TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Oliver Kristopher Ruut 211976IVGM

Emerging cyber threats in Estonian public sector during and after COVID-19

Master's thesis

Supervisor: Sille Arikas
MSc

Tallinn 2023

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Oliver Kristopher Ruut 211976IVGM

Eesti avalikus sektoris enne ja pärast COVID-19 esilekerkinud küberohud

Magistritöö

Juhendaja: Sille Arikas
MSc

Tallinn 2023

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Oliver Kristopher Ruut

08.05.2023

Abstract

Cybersecurity is an essential aspect of our modern digital world. With the increasing dependence on technology and the internet, protecting sensitive information and critical infrastructure from cyber threats has become more critical than ever before. The field of cybersecurity is constantly evolving, as new threats emerge, and existing threats become more sophisticated.

As our reliance on technology continues to grow, the importance of cybersecurity will only increase. It is an exciting and constantly changing field that requires individuals to stay up to date with the latest threats and technologies.

The aim of this paper is investigation of new emerging threats in cybersecurity mainly during the COVID-19 crisis, but also after the COVID-19. Analysing their impact on organizations and its staff and providing a set of recommendations for people who are more susceptible to falling a victim of cyberattacks.

This thesis is divided into three main chapters (Cyber threat landscape, Methodology, and Analysis). Building upon the insights and findings from the expert interviews and document analysis, chapter five presents a comprehensive set of recommendations aimed at mitigating the growing cyber threats and protecting the individuals and organizations that are more vulnerable to cyber-attacks.

Keywords: Cyber awareness, cybersecurity, public sector, COVID-19, e-governance.

This thesis is written in English and is 80 pages long, including 6 chapters and 7 figures.

Annotatsioon
Eesti avalikus sektoris enne ja pärast COVID-19 esilekerkinud küberohud

Küberturvalisus on meie kaasaegse digimaailma oluline aspekt. Seoses kasvava sõltuvusega tehnoloogiast ja internetist, on tundliku teabe ja kriitilise infrastruktuuri kaitsmine küberohtude eest muutunud kriitilisemaks kui kunagi varem. Küberturvalisuse valdkond on pidevas arengus, kuna ilmnevad uued ohud ning olemasolevad ohud muutuvad keerukamaks.

Meie sõltuvusega tehnoloogiast kasvab ka küberturvalisuse tähtsus. See on pidevalt muutuv valdkond, mis nõuab inimestelt uute esile kerkivate ohtude ja tehnoloogiatega kursis olemist.

Magistritöö eesmärk on uurida peamiselt COVID-19 kriisi ajal, aga ka pärast COVID-19 esile kerkinud küberohtusid. Töös analüüsitakse esilekerkinud ohtude mõju organisatsioonidele ja nende töötajatele ning antakse soovitusi inimestele, kes on vastuvõtlikumad küberrünnakute ohvriks langemiseks.

See lõputöö on jagatud kolme põhipeatükki (Küberohtude maastik, Metodoloogia ja Analüüs). Tuginedes ekspertintervjuude ja dokumendianalüüsi arusaamadele ning järeldustele, esitatakse viiendas peatükis soovituste kogum küberohtude maandamiseks ning küberrünnakute suhtes haavatavamate isikute ja organisatsioonide kaitsmiseks.

Märksõnad: Küberteadlikkus, küberturvalisus, avalik sektor, COVID-19, e-valitsemine.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 80 leheküljel, 6 peatükki ja 7 joonist.

List of abbreviations and terms

RIA	Riigi Infosüsteemi Amet / Information System Authority
IT	Information technology
IS	Information systems
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems
SIEM	Security Information and Event Management
BEC	Business email compromise
CERT-EE	Computer Emergency Response Team Estonia
ETL	ENISA Threat Landscape
RaaS	Ransomware as a service
DDoS	Distributed Denial of Service
DrDoS	Distributed Reflection Denial of Service attack
JRC	European Commission's Joint Research Centre
EU	European Union
MKM	Majandus- ja Kommunikatsiooniministeerium/ Ministry of Economic Affairs and Communications
E-ITS	Eesti Infoturbestandard/ Estonian Information Security Standard

Table of Contents

List of figures

1. Introduction

The emergence of cyber threats in the public sector has become a major concern for governments around the world, particularly in the wake of the COVID-19 pandemic. In Estonia, a country with a highly digitized public sector, the threat of cyberattacks has been a long-standing issue. The Estonian public sector is no exception having 99% of governmental services available online (e-Estonia, 2022), the need for robust cybersecurity measures has become highly important. Common cyber threats such as phishing, malware, and compromising attempts have become more prevalent and sophisticated, and the public sector must adapt to stay secure. The COVID-19 pandemic has created new challenges for the Estonian public sector, as organizations have had to move to remote work and online service delivery. Not only has this improved the efficiency and availability of the services but has also increased the attack platforms.

Cybercrime evolves at a fast pace, new trends are constantly emerging and therefore the need for constant monitoring and adaption is required, relying previous knowledge alone is not sufficient. It is important to provide a timely set of rules and frameworks to organizations and people.

The aim of this paper is investigation of new emerging threats in cybersecurity mainly during the COVID-19 crisis, but also after the COVID-19. Analysing their impact on organizations and its staff and providing a set of recommendations for people who are more susceptible to falling a victim of cyberattacks.

In order to achieve these goals, the following Research Questions (RQ) and Sub-questions (SQ) have been drafted:

RQ1. How has COVID-19 affected the cybersecurity readiness of individuals, and organizations in the e-government field?

SQ1. Have there been an emergence of new cyber threats and trends and what can be done to mitigate the risks?

RQ2. How to determine the receptiveness of falling a victim of a cyberattack of the personnel and what are the methods to reduce the chances of falling a victim of a cyberattack?

The research questions require the collection of data in a qualitative manner. A qualitative study was chosen as an appropriate method for data collection. By using this method of collecting, we can gain an overview of the opinions and insights of the experts who will participate in the study. The author has decided to use a case study since case studies capture a range of viewpoints, as opposed to the one perspective you acquire from a survey or only an interview. Thus, you can gain a deeper understanding of the subject at hand. Furthermore, it reduces the likelihood of biases by diluting the agenda of a particular individual (Salmon, 2017). The case study is based on Estonia's experience, and it is exploratory as it aims to provide an insight on how public sector is arranging it cybersecurity procedures and processes during and after the COVID-19 crisis.

The author defines qualitative research as the central methodology to be used in answering the research questions.

The main method of collecting data is through semi-structured interviews with experts in the field, policymakers, and government officials. In addition to interviews, document analysis will provide another important source of data, including peer-reviewed scholarly papers and articles in the field, governmental decrees, reports, studies, literature, and other related materials. In addition, works previously written by the author have also been used: “Threats in cybersecurity during covid crisis”.

Thesis is divided into three main chapters Cyber threat landscape, Methodology, and Analysis. The first chapter investigates the theoretical background and provides an overview of the cyber threat landscape during the COVID-19 period, investigates different attack vectors that cybercriminals use and the Estonian cybersecurity strategy.

Second chapter provides an overview of the methods used for research methodology along with theoretical background. The author has decided to use institutional theory for the thesis. Institutional theory provides a useful lens for analysing the response of the Estonian public sector to the emerging cyber threats during and after COVID-19. Institutional theory emphasizes the social, cultural, and political factors that influence organizational behaviour and decision-making.

Third chapter provides an in-depth analysis of the semi-structured interviews conducted with experts in the cybersecurity field, as well as an examination of the current cybersecurity trends and changes that have occurred in Estonia between 2020 and 2022.

Building upon the insights and findings from the expert interviews and document analysis, chapter five presents a comprehensive set of recommendations aimed at mitigating the growing cyber threats and protecting the individuals and organizations that are more vulnerable to cyberattacks.

1.1 Relevancy

The work is relevant since public sector is of critical importance due to the potential impact on national security, public safety, and the economy. As most of our lives have moved online, the public sector services have also moved online due to high demand of the citizens looking for an easy way to communicate with their state. The Estonian public sector is particularly relevant as well as vulnerable due to the country's high level of digitization and reliance on technology. In recent years, Estonia has been the target of several high-profile cyber attacks (MKM, 2019), including a 2007 attack that disrupted government services and caused widespread panic. (Välisministeerium, 2007). Given the rapidly changing nature of the cyber threat landscape, there is a need for further research on how cyber threats have evolved in the Estonian public sector during and after the pandemic. This subchapter will outline the relevance of this topic and why previous knowledge is not enough to fully understand the current situation.

The COVID-19 pandemic has created new challenges for the Estonian public sector, as organizations have had to adapt to remote work and moving public services online at a fast pace without much preparation. This has created an additional attack surface and increased the risk of falling a victim of a cyberattack, as cyber criminals have sought to take advantage of the situation. For example, phishing attacks targeting remote workers have increased significantly during the pandemic. (Statista, 2021)

Understanding the nature of cyber threats in the Estonian public sector during and after the COVID-19 pandemic is critical for ensuring the security of the country's digital infrastructure. As the author conducted research on this topic, it was possible to identify the most significant threats and develop effective strategies to mitigate them.

While there has been some research on cyber threats specifically targeting Estonian public sector, much of this research has focused on the period before the COVID-19 pandemic.

This research conducted by the author has provided valuable insights into the nature of cyber threats against Estonian public sector and the strategies used to mitigate them.

However, the COVID-19 pandemic has created new challenges and vulnerabilities that were not present before. For example, the rapid shift to remote work has increased the risk of cyberattacks targeting remote workers with low cybersecurity awareness. Similarly, the increased reliance on online services has created new opportunities for cybercriminals to exploit vulnerabilities in digital infrastructure.

Given the rapidly changing nature of the cyber threat landscape, there is a need for further research on how cyber threats have evolved in the Estonian public sector during and after the COVID-19 pandemic. This research can help identify new threats and vulnerabilities and develop effective strategies to mitigate them.

Furthermore, by conducting research on this topic, it was possible to gain a deeper understanding of the institutional and organizational factors that influence the ability of the Estonian public sector to respond to cyber threats. This can help to identify areas of improvement in terms of policy, practice, and training.

2. Cyber Threat Landscape during COVID-19

World health authorities faced a new highly infectious disease called COVID-19 in the year 2020. As a result of the COVID-19 pandemic, significant social, economic, and political disruptions have occurred across the globe. (Nkengasong, 2021) The COVID-19 crisis has shown us how fragile our systems are, how interconnected our world is, and how much we rely on each other for survival. (Bachelet & Grandi , 2020)

The virus spread rapidly throughout the world, leading to various measures taken by governments and public health authorities to contain it. These measures included lockdowns, travel restrictions, mandatory mask-wearing, and social distancing. (Ayouni, et al., 2021) People and communities were forced to adapt to a new way of living and working because of these measures.

There was a disproportionate impact of the virus on vulnerable groups such as the elderly and the sick. (Cucinotta & Vanelli, 2020) Social inequalities, such as health disparities, education disparities, and economic inequality, also emerged because of the crisis. (Bambra, Riordan, Ford, & Matthews, 2020)

There have been significant economic ramifications of the COVID-19 pandemic besides its health consequences. A large number of businesses closed, and many people lost their jobs or experienced reduced incomes. In addition to disrupting global supply chains, the pandemic caused shortages of essential goods and services. Globally, the crisis has been felt as recessions and financial instability have gripped many countries. (Pak, et al., 2020)

Estonia was no different from the rest of the world. The Health Board's crisis team began working on January 28 (Regionaalhaigla, 2020) and was able to detect COVID-19 virus independently on January 31. (Krjukov, 2020) In January, the health board agency also raised its risk assessment of infection introduction from low to medium. (Terviseamet, 2019-nCoV andmed 31.01.2020, 2020)

On February 27, Estonia confirmed its first case of COVID-19 infection. (Ots & Kook, 2020) In addition, on 27 February, the Board of Health changed the risk assessment of introducing the disease from medium to high. (Terviseamet, 2020)

Estonian government declared a state of emergency late at night on March 12 in response to the spread of COVID-19 worldwide and the possibility of it spreading within the

country (Kook, 2020). The state of emergency meant that all public gatherings were prohibited, the usual study was transferred to online learning. Border control was restored, museums, and cinemas remained closed until the first of May. Concerts, conferences, and sports competitions were cancelled. (Postimees, 2020)

The Prime Minister added that the state's actions alone are no longer enough to overcome the crisis. "We have reached a situation where every person must contribute to the protection of public health. I understand the discomfort declaring a state of emergency causes for all of us, but not only people's health is at stake, but also the protection of lives." (Kook, 2020)

Many people experienced fear and confusion during this period. Using phishing emails and phone messages, as well as calling people over the phone directly, the criminals exploited people's fears and ignorance for profit. As our daily lives as we know came to a halt, most of it moved to the digital world without any prior preparation and security awareness training for many people.

Cyberspace was also impacted by the COVID-19 outbreak. RIA's cyberspace monitoring during COVID-19 period, saw the increase of phishing and fraudulent e-mails taking advantage of people's fears and ignorance related to pandemic. Several companies and institutions stated that they were not prepared for moving all their services online the time. (BNS, 2021) For example, some companies' data was obtained by scammers due to improperly set up teleworking solutions, said Mart Hiietamm, head of the analysis and prevention department at RIA. No area is safe from cyberattacks, according to Hiietamm. He states that: "Every person, company and institution must constantly contribute to their own protection in cyberspace."(BNS, 2021)

2.1 Cybersecurity

Cybersecurity is a critical field that is concerned with protecting computer systems, networks, and data from unauthorized access, theft, damage, and disruption. With the increasing digitization of modern society, cybersecurity has become a major concern for individuals, organizations, and governments around the world. (Ursillo & Arnold, 2019)

This subchapter introduces the field of cybersecurity, including the definition of cybersecurity, the importance of cybersecurity, and the key components of a cybersecurity strategy.

2.1.1 Definition of Cybersecurity

The concept of cybersecurity refers to the protection of computer systems, networks, and data from unauthorized access, theft, damage, and disruption. Malware, phishing attacks, and hacker attempts are among the threats to be protected against. (Shea, Gillis, & Clark, 2023)

Cybersecurity includes encryption, firewalls, intrusion detection and prevention systems, and vulnerability scanners. Security threats can be identified and responded to using such tools, and sensitive data can be prevented from being accessed unintentionally with the help of these tools. (Bacon, 2023)

There are several reasons that make cybersecurity important both for the institution but also for an end-user. Most importantly, cyberattacks can damage computer systems and networks, causing data loss, disruption of business operations, and sensitive information theft. The cyberattacks pose serious threats to national security, public safety, and economy. They can cause a widespread disruption and chaos through when targeted against critical infrastructure, such as power grids and transportation systems, that also disable the use of several other services which are in example depending on electricity.

From an individual perspective, being aware of cyber risks has a significant role in protecting individual privacy. As more and more data is stored and transmitted electronically, identity theft and other forms of cybercrime targeting individual's data, are becoming more common.

Among the components of a comprehensive cybersecurity strategy are risk assessment, prevention, detection, and response. The process of identifying and evaluating security risks and vulnerabilities is called a risk assessment. (Broadtek, 2023)

Keeping software up to date, using strong passwords, and implementing firewalls are some measures you can take to prevent security breaches. A security breach is detected

by monitoring computer systems and networks for unusual network activity or malware presence. (Broadtek, 2023)

An effective response involves removing infected computers from the network and restoring backups to minimize the impact of a security breach. (Broadtek, 2023)

The implementation of effective cybersecurity measures requires not only these components, but also training the employees and users to recognize and respond to security threats and developing policies and procedures to govern how computer systems and data are used. (Broadtek, 2023)

Cybersecurity involves protecting computers, networks, and data from intrusions, thefts, and physical damage. In order to ensure the security of computer systems and data, a comprehensive cybersecurity strategy must be implemented by any organization.

