees on a general level do not consider their role in IT security enough and this leads to security threats. One said that especially the further the employee's tasks are from IT and IT security the bigger the separation of including yourself, from employees' point of view, in them can be. An example he gave was someone working in logistics, who has access to very restricted information and the fact that they do not associate themselves with IT security is a real security concern.

Topics such as what training for employees should be and what it means when they are aware of their role were discussed. An opinion one of the interviewed stated was that if an employee stops what they are doing and considers if it is a security risk, then that already is a great position to be in. This could count as awareness for the employees and one other mentioned in the interview that if employees are not trained to handle security threats and what channels to report them by, then they do not have the proper tools to intervene. So, if an employee stops their day-to-day tasks to question whether something is a security risk and then reports it via the official channels, then that would be an ideal situation to be in.

Based on the interviews, it seemed like employees are commonly willing to include the aspect of IT security in their work life if it is presented to them well, the importance is explained, and it is connected to the culture of the organization.

4.6 Challenges with the human element

One of the difficulties surrounding IT security discussed in the interviews was that IT security, often times, is only as strong as its weakest link. This combined with the findings from Chapter 4.2 leads to one of the biggest challenges with the human element in IT security, it plays a big role and affects all employees within an organization. One of the examples an interviewed gave, was that if a classified document is printed and left at your workstation, no matter how good the firewalls are, anyone who has access to that workstation can take the information. This example gave good insight into how dealing with IT security threats involving the internal human element require solutions much more complex than just IT solutions. As discussed in the interviews and Chapter 2.3, IT solutions are a massively useful tool in IT security even when dealing with the human element, but they alone are not enough.

From the interviews, the need of individual employees to understand their role in IT security and awareness of risks they face seemed to play a big factor in overall improved security. This goes back the to point of IT security being part of organizations culture, which based on interviews, is one of challenges with the human element in IT security. One interviewed also said that the human element and technological solutions should work together to provide better security.

Other challenges mentioned that supported the need for IT security to be part of the organization's culture were getting employees to report security risks, even if they themselves caused it, without fear of being found out that they had an accident. From the answers and discussions had during the interviews, this one point, integrating the culture of IT security into organizations, seemed like the biggest challenge with the human element in IT security whilst also providing the most benefit when done correctly.

Other challenges with the human element were also mentioned in the interviews including finding a balance between IT security and how it affects employees' daily routines. Sometimes solutions can be presented but their impact on employees work performance or daily routines might be too costly. One interviewed made a similar comment and emphasized how if IT security is part of the culture, then people are more willing to use resources on it. Based on answers provided, balancing the impact of solutions and their effectiveness is still a challenge with the human element in IT security.

Organization sizes were also discussed in regard to challenges, whilst most of the interviewed found larger organizations generally having an easier time of including the human

element in IT security due to for example resources, some discussion was had revolving the possible challenges of the logistics of organizing such things.

The last challenge discussed with the human element in IT security was to do with outsourcing IT security or certain aspects of it. In general, based on discussions, outsourcing IT security and certain aspects of it in itself is not bad standard, quite the opposite, the interviewed stated that organizations who usually get outsourced IT security or aspects of it, specialize in those tasks and generally perform them well. The challenge with outsourcing discussed was more to do with the organization doing the outsourcing. Even if aspects of IT security are outsourced, the need for organizations to still be aware of how those aspects are handled and not try to outsource all the responsibility or actions required became apparent from the answers.

4.7 Effective methods and tools

When asked about effective methods and tools with regard to the internal human element in IT security, one important aspect discussed was integrating IT security into the organizations culture. This has been part of previous topics in chapter and the importance of it throughout the interviews was very apparent, and hence should be empathized also here.

From the interviews different methods for achieving increased IT security involving the human element were presented such as frameworks. Two of the interviewed, both working in IT security in the IT field, mentioned ISO 27001 without it being part of previous conversations or questions regarding frameworks. This, in combination with the fact that many answers reflected certain Annexes in the ISO 27001, leads to the conclusion that ISO 27001 is a strong tool to help protect organizations with regards to threats involving the internal human element based on the interviews. One of the interviewed mentioned frameworks as something that organizations should not just implement in order to check a box in their security or just for the sake of gaining a certificate but rather organizations should know what they are implementing and why. Discussion was also had about combining different frameworks, only using parts of frameworks in situations where needed, or as a foundation for developing IT security, depending on the organizations needs and not just always following one framework.

Another effective tool mentioned by one of the interviewed was using risk assessment charts to identify, prioritize and prepare for different risks. Many of the answers revolved around the training of employees and what good practices for it are. One interesting as-

pect brought forth by one the interviewed was to ensure the employees are genuinely interested in the topic of IT security by giving real life examples and referred to a lecture held by F-secure where F-secure discusses security incidents they had dealt with.

Another aspect discussed in regard to employee training was the repetition of the training and awareness. Many of the interviewed gave this opinion at different points in the interviews and generally talked about how it should be part of employees work life often enough in order to become part of the culture. The methods to achieve this varied depending on person interviewed and included parts such as more structured organization plans revolving the topic, meetings with employees revolving around IT security often enough, memos and updates on intranet, and other tools to keep IT security in employees mind at most times even if they are not actively thinking about it.