As cybercrime evolves at an incredibly fast pace, new trends are constantly emerging. Cybercriminals are becoming more agile, implementing new technologies, adapting their attacks using new methods, and collaborating in ways we have never seen before. (Interpol, 2021)

Cybersecurity has become an increasingly important consideration in the research and practice of information technology (IT) and information systems (IS). Organizations have suffered heavy losses due to cyber security breaches. (Zadeh, Jeyaraj, & Biros, 2020) Uber reported unauthorized access to data for 57 million users, data of 540 million Facebook users got leaked, and First American Financial Corporation revealed the personal data of 885 million users due to breach over several years. The company's losses can run into hundreds of millions of dollars, not only due to data loss but also through following fines and lawsuits. (Zadeh, Jeyaraj, & Biros, 2020)

The data breaches do not only impact private establishments but also government databases. These are matters pertaining to the citizens of that country, materials intended for internal use by institutions, and the loss of that data can have significant consequences. (Interpol, 2021) That is why the authorities need to keep pace with new technology to understand the opportunities created for criminals and how they can be used as tools to fight cybercrime. (Interpol, 2021)

2.2 Attack vectors

For organizations to maintain their safety in today's dangerous cyber landscape, they must position themselves ahead of cybercriminals. To achieve cyber resilience, you must identify your weaknesses, understand how your organization might be compromised, and implement the most appropriate prevention and detection methods. (Soare, 2022) In order to prevent disruptions to your business, you must first understand what vectors of attack can be encountered. (Soare, 2022)

Attack vectors are ways for attackers to gain access to networks and systems. Among the most common attack vectors are social engineering attacks, credential theft, and exploiting technical vulnerabilities of the systems. Mitigating attack vectors whenever possible is an important part of information security. (Cloudflare, 2023)

The majority of attack vectors tend to be intentional threats rather than unintentional threats, as they require some planning and analysis. (Soare, 2022)

The vectors of attack may be exploited by a range of entities, including upset former employees, malicious hackers, cyber espionage groups, as well as competitors. It does not matter who or what is involved, the damage they can cause your business is the same. They may try to disrupt your business, steal your technology, or extort money. (Soare, 2022)

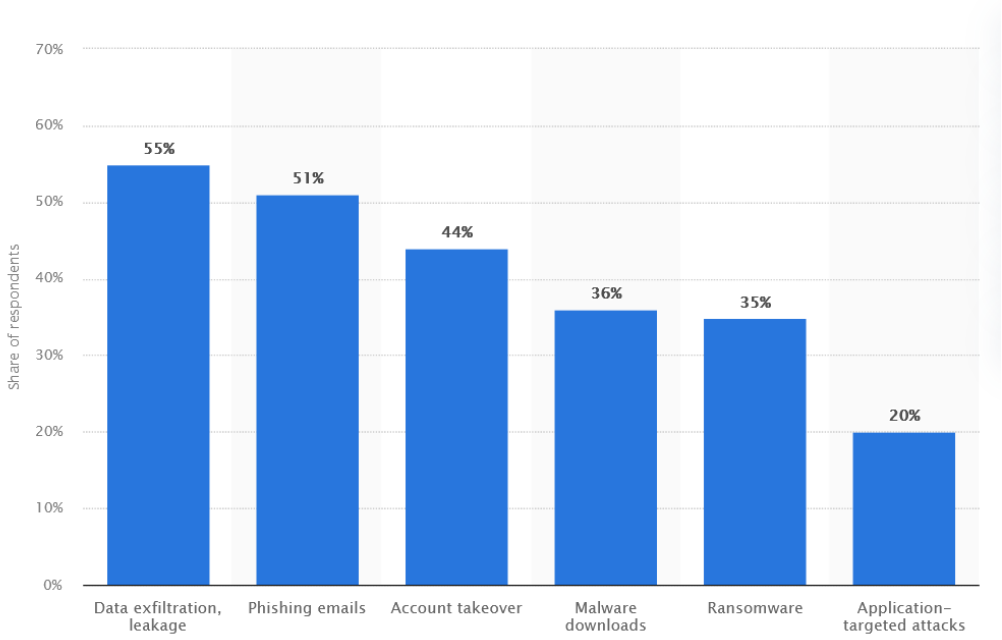
2020 was an unprecedented year. The COVID-19 epidemic did and continues to do great damage, and the consequences of the global crisis are still being learnt. Working remotely has remained the dominant way of working, with less and less physical involvement required to consume the services. Any crisis or new situation favours development, including negative ones. Criminals most commonly cannot get into a face-to-face meeting, but in case no protection has been implemented, they can access an online meeting. It is no coincidence that during the pandemic, phishing campaigns became more frequent, through which scammers tried to gain access to not only people's data and money but also credentials to access business information. Companies had to deal with the recovery of websites, including information, that had been stolen. (RIA, Küberturvalisuse aastaraamat 2021, 2021)

COVID-19 reached Estonia in February, and on March 12, the government declared a state of emergency to limit its spread. (RIA, Küberturvalisuse aastaraamat 2021, 2021) In

just a few days, companies and institutions switched to teleworking and schools to online learning. The digital state was put to the test: the use of e-services grew exponentially in all fields: studying, working, shopping, entertainment, and obtaining information. The electronic learning information system eKool did not withstand the abrupt increase in workload on the first day of distance learning and was unavailable for the users' additional resources were added for the server running eKool. New digital services were quickly introduced but new accounts were unfortunately created by new users using their old passwords (RIA, Küberturvalisuse aastaraamat 2021, 2021).

From Figure 1 we can see more than fifty percent of experts saw an increase in data exfiltration, leaks, and phishing emails. Additionally, the IT professionals observed an increase in account takeovers and malware execution.

Figure 1. Where do IT professionals see an increase in cyberattacks and attack attempts following the COVID-19 pandemic based on Statista?



Source: (Statista, 2021)

2.2.1 Data exfiltration

It is widely acknowledged that data theft also known as data exfiltration is the main cause behind many cyberattacks, regardless of whether they are committed by organized crime, commercial competition, governments, or hacktivists (Ullah, et al., 2018).

Cyberattacks with the goal of a data theft can be classified as data exfiltration attacks (Kost, 2023). It has become highly difficult to prevent data exfiltration for two main reasons. First of all, it should be noted that cybercrime has evolved from an individual act to one committed by organizations in recent years. The transformation has enabled attackers to become more professional at exfiltrating data because of access to a high budget, resources, and sophistication of tools that has become more common and easily available. Second, the existing data infrastructure can also be used to exfiltrate data using several methods originally intended for legitimate data exchange (Ullah, et al., 2018).

When companies' data is exfiltrated, there is no limit to what they are likely to lose: valuable business confidential information like future project information, and customer profiles, which can cause economic and reputational damage but has a high value for their competitors. Data exfiltration can have even greater consequences for governments when national secrets or information about political settlements fall into a possession of a hostile nation states. Security experts have developed several security systems to deal with such a serious concern. These systems include Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), firewalls, and Security Information and Event Management tools (SIEM). Despite the available solutions, these systems cannot prevent data exfiltration as the data is unstructured and in constant change (Ullah, et al., 2018).

Security experts and researchers devise data exfiltration countermeasures to overcome this limitation. These countermeasures are intended to detect, prevent, or investigate data exfiltration. As opposed to traditional security systems (e.g., IDS, IPS, and firewalls), which are supposed to prevent an attacker from entering an organization, data exfiltration countermeasures are expected to prevent an attacker from returning with sensitive data from the organization (Ullah, et al., 2018). The key to mitigating these attacks is understanding the malicious processes that precede data exfiltration. As a result, they allow security controls to be implemented leading up to a final data loss event to obfuscate a significant part of an attack sequence (Kost, 2023).

2.2.2 Phishing

The most common threat to organizations and individuals regardless of their location or field of work are the phishing attacks. Cybercriminals use phishing to gain access to networks and systems to later deliver malicious payloads (e.g., ransomware) or steal valuable and sensitive information (e.g., online banking or e-commerce login credentials) from their potential victims. (Darem , 2021)

Fraudulent emails sent and phishing websites claiming to be the legitimate sources are primary factors in phishing. (Darem , 2021)

Unless checking the website address, it may be difficult to distinguish phishing websites from the genuine ones as many of them are exact copies of the genuine ones being created by copying the original website's code. Aside from creating phishing websites and sending phishing emails, cybercriminals exploit human psychology by using social engineering techniques. The most prevalent human weakness cybercriminals exploit is the inability of people to distinguish between legitimate enterprise websites and phishing sites, their interactions with systems, and their understanding of alert messages. To further compel their victims, attackers often use factors such as urgency or intimidation in their messages by threatening with loss of access to the mailbox or suspicious activity happening on the bank account. By inserting legitimate information to a phishing site, the unsuspecting recipient may reveal sensitive financial or personal information on a spoofed website that looks trustworthy. (Darem , 2021)

Types of phishing attacks

Bulk phishing emails

One of the most common types of phishing attacks is bulk email phishing. The phishers create emails that appear to originate from large, well-known legitimate businesses and organizations - like a national or global bank, email service provider, a large online retailer, the makers of a popular app or software - and send them to millions of recipients. It is a numbers game: the larger or more popular the impersonated sender is, the more

likely the recipient is to be a customer, subscriber, or member and might consider the message a legitimate one. (IBM, 2023)

To get the recipient's attention, the impersonated sender addresses a topic with strong emotions and appeals to strong emotions like fear, greed, curiosity, urgency, or time pressure (IBM, 2023). Appendix 4 illustrates these types of examples.

Email recipients are instructed to take action that seems reasonable under the circumstances and consistent with the subject matter, but it will lead to them divulging sensitive information, such as social security numbers, bank account numbers, credit card numbers, or login credentials. In some cases, even downloading a file that might infect their system. The recipient might be directed to “click this link to update your profile”, while navigating to a phishing website, where their legitimate login credentials are entered. Alternatively, they may be told to open an attachment that appears legitimate but contains malware. (IBM, 2023)

Spear phishing

In spear phishing, the scammer targets a specific person - usually someone who has privileged access to sensitive data or network resources, or who has special authority the attacker can exploit. (IBM, 2023)

When spear phishing, the attackers previously gather information about the target to pose as a person or entity that the target might trust, such as a friend, manager, colleague, trusted vendor, or financial institution. A rich source of spear phishing information are social media and social networking sites, where people publicly congratulate colleagues, endorse colleagues and vendors, and share information about meetings and events. Spear phishers can use this information to send a message containing specific financial or personal data, along with credible requests. (IBM, 2023)

Business email compromise (BEC)

In some spear phishing emails, additional information is sought, in anticipation of a larger attack. BEC (business email compromise) is a type of phishing attack that is particularly dangerous, designed to convince the accountant into sending money and valuable assets to an attacker instead of the actual entity. As part of BEC, perpetrators pose as executives (CEO, CFO, president, senior manager, etc.) or representatives of the company claiming to handle critical and confidential information (Reuters, 2016). High-level contacts (such as attorneys, key business partners, or large vendors) send or appear to send BEC emails from their email accounts and contain enough detail to appear trustworthy. (IBM, 2023)

Getting the information needed for a successful BEC attack isn't limited to spear phishing. It is also possible for hackers to gain access to email account data by deploying malware or exploiting system vulnerabilities. A successful BEC attack is among the most expensive cyberattacks, regardless of the tactics employed. During one of the most prominent BEC cases, the attackers impersonating a CEO earned nearly 50 million euros that were transferred into a bank account used by the attackers. (Reuters, 2016)

Security professionals face the challenge of defending enterprise networks against attacks that exploit human frailty effectively and efficiently. As phishing attacks are commonly used to penetrate the defences of a firm, it is important to detect phishing attempts as early as possible. By responding earlier in the attack chain, the greater is the chance of stopping, containing, and responding to the attack. Most commonly the corporations have technical defences in place to detect and prevent phishing messages before they reach employees' inboxes. Cybercriminals, however, are constantly refining their attack techniques and innovating new attack tactics making phishing attacks more sophisticated and evading detection even with advanced technical countermeasures being implemented. (Darem , 2021)

2.2.3 Account takeovers

In order to access business and personal websites, applications, and systems, most people have several online accounts. As the name implies, account takeover attacks are attempts to gain access to those accounts, allowing the attacker to steal data, deploy malware, or take advantage of legitimate access and permissions. (Cloudflare, What is account takeover?, 2023)

Authentication information, such as a username and password, is required for an account takeover attack to succeed. A variety of methods are available to attackers for obtaining this information, including credential stuffing. Credential stuffing attacks automatically attempt to log in to a user's account using a list of common or breached passwords. In many cases, the passwords on user accounts are weak or reused, which make these attacks possible. Both phishing and malware can be used to gain access to those accounts. (Cloudflare, What is account takeover?, 2023)

As a result of a successful account takeover, the attacker gains access and obtains the permissions of the legitimate account owner. The attacker can then perform a variety of actions, such as stealing data, delivering malware, and using the account for lateral movement to gain higher privileges in the system.

In 2017, RIA's cyber incident department CERT-EE was informed of several accounts being hijacked. For such cases, RIA received reports of Facebook account takeovers, but the same technique can be used in other environments. (Kuik, 2022) Facebook chat is a popular starting point for account takeovers. An individual receives a message from a friend inviting them to click on a web link. In one example, there is the text "Is that you in this video?" After someone clicks on a link, a malicious redirect is triggered to either a phishing site that requires a login or a malicious payload will be triggered. The method worked on both desktop computers and mobile devices. (Kuik, 2022)

2.2.4 Malware

As a general term, malware is any software with the intent of performing a malicious activity that adversely impacts a system's confidentiality, integrity, or availability.

Malware is most commonly a code-based entity that infects a host, such as viruses, worms, trojan horses or other code-based entities and can also include spyware and adware. (ENISA, 2022)

There is a common misconception that viruses and malware are the same thing, but from a technical perspective, they are not. You can think of malware as malicious code. Viruses are just one type of malware with the ability to self-replicate. Malicious code is what causes computer viruses to spread across networks and computers. (Belcic, 2023)

Malware follows a similar pattern: You get infected when you unknowingly download or install malicious software, often by clicking on an infected link and visiting an infected website or downloading software from non-official sources. (Belcic, 2023)

An inadvertent act triggers the downloading of malware most of the time. You might do this by clicking on a link in an email leading to a malicious website or simply end up visiting a malicious website while browsing the internet. Another way hackers spread malware is through free software download bundles and peer-to-peer file-sharing services. It is possible to spread malware across a wide user base by embedding malicious computer code in popular torrents or downloads. (Belcic, 2023)

Ransomware

As defined in ENISA's Threat Landscape for Ransomware Attacks report, ransomware attacks involve threat actors taking control of a target's assets and demanding a ransom to restore the asset's functionality. The action-agnostic definition is necessary to cover the changing ransomware threat landscape, the prevalence of multiple extortion techniques, and the various goals of the perpetrators beyond financial gain. In the reporting period, ransomware was a major threat, with several high-profile and widely publicized incidents. (ENISA, 2022)

Open-source ransomware programs are easily accessible to attackers. The profits from successful attacks can be enormous, with some ransomware operators earning millions and forcing companies, individuals, and governments to manage the consequences of the attack. In recent years, cybercriminals have increased their efforts to commit ransomware attacks due to the potential rewards. (Seguin & Latto, 2023)

This was especially evident during the COVID-19 pandemic, when cybercriminals targeted hospitals with ransomware, further aggravating an already dire situation where the victims had no other chance than to pay as the provided services were vital to a person's life (Greig, 2021).

Ransomware is most commonly spread by e-mails or by gaining access to the systems using remote access tools. With generic interpreters, attackers can create cross-platform ransomware that can do a lot of damage in a short period of time. An increase in attacks is due to new techniques such as encrypting whole disks rather than individual files. The spread of ransomware attacks and other malware has become even easier thanks to malware kits and ransomware as a service (RaaS). (Seguin & Latto, The Essential Guide to Ransomware , 2023)

Spyware

The goal of spyware is to remain hidden while it collects information and tracks your online activities on your computer or mobile device. Your entries, uploads, downloads, and storage can be monitored and copied. In certain strains of spyware, cameras and microphones can be activated to spy on and listen to user activities. (Seguin, 2022)

The nature of spyware makes it dangerous because it is invisible by definition. According to Seguin: "Spyware is designed to be invisible, which is one of its most harmful attributes - the longer it goes undetected, the more damage it can cause." (Seguin, 2022)

Computers and mobile devices can be monitored and recorded using spyware. Data and personal information are collected by cybercriminals using spyware; some strains have specific behaviours. (Seguin, What Is Spyware, Who Can Be Attacked, and How to Prevent It, 2022)

As well as monitoring and storing targets online activities and capturing sensitive data, spyware has other uses. It is possible for some strains to force unwanted pop-up ads into your web browsing experience or to overtax your computer or mobile device's processor. There are others that are used to drive traffic to websites. (Seguin, What Is Spyware, Who

Can Be Attacked, and How to Prevent It, 2022) The following is a list of some of the most common spyware types:

1. **Adware** - advertisements are displayed automatically when you use advertising-supported software or browse the internet. The purpose of adware in malware is to secretly install itself on your computer or mobile device, spy on your browsing history, and then display intrusive ads to you. (Seguin, What Is Spyware, Who Can Be Attacked, and How to Prevent It, 2022)
2. **Keyloggers** - malware that records all your keystrokes and saves them into encrypted log files. Keystroke logging spyware collects all text messages, emails, usernames, and passwords you type into a computer, smartphone, or tablet. (Seguin, What Is Spyware, Who Can Be Attacked, and How to Prevent It, 2022)
3. **Infostealers** computers and mobile devices can be used by infostealers to steal your information. Unlike keyloggers, other types of infostealers can do much more than record and store keystroke information. Your browsing history, documents, and instant messaging sessions can also be harvested, for example, by scanning your computer for specific information. (Seguin, What Is Spyware, Who Can Be Attacked, and How to Prevent It, 2022)

2.2.5 Distributed Denial of service

Distributed Denial of Service (DDoS) attacks take place when a system or service does not provide users with the data, services, or other resources they need. It is possible to accomplish this by exhausting a service's resources or overloading an infrastructure component. (ENISA, 2022)

Cloud computing is a primary threat vector for DDoS attacks that use web-based attacks, which are often distributed through web applications. Web-based attacks can be used to build botnets on the cloud that can be used to launch denial of service attacks against a system.

Since COVID-19 pandemic emerged, existing threats have been amplified to exploit its uncertainties. During COVID-19, DrDoS and extortion by DDoS increased during July and August 2020, mostly targeting e-commerce, finance, and travel businesses. DDoS

attacks are still targeting websites related to COVID-19 sites. A DDoS attack was targeted against a Philippine vaccination registration site as well against a Dutch website distributing QR codes for cafes and cultural attractions in that required proof of vaccination. DDoS attacks have also affected Italian and Bulgarian COVID-19 services, with government agencies, including those in the EU, experiencing an increase in DDoS extortion attacks linked to COVID-19 protocols, affecting several critical services. (ENISA, 2022)

2.2.6 Misconfiguration

An example of a misconfiguration vulnerability is a weakness in the configuration of a software component or subsystem. Web server software, for example, can be provided with default user accounts that are easily obtainable for cybercriminals who can use these to access the system. It may also be provided with a known set of configuration files or directories that a cybercriminal can exploit to gain access to the system. (Dizdar, 2021)

Misconfiguration vulnerabilities in software can expose applications to attacks that target any component of the stack, including remote administration operations. (Dizdar, 2021)

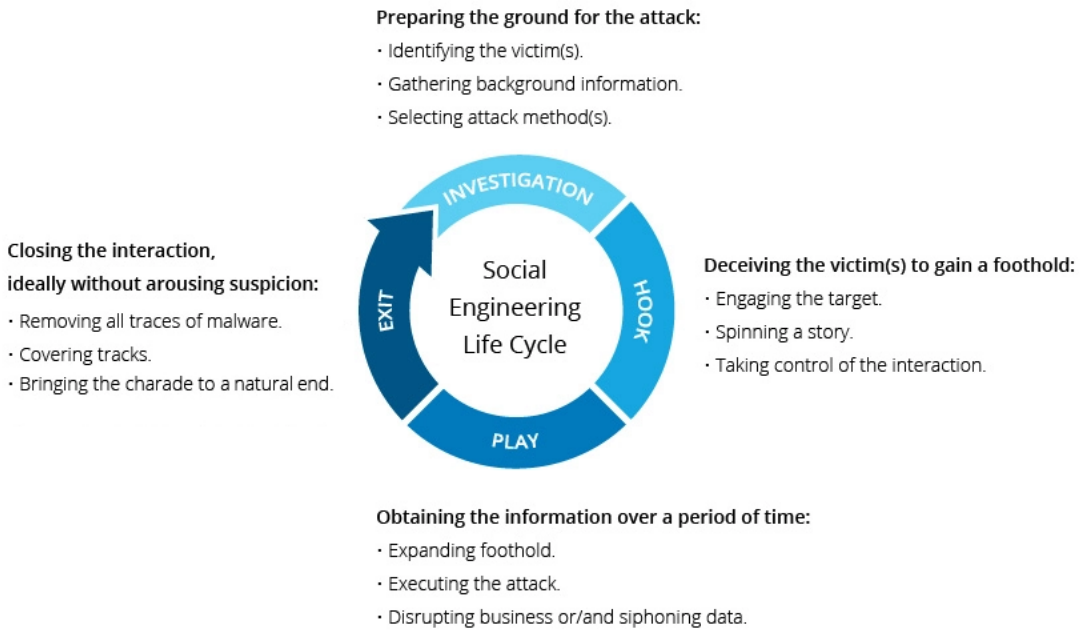
Any level of an IT infrastructure can be compromised by misconfigurations, including operating systems, network devices, servers, databases, and applications. Misconfiguration can occur for a variety of reasons, including human error, software bugs, and inadequate security controls. (Reciprocity, 2022)

2.2.7 Social engineering attacks

The term "social engineering" refers to a broad range of activities aimed at exploiting human error or behaviour to gain access to information or services. Victims are tricked into making mistakes or handing over sensitive or secret information through various forms of manipulation. Despite the use of technology in these tricks, they always depend on a human element to work. (ENISA, 2022)

As a part of social engineering attacks, a perpetrator first investigates the target to gather information, such as potential entry points and weak security protocols, so that he can proceed with the attack. Once the attacker has gained the victim's trust, the attacker can provide stimuli for subsequent actions that violate security practices, such as revealing sensitive information or granting access to critical resources (Imperva, Social Engineering, 2022). Figure 2 illustrates the lifecycle of social engineering from beginning to end.

Figure 2. Social Engineering Attack Lifecycle



Source: (Imperva, Social Engineering, 2022)

Due to the fact that social engineering relies on human error rather than software and operating system vulnerabilities, it is particularly dangerous. Legitimate users' mistakes are less predictable than malware-based intrusions, making them more difficult to identify and mitigate. (Imperva, Social Engineering, 2022)

2.2.8 Disinformation and misinformation

According to a JRC report, misinformation narratives emerged during the pandemic that focused on more than just health issues. Most of them focused on political and societal topics, making misleading or false claims about policy actions. (JRC, 2023)

Often, these stories were based on pre-existing conspiracy theories. It was most discussed that the virus was not naturally occurring (especially early during the pandemic), that the pandemic was orchestrated, or that a vaccine was being developed with hidden purposes. As vaccination became more relevant, the latter narratives became more prevalent. (Bruns, Dessart, & Pantazi, 2022)

False information and information manipulation also lead to distrust of government, political leaders, and public institutions, not just health issues. Every policy area should be concerned with the threat of misinformation to social cohesion and democracy. (Bruns, Dessart, & Pantazi, 2022)

COVID-19 has been plagued by misinformation, with false information being spread about its origins, transmission, and potential treatments during the pandemic. As a result, public health authorities have had difficulty managing the pandemic effectively due to confusion and mistrust. Misinformation has even resulted in dangerous behaviours, including the consumption of harmful substances, to treat or prevent COVID-19. (Brennen, Simon, Howard, & Nielsen, 2020)

Due to the speed and reach of online platforms, misinformation has spread quickly and widely during the pandemic. Even if the information is false, social media algorithms tend to amplify content that generates strong emotional reactions, such as fear or outrage. As a result, misinformation has spread rapidly and widely, often before it can be debunked or fact checked. (Kranhold, 2020)

The use of false information can also pose a threat to cybersecurity, particularly in the public sector. False information about the COVID-19 pandemic, for example, has been used to spread malware and launch phishing attacks. (Saleous, et al., 2023) Additionally, misinformation can undermine trust in institutions and organizations responsible for cybersecurity, making it difficult to implement effective security measures.

2.3 Strategy

Effective cybersecurity is essential for any organization that relies on computer systems, networks, and data to carry out its business operations. A comprehensive cybersecurity strategy involves several key components, including risk assessment, prevention, detection, and response. (Shea, Gillis, & Clark, 2023)

A risk assessment is the process of identifying and evaluating potential security risks and vulnerabilities. This involves analysing the organization's IT systems and identifying potential security threats. Prevention involves implementing measures to reduce the likelihood of a security breach, such as using strong passwords, implementing firewalls, and keeping software up to date. This may also include measures such as restricting access to sensitive data and limiting the use of external devices.

Detection involves monitoring computer systems and networks for signs of unauthorized access or other security breaches. This may involve the use of intrusion detection systems, firewalls, and other security technologies. Rapid response is critical in the event of a security breach, and organizations should have an incident response plan in place to minimize the impact of any security incidents.

In addition to these technical measures, effective cybersecurity also requires organizational policies and procedures to ensure that employees understand their roles and responsibilities in maintaining cybersecurity. This may include training programs, awareness campaigns, and regular security audits to identify potential vulnerabilities.

2.3.1 Estonian Cybersecurity Strategy

As a result of the first coordinated cyber attack against Estonia in 2007, awareness of cyber threats reached a new level in international security, not only because of the coordinated cyber attack against Estonia as a nation, but also because of a number of large-scale cyberattacks that affected important information systems in many other countries (Kaitseministeerium, 2008). Increasing cyberattacks signal the arrival of a new era, where cyberspace is taking on global security dimensions, and protecting critical information systems is as critical as nation-state defence capability. A coordinated cyber attack against Estonian government institutions, banks, media, and telecommunications

companies has proven the vulnerability of society's information systems is an aspect of national security that needs more attention than ever before (Kaitseministeerium, 2008). Even though Estonia has clearly and unambiguously recognized the need for protecting information systems, the measures taken for this purpose have not always been sufficient. In order to ensure cyber security for an entire country, the entire society must be involved, and a clear national division of labour must be established to prevent cyberattacks, as well as increasing information security competences as well as raising society's awareness of cyberspace's dangers.

Estonia has had three cybersecurity strategies: Cybersecurity Strategy 2008-2013, Cybersecurity Strategy 2014-2017, and Cybersecurity Strategy 2019-2022.

Estonia's third national cybersecurity strategy documents define long-term visions, objectives, priority action areas, roles, and tasks for the domain, forming the basis for activity planning and resource allocation. Lessons learned from the previous two strategy periods (2008-2013 and 2014-2017) are incorporated into the new strategy (MKM, 2019). It involves all contributing stakeholders in Estonia: the public sector (civil and defence), essential service providers, sectoral entrepreneurs, and academia. The aim of this document is to establish a comprehensive, systematic, and inclusive sectoral policy and to set up conditions for its implementation (MKM, 2019). Performance areas connected to planning activities necessary for implementing the objectives of the Cybersecurity Strategy and the structure of System for management of the cybersecurity sector are illustrated in Appendix 2.

Estonian cybersecurity strategy was among the first of its kind worldwide. In today's world, national cybersecurity strategies are commonplace, as was the approach used by Estonia in its first cybersecurity strategy (MKM, 2019). In 2013, the European Union (EU) cybersecurity strategy defined national cybersecurity baselines (identifying national competent authorities, creating national incident response teams, developing national cybersecurity strategies); these were incorporated into the 2016 EU Network and Information Systems Security Directive as legal obligations (MKM, 2019).

The Estonian Cyber Security Strategy emphasizes education and awareness, recognizing that effective cybersecurity requires active participation by all stakeholders. As part of the strategy, cybersecurity education is being promoted in schools and universities, as well as public awareness campaigns aimed at encouraging individuals to adopt secure

online behaviours. Cybersecurity in Estonia is a comprehensive, coordinated approach, providing a strong foundation for safeguarding the country's digital infrastructure.

2.3.2 E-ITS

E-ITS is the Estonian standard for information security management. Using Estonian language and Estonian legal system, the standard is in accordance with current legislation. It complies with the internationally recognized ISO/IEC 27001 information security management standard. (RIA, Estonian information security standard (E-ITS), 2022).

EVS-ISO/IEC 27001:2014 and German BSI IT-Grundschutz (BSIG) are the foundation for the E-ITS (RIA, Estonian information security standard (E-ITS), 2022).

The goal of E-ITS is to provide a basis for organisations for managing information security that would be written in Estonian and compatible with the laws of Estonia and the ISO/IEC 27001 standard. Organizations can achieve an appropriate level of security by using benchmark measures and an implementation system from E-ITS (RIA, Cyber Security in Estonia 2021, 2021).

3. Methodology

The purpose of this chapter is to describe the process of conducting the research. It provides an overview of the research process, research design, sampling, data collection, and analysis method. A qualitative case study forms the basis of the master's thesis. Due to the nature of the research questions, a qualitative study was chosen for this work. As a result of this collection method, we can gain a better insight of the opinions of the study participants. The case study would be based on Estonia's experience; it would be exploratory, seeking to provide insight into the phenomenon.

3.1 Case study

The use of a case study is a suitable method for investigating the emerging cyber threats in the Estonian public sector during and after COVID-19. The complexity of the topic, the need for a detailed examination of specific cases, and the availability of rich data sources make a case study an appropriate method for this research A case study is an appropriate method for this research because of the complexity of the topic, the need to examine specific cases in depth, and the availability of rich data sources. Through the case study approach, specific cases can be examined in-depth, providing a nuanced understanding of the issues, and informing future cybersecurity strategies in Estonia.

Case studies are a valuable tool for understanding the complex and multifaceted events. They provide detailed insights into the experiences of individuals and communities, offer multiple perspectives on the challenges and opportunities of the pandemic, and allow for a nuanced analysis of specific policies and interventions. By utilizing case studies, we can develop more inclusive, evidence-based, and effective responses to the ongoing crisis and better prepare for future.

Research methods such as case studies are widely used in social sciences to study complex phenomena or events. Case studies, as defined by Robert K. Yin in his book "Case Study Research: Design and Methods," are empirical investigations of contemporary phenomena in their real-life context, particularly when there are no obvious boundaries between phenomenon and context. (Yin, 2008)

Case studies are conducted in order to gain a deeper understanding of a particular case by examining multiple data sources, such as interviews, observations, documents, and artifacts. According to Yin, case studies are particularly useful when the phenomenon of interest is rare or unique, if it is hard to observe directly, or if it is embedded in a complex system. (Yin, 2008)

Yin describes the steps involved in conducting a case study as follows (Yin, 2008):

1. Identification of research questions: The researcher must identify the research questions that will guide the investigation. Open-ended questions should allow for exploration of the case in its real-life context.

2. Identifying the case or cases to study: The researcher must identify the case or cases to study. Cases can be individuals, groups, organizations, communities, or phenomena.

3. Data collection: The researcher collects data from a variety of sources, including interviews, observations, documents, and artifacts. It is important to collect data in a systematic and rigorous manner, and the researcher should triangulate the findings using multiple sources.

4. Research techniques include coding, categorizing, and theme development to analyse data. Identifying patterns, themes, and insights related to the research questions is the goal of the analysis.

5. A narrative format is used to present the findings in response to the research questions. In addition to providing evidence-based conclusions, the report should be clear, concise, and well-written.

According to Yin, there are three types of case studies: exploratory, descriptive, and explanatory. A descriptive case study provides a detailed description of a particular case, while an exploratory case study aims to gain a preliminary understanding of the phenomenon. The purpose of explanation case studies is to test or develop theories, and they typically involve multiple cases. (Yin, 2008)

Despite their value, case studies do have some limitations. A common criticism of case studies is that they are subjective, unrepresentative, and lack generalizability. It is possible, however, to make case studies more rigorous and credible by triangulating the

findings, using a variety of data sources, and providing evidence-based conclusions, according to Yin. (Yin, 2008)

3.2 Institutional theory

In the social sciences, institutional theory has been widely used to study the interaction between organizations and their environments. According to this theory, organizations are shaped by social and cultural norms, values, and beliefs within their environment. Norms, values, and beliefs are often taken for granted and regarded as valid and authoritative. Organizational change, innovation, and legitimacy have all been studied using institutional theory. As a basis for understanding emerging cyber threats in the Estonian public sector during and after COVID-19, institutional theory will be used.