Some discussions was had about possible connections between other aspects of organizations security such as camera surveillance, check points, procedures, etc. and the link to how well employees react to potential IT security threats but no confirmable conclusions could be made due to no quantifiable data present at the meetings during that time. Other effective methods discussed were how IT security must also originate from management and other notable people within the organization in order to spread effectively into the culture. One perspective from the interviewed was that if management and key figures within the organization are indifferent or careless towards IT security them most likely others are to follow.

During the interview's discussions were also had on physical and IT related solutions to threats involving the internal human element. In regard to the physical solutions, solutions such as separate locked trash bins for classified paper waste, minimization of paper usage, proper physical security for required areas and physical reminders for employees for example next to printers in the form of posters reminding employees not to leave documents and prints near printer after they finish printing.

In regard to IT solutions, one tool mentioned in multiple interviews was the use of MFA (multi-factor authentication), which based on interviews provides a very good layer of defence in regard to for example phishing cases where employees might accidentally give away their credentials. Other IT solutions mentioned in the interviews included tools used in certain environment such as Microsoft data loss prevention and Azure Information Protection, which can be used to scan documents for sensitive information and then set policies depending on information such as preventing accidental sharing of sensitive infor-

mation or forcing encryption if it handles sensitive information such as social security numbers. IT solutions were also presented in the form of monitoring user logins based on location and automating responses to certain events such as a user logging in from Finland one moment and minutes later logging in from some other country. Other IT solutions included tools for opening messages and links in an enclosed sandbox environment first to check for potential threats.

Discussion also included the human elements practices in handling certain events such as verifying emails by calling the person who sent the email, if there is any reason to doubt it and using bookmarks or the intranet to navigate to resources linked in emails. The practice of how easy it is for employees to report potential threats was also discussed by some to be an effective method for employees to report more risks, saying that if an employee had to come up with a way to report the threat, then they are less likely to report it compared to when channels are created for this purpose and employees are taught and reminded about these channels. Overall, many effective methods and tools were given by the four people interviewed and had the interviews been longer, surely more methods and tools would have been discussed.

4.8 Future of human element

The general consensus from the interviews about the internal human element in IT security was that it will keep playing an important role in it moving forward but technology will most likely keep advancing to help provide better IT security. Examples of how this has happened in the past were provided in the interviews with examples such as MFA and encrypting (or the rising trend of it) being technologies that over time have proven to help when dealing with threats involving the human element.

Discussion was also had about how AI and machine learning could be utilized in the future with threats relating to the internal human element and how that could change things, but it is impossible to say for certain the exact effects of it in the field. One interviewed also brought forth the opinion that people entering job markets nowadays have grown up with technology and it has always been part of their life to a heavier extent than some older generations in the work force, which could also affect the subject positively.

One interviewed also suspected that the awareness and importance of the human element in general will continue to rise with time as the human element’s role is recognized more and more research is done on the topic. The overall opinion seemed to be that there will always be risks related to the internal human element in the field of IT security.

4.9 Other important factors

When asking people interviewed if there were other important factors to consider regarding the internal human element of IT security, answers were given not discussed in this research until now. The first of these is to do with how IT security as a whole is a concept that has many regulations and laws revolving around it. This according the to the interviews helps the overall security a lot since it is not always something an organization can choose to neglect or decide to actively overlook since there are laws and directives regarding the issues. This also helps with the internal human element threats and how certain things involving them are handled even according to law. Despite this many of the interviewed noted that there are still simple IT security mistakes organizations make such as how passwords are stored and the actual strength of passwords, the laws are there to help but cannot control all security aspects. Another important aspect with organizations IT security overall was noted by one interviewed when he mentioned organizations not always even being aware when they need more IT security.

A “zero trust policy” was also mentioned by one of the interviewed, which had not been talked about before in this research, which he explained as employees not trusting links, emails and such by default but rather verifying information from other sources especially when it seems even a little suspicious as an important factor to increase security. When asked about the other factors, answers were given on how small acts such as little reminders like wearing ID badges or in some ways employees being reminded of IT security can go a long way in providing a better IT security overall. Other parts of effective tools and methods importance were emphasized at the end of the interviews such as management’s role in IT security culture, individuals’ awareness for IT security and overall importance of IT security culture in organizations.

5 Results and conclusions

This chapter goes over the findings in this research and how they correlate to the research questions asked in Chapter 1.1. The main objective of this research, as stated in Chapter 1.1, was to *find how the internal human element of organizations, employees, play a role in IT security and how the threats to do with this source can be protected against efficiently.* In this chapter the findings of previous chapters are combined for conclusions on the topic. This is done to make sure if the research problems were answered and if the research objective was achieved. This chapter starts by first analysing the findings regarding each of the research questions and then further analyses the conclusions reached with this research.