It is important to place the concept of institutional logics within the context of institutional theory and institutional analysis to better understand it. Organizational analysis has a long history of studying institutions, beginning with Selznick's empirical analyses of organizations and their institutional environment, and Parson's theoretical work, based on universalistic rules, contracts, and authority that integrate organizations with other organizations in society. (Thornton & Ocasio, 2008)

Meyer and Rowan and Zucker introduced a new approach to institutional analysis in the 1970s, which highlighted the role of culture and cognition. According to Meyer and Rowan, modernization rationalizes taken-for-granted rules, resulting in isomorphism in formal organizational structures. For organizations to be legitimate, they had to conform to the requirements of external environments, which meant loosely coupling their technical cores from their external environments. Among Meyer's concerns was the importance of rationality in the account of western culture, as well as the development of formal organizational structures within world society and its cultural system. Zucker also emphasized the taken-for-granted nature of institutions and the role cultural persistence played in institutionalization. (Thornton & Ocasio, 2008)

Meyer and Rowan's focus on isomorphism was extended to organizational fields by DiMaggio and Powell. In their approach to isomorphism, DiMaggio and Powell focused on coercive, normative, and mimetic sources. (Thornton & Ocasio, 2008)

A key concept in institutional theory is institutional isomorphism, which refers to organizations conforming to the values and norms of their environment. This conformity is driven by three main actors: coercive, mimetic, and normative. (DiMaggio & Powell, 1983)

An external actor, such as regulators, can enforce institutional norms and values through coercive pressure. (Scott, 2008) Regulatory bodies or international organizations that implement cybersecurity standards and regulations may exert coercive pressure in response to emerging cyber threats.

The concept of mimetic pressure refers to organizations imitating other organizations in their environment. In many cases, this is caused by uncertainty and a lack of knowledge about effective practices. (Scott, 2008) Cyber threats may lead organizations to imitate successful or reputable cyber practices of other organizations in order to protect themselves.

In organizational behaviour, normative pressure refers to the influence of cultural and social norms. In many cases, this pressure is based on a belief that certain practices are morally or socially acceptable. (Scott, 2008) Public expectations and the desire to appear responsible and trustworthy may contribute to normative pressure in the context of cyber threats.

Institutional theory is a sociological theory about how organizations and institution's function and respond to external pressures. Organizational behaviour and decision-making are shaped by formal and informal rules, norms, and values. Social, cultural, and political factors also influence organizations, according to institutional theory. (DiMaggio & Powell, 1983)

Three levels of analysis are often distinguished by institutional theorists:

1. An organization's institutional environment is its broader social, cultural, and political context. Legal frameworks, cultural beliefs, and social expectations all contribute to the institutional environment that shapes organizational behaviour. (Scott, 2008)
2. The concept of organizational fields refers to the grouping of organizations that participate in similar activities and compete for the same resources. To gain

legitimacy, organizations within a field often conform to the norms and practices of their peers. (DiMaggio & Powell, 1983)

3. Organizations: Individual organizations and their responses to external pressures from the institutional environment and their organizational field. In order to gain legitimacy or conform to field-level expectations, organizations may adopt certain practices or structures. (Scott, 2008)

In analysing the Estonian public sector's response to the emerging cyber threats during and after COVID-19, institutional theory provides a useful lens. A key feature of institutional theory is its emphasis on social, cultural, and political factors that influence organizational behaviour. This chapter examines the Estonian public sector's response to cyber threats using Institutional theory.

3.2.1 The e-Estonian institutional environment

Cybersecurity is significantly influenced by the institutional environment in which the Estonian public sector operates. Estonia is a member of the European Union and NATO, which have established procedures, regulations, and legal frameworks related to cybersecurity. The Estonian government is also seen as a leader in e-governance and digitalization, which has also made it a target for cyberattacks.

The institutional environment changed rapidly during the COVID-19 pandemic as governments and organizations shifted to online services and remote work. As a result of this new reality, the public sector in Estonia had to adapt quickly., This posed new challenges and risks for cybersecurity. In addition, the pandemic changed the institutional environment, increasing awareness of and attention to cybersecurity risks.

Organizational fields

Government and public administration encompass the Estonian public sector. There is a high degree of interdependence and competition for the resources in the field which makes many services interdependent of each other and requires involvement of multiple stakeholders to solve an incident.

There are established norms and practices related to risk management, information sharing, and collaboration in the field of cybersecurity. Estonian public sector is also obliged to report all their cybersecurity incidents to CERT-EE.

As a result of the COVID-19 pandemic, government and public administration have been forced to adapt to new ways of working and interacting. As a result, organizations had to find new ways to manage risks and collaborate with one another, which included changes to norms and practices around cybersecurity.

Organizations

The Estonian public sector includes a wide variety of organizations, including government ministries and agencies as well as local governments. All organizations have their own cultures, structures, and practices, which are influenced by their institutional environment and no two organization cultures are exactly alike.

Every organization manages risk differently, shares information differently, and collaborates differently when it comes to cybersecurity. Depending on their resources and priorities, some organizations have more advanced cybersecurity measures than others.

Each organization interviewed faced the challenge of adapting its cybersecurity practices during the COVID-19 pandemic. A number of changes were made to policies and procedures, as well as investments in new technology and employee training.

Using Institutional Theory to analyse the Estonian public sector's response to cyber threats during and after COVID-19 provides a useful framework for analysing the social, cultural, and political factors that have influenced organizational behaviour. We can gain a deeper understanding of the emerging cyber threats by analysing the institutional environment, the organizational field, and individual organizations.

3.3 Interviews

The choice of semi-structured interviews as a data collection method for this thesis is based on several reasons. First, interviews allow for a deeper understanding of the emerging cyber threats in the Estonian public sector during and after COVID-19. Second, interviews provide an opportunity to explore the experiences and perspectives of cybersecurity experts in the Estonian public sector. Third, interviews allow for a flexible and interactive data collection process, which can produce rich and detailed data.

Interviews are a useful method for gaining insight into complex and nuanced issues (Laherand, 2010), such as emerging cyber threats. Through interviews, the researcher can explore topics in depth and ask follow-up questions to clarify and expand upon participants' responses. (Laherand, 2010) Interviews also allow for the exploration of participants' experiences and perspectives, which can provide valuable insights into the specific challenges and opportunities faced by cybersecurity experts in the Estonian public sector.

Prior to the study, the supervisor contacted the experts, either digitally or orally, and explained the purpose, planned interview, and consent process. Additionally, the time and location of the interview were discussed. As part of the study's ethical requirements, it was explained that all participants are free to participate, and their confidentiality will be maintained. In total 11 experts were contacted with a request for an interview. Out of 11 only 2 replied. This means that the results of the interviews cannot be used for generalization for the entire public sector.

Interviewees chose the location for semi structured interviews. Individual interviews were conducted with the experts. As part of each interview, the purpose of the study was explained, and participants were encouraged to talk freely about their experiences, emphasizing confidentiality and the importance of every opinion and experience.

The data obtained from the interviews was transcribed. Converting recorded interviews into text is called transcription or literalization. (Taylor, 2023) In this way, it is better and more comprehensive to interpret the data.

In order to improve the understanding of the written text and convey non-verbal communication (such as pauses, speech rhythm, change in tone of voice, etc.) specific signs were being used during transcription. The following characters have been used in transcribing the interviews of this master's thesis (Laherand, 2010):

- Italics - interviewer's speech
- (.) - short but noticeable pause
- (2) - a longer pause, the duration of which is displayed in seconds
- = - no pause between words
- (laughter) general laughter
- (hhh) exhalation
- (.hhh) audible inhalation
- underlined emphasized place

3.3.1 Semi structured expert interviews

An interview that is semi-structured allows the researcher to collect detailed and rich data on a particular subject. The purpose of this thesis is to gather data on cyber threats affecting the Estonian public sector during and after COVID-19 through semi-structured interviews. Structured and unstructured interviews can be combined in semi-structured interviews. In contrast to an unstructured interview, the interviewer knows what questions to ask. (George, 2022) The order and phrasing of the questions are not fixed in a semi structured interview. The nature of semi-structured interviews allows them to be flexible, as they are often open-ended. The use of set questions in a set order can make comparisons easier, but it can also be restrictive. By allowing for comparisons between respondents, you can discover patterns with less structure. (George, 2022)

3.4 Material sample

It is important to use multiple sources of evidence when conducting academic research in order to ensure data validity, accuracy, and quality to ensure that the researchers are able to compare and understand information obtained from stakeholders. Semi-structured

expert interviews and documents were the primary sources of evidence in this thesis. The analysis of document sources, including peer-reviewed scholarly papers and articles in the field, governmental decrees and reports, studies, and literature, will also contribute to the collection of data.

Document analysis is used as a data analysis method in this work. Since the aim of the thesis is to investigate emerging cyber threats in the Estonian public sector during and after COVID-19, such institutions as RIA, ENISA and the Ministry of Economic Affairs and Communications were suitable for collecting data. Furthermore, documents produced by non-government organizations and policy-making organizations will be used. The material will also be drawn from a variety of online news sites. A large portion of the impact of academic literature is attributed to reports, reviews, and books. The following words and their combinations were used to search for a sample of sources:

Cyber literacy, cybersecurity, covid-19, e-governance, local government, digital literacy, pandemic, covid.

"cybersecurity" AND "covid-19" OR "covid"

"cybersecurity" AND "covid-19" OR "covid" AND "e-government"

"cybersecurity" AND "covid-19" OR "covid" AND "e-government" AND "local government"

" cybersecurity" AND "covid-19", "cybersecurity", "digital literacy"

After sorting the obtained results, the author also narrowed the time period discussed in the articles to coincide primarily with that of the COVID-19 period. As a final step, the author ensured that the literature covered the topic in general and the sources cited were legitimate.

In addition, works previously written by the author have also been used: “Threats in cybersecurity during covid crisis”.

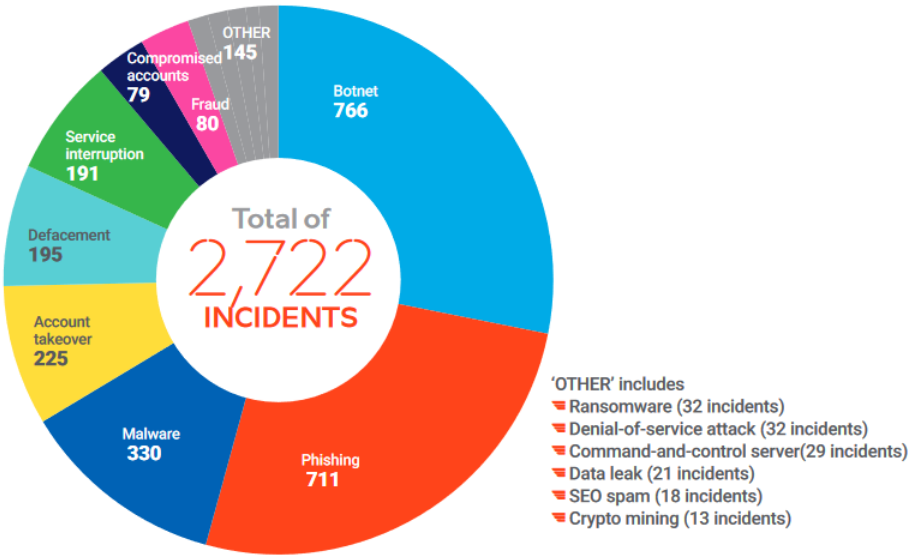
4. Analysis

In Chapter 4, expert interviews and data analysis are used to provide an in-depth analysis of cybersecurity trends and changes in Estonia. In this chapter, insights into the current state of cybersecurity will be provided by semi-structured interviews conducted with public sector cybersecurity experts in Estonia. Using the views and experiences of cybersecurity experts, this chapter provides valuable insights into the evolving threats and opportunities in Estonian cybersecurity. In total 11 experts were contacted with a request for an interview. Out of 11 only 2 replied. This means that the results of the interviews cannot be used for generalization for the entire public sector.

4.1 Cybersecurity trends and changes in Estonia

The purpose of this subchapter is to highlight various cyber threats that threaten Estonian users. As a result of analysing trends and changes among cybersecurity incidents, we can identify weaknesses and focus on improving defences against specific threats. Cybersecurity threats are constantly evolving, as illustrated by the trends presented in this chapter. With the development and adoption of new technologies, new vulnerabilities, and attack vectors as well as change of tactics by cybercriminals also emerge. The data presented is based on RIA's annual reports.

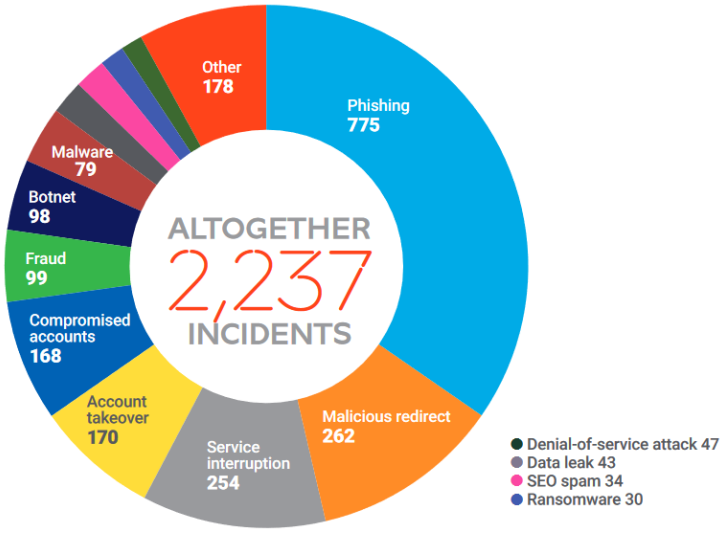
Figure 3. Incidents with an impact in 2020



Source: (RIA, 2021)

From the data presented in Figure 3, it can be observed that in 2020, there were a total of 2722 incidents with varying impact. The highest number of incidents were related to botnets (766) and phishing (711), followed by malware (330), account takeover (225), defacement (195), service interruption (191), fraud (80), compromised accounts (79), and other (145). The other category included ransomware (32), distributed denial of service attack (32), command-and-control servers (29), data leaks (21), SEO spam (18), and crypto mining (13).

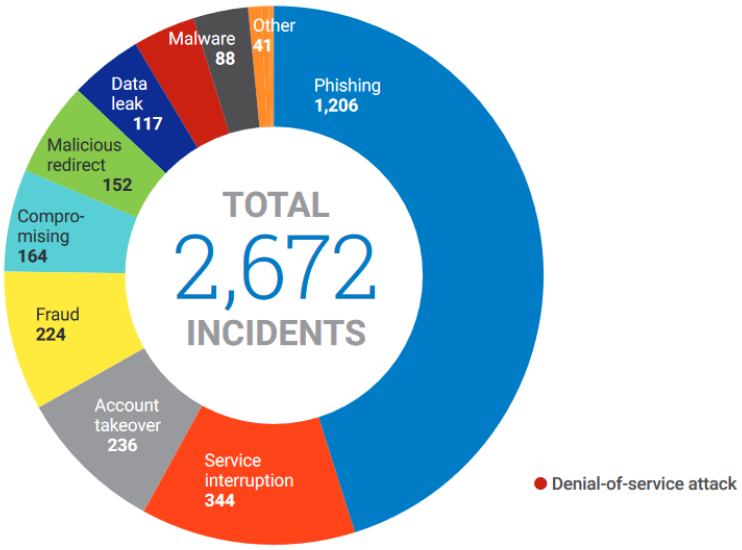
Figure 4. Incidents with an impact in 2021



Source: (RIA, 2022)

In Figure 4, the trend for 2021 shows that the total number of incidents decreased to 2237, but phishing became the highest number of incidents with 775. Malicious redirect (262) and service interruptions (254) were the second and third highest incidents. Account takeover (170) compromised accounts (168), and fraud (99) were also significant. The other incidents reported were botnet (98), malware (79), distributed denial of service attack (47), data leak (43), SEO spam (34), ransomware (30), and other (178).

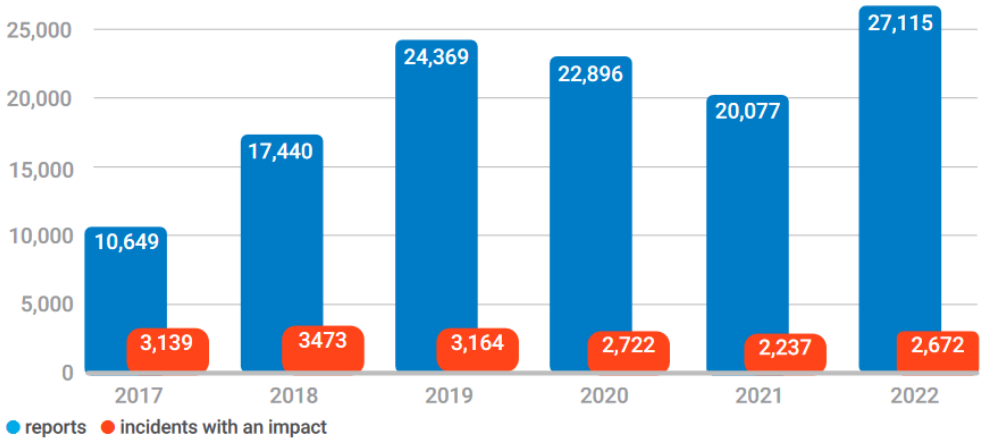
Figure 5. Incidents with an impact in 2022



Source: (RIA, 2023)

From Figure 5, it can be concluded that phishing became the most common type of incident reported in 2022, with 1206 incidents. Service interruption (344) and account takeover (236) were also significant. Fraud (224) and compromising (164) incidents were also high. Malicious redirects (152), data leaks (117), distributed denial of service attack (100), and malware (88) were also reported, with other incidents making up only a small percentage of the total.

Figure 6. Number of incidents and reports submitted to CERT-EE



Source: (RIA, 2023)

From Figure 6, it can be seen that there was a steady increase in the number of reports submitted to CERT-EE from 2017 to 2022. While there was a slight dip in 2020 and 2021 in the number of incidents, there was a significant increase in the number of reports submitted in 2022. This trend may suggest that more people are reporting cybersecurity incidents or that there was an increase in the number of incidents that occurred.

From Figure 3, we can see that in 2020, the most common types of incidents with an impact were botnets and phishing attacks, followed by malware and account takeovers. Defacement and service interruptions were also significant. In comparison, Figure 4 shows a shift in 2021, where phishing attacks became the most common type of incident with an impact, followed by malicious redirects and service interruptions. Botnets and malware dropped in frequency, but account takeovers and compromised accounts remained significant. Additionally, there were notable increases in data leaks, SEO spam, and ransomware incidents.

From 2022, Figure 5 shows that phishing attacks continue to dominate as the most common type of incident with an impact, followed by service interruptions and account takeovers. Fraud has now become a significant threat, with compromising and malicious redirects also increasing in frequency. However, the number of incidents classified under "other" has significantly decreased.

Figure 6 provides a broader view of incident trends over the past six years, as reported to CERT-EE. The number of reports submitted has steadily increased each year, apart from 2021, which saw a slight decrease. Despite this, the number of incidents with an impact has generally decreased, with a notable drop in 2020. This might be possible due to increased cybersecurity measures in response to the pandemic but cannot be confirmed by any sources for the statistics as qualitative research in the incidents has not been performed by CERT-EE regarding this specific decrease.

In conclusion, the data suggests that while the types of incidents with an impact may shift from year to year, the overall trend is one of increasing incidents, though decreasing severity. However, certain types of incidents, such as phishing attacks and account takeovers, remain persistent and significant threats to cybersecurity regardless of the situation in the world. It is essential to implement and maintain comprehensive cybersecurity policies to mitigate these threats and protect against potential damage, data loss, and disruption.

4.2 Interview results

The results of the research are summarized and interviews with experts are analysed in this subchapter. In total, 2 experts were interviewed. An interview invitation was sent to 11 experts, 2 of the experts responded and meetings were scheduled. The experts were given the option to remain anonymous and both participants used it. Participants are referred to as expert 1 and expert 2 in the future text. The interviewee chose the location. Interviews took place face-to-face and over the internet (Microsoft Teams). Online interviews were recorded with an EaseUS RecExperts audio recorder and face-to-face interviews were recorded with a mobile phone. The interviews were conducted in Estonian. The obtained data was transcribed using the Estonian Speech Recognition and Transcription Editing Service (Olev & Alumäe, 2022) solution developed by Aivo Olev and Taivo Alumäe. The interviews lasted between 27 and 44 minutes. The average duration of the interview was 35.5 minutes. A total of 17 semi-structured interview questions were asked, which are presented in Appendix 3.

It is critical to note that the sample size for the interviews conducted in this analysis is limited to two participants. Although their insights and perspectives are highly valuable, the small sample size may not be used for generalization for of the actual situation in the Estonian public sector. It may not be representative to all public sector institutions and may lack diversity. Thus, any further research should aim to increase the sample size to increase the generalizability of the results. It is also important to note that the organizations interviewed had an established high level of cybersecurity. It is highly likely that the overall Estonian public sector does not have the same cybersecurity standard and level of awareness. Moreover, the main target group, which is most vulnerable to cyber security attacks, was not reached, namely local governments. Out of 11 invitations for interviews, 9 were sent out to local governments but no response was received from any of the contacted IT personnel.

As part of the semi-structured expert interviews, the author asked the participants some questions about themselves and their backgrounds. It served a crucial purpose in establishing a baseline of the participants' expertise and experience to contextualize their responses to the later questions and assess the extent to which their professional roles and experiences influenced their responses.

Furthermore, by establishing a connection with the interviewees, it assisted in creating a more relaxed and open environment for the interview, making it easier for them to share their thoughts and experiences. In addition, it allowed me to personalize the interview process, making participants feel valued, and demonstrating a genuine interest in their own perspectives, not just those of their organizations.

It appeared that both experts agree that the most significant cyber threats against the Estonian public sector are related to data protection and vulnerabilities in legacy as well as up to date software and systems. Additionally, Expert 2 emphasized the vulnerability of local governments, hospitals, and other healthcare service providers due to their weaker data protection infrastructure and the risk of malware or intrusion into servers through vulnerabilities. These entities have requirements for data protection but quite often do not have the necessary expertise or service providers to manage it, making them potentially vulnerable to cyber attacks. The weakest links in the chain can be exploited to gain access to sensitive information, including identity codes of Estonian persons.

Expert 1: "If we talk about the overall picture, which are the biggest cyber threats in general, then in my view today, they are legacy and software problems."

Expert 2. „The rejection of legacy is certainly becoming increasingly important and because each area of government is responsible for itself, certain parts of the government, which, well, are not so strongly related to national security, should pay more attention to what is now happening, say what happens under Estonian IT Centre. “ Expert 2: "To whom not enough attention has been paid, perhaps the most threatening in this area, as such, are local governments. And certainly hospitals, family doctors, dentist offices, because, well, they have the requirements, but they don't have the kind of service providers that would manage all of this, which clearly now seems to have tightened up the rules in the field of data protection. In other words, if I wanted to get hold of all the identity codes of Estonian persons, well, even those of persons with a residence permit, then maybe it is no longer necessary to attack this or that central infrastructure, but you can get the same information from the weakest link.“ Expert 2: "In general these attacks are actually divided into two, that there are still attacks against public services, front end servers, mostly with the aim of either simply causing damage or obtaining data. That this gathering of information, so to speak, is definitely one aspect, and the other is definitely yes, this so-called expanded critical infrastructure that they want to cause damage to, and certainly here, well, our weakest point right now is still hospitals and local governments.

And now this a technique that, no matter how they get in, they are generally either malware or, in fact, intrusion into servers through a vulnerability. They are like two basic ways"

The question "In your opinion, what are the biggest shortcomings of public sector employees when it comes to awareness about cyber threats?" prompted insightful responses from both experts.

Expert 1: "The first thing they lack is probably the sense of danger. That if they don't understand what threatens them or how something threatens them, then they don't feel the need to develop themselves, and well, I can train them until the end of times, but if they don't understand why they need it, then they won't learn it." To summarize - if employees don't see the potential risks and dangers of cyber threats, they may not take proactive measures to protect themselves and their organization.

Expert 2: "The biggest shortcoming is definitely that top managers and leaders don't want to educate themselves. They feel extremely self-confident, which means that they are not willing to participate in training. Of course, it can always be improved by making it mandatory. But since this is how remote work is nowadays, training activities can also be done through remote work, different videos are watched. Questions can be submitted by e-mail."

Expert 2 also acknowledged the potential limitations of remote training, noting that while it can be a useful tool, it may not necessarily achieve the desired level of cybersecurity awareness and mistakes due to user negligence can still occur. "Perhaps the sought-after level will not be achieved, and in fact, in the group of public servants, it can be seen that these mistakes due to user negligence do happen."

Regarding cybersecurity training during and after COVID-19, both organizations mentioned that regular trainings take place annually. Both interviewed organizations organize security days once a year. Expert 2: "If you work here as a public servant, let's say, you'll definitely get three trainings in the cyber field a year, and you'll definitely get some tests as well."

Expert 1: "Basic hygiene training is what is actually done every year, that kind of basic hygiene of digital awareness."

Expert 2 also stated that: "I think we have an overabundance of trainings, which is also perhaps due to the fact that some trainings tend to be taken less, at least in the sense that since we have classified information in use, we have a lot of classified information trainings like these. But there are these information security trainings, so that everyone who travels in and out, that is, goes abroad, is told about the sources of danger in foreign countries. Furthermore, family security at long term rotations is a completely separate issue because families travel with them. And, so to speak, family members are in an extremely vulnerable state from a cyber perspective. You go to a new place of residence, a completely new environment, everyone moves in, opens new bank accounts, new schools, everyones distracted. New telco, does the new operator have full control of this router."

In addition, they noted that both institutions order an external service to test the receptiveness to cybersecurity threats of their own employees.

Expert 1: "We perform social engineering testing all the time, we have procured it as a service. These tests take place on ongoing basis, in fact, keeping awareness is a constant job. We procure them from an external service provider. We have an agreement with another institution that they don't even say when will these social engineering tests take place nor provide us with a sample of the test. Even I don't know when and what they will do. The last time, they tried to send me an e-mail and see if I clicked on it or not, that time it didn't go through. This is done on a continuous basis and small campaigns at a time, just so that people stay alert"

Expert 2 also noted that they have a similar service but, that they have moved a bit away from this option: „This component exists, that in this sense we actively evaluate the receptivity to cyberthreats of our public servants, so to speak. But I have to say that, well, we have perhaps somewhat deviated from this position of incrimination, that, well, I understand that it is reasonable to test it, but it is more like for the evaluation of the institution, not so much as for the evaluation of a specific employee, right? Let's say such an ideal person does not exist. “

Expert 1 was of the same opinion " If they make a targeted attack on me like a real targeted attack. I am absolutely sure that if they try a little bit, I will click on that email or link."

Both experts acknowledged that there have been situations caused by the lack of cybersecurity related training. Expert 1 stated that "Emails are still sometimes clicked,

users insert passwords where they should not be inserted. “ „In case someone tells you that they haven't been doing that, they are lying."

Meanwhile, expert 2 mentioned a specific scenario that occurred during the COVID-19 pandemic, where people working from home tried to connect their hardware to printers without proper security measures.

Both experts highlight the significant change in the work environment due to the pandemic, with many people transitioning to remote work. This change brought along new challenges and threats, as the environment became less controlled and more vulnerable. Expert 1 emphasized that the main change in cyberthreats was due to the change in the environment itself. The threats that existed in the office environment also existed at home, but the uncontrolled environment made it easier for the attackers to exploit vulnerabilities, employees were at home that have not been protected by the employer. Expert 1: "From the point of view of cyber threats, the fact that you go from a controlled environment to an uncontrolled environment is a common threat. So that you either lock the screen at home or you don't look who is around you. Well, let's say this, the main thing is that the environment changed and, consequently, everything that is a cyber threat due to the environment changed with it. So, well, I think that maybe not everyone went home to do their work, who went to work in the park when the weather was nice, who went to work on the beach, who went to work in Spain, that in this regard the environment changed and, so to speak, everything that is caused by the surrounding environment, brought along changes to the threats along with the change of environment."

Expert 2 notes that the organization had to adapt quickly to the new remote work reality and put in place measures such as increasing VPN connections, reviewing access rights, and purchasing new security devices. Both experts agree that remote work is a semi-untrusted environment that requires extra security measures to ensure the safety of the organization's data and systems.

Expert 2: "When this difficult movement restriction started to hit, in fact already then we developed different solutions and increased the possible number of VPN connections. We certainly also went through a large number of algorithms, reviewed all access rights. Well, it's clear that no network administration actually takes place in the remote work mode, at least not on such a normal scale, right? That, that also means that it had to be created for administrators who do their remote work, right? Well, it's not the same thing as remote

work for a regular user. Seeing a situation where the introduction of remote work is inevitable, so to speak, on a wider scale, we purchased various security devices and significantly changed the configurations in the computer network. And well, I think the focus on remote work is that the fact that it's like a semi-untrusted environment, I don't want to insult anyone's home, but because of that, all these extra security measures were developed. If previously, the remote work thing was rather limited to the recommendation not to use any unprotected dubious Wi-Fi at all, now it was , so to speak, the basic network. It is no longer so important in the sense that a lot of people used to go to Wi-Fis at the hotels, but now there is a mobile data hotspot for that, you don't have to go to a network that is prepared for an attack."

It appeared that both experts agree that there were changes in the environment due to COVID-19, which brought about new challenges in terms of cyber threats. However, it appears that there were no significant changes in response to these emerging threats. Expert 1 states that, despite the changes in the environment, in practice, nothing could be done for these threats, as no one goes home to watch what people do.

Expert 1: "Well, no, I mean, it didn't directly affect any of them. The only difference, which is not directly related to the cyber threats that existed, was the change that you have to manage in a different way. That if you used to lead people who sat next to you, now you lead people you don't see for weeks in between. In the field of cyber, well, nothing changed in practice, that these threats changed, but in practice nothing can be done for them, no one goes home to watch what they do. It all remained the same, because remote work was already such a very, very common practice for us, it just became the norm now."

Expert 2 explains that their team continued to guarantee their work capacity for others, and that they understood that the level of preparedness expected of them was higher than from others. Expert 2: "There was no difference in the sense that we are still like a support unit, which means that the support unit still had to guarantee the work capacity for others. This means that we all still went to work, and if someone got sick, we behaved accordingly, but let's say that we understood that at that moment, in fact, the level of preparedness that was expected from us was higher than others. That in fact we clearly went to work more intensively than at other times."

It seems like one of the biggest challenges faced by the Estonian public sector during and after COVID-19 was the sudden need to provide laptops for remote work. There were delivery difficulties and ad-hoc procurement contracts had to be extended to accommodate these needs.

Expert 1: "From the point of view, or what I saw cognitively from the sidelines, laptops. The biggest concern, otherwise, people worked in the office with a desktop computer, which is three times cheaper than a laptop. Then the pandemic came, and it was necessary to work at home overnight, then a desktop computer, well, it was very rarely carried home, the lack of laptops was a problem. But solutions were found operatively, and procurements were made quite quickly. That is like what felt as a bystander. Because from the point of view of our institution, the change was not so strongly felt at all, that everything that happened, it just happened. Well, remote work was before also relatively the norm in our institution."

Expert 2: "What made it more difficult was still the fact that there was a difficulty in the delivery of the hardware. Yes, that means there were major delivery difficulties and, well, yes, in the sense that those procurement contracts had to be extended."

In addition to these usual supply problems, one organization had more specific problems related to cybersecurity requirements, such as ensuring the security of the hardware they purchase. They also faced challenges when ordering hardware from potentially hostile countries where the regime may not be democratic, and where firmware's may have been changed. This made it difficult for them to ensure the security and functionality of the hardware they need for their work.

Expert 2:"Unlike other institutions, our organization can order to other locations. That, we can directly deliver to the remote location, it does change things a bit, yes, it does, because the security of the hardware is important to us, which means that, well, we can't make purchases on the spot, from every country. That if it is a hostile country, the fact that we buy an iPhone or a computer from there is not possible for several reasons, because first of all, in those countries where the regime may not be democratic. The firmware has often already been changed in these countries. Either Apple's iPhone may not be VPN-capable at all, it may not accept any foreign SIM cards, it may have a SIM card lock, it may not have that Facetime audio, which is encrypted and, so to speak, voice communication, may not have this support at all. "

The COVID-19 pandemic has highlighted the importance of cybersecurity preparedness and response. According to expert 1, it is crucial to choose proportional technical measures that are selective and tailored to the specific data set or access being protected, rather than implementing broad measures based on the institution or available funds. This approach will help to allocate resources more efficiently and effectively.