5.1 What are the threats

The main research question presented in Chapter 1.1 is: "*What are the threats within organizations involving the internal human element?".* The purpose of this research question is to prepare organizations better by knowing what the specific threats involving their employees are in regard to their IT security. This research sought answers to this question by examining both statistics of IT security threats in Chapter 2.1 and examining individual cases of security incidents in Chapter 3.

The findings from these chapters lead to giving examples of individual threats organizations need to prepare for, such as accidentally publishing classified information (Chapter 3.2.1) or an internal individual with malicious intent being able to allow malware into an update (Chapter 3.1.1). With further research it became more apparent that the research question as presented could not be fully answered. The number of threats involving the internal human element are numerous and listing them all out would not be an effective way to prepare organizations for them. This research found it more effective to categorize the threats to give a better overview of the threats as done in Chapter 2.2, instead of listing each threat individually, and explaining what the threats with the internal human element are based on existing frameworks, as explained in Chapter 2.5.

In addition to the categorization of threats in Chapter 2.2 and use of frameworks in Chapter 2.5 this research also analysed organizations threats based on the organization's current situations. This was done in the form of comparing how the organizations size affects their threats in Chapter 2.4 to provide a better understanding of where some of the threats may originate from and what the challenges with different organizations sizes might be. The findings from Chapter 2.4 indicated that smaller companies and organizations may

lack the resources and personal to keep up to date on the changing IT security environment and required methods to sustain well-structured IT security within the organization. This was further expanded upon via the interviews in Chapter 4.6 where the interviewed expressed similar opinions and also added the possible logistic problems of managing training on a large scale in larger organizations.

5.2 Overall affect

Another research question presented in Chapter 1.1 was: "*How big of a role does the internal human element play in organizations IT security?".* The significance of this question was to provide an understanding of how relevant threats involving this topic are. If the threats involving the internal human element are limited in quantity when compared to other threats such as ones originating from software bugs or injections, then spending more resources on the threats discussed in this research could be more unlikely, though this is somewhat also counteracted by proper use the risk assessment chart presented in Chapter 2.5. This question however aims to give a realistic view of the internal human element's role within organizations in regard to its portion of threats in IT security and the potential trends involving it.

The findings from this research indicate the internal human element having a large impact on the IT security of organizations. This is based on the quantitative data from Chapter 2.1 where it was stated that already in 2020 cyberattacks methods against organizations included forms of social engineering 59% of the time (Positive Technologies 2020a) and the qualitative data from the interviews in Chapter 4 during which two of the interviewed directly stated it being one of the most vulnerable parts of IT security.

In addition to the quantity of threats involved with internal human element in organizations, another important factor to consider when determining how big of a role the internal human plays in the organization's IT security is the severity of the threats. When using the risk assessment chart presented in Chapter 2.5, it is clear that even if the likelihood of a threat happening is low, if the impact is high then its role in the IT security is increased. Examples of where impact from threats involving the internal human was high are presented multiple times in Chapter 3. With the number of threats involving the human element and the threats severity at times, this research found the internal human element in organizations to play a large role in organization's IT security.

5.3 Preparing for the threats

The research questions' "*How can these threats be categorized and prepared for?"* in Chapter 1.1 role is to both bring more of a structured view to the threats rather just a listing of them and to present solutions to countering them. As discussed in Chapter 5.1 the number of threats was numerous and hence a list covering the threats would not suffice organizations as a way to prepare for these threats. The way this research countered this was by categorizing the threats into groups based on their origin in Chapter 2.2. This research found there to be 5 main sources of IT security threats involving the internal human element as listed below:

- Human error
- Social engineering
- Phishing
- Malicious intent (internal)
- Other

Each of these categories is explained further in Chapter 2.2 and the real security incidents involving them are examined in Chapter 3. The process of categorizing the threats was performed by analysing incidents recorded for this research and comparing it with the information gathered from the interviews in Chapter 4. Once the categories were created the main ones were listed as above and incidents from the categories were examined further in Chapter 3. The list serves the purpose of giving a better understanding to the possible threats as categories rather than individual threats since each category itself contains multiple different threats.

After categorizing the threats accordingly, the matter of the preparing for them is relevant. Where each security threat itself may be prepared for via certain tools or methods, such as the ones mentioned at the end of the incidents in Chapter 3 subchapters, this research came to the conclusion that preparing solely individually for each threat is inefficient. A better method is proposed in Chapter 2.5 in form of frameworks. This in combination with the information from the interviews in Chapter 4.7 lead this research to come to the conclusion that implementing frameworks in organizations tackles the issues from the macro perspective and gives a better structured way to prepare for the threats, instead of only focusing on the micro aspect of trying to counter each threat as a single entity. Frameworks work as a good structure to implement solutions and ensure most important aspects are taken into account. However, it does not remove the need for micro level actions but rather ensures the macro level is taken care of. Based on the research in Chapter 2.5 and the interviews in Chapter 4, one framework that takes the internal human element in organizations into consideration well and increases the organizations IT security revolving the internal human element in organizations is the ISO 27001.