Expert 1: "Proportional technical measures, in order not to choose measures based on which institution I am in or which the funds available to me are only more, so to speak, to choose measures and, so to speak, oblige to implement measures according to which data set I work with, or which access I have, so that there are more selective measures, which I would recommend. Not that if I work in the field of security, then you have to paranoidly protect everything that belongs to this institution, well, there is no need for that. Maybe those places where it seems like a pointless field, but in fact some pieces still need protection, because of some vital infrastructure or something small. More selectivity, looking at what is being protected and then choosing the measures where this money will be put, because every measure requires a large investment and there are large sums at stake."

Expert 2 emphasizes the importance of seeking professional help and not relying solely on intrusion prevention systems (IPS), as they may not be enough to detect and prevent all cyber threats. Intrusion detection systems (IDS) may also be necessary in some cases, especially when dealing with a large number of instructions that an IPS may struggle to handle. Overall, the pandemic has highlighted the need for a comprehensive and flexible cybersecurity strategy that can adapt to evolving threats and changing circumstances.

Expert 2: "Well, one thing is for sure that RIA offers a lot of professional help, and it pays to use it. In the sense that IPS is not always enough, IDS is also needed, IPS is like one that generally okay, it's like on the one hand preventive, on the other hand, some kind of connection must take place in order for it to react at all. But sometimes the number of these instructions is so large that no IPS can calculate, well, so to speak, or well, maintain this proper data communication ability at it."

According to expert 2, one of the key lessons learned from the COVID-19 pandemic in terms of cybersecurity preparedness and response is the importance of practicing preparedness. "The fact that you have to practice preparedness, on the other hand, COVID-19 gave us good preparation for the crisis in Ukraine, and in fact there were still

intermediate stages. In a word, first there was COVID-19, then there were the hardware shortcomings of COVID-19, so to speak, then the next thing was that Estonia's preparedness definitely increased with the fact that when the situation on the borders of Lithuania and Belarus intensified, there was a threat of revolution in Belarus. That in this sense, I have to say that such preparedness for a crisis had not been so well practiced. That, sectoral crises were like the ash cloud of Iceland. There were once 2007 cyber attacks, but they were still sectoral so that, so to speak, this preparedness became like extensively tested"

In terms of specific technologies or practices to improve responding to cyber threats, Expert 2 recommended eliminating the use of USB memory sticks, as they can be a common vector for malware. They also advised training employees regularly on cyber security and malware threats and keeping them up to date with the latest information in the field of cybersecurity.

Expert 2: "Well, we have eliminated USB memory sticks a long time ago, that's definitely one thing. Let's say that since we have a heightened threat of cyberespionage software here, the advice to users is that everything should not be classified or hidden somewhere, on the contrary, you still have to train your employees with examples of cyber security or, well, so to speak, malware. That all the time they still have to be up-to-date, all these slides talk about the threats that have just appeared, when some completely new threats appear, don't wait for the training cycle, send notification letters immediately."

However, due to strong protection, other problems can also arise. Expert 2:"Since this thing works, in the sense that if you have very, very strong cyber security administrators, like we have, then, yes, completely different places will start to appear. That there will be this logic on the other hand, that like, well, as in example in organization, we proudly say that they have some of the cleanest mailboxes so far. Well, the user's attention is more distracted, because they don't have the daily experience of such filth coming in from the mailboxes as it will be taken down by the filters implemented by the IT team."

Based on the responses of both experts, it is clear that cybersecurity training and education are crucial in protecting individuals from cyberattacks. Expert 1 emphasizes the importance of implementing mitigation measures such as anti-virus protection, isolation of systems, and monitoring user behaviour.

Expert 1: "According to the situation, if someone enters these passwords, their account needs to be reset, we explain what happened to them, if they really clicked on a malicious link, we look at the computer and investigate what really happened. "

In addition, an additional question was asked about elderly users, who are in a higher risk group being more receptive of cyberattacks since this is something that was not an existing trend when they started their working lives. In terms of vulnerable groups such as older individuals, Expert 1 acknowledges that they may require more training to prevent cyberattacks. They suggest that everyone, regardless of age or experience level, is susceptible to cyber threats and risks can never be fully mitigated.

Expert 1: "Well, let's say that the thing with this older person is that they have to learn some things. That there is no choice, that if, for example, every Wednesday they get a crypto virus into my system, and I must restore it all the time, there are choices to be made. That there's no helping it, but, but they're a greater risk until the end of time than, say, well, compared to someone with average experience like that but, well, the sad thing is that we can have that senior citizen example, but if we take today's newcomers, so to speak, that picture isn't much better either. If that senior citizen knows that they don't know and won't click on anything, then this newcomer thinks they know everything. And, well, there are risks at every level." „Furthermore, there are several possible mitigation measures - anti-virus protection, isolation of systems, monitoring of user behaviour, that, well, they mitigate all these risks. If someone somewhere does something wrong, some system picks it up. That, in this respect, it is manipulation of risks, that some things can be mitigated with measures, but the risk can never be fully mitigated, and such a person should not be employed at certain positions."

Expert 2: "It is important to conduct trainings and to do workshops, in this respect, to perhaps explain the context there. We should basically help these people with knowledge of basic information technology, and if they now go abroad for a longer rotation, then, well inevitably, they have to figure out what a router is, there's nothing to do, and you also have to figure out the VPN as well." "We approach them one by one. It is always possible to hold personal trainings, and we have also considered that in the sense that it significantly relieves this tension, and the person feels that they are being dealt with personally."

It seems that there have been significant changes in funding for IT and cybersecurity in some organizations during and after COVID-19, while others have not experienced much change. In the case of Expert 2's organization, the budget has increased during COVID-19, with more money being put into cybersecurity, particularly for securing remote work. Before COVID-19, the resources were inadequate.

Expert 2: "Yes, the budget has increased during COVID-19 and more money has been diverted into cyber security. During COVID-19, the targeted funding was for stronger and smoother remote work. COVID-19 essentially ushered in the war in Ukraine, then at the management level we were already used to the fact that we had to invest more than before. And I have to say that before COVID-19 the resources we had were highly inadequate. Security financing is no longer looked at separately for a long time, because security must be integrated into all parts."

Expert 2 also mentioned that specific positions for cybersecurity have been created, which is a positive development. "Surprisingly, we have also received specific positions for cybersecurity, which must be highlighted because it is not generally available."

In Expert 1's organization, there were no big financial changes during COVID-19, but there was a relatively big change in terms of funding during the Ukrainian war. "From the cyber perspective, there was a relatively big change in terms of money. But Ukraine changed it, COVID-19 not so much. A lot of one-time funds were moved and are still moving because this situation is very hectic. The cyber world is not what it was a year ago. Important changes take place in months."

It is important to note that the situation may vary depending on the organization and its specific circumstances.

4.2.1 Remote working

Global labour markets were disrupted by COVID-19 during 2020. A sudden and severe outcome resulted in millions of people being laid off or losing their jobs. Others quickly adapted to working from home after offices were closed. Workplace changes brought by COVID-19 are most obvious in the dramatic growth of remote workers (Lund, et al., 2021).

COVID-19 has prompted authorities to move to remote arrangements based on remote access to critical systems and data. Considering the widespread transition to working remotely and the inherent vulnerabilities involved, we can expect to see more and more cyberattacks in the near future. Security controls for remote access should be implemented by organizations if they have not already done so (Adelmann & Gaidosch, 2020).

As part of my research interviews were conducted with two experts to learn more about the role of remote work during the pandemic. The purpose of this subchapter is to present insights on two key questions: whether their organizations offer remote working, and whether they have experienced cyber incidents because of remote working.

Both experts confirmed that remote work can be done in their organizations. One organization had certain restrictions on processing classified information. However, expert 2 noted that "You can definitely organize your work by doing things on time and you can do it by combining the fact that you can do normal work in your home office and for classified information you have to come to the office".

One of the questions asked by the author during the interviews was whether there were any cyber incidents due to remote work. Both experts stated that their organizations had not experienced any significant incidents specifically caused by remote work.

Expert 1 pointed out that "No, in this regard, it would not be said that something special has happened because of remote work., Nothing that is worth mentioning separately, due to that, that we do remote work and that's why things happened, things still happen regardless of whether it is remote work or not".

Expert 2 also noted that "Not directly in the sense that, remote work is actually still the computer itself. The computer has a number of cryptographic security functions, so that the computer itself has somehow become more vulnerable because of this, rather no."

It is important to emphasize that the organizations that were interviewed had a high level of cybersecurity measures in place, and remote work was not a new practice for them. Therefore, it can be assumed that the lack of significant cyber incidents caused by remote work might be attributed to the organizations' robust cybersecurity practices and experience with remote work.

4.2.2 War in Ukraine

On 24 February 2022, Russia launched a full-scale war against Ukraine, Estonia suffered an unprecedented number of DDoS attacks because of the conflict that expanded into cyberspace (RIA, Cyber Security in Estonia 2023, 2023).

A wave of DDoS attacks hit Estonia in 2022, the likes of which had not been experiences previously. The attack volumes were sometimes several hundred times higher than in 2007. While a few governmental websites or services would run slower than usual or be unavailable for a short while DDoS attacks were managed so that the public did not even notice any disruption of the services (RIA, Cyber Security in Estonia 2023, 2023).

Both Expert 1 and Expert 2 have stated that there have been notable cyberattacks and incidents in the organization during and after COVID-19. Expert 1 mentions that there were waves of DDoS attacks affecting the entire public sector in Estonia during the Ukrainian War, with some successful and some less successful attempts.

Expert 1: "COVID-19 was not the indicator or, well, during COVID-19, some minor things also started to happen, but when the war started in Ukraine, the wave of DDoS affected the entire public sector in Estonia." This is illustrated in Figure 7, three main DDoS attacks should be highlighted. Firstly, the attack in April 2022, when nearly 700 million malicious inquiries were sent to Estonian websites between Friday morning and noon, mostly from outside of Europe. According to RIA, they may have been timed to coincide with the Locked Shields cyber defence exercise. (Wright, DDos cyberattacks against Estonian state websites continue, 2022)

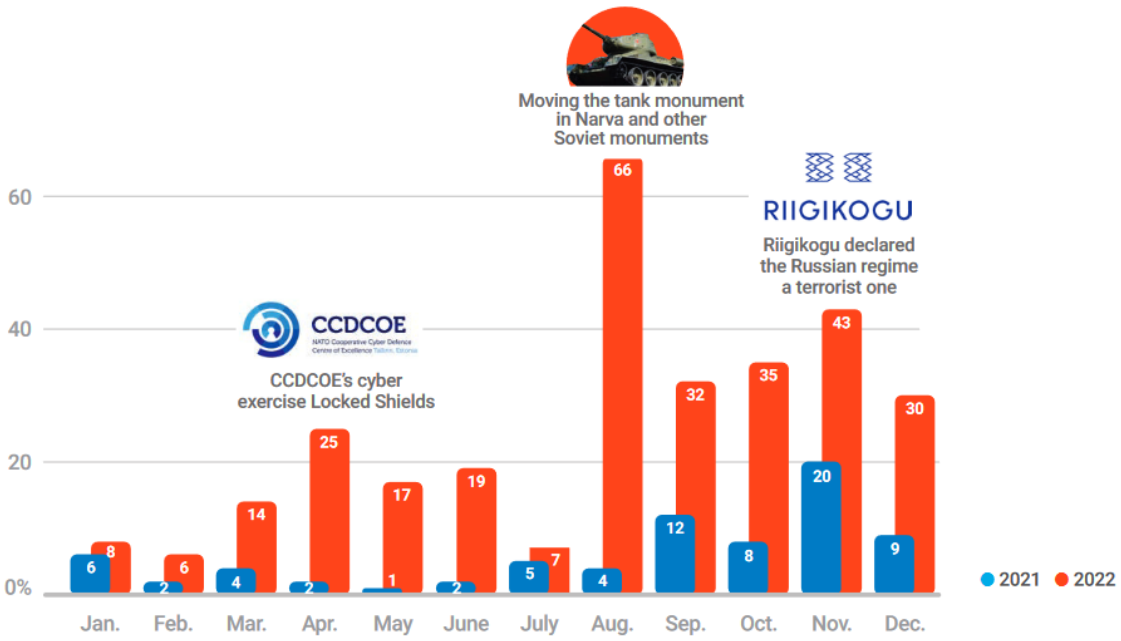
Following the removal of several Soviet monuments, including a tank, from the eastern border city of Narva during the attacks in August 2022, Estonia experienced its most extensive cyberattack since 2007. Public and private institutions were both targeted by DDoS attacks. (Wright, Estonia subjected to 'extensive' cyberattacks after moving Soviet monuments, 2022)

Finally, the attacks in November 2022 after the Estonian parliament declared the Russian regime a terrorist regime. As soon as the Russian regime was declared a terrorist regime, the Riigikogu website was attacked (RIA, Cyber Security in Estonia 2023, 2023).

These attacks targeted both public and private institutions and were politically motivated, coinciding with events such as the removal of Soviet monuments and the Estonian

parliament's declaration of the Russian regime as a terrorist regime. The attacks highlight the importance of effective cybersecurity measures, particularly in a geopolitical context where there may be increased attention and potential threats from hostile foreign actors.

Figure 7. The number of DDoS attacks in 2022



Source: (RIA, 2023)

According to Expert 1: "Many, of the attacks impacted us as well. I know that we have in my opinion maybe even five times, they have come against us, so to speak, sometimes successfully, sometimes less successfully. Each time we learn and implement new solutions."

Based on the statements of Expert 1 and Expert 2, it appears that the Ukrainian War and ongoing cyberattacks have placed a significant workload on security teams. While Expert 1 suggests that this workload may be greater than the one caused by the COVID-19 pandemic, Expert 2 notes that it is difficult to assess whether the intensity of cyberattacks increased during the pandemic. However, both experts agree that hostile special services have been monitoring and engaging in cyber attacks in the region for a longer period of time.

There were noticeable cyber attacks and incidents. According to Expert 2, it was difficult to assess whether it became more intense during COVID-19 period: "It is difficult to assess, because these hostile special services of the two eastern countries have been looking in this direction all the time. Maybe it changed, that earlier they didn't go to the front-end servers as much. Well, more local administration and since people are away, the option is to come through the servers, not with e-mails, but just to get something through the front-end somehow successively towards the interior and rather quietly take over the entire network and hope that no one notices. And continuously improve your cover channels and then live there in the network. This is the ultimate goal, cyber intelligence is anyway. But to take advantage of this distracted attention of the administrators, so that such a qualitative shift, as it still happens, is significant. “

Based on Expert 2's statement, it seems that the cyber threat landscape in Estonia has remained consistently high throughout the COVID-19 period and the Ukrainian war. Estonia's foreign policy position and influence in the region seem to be contributing factors to the heightened attention and expectations from the general public. Additionally, the ongoing nature of the cyber threats has made it a routine concern for administrators in the cyber field, leading to potential overload and fatigue.

Expert 2 responded to a question about the COVID-19 period and Ukrainian war as follows: „It has remained the same rather that it is this so-called period that behaves like one period, in fact we can say that there was a period before 2020 and after that there is one period that has not subsided yet. What is important, why it has not fallen, is that Estonia's foreign policy position is high, and Estonia seems to be expected to give answers and display initiative. Being such an influential member state, we have received such heightened attention from the public. In other words, as of 2020, we can say that we are still in the background of this conversation, and to some extent it has already become a routine for us. But this kind of overload and fatigue of administrators in the cyber field can be felt. “

5. Recommendations

The main goal of this research was to explore the impact of cyber threats on Estonia during the COVID-19 pandemic and to provide recommendations for improving cybersecurity in the organizations and protecting vulnerable individuals and organizations. In the previous chapters, various types of cyber threats that Estonia has faced have been highlighted, including phishing, DDoS attacks, and ransomware, and the challenges of addressing them effectively.

The objective of this chapter is to present a set of recommendations for mitigating cyber threats and protecting those who are more vulnerable to cyberattacks. A particular focus will be on measures that can be taken at the individual, organizational, and national levels to strengthen cybersecurity. It is important to acknowledge that there is no foolproof way to protect oneself from cyberattacks. The very act of using the internet and sharing personal information online creates risks. The only way to completely avoid these risks is to stay offline, which is unrealistic in today's world. However, by taking the recommended steps individuals and organisations can greatly mitigate the risks of falling victim to a cyber attack. It is also important to remember that risks will always be present, and they cannot be fully eliminated. To protect oneself and one's assets from cyber threats, one must stay vigilant and take proactive measures.

First suggestion is to improve and invest into cybersecurity education. Raising awareness about cyber threats and providing education on how to protect oneself online is crucial. This can be achieved through internal and public awareness campaigns, workshops, and training programs. During the interview, both experts confirmed that training was of primary importance. It is impossible for technology to help where a person himself behaves carelessly. As a result, RIA examines technologies, people, and organizations. “Most information security experts state that in 2021, the person behind the computer or smart device will still be the weakest link. Improved cyber hygiene can help achieve better results in this area and increase security. The police have not stopped explaining that wearing a seat belt can save your life. This has been emphasized for 30 years, and although most people understand it, some still need to be reminded. Speaking of cyber hygiene, it's like we're still in the 2000s, when taxi drivers put a clip in their seat belt slot that stopped the alarm beeping incessantly. So, the drive could continue without a seat belt.” (Auväärt, 2021) “In order to make sure that employees are equipped with the

necessary digital skills, organizations must continue to train them. RIA is also glad to lend a helping hand here. In addition to various campaigns and information days, RIA has opened an environment called itvaatlik.ee, a portal that shares clear cyber advice, that has been available to public for some time now. The "Ole IT-vaatlik" campaign was carried out by RIA from October 2019 until the end of the year. The target group of the campaign is the wider public, who in one way or another are currently affected by the organization of distance work and learning " (Auväärt, 2021).

Second suggestion is to improve and implement cybersecurity measures like policies and procedures along with the technical solutions. The risk of cyberattacks can be significantly reduced by ensuring that all software and systems are updated with the latest security patches, strong password policy have been implemented along with multi-factor authentication. Additionally access to organization's resources should be restricted to use over VPN solutions.

Third suggestion would be to increase the offer of government. RIA offers professional help in several fields, and it would be highly beneficial to use the available resources. The government agencies can provide support to vulnerable individuals and businesses by offering cybersecurity services, such as software and security assessments. The goal is to raise awareness of the opportunities and threats of the information society and the developments of the Estonian e-state to facilitate planning, development, and deployment of the ICT services infrastructure. (RIA, ELi struktuuritoetuse toetusskeem "Infoühiskonna teadlikkuse tõstmine", 2022)

Fourth suggestion, public-private partnership and collaboration between industries and organizations is crucial to strengthen cyber defences as cyber attacks can affect multiple industries and organizations. By working together, industries can share their experiences and best practices for responding to cyber threats. Collaboration can also help in identifying new attack methods and developing effective countermeasures. Moreover, sharing threat intelligence can help in identifying new and emerging threats, and allow organizations to take proactive measures to mitigate the risks. It is particularly important for critical infrastructure sectors to collaborate and share information, as any disruption to these sectors can have serious consequences on public safety and the economy. Governments can play a key role in facilitating collaboration between industries by creating platforms and frameworks that enable the sharing of information and best practices.

Sixth suggestion, creating regular backups of important data to prevent data loss in case of a cyberattack. Regular backups should be stored securely and kept off-site to ensure that they are not compromised in the event of a cyber attack. It is also important to regularly test the backups to ensure that they can be used for restoring in case of a loss of data. In addition, organizations should have a clear backup and disaster recovery plan in place that outlines the steps to be taken in case of a cyber attack, including who is responsible for what tasks and how communication will be handled. This plan should be regularly reviewed and updated as needed to ensure that it remains effective and relevant.

Seventh suggestion, continuous monitoring of systems and networks. This can help to identify and respond to cyber threats in a timely manner. By implementing these best practices, individuals and businesses can significantly reduce their vulnerability to cyber attacks. Additionally, the implementation of the information security standard. As of 2023, Estonia is enforcing a new Estonian Information Security Standard (E-ITS), which provides the organization with an information security management system to deal with information security risks (Auväärt, 2021). Implementing E-ITS does not make it impossible to attack the organization but it makes it more difficult to attack you and helps you put in place a concrete plan to quickly get back on your feet after an attack and restore the organization's operations (Auväärt, 2021).

5.1 Recommendations for further research

First, promote collaboration between public sector and academia. This would be beneficial for both sides as it would assist the public sector institutions, local governments more specifically, to obtain new data relevant to their work as well as suggestions for improvement. This would also be beneficial for the academia to obtain input relevant for the research and serve as a basis for further research.

Secondly, elaborated qualitative and quantitative research to investigate the impact of COVID-19 specifically for the Estonian public sector. To reach this goal, a collaboration between RIA, MKM, and TalTech would have to be agreed on, to obtain a relevant data set that can be used for generalization. This research could also be promoted at specific events aimed at local governments, like Linnade ja Valdade Päevad, and through

organizations that gather local municipalities under itself, like Linnade ja Valdade Liit or through local municipalities' unions.

6. Summary

The world and our ways of live have changed quite a lot since the emergence of COVID-19 in 2019, and the cybersecurity landscape is no exception as most of the changes involve digitalization and making the services available online. As organizations and individuals adapt to new ways of working and interacting online, cyber threats have become more prevalent and sophisticated, brining along the need for robust cybersecurity measures. The Estonian public sector, with its highly digitized services and infrastructure, is particularly vulnerable to these threats, and it is essential that its cybersecurity practices keep pace with the evolving threat landscape.

The goal of this paper was to investigate the new emerging cyberthreats that have emerged during and after the COVID-19 crisis. Through the analysis of their impact on organizations and their staff as well as data analysis, it has become clear that these threats pose a significant risk to the security of sensitive data and information. It is of utmost importance to acknowledge that individuals have a crucial role in ensuring cybersecurity both on individual and organizational level. Despite advancements in technology, human error and negligence remain a significant weakness in the cybersecurity attack chain. According to many cybersecurity professionals, the weakest link in a computer or smart device is the individual using it. Therefore, enhancing cyber hygiene practices can significantly improve security measures and reduce the risk of cyberattacks.

All research questions and sub-research questions were answered successfully. These questions are summarized below along with the answers:

RQ1. How has Covid-19 affected the cybersecurity readiness of individuals, and organizations in the e-government field?

The transition to remote work has created new challenges and threats, as the environment became less controlled and more vulnerable. Expert 1 emphasizes that the main change in cyber threats was due to the change in the environment itself. The threats that existed in the office also existed at home, but the uncontrolled environment made it easier for cyber attackers to exploit vulnerabilities.

Expert 2 notes that the organization had to adapt quickly to the new remote work reality and put in place measures such as increasing VPN connections, reviewing access rights, and purchasing new security devices. Both experts agree that remote work is a semi-

untrusted environment that requires extra security measures to ensure the safety of the organization's data and systems

Expert 2 also acknowledged the potential limitations of remote training, noting that while it can be a useful tool, it may not necessarily achieve the desired level of cybersecurity awareness and mistakes due to user negligence can still occur. “Perhaps the sought-after level will not be achieved, and in fact, in the group of public servants, it can be seen that these mistakes due to user negligence do happen."

SQ1. Have there been an emergence of new cyber threats and trends and what can be done to mitigate the risks?

It appears that both experts agree that there were changes in the environment due to COVID-19, which brought about new challenges in terms of cyber threats. However, it appears that there were no significant changes in response to these emerging threats. Expert 1 states that, despite the changes in the environment, in practice, nothing could be done for these threats, as no one goes home to watch what people do. Expert 1: "Well, no, I mean, it didn't directly affect either of them, the only difference, which is not directly related to the cyber threats that existed, was the change that you have to manage in a different way. That if you used to lead people who sat next to you, now you lead people you don't see for weeks in between. that in the field of cyber, well, nothing changed in practice, that these threats changed, but in practice nothing can be done for them, no one goes home to watch what they do. It all remained the same, because homework was already such a very, very common practice for us, it just became the norm now."

Based on the interview result it appears that one of the biggest challenges faced by the Estonian public sector during and after COVID-19 was the sudden need to provide laptops for remote work as many employees were using a desktop computer and had no remote access to work environments. There were delivery difficulties and procurement contracts had to be extended to accommodate these needs.

In addition to these usual supply problems, one organization had more specific problems related to cybersecurity requirements, such as ensuring the security of the hardware they purchase. They also faced challenges when ordering hardware from potentially hostile countries where the regime may not be democratic, and where firmware’s may have been changed. This made it difficult for them to ensure the security and functionality of the hardware they need for their work.

RQ2. How to determine the receptiveness of falling a victim of a cyber attack of the personnel and what are the methods to reduce the chances of falling a victim of a cyberattack?

Education is the key - Raising awareness about cyber threats and providing education on how to protect oneself online is crucial. This can be achieved through public awareness campaigns, workshops, and training programs. During the interview, both experts confirmed that training was of primary importance in awareness raising. It is impossible for technology alone to prevent an attack where a person himself behaves carelessly. Most information security experts state that the person behind the computer or smart device will still be the weakest link. Improved cyber hygiene can help achieve better results in this area and increase security. Moreover, there are various mitigation measures such as anti-virus protection, system isolation, and monitoring user behaviour, which can effectively reduce these risks. In case of any malicious activity, these systems are designed to detect and alert the relevant personnel (Auväärt, 2021).

It is critical to note that the sample size for the interviews conducted in this analysis is limited to two participants. Although their insights and perspectives are highly valuable, the small sample size may not be used for generalization for of the actual situation in the Estonian public sector. It may not be representative to all public sector institutions and may lack diversity. Thus, any further research should aim to increase the sample size to increase the generalizability of the results. It is also important to note that the organizations interviewed had an established high level of cybersecurity. It is highly likely that the overall Estonian public sector does not have the same cybersecurity standard and level of awareness. Moreover, the main target group, which is most vulnerable to cyber security attacks, was not reached, namely local governments. Out of 11 invitations for interviews, 9 were sent out to local governments but no response was received from any of the contacted IT personnel.

Cybersecurity is an essential aspect of our modern digital world. With the increasing dependence on technology and the internet, protecting sensitive information and critical infrastructure from cyber threats has become more critical than ever before. The field of cybersecurity is constantly evolving, as new threats emerge, and existing threats become more sophisticated.

As our reliance on technology continues to grow, the importance of cybersecurity will only increase accordingly. It is a constantly changing field that requires individuals and

organizations to remain up to date with the latest threats and technologies in order to avoid falling a victim of a cyberattack.

References

Adelmann, F., & Gaidosch, T. (2020). *Cybersecurity of Remote Work During*. Retrieved 04 26, 2023 from IMF: https://www.imf.org/-/media/Files/Publications/covid19-special-notes/en-special-series-on-covid-19-cybersecurity-of-remote-work-during-pandemic.ashx

Auväärt, G. (2021). *Kuidas muuta ettevõte küberkurjategijate jaoks keeruliseks sihtmärgiks?* Retrieved 05 05, 2023 from Riigi Infosüsteemi Ameti blogi: https://blog.ria.ee/category/it-vaatlik/

Ayouni, I., Maatoug, J., Dhouib, W., Zammit, N., Fredj, S. B., Ghammam, R., & Ghannem, H. (2021). Effective public health measures to mitigate the spread of COVID-19: a systematic review. *BMC public health, 21(1)*, 1015. doi:https://doi.org/10.1186/s12889-021-11111-1

Bachelet , M., & Grandi , F. (2020). *The coronavirus outbreak is a test of our systems, values and humanity*. From The UN Refugee Agency: https://www.unhcr.org/news/latest/2020/3/5e69eea54/coronavirus-outbreak-test-systems-values-humanity.html

Bacon, M. (2023). *security*. Retrieved 04 08, 2023 from Techtarget: https://www.techtarget.com/searchsecurity/definition/security

Bambra, C., Riordan, R., Ford, J., & Matthews, F. (2020). The COVID-19 pandemic and health inequalities. *Journal of epidemiology and community health, 74(11)*, 964-968. doi:https://doi.org/10.1136/jech-2020-214401

Belcic, I. (2023). *What Is Malware and How to Protect Against Malware Attacks?* . From Avast: https://www.avast.com/c-malware#topic-1

BNS. (2021). *RIA yearbook: Cyber criminals took advantage of COVID-19 fears*. From Eesti Rahvusringhääling: https://news.err.ee/1608168793/ria-yearbook-cyber-criminals-took-advantage-of-covid-19-fears

Brennen, J. S., Simon, M. F., Howard, P. N., & Nielsen, R. K. (2020). Types, Sources, and Claims of COVID-19 Misinformation. *Reuters Institute Factsheet*, 1-14. Retrieved 04 08, 2023 from https://www.researchgate.net/publication/340502400_Types_Sources_and_Claims_of_COVID-19_Misinformation

Broadtek. (2023). *Why is Risk Management Important in Cyber Security?* Retrieved 04 08, 2023 from Broadtek: https://broadtek.com/blog/why-is-risk-management-important-in-cyber-security/

Bruns, H., Dessart, F. J., & Pantazi, M. (2022). *Covid-19 misinformation: Preparing for future crises.* Luxembourg: Publications Office of the European Union. doi:http://dx.doi.org/10.2760/41905

Cloudflare. (2023). *What is account takeover?* From Cloudflare: https://www.cloudflare.com/learning/access-management/account-takeover/

Cloudflare. (2023). *What is an attack vector?* Retrieved 04 08, 2023 from Cloudflare: https://www.cloudflare.com/learning/security/glossary/attack-vector/

Cucinotta, D., & Vanelli, M. (2020). WHO Declares COVID-19 a Pandemic. *Acta bio-medica : Atenei Parmensis, 91*, 157–160. doi:https://doi.org/10.23750/abm.v91i1.9397

Darem , A. (2021). Anti-Phishing Awareness Delivery Methods. *Engineering, Technology & Applied Science Research 11*, 7944-7949. doi:https://doi.org/10.48084/etasr.4600

DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Association*, 147-160. doi:https://doi.org/10.2307/2095101

Dizdar, A. (2021). *Misconfiguration Attacks: 5 Real-Life Attacks and Lessons Learned*. Retrieved 04 08, 2023 from bright: https://brightsec.com/blog/misconfiguration-attacks/

e-Estonia. (2022). *e-Estonia guide*. Retrieved 05 05, 2023 from e-Estonia: https://e-estonia.com/wp-content/uploads/eestonia_guide_a5_230206_rgb.pdf

ENISA. (2022). ENISA Threat Landscape 2022. From https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport

George, T. (2022). *Semi-Structured Interview | Definition, Guide & Examples*. Retrieved 04 08, 2023 from Scribbr: https://www.scribbr.com/methodology/semi-structured-interview/

Greig, J. (2021). *Ransomware groups continue assault on healthcare orgs as COVID-19 infections increase*. Retrieved 05 06, 2023 from ZDNET: https://www.zdnet.com/article/ransomware-groups-continue-assault-on-healthcare-orgs-as-covid-19-infections-increase/

IBM. (2023). *What is phishing?* From IBM: https://www.ibm.com/topics/phishing

Imperva. (2022). *Social Engineering*. Retrieved 04 08, 2023 from Imperva: https://www.imperva.com/learn/application-security/social-engineering-attack/

Imperva. (2023). *Phishing attacks*. Retrieved 05 06, 2023 from Imperva: https://www.imperva.com/learn/application-security/phishing-attack-scam/

Interpol. (2021). *Cybercrime*. From Interpol: https://www.interpol.int/en/Crimes/Cybercrime

JRC. (2023). *Misinformation on COVID-19: what did we learn?* Retrieved 04 08, 2023 from Joint-research-centre: https://joint-research-centre.ec.europa.eu/jrc-news/misinformation-covid-19-what-did-we-learn-2023-02-21_en

Kaitseministeerium. (2008). *Küberjulgeoleku strateegia 2008–2013*. Retrieved 04 09, 2023 from Kaitseministeerium: https://energiatalgud.ee/sites/default/files/images_sala/e/ea/Kaitseministeerium._K%C3%BCberjulgeoleku_strateegia_2008_-_2013._Tallinn_2008.pdf

Kook, U. (2020). *Valitsus kuulutas välja eriolukorra*. From Eesti rahvusringhääling: https://www.err.ee/1063213/valitsus-kuulutas-valja-eriolukorra

Kost, E. (2023). *How to Detect Data Exfiltration (Before It's Too Late)*. From UpGuard: https://www.upguard.com/blog/how-to-detect-data-exfiltration

Kranhold, K. (2020). *Social Media in 2020: A Year of Misinformation and Disinformation*. Retrieved 04 08, 2023 from The Wall Street Journal: https://www.wsj.com/articles/social-media-in-2020-a-year-of-misinformation-and-disinformation-11607712530

Krjukov, A. (2020). *Terviseameti labor sai võimekuse iseseisvalt koroonaviirust tuvastada*. From Eesti Rahvusringhääling: https://www.err.ee/1030454/terviseameti-labor-sai-voimekuse-iseseisvalt-koroonaviirust-tuvastada

Kuik, S. (2022). *Võõrale lingile vajutanu võib kaotada Facebooki konto* . From RIA: https://www.ria.ee/uudised/voorale-lingile-vajutanu-voib-kaotada-facebooki-konto

Laherand, M. L. (2010). *Kvalitatiivne uurimisviis.* Tallinn: Sulesepp.