Whereas the ISO 27001 was found useful in this research to handle the macro aspect, the solutions on the micro level were also examined. This research examined general solutions to threats involving the internal human element from the perspective of what qualifies as a good solution in Chapter 2.3 by examining solutions involving technology and solutions more focused on employee training. The result of this research was that employees are often considered the front line defence for threats involving the human element but solutions only involving training the employees do not provide the most efficient defence. The best defence based on the research done is the combination of the human and technological solutions.

The human solutions involve both training employees but also based on the interviews, getting individuals and organizations to consider IT security in their organizations culture. In this research this was found to have numerous benefits such as employees being more consensus of their actions from the perspective of IT security and management giving the required resources, time and money primarily, to projects to include IT security in their tasks.

The technological solutions were examined in Chapter 2.3 with the result of technological solutions providing often times a good safety net for organizations even if the threat originates from the internal human element. One of the best technological solutions covered based on this research is the use of MFA (multi-factor authentication). Based on this research it was found to be most efficient when the two, human and technological solution, support each other in the threat. The employee maybe trained to not open suspicious emails, but the technological solutions can reduce the number of times these threats occur or even limit risks associated with threats such as these. Examples of this are discussed in Chapter 4.7 in the form of tools helping prevent accidental sharing of classified information.

Another important factor this research concluded from the perspective of how to prepare for the threats is the aspect of how IT security should not be an afterthought but rather an ongoing process. This is discussed regarding the technological solutions in Chapter 2.3 and from the human element's perspective in the interviews in Chapter 4.2. This is also where the ISO 27001 would be a good addition based on the results of this research.

5.4 IT security incidents

The research problem, "*Finding examples of real-world IT security incidents where the internal human factor played a vital role",* was created to establish the correlation of the theoretical parts of the research to the real world cases. This was achieved by examining real world security incidents from each of the categories listed in Chapter 2.2 and going over how the internal human element played a part in the incidents, what the ramifications from the incidents were, and how the incidents could have been prevented. The security incidents were chosen based on their impact and relevance to the topics discussed in this research. Another reason for the research problem was to provide examples of what the negligence of not properly preparing for threats with internal human element can result in.

The results from this research in Chapter 3 proved the potential severity of IT security threats involving the human element. The cases in Chapter 3 show examples of this by examining the ramifications, for example personal data being leaked due to human error in Chapter 3.2.1, and 10% of Ukraine's computers being destroyed in Chapter 3.1.1.

Another aspect of the research problem was to choose interesting and relevant incidents for the research in Chapter 3. The interest of incidents is subjective, but this was attempted to be achieved by choosing incidents on certain factors such as scale of impact, relevance to research, likelihood and other factors. The final result for this research problem consist of examining the five cybersecurity incidents in further detail and covering two other sources of threats in Chapter 3. These cybersecurity incidents are used to further explain the research topic on a practical level rather than just a theoretical one and provide examples on how to counter possible threats as discussed in Chapter 2.3.

5.5 Conclusion

In the beginning of this research, in Chapter 1.1, the objective of this research was stated as follows: "*find how the internal human element of organizations, employees, play a role in IT security and how the threats to do with this source can be protected against efficiently".* Everything in this research has been performed to achieve the mentioned objective. Upon having all the information gathered for the research it is possible the state the findings and conclusions regarding this objective.

The first finding is to do with the nature of how the internal human element plays a role in the organization's IT security. In this research the role was first examined from the perspective of direct correlation to threats in the form of actions of the individual resulting in

security incidents. Whilst this plays a part in the internal human element's role in organizations IT security, this research also covered the involvement from a less direct correlation, IT security culture. The importance of IT security culture in organizations forming from the collective of individuals plays a large role in the overall IT security. It is through this, IT security being part of organizations culture, where some of the most efficient solutions and protections were found. If organizations are able to incorporate IT security into their culture effectively then based on the findings in this research, this can lead to both better resource management in regard to IT security and conscious IT security actions from individuals whilst performing their tasks. This research has however also come to the conclusion that achieving this in organizations is not a simple task.

In regard to the role of the internal human element in organizations IT security from the perspective of relevance, this research came to the conclusion that the importance of the internal human element in organizations IT security not only currently plays a large role, but there is a rising trend currently of cybersecurity incidents involving and targeting the internal human element. If this trend continues, then in the future the internal human element's role may continue to increase.

How organizations can protect against threats involving the internal human element in IT security and can be broken into parts. The first solution is from the macro perspective and is the use of a framework, combination of frameworks or parts of a framework to achieve a structured and systematic approach to the security threats involving both the internal human element and other factors. This in combination with a successful integration of IT security into organizations culture would prove great assets in protecting against the threats discussed in Chapter 2.2 based on the findings of this research. The large macro solutions could also impact small events such as how aware employees are of certain IT security threats and how they handle them if there is a larger presence of IT security within the organization.

The second part is from the micro perspective of how individual threats are handled. Individual threats should not be isolated instances, handled purely by a case to case basis without regard for the larger picture, but should rather be part of the macro solution, the framework when possible. When considering solutions for individual threats, often times automation of technological solutions working in harmony with the training of the human element is the best approach found in this research. The two were found to complement each other and provide a wider security net rather than relying on one or the other to prevent security incidents.

In conclusion, the internal human element's role in organization IT security plays an important role with trends indicating a possibility of its importance increasing. Whilst the solutions to prepare for and counter threats involving the internal human element are numerous and hard to achieve at times, there are tools and methods to help organizations increase IT security regarding these matters. One of the most important factors in achieving better IT security, in regard to the threats involving the internal human element, is for both organizations and individuals within the organizations to integrate the aspect of IT security into all aspects of their lives instead of IT security being an afterthought.

6 Discussion

This final chapter goes over how trustworthy the findings can be considered and what future developments could be done with both this research and on topic discussed in this research overall. This chapter also goes over how the research could have been improved and what can be done in the future for further research on the topic of internal human element in IT security. Finally, this chapter goes over self-evaluation of the thesis and own learning.

6.1 Trustworthiness

It is important to discuss the trustworthiness and reliability of this research in order to understand what it aims to achieve and potential further studies examining parts of it. At the start of the research, the research was stated to be mostly qualitative research, not based on opinions of the researcher, but rather on professionals of the field, people who interact with the human element in IT security and other sources. The qualitative data in this research was used to understand key elements of the human element in IT security. This brings forth different potential problems when examining the trustworthiness of the research.

First one is that the broader topic of IT security, as whole, is extremely large and cannot be discussed to its full extent in this research. This leads to the potential of important information and aspects, even regarding the internal human element, being left out due to the scope of this project. This became more apparent in the research during the interviews segment, when aspects of the human element in IT security, such as organizations IT security culture and laws revolving IT security, were stated by the interviewed and thus far had not been discussed in the research, or at least not adequately. It is hard to know if other such important aspects were not discussed in this research.

The second potential problem with the trustworthiness of the research is to do with geographical preferences. This research was conducted in Finland, the people interviewed were Finnish and most of the references for the research originate from sources within the EU, USA or Russia. Due to this, some aspects importance or other certain elements may vary globally or in specific countries.

Another issue with the trustworthiness of this research is with the qualitative interviews both done in this research and referenced in this research. Interviews vary depending on people interviewed and data from interviews can be interrupted differently (Brinkmann 2013, 143).

With these aspects in mind, the main objective of this research was to find what role the internal human element plays in IT security and what threats involve it. Whilst the threats and their importance may vary depending on source, multiple sources were used and referenced in this research to try and provide the best possible overview of the topic in this research. The quantitative data from Chapter 2.1 combined with the qualitative data from Chapter 4 overlapping heavily on other chapters of this research, implies most important aspects and threats to do with the internal human element were discussed in this research.

The other objective of this research, bringing awareness to the internal human element in IT security is partially based on the trustworthiness of the incidents examined in “3: Gathering threats” and other findings in this research. The trustworthiness of the incident and other findings in this research were attempted to make more trustworthy by either including trustworthy sources, such as well-known organizations, governments, etc. or references multiple sources covering the topics.

6.2 Development ideas

Future development ideas for this research could include comparing the categories of threats discussed in Chapter 2.2 to the annexes of the ISO 27001 and going over if all the categories are covered with the framework or what additions would need to be made in order to fully cover all threats in one framework from the perspective of the internal human element. Another development idea to do with frameworks would be to see which frameworks could complement each other the most with the threats discussed in this research and how to hybrid framework could be integrated in practice into organizations IT security.

Another development, which in regard to this topic, would provide valuable information is research on the matter of how organizations can best include IT security into their culture. The importance of this matter has been discussed in this research, but due to the scope of the research the practicality of the implementation and methodology of achieving it was left out. This topic however could benefit the IT security industry if functional and practical new methods for achieving it are researched and developed.

6.3 Suggestions for further research

For the topic as a whole discussed in this research, possible further research done on the topic consists of multiple different options and methods, which are being worked on glob-

ally by different institutes and organizations due to the importance of the topic (with no affiliation to this research but independently). This includes quantitative research by organizations, such as presented partly in this research in Chapter 2.1 and improvement of current methods used to protect against these threats, such as integrating AI more into IT security. On a general level, more information and data are being presented about this topic overtime and more research is done on it constantly.

For individuals wishing to learn more about this topic and wanting to go deeper into the details about it, the ISO 27001 would be a good place to start. The ISO 27001 can also be used to expand to threats outside of the scope of this project for a better overall picture of IT security as a whole. Multiple different organizations also hold panels and presentations on the topics of IT security and the human element in it, these are usually recorded and uploaded online for people to view. These recordings can also be utilized by those wishing to learn more about the internal human element in IT security, though some repetition with this research can be expected.

6.4 Thesis process

The research topic was chosen based on the researcher's interest in the topic and want to raise awareness of it. The process of creating this research included quite a few changes over time. The original concept of the research was to examine threats to do with the internal human element in organizations by creating a type of list revolving around IT security incidents and workplace accidents caused by employees and coming up with solutions on how to counter these threats in the form of a type of guide. Upon beginning research on the topic, certain aspects of it became clearer over time. Certain types of incidents, such as phishing, were mentioned in multiple sources and the origins of the threats, though to do with the internal human element, did not always originate from the internal human element.

This led to the need of categorizing the different threats and acquiring more background knowledge on the topics. With more and more research into the topics, the scope of the topic, which is relatively big, became more apparent and the gave insight on how better present the IT security threats involving the internal human element. As research continued, the idea of a checklist organizations could use to help prevent against certain threats seemed more distant due to the nature of the threats. A checklist consisting of the threats found throughout the research would not suffice to adequately protect organizations from threats involving the internal human element.

As research moved forward the research started taking more its final state, which is to focus on what threats involve the internal human element in IT security, how these can be prepared for and to raise awareness to the topic. The research had shifted from creating a guide to more of an overview of the topic and directing organizations to certain already created methods to protect against the IT security threats listed in research. This was done due the fact that as more research on topic was done, more effective tools, and especially frameworks were discovered by the researcher. These frameworks have been created by the combined efforts of multiple professionals in the field working together to best protect against these threats and served as superior guides.

This does not mean that the research segment was in vain, quite the opposite. This research was done to create a relatively short overview to the large topic, raise awareness for it and to help people not specialised in IT security better comprehend their importance in it without being held back by too many technical terms and industry specific language.

6.5 Own learning

This was the researchers first relatively long research and the process of creating it has given a better understanding for how to tackle such projects in the future. There were many aspects of creating a research over 50 pages that were learned during the process and can be used by the researcher later on. These aspects include proper planning, time management, scheduling, formatting text, planning and performing interviews, referencing and other useful skills in regard to creating a thesis or research. Looking back on the research from the researcher's point of view, there are things that could have been done differently to improve the final version but that is one point of this research, to know how to improve for the next time.

During the process of this research the researcher has achieved a better understanding of IT security, not just from the perspective of the internal human element but as a whole. In order to better understand how the internal human element plays a role in IT security the researcher had to examine how other IT security threats and incidents were both recorded and prepared for. This gave good insight into threat management and methods to distribute resources in accordance with the needs in the form of risk assessment charts and frameworks. One of the most important tools discussed in the research from the researcher's point of view was the ISO 27001. The reasoning for this is that frameworks such as this are designed with the whole picture of IT security in mind and cover multiple different sources of threats and how to properly prepare for these threats. The frameworks work as both a window into what the actual threats in IT security are and how organizations are currently preparing for those threats.

Another important factor learned by the researcher during the process of the research, especially during the interviews, was how individuals' actions actual affect IT security. It is relatively simple to comprehend the direct impact of a single individual neglecting IT security and performing tasks without thought of possible threats such as opening a suspicious email to check where the link leads but during the research the much more complex true nature of individuals attitude towards IT security was further understood. This comes in the form of culture within organizations and how the collective treats an issue such as IT security. When someone from management for example does not consider the impact, for example financial resources and time, required to maintain an IT security conscience environment then this can directly travel down to lower ranking employees and lead to negligence in their daily tasks. Based on interviews and research this can also happen within organizations teams when influential employees, not based on ranking but rather social standing, neglect the importance of IT security and others follow suite. This information gave the researcher a new perspective on IT security.

From the researcher's point of view the thought of integrating IT security into the organizations culture is a fascinating thought, which the researcher will keep in mind long after the research. Each individual has the capability to increase organizations IT security not by just their own actions, but also by how they affect others perspective on the matter. Though there is no simple and direct method to integrate IT security into any organizations core culture, big solutions such as frameworks in combination with smaller day to day actions from individuals can lead towards improved IT security in an organization. This knowledge will affect how the researcher deals with IT security in his professional life moving forward.

References

Advisera 2020. What is ISO 27001? Quick and easy explanation. URL: https://advisera.com/27001academy/what-is-iso-27001/. Accessed: 15 January 2021.

Australian Cyber Security Centre 2020. Malicious insiders. URL: https://www.cyber.gov.au/acsc/view-all-content/threats/malicious-insiders. Accessed: 10 December 2020.

Baseline 2012. CISO Warns Against Security Complacency. URL: http://www.baseline-mag.com/c/a/Security/CISO-Warns-Against-Security-Complacency-546842. Accessed: 25 November 2020.

BBC 2020. Coronavirus: 18,000 test results published by mistake. URL: https://www.bbc.com/news/uk-wales-54146755. Accessed: 10 December 2020.

Brinkmann, S. 2013. Qualitative Interviewing. Oxford University Press, Incorporated. Oxford.

Carrazana, L. 2018. The Economics of Cybersecurity and Cyberwarfare: A Case Study. ECON Colloquium. URL: https://austrianstudentconference.com/wp-content/uploads/2019/02/ASSC-2019-Lorenzo-Carrazana.pdf. Accessed: 4 January 2021.

Chartered Institute of Information Security 2020. Over Half of Cyber Security Professionals Affected by Overwork or Burnout, CIISec Survey Finds. URL: https://www.ciisec.org/CIISEC/News/Over%20Half%20of%20Cyber%20Security%20Professionals%20Affected%20by%20Overwork%20or%20Burnout,%20CIISec%20Survey%20Finds.aspx?WebsiteKey=a17cb243-464e-4ad3-96f8-2635490f727a. Accessed: 10 January 2021.

Conheady, S. 2010. Social Engineering Training for IT Security Professionals. Information Security Ltd. First Defence. Seminar presentation recording. Vienna.

Cybersecurity & Infrastructure Security Agency 2021. Ransomware guidance and resources. URL: https://www.cisa.gov/ransomware. Accessed: 6 February 2021.

Dawson, H. 2019. The Most Influential Security Frameworks of All Time. URL: https://www.infosecurity-magazine.com/opinions/most-influential-frameworks-1-1-1/. Accessed: 20 January 2021.

DMARC s.a. What is DMARC. URL: https://dmarc.org/. Accessed: 2 February 2021.

European Commission 2019. What personal data is considered sensitive?. URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en. Accessed: 10 December 2020.

European Union Agency For Cybersecurity 2020. Incident Reporting. URL: https://www.enisa.europa.eu/topics/incident-reporting. Accessed. 15 February 2021.

Forbes 2020. Global 2000 The World's Largest Public Companies. URL: https://www.forbes.com/global2000/#5b0dd03c335d. Accessed: 5 January 2021.

Globalquest Solutions 2018. Employee Awareness Training – Your First Line Of Defense Against Cyber Threats. URL: https://www.globalquestinc.com/employee-awareness-training-your-first-line-of-defense-against-cyber-threats. Accessed: 5 January 2021

Greenberg, A. 2018. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired. URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. Accessed: 8 January 2021.

Hadnagy, C. & Wozniak, S. 2018. Social Engineering. 2nd ed. Wiley 2018.

Help Net Security 2020. Human error: Understand the mistakes that weaken cybersecurity. URL: https://www.helpnetsecurity.com/2020/07/23/human-error-cybersecurity/. Accessed: 7 November 2020

IBM 2020. Cost of a Data Breach Report 2020. URL: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf. Accessed: 12 November 2020.

IBM 2020. AI for cybersecurity. URL: https://www.ibm.com/security/artificial-intelligence. Accessed: 29 January 2020.

Imperva 2020. Phishing attacks. URL: https://www.imperva.com/learn/application-security/phishing-attack-scam/. Accessed: 25 January 2021.

ISG 2019. Conducting a Successful Security Risk Assessment. URL: https://isg-one.com/third-party-management/articles/conducting-a-successful-security-risk-assessment. Accessed: 20 November 2020.

ISMS online 2021. What is ISO 27001?. URL: https://www.isms.online/iso-27001/. Accessed: 10 February 2021.

Kaspersky 2017. The Human Factor in IT security: How Employees are Making Businesses Vulnerable from Within. URL: https://www.kaspersky.com/blog/the-human-factor-in-it-security/. Accessed: 17 November 2020.

Limbago, A. L. 2018. Cyber Risk Wednesday: The Human Element of Cybersecurity. Chief Social Scientist. Virtu. Seminar presentation recording. Webcast.

Lord, N. 2020. The cost of a malware infection? For Maersk, $300 million. Digital Guardian. URL: https://digitalguardian.com/blog/cost-malware-infection-maersk-300-million. Accessed: 8 January 2021.

Michael, M. 22 October 2019. Episode 30 | Talking Infosec to Nin-Infosec Folks. F-secure. URL: https://blog.f-secure.com/podcast-talking-infosec/. Accessed: 20 January 2021.

Microsoft 2018a. Interactive logon: Machine inactivity limit. URL: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-machine-inactivity-limit. Accessed: 12 January 2021.

Microsoft 2018b. File Server Resource Manager (FSRM) overview. URL: https://docs.microsoft.com/en-us/windows-server/storage/fsrm/fsrm-overview. Accessed: 10 February 2021.

Mutune, G. 18 September 2019. 23 Top Cybersecurity Frameworks. URL: https://cyberexperts.com/cybersecurity-frameworks/. Accessed: 22 January 2021.

National Cyber Security Centre 2018. Phishing attacks: defending your organization. URL: https://www.ncsc.gov.uk/guidance/phishing. Accessed: 2 December 2020.

National Institute of Standards and Technology 2018. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Accessed: 10 January 2021.

NIST 2018. The Five Functions. URL: https://www.nist.gov/cyberframework/online-learning/five-functions. Accessed 10 January 2021.

Obama White House 2014. Cybersecurity – Executive Order 12636. URL: https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/eo-13636. Accessed: 22 January 2021.

Ozkaya, E. 2018. Learn Social Engineering: Learn the Art of Human Hacking with an Internationally Renowned Expert. 1st ed. Packt Publishing, Limited.

Poggi, N. 2020. Cybersecurity Frameworks 101 – The Complete Guide. URL: https://preyproject.com/blog/en/cybersecurity-frameworks-101/. Accessed: 20 January 2021.

Positive Technologies 2017. Cybersecurity threatscape: Q1 2017. URL: https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-q1-2017/?sphrase_id=82458. Accessed: 25 October 2020.

Positive Technologies 2020a. Cybersecurity threatscape: Q2 2020. URL: https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2020-q2/. Accessed: 25 October 2020.

Positive Technologies 2020b. Analytics. URL: https://www.ptsecurity.com/ww-en/analytics/. Accessed: 25 October 2020.

Powell, A. 5 December 2019. Implementing the Lessons Learned From A Major Cyber Attack. CISO. Maersk. Seminar presentation recording. London.

Ryan, T. 2010. Getting in bed with Robin Sage. Provide Security. URL: https://www.privacywonk.net/download/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf. Accessed: 2 March 2021.

Sangoma 2019. SMB, SME, and Large Enterprise: Why Your Business Size Classification Matters. URL: https://www.sangoma.com/articles/smb-sme-large-enterprise-size-business-matters/. Accessed: 11.11.2020

Schwartz, S. 2019. CISO of the Year: Andy Powell, Maersk. CIO Dive. URL: https://www.ciodive.com/news/ciso-maersk-notpetya-infosec-dive-awards/566241/. Accessed: 10 January 2021.

Thales 2016. 10 years of cyber security; what the past decade has taught us. URL: https://dis-blog.thalesgroup.com/security/2016/06/06/10-years-cyber-security-past-decade-taught-us/. Accessed: 10 November 2020.

Tipton, H. F. & Krause, M. 2006. Information Security Management Handbook. URL: https://books.google.fi/books?id=5sIJ4Ho5yLUC&pg=PT3800&redir_esc=y#v=onepage&q=tape%20reel&f=false. Accessed: 2 March 2021.

Training Journal 2020. A human firewall: The first line of defence. URL: https://www.trainingjournal.com/articles/features/human-firewall-first-line-defence. Accessed 5 January 2021.

Trend Micro 2016. Spear Phishing Attack Exposes Tac Information of 3,000 Community College Employees. URL: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/spear-phishing-attack-exposes-tax-information-of-3-000-community-college-employees. Accessed: 25 January 2021.

University of Central Lancashire 202. Tired and overworked employees pose huge risk to business' data. URL: https://www.uclan.ac.uk/news/tired-and-overworked-employees-pose-huge-risk-to-business-data. Accessed: 16 April 2021.

University of San Diego 2020. Top Cybersecurity Threats in 2020. URL: https://onlinedegrees.sandiego.edu/top-cyber-security-threats/. Accessed: 15 November 2020.

Voeller, J. G. 2014. Cyber Security. 1st ed. John Wiley & Sons, Incorporated.

Waterman, S. 2010. Fictious femme fatale fooled cybersecurity. The Washington Times. URL: https://www.washingtontimes.com/news/2010/jul/18/fictitious-femme-fatale-fooled-cybersecurity/. Accessed: 2 March 2021.

Watson, G. & Mason, A. & Ackroyd, R. 2014. Social Engineering Penetration Testing: Executing Social Engineering Pen Tests, Assessments and Defense. 1st ed. Elsevier Science & Technology Books.

Weatherill, M. 2017. How four eyes fits with cyber security. Alpha-gen. URL: https://www.alpha-gen.co.uk/blog/how-four-eyes-fits-cyber-security/. Accessed: 20 March 2021.

Whitney, L. 2020. How to defend your organization against social security engineering attacks. TechRepublic. URL: https://www.techrepublic.com/article/how-to-defend-your-organization-against-social-engineering-attacks/. Accessed: 4 March 2021.

Appendices

Appendix 1. Interview questions

1) What is the name of the Organization you work for?

2) What is your personal role within the organization?

3) What are the main components/elements in IT security, in your opinion?

4) How big of a role does the internal human element play in organizations IT security in your opinion?

5) What are the most common security threats to do with human element in organizations in your opinion?

6) How big of risks would you categorize these subjects as when dealing with the human element in IT security?

i. Human error
ii. Social Engineering
iii. Phishing
iv. Malicious intent

7) Are there other subjects to do with the internal human element that you find potential sources of threat from? If so, can you explain these subjects further?

8) How well do you feel organizations take the human element into consideration for their IT security?

9) How well do you think individual employees in general are aware of the potential IT security threats regarding the human element, such as being scammed by phishing and how well are they prepared for it?

10) What are some of the challenges when implementing security plans/policies to do with the internal human element (as supposed to threats where the code/program is the main source of threat)?

11) In general, what has your organization done, or what is something other organizations could do to combat IT security issues regarding the internal human element?

12) How big of a role do you feel human element will play in IT security in the future? Will technology for example help remove some of these threats or will these continue to be security threats for a long time still?

13) Are there any other important factors regarding the internal human element in IT security that you feel were not discussed in this interview?