Lund, S., Madgavkar, A., Manyika, J., Smit, S., Ellingrud, K., & Robinson, O. (2021). *The future of work after COVID-19*. Retrieved 04 26, 2023 from McKinsey Global Institute: https://www.mckinsey.com/featured-insights/future-of-work/the-future-of-work-after-covid-19#/

MKM. (2019). *Cybersecurity Strategy 2019-2022*. Retrieved 04 08, 2023 from MKM: https://www.mkm.ee/media/703/download

Nkengasong, J. N. (2021). COVID-19: unprecedented but expected. *Nature Medicine*, 364. doi:https://doi.org/10.1038/s41591-021-01269-x

Olev, A., & Alumäe, T. (2022). Estonian Speech Recognition and Transcription Editing Service. *Baltic J. Modern Computing, Vol. 10, No. 3*, 409-421. doi:https://doi.org/10.22364/bjmc.2022.10.3.14

Ots, M., & Kook, U. (2020). *Eestis leiti esimene koroonaviirusesse nakatunu*. From Eesti rahvusringhääling: https://www.err.ee/1057192/eestis-leiti-esimene-koroonaviirusesse-nakatunu

Pak, A., Adegboye , O. A., Adekunle , A. I., Rahman , K. M., McBryde , E. S., & Eisen , D. P. (2020). Economic Consequences of the COVID-19 Outbreak: the Need for Epidemic Preparedness. *Frontiers in Public Health*. doi:https://doi.org/10.3389/fpubh.2020.00241

Postimees. (2020). *Korduma kippuvad küsimused ⟩ Miks on Eestis eriolukord ja mida see tähendab?* From Postimees: https://tervis.postimees.ee/6937204/korduma-kippuvad-kusimused-miks-on-eestis-eriolukord-ja-mida-see-tahendab

Reciprocity. (2022). *Security Misconfigurations: Definition, Causes, and Avoidance Strategies*. Retrieved 04 08, 2023 from Reciprocity: https://reciprocity.com/blog/security-misconfigurations-how-to-avoid-them/

Regionaalhaigla. (2020). *Terviseameti kriisistaabiga liitus Regionaalhaigla kiirabikeskuse juhataja dr Arkadi Popov*. From Regionaalhaigla: https://www.regionaalhaigla.ee/et/terviseameti-kriisistaabiga-liitus-regionaalhaigla-kiirabikeskuse-juhataja-dr-arkadi-popov

Reuters. (2016). *Austria's FACC, hit by cyber fraud, fires CEO*. From Reuters: https://www.reuters.com/article/us-facc-ceo-idUSKCN0YG0ZF

RIA. (2021). *Cyber Security in Estonia 2021*. Retrieved 04 09, 2023 from RIA: https://www.ria.ee/en/media/1494/download

RIA. (2021). *Küberturvalisuse aastaraamat 2021*. From RIA: https://www.ria.ee/media/1493/download

RIA. (2022). *Cyber Security in Estonia 2022*. Retrieved 04 09, 2023 from RIA: https://www.ria.ee/en/media/1490/download

RIA. (2022). *ELi struktuuritoetuse toetusskeem "Infoühiskonna teadlikkuse tõstmine"*. Retrieved 05 05, 2023 from RIA: https://www.ria.ee/riigi-infosusteem/infouhiskonna-teadlikkuse-tostmine/eli-struktuuritoetuse-toetusskeem

RIA. (2022). *Estonian information security standard (E-ITS)*. Retrieved 04 09, 2023 from RIA: https://www.ria.ee/en/cyber-security/management-state-information-security-measures/information-security-standard-e-its

RIA. (2023). *Cyber Security in Estonia 2023*. Retrieved 04 09, 2023 from RIA: https://www.ria.ee/en/media/2702/download

Saleous, H., Ismail, M., AlDaajeh, S. H., Madathil, N., Alrabaee, S., Choo, K.-K. R., & Al-Qirim, N. (2023). COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. *Digital Communications and Networks Volume 9, Issue 1*, 211-222. doi:https://doi.org/10.1016/j.dcan.2022.06.005.

Salmon, L. (2017). *The importance of case studies in social research*. Retrieved 05 05, 2023 from Changeworks: https://www.changeworks.org.uk/news-and-events/blog/the-importance-of-case-studies-in-social-research

Scott, R. W. (2008). *Institutions and Organizations: Ideas and Interests.* Los Angeles: Sage Publications.

Seguin, P. (2022). *What Is Spyware, Who Can Be Attacked, and How to Prevent It*. From Avast: https://www.avast.com/c-spyware#topic-1

Seguin, P., & Latto, N. (2023). *The Essential Guide to Ransomware* . From Avast: https://www.avast.com/c-what-is-ransomware#topic-1

Shea, S., Gillis, A. S., & Clark, C. (2023). *What is cybersecurity?* Retrieved 04 08, 2023 from Techtarget: https://www.techtarget.com/searchsecurity/definition/cybersecurity

Soare, B. (2022). *What Are the Main Attack Vectors in Cybersecurity?* Retrieved 04 08, 2023 from Heimdalsecurity: https://heimdalsecurity.com/blog/attack-vectors/

Statista. (2021). *Where do IT professionals see an increase in cyber attacks and attack attempts following the COVID-19 pandemic?* From Statista: https://www.statista.com/statistics/1258261/covid-19-increase-in-cyber-attacks/

Taylor, L. (2023). *How to Record, Transcribe and Edit Interviews*. Retrieved 04 08, 2023 from Notta: https://www.notta.ai/en/blog/interview-transcription

Terranova Security. (2023). *19 Examples of Common Phishing Emails*. Retrieved 05 06, 2023 from Terranova Security: https://terranovasecurity.com/top-examples-of-phishing-emails/

Terviseamet. (2020). *2019-nCoV andmed 31.01.2020*. From Terviseamet: https://www.terviseamet.ee/et/uudised/2019-ncov-andmed-31012020

Terviseamet. (2020). *COVID-19 andmed 27.02.2020*. From Terviseamet: https://www.terviseamet.ee/et/uudised/Covid-19-andmed-27022020

Thornton , P. H., & Ocasio, W. (2008). Institutional Logics. *SAGE Publications Ltd*. doi:http://dx.doi.org/10.4135/9781849200387.n4

Ullah, F., Edwards, M., Ramdhany, R., Chitchyan, R., Babar, A. M., & Rashid, A. (2018). Data exfiltration: A review of external attack vectors and countermeasures. *Journal of Network and Computer Applications (101)*, 18-54. doi:https://doi.org/10.1016/j.jnca.2017.10.016.

Ursillo, S., & Arnold, C. (2019). *Cybersecurity Is Critical for all Organizations – Large and Small*. Retrieved 04 08, 2023 from IFAC: https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small

Välisministeerium. (2007). *Küberrünnakud Eesti vastu*. Retrieved 04 08, 2023 from vm: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiwve_jk5v-AhVN_CoKHfBiDAwQmuEJegQIEBAB&url=https%3A%2F%2Fvm.ee%2Fsites%2Fdefault%2Ffiles%2Fcontent-editors%2Fweb-static%2F115%2Fcyber_attacks.pdf&usg=AOvVaw1ZBZE2jRVM

Wright, H. (2022). *DDos cyberattacks against Estonian state websites continue*. Retrieved 05 04, 2023 from ERR: https://news.err.ee/1608573811/ddos-cyberattacks-against-estonian-state-websites-continue

Wright, H. (2022). *Estonia subjected to 'extensive' cyberattacks after moving Soviet monuments*. Retrieved 05 04, 2023 from ERR: https://news.err.ee/1608688201/estonia-subjected-to-extensive-cyberattacks-after-moving-soviet-monuments

Yin, R. (2008). *Case Study Research: Design and Methods (Applied Social Research Methods).* Sage Publications.

Zadeh, A. H., Jeyaraj, A., & Biros, D. (2020). Characterizing Cybersecurity Threats to Organizations in Support of Risk Mitigation Decisions. *e-Service Journal 12(2)*, 1-34. doi:https://doi.org/10.2979/eservicej.12.2.01

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis

Plain licence for allowing the thesis to be available and reproducible for the public

I Oliver Kristopher Ruut 20.06.1996

1. Allow the Tallinn University of Technology without any charges (Plain licence) my work

"Emerging cyber threats in Estonian public sector during and after COVID-19"

supervised by Sille Arikas,

1.1. to be reproduced for the purpose of conservation and electronic publication, including the digital repository of the Tallinn University of Technology, until the end of copyrighted time limit;
1.2. to be available to the public through the Tallinn University of Technology online environment, including the digital repository of the Tallinn University of Technology, until the end of the copyrighted time limit.

2. I am aware, that all rights, named in section 1, will remain to the author.

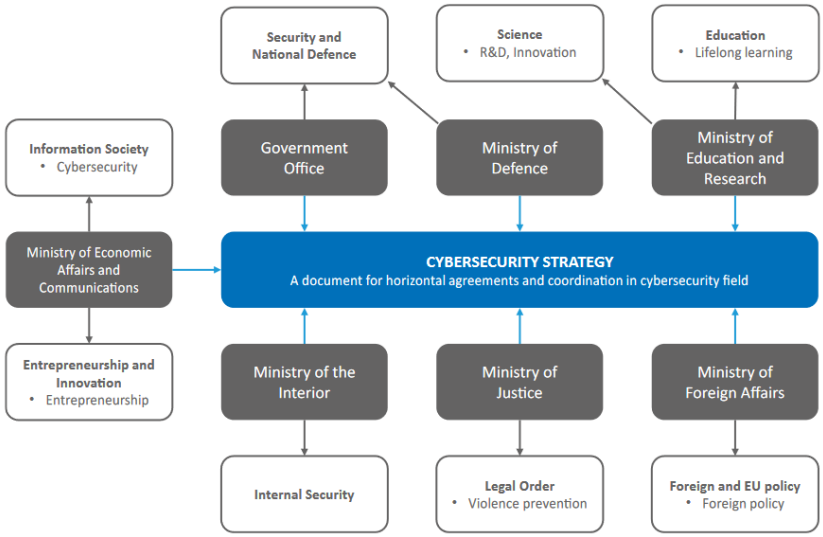
3. I confirm that by allowing the use of the Plain licence, no intellectual rights of third parties will be violated as set in the personal data protection act and other legislation.

Signed digitally

08.05.2023

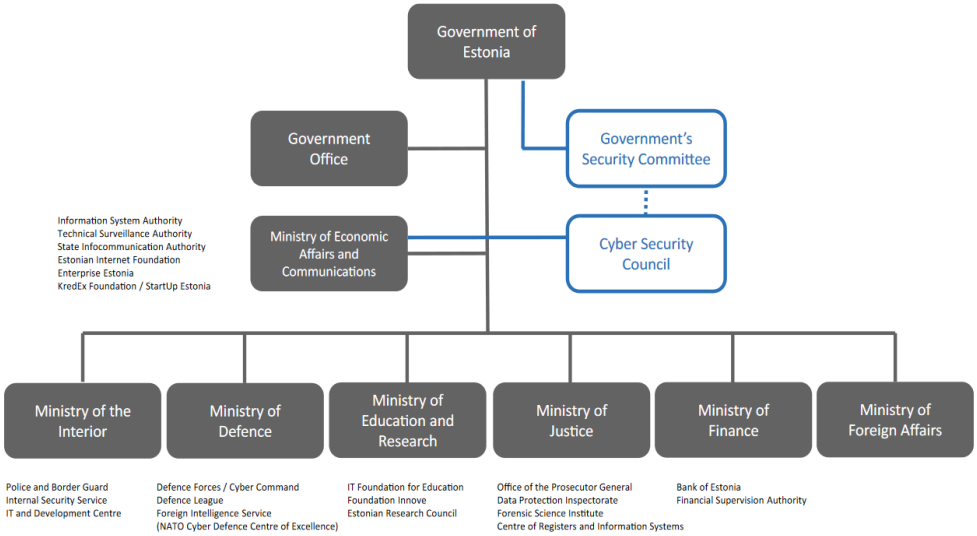
Appendix 2 – Performance areas connected to planning activities necessary for implementing the objectives of the Cybersecurity Strategy and the structure of System for management of the cybersecurity sector

Performance areas connected to planning activities necessary for implementing the objectives of the Cybersecurity Strategy



Source: (MKM, 2019)

System for management of the cybersecurity sector



Source: (MKM, 2019)

Appendix 3 – Interview questions

1. Could you tell me about yourself and your background a bit?
2. In your opinion, what are the most significant cyber threats against Estonian public sector?
3. Does your organization provide the opportunity for remote working?
4. Have there been any incidents due to remote work?
5. In your opinion, what are the biggest shortcomings of public sector employees when it comes to awareness about cyber threats?
6. During COVID-19, what changes did you experience in regards to cyber threats against your constituency?
7. How did you respond to the emerging cyber threats during and after COVID-19? Have there been any significant changes in policies or practices?
8. In your experience, what were the biggest challenges that the Estonian public sector is facing when addressing cyber threats during and after COVID-19?
9. How has the Estonian public sector collaborated with other stakeholders addressing cyber threats during and after COVID-19?
10. What lessons have you learnt from the COVID-19 pandemic in terms of cybersecurity preparedness and response?
11. In your opinion, what steps should the Estonian public sector take to improve its cybersecurity posture?
12. Are there any specific technologies or practices you can recommend in order to improve responding to cyber threats?
13. Have there been any notable cyber attacks or incidents in your organization during or after COVID-19? How were these incidents managed? What were the biggest challenges?
14. Have the employees of your organization been trained and educated on cybersecurity during and after COVID-19? What is the type of the training and frequency?
15. Have you had any potential situations caused due to the lack of cybersecurity related training? How have you responded to them?
16. In your opinion, what is the best way to help the people who are more susceptible to cyberattacks?

17. Have there been any significant changes in funding IT or even cybersecurity for your organization during and after COVID-19?

Interview questions in Estonian

1. Kas te räägiksite mulle natuke endast ja oma töö taustast?
2. Millised on Teie meelest kõige olulisemad Eesti avalikku sektorit ohustavad küberohud?
3. Kas Teie organisatsioonis on kaugtöö võimalus?
4. Juhul kui Teie organisatsioonis on kaugtöö lubatud, kas see on teadaolevalt küber intsidente põhjustanud?
5. Millised on Teie arvates avaliku sektori töötajate küberturvalisuse teadlikkuse suurimad puudujäägid?
6. Milliseid muutuseid Teie organisatsioonis COVID-19 ajal küberohtude vaates esines?
7. Kuidas Te COVID-19 ajal esilekerkinud küberohtudele reageerisite? Kas sellest ajast alates on Teie organisatsioonis toimunud küberturvalisuse vaatest olulisi muutuseid praktikates ja/või sisekorraeeskirjades?
8. Teie kogemuse põhjal - millised olid Eesti avaliku sektori asutuste peamised murekohad COVID-19 ajal küberohtudele reageerimisel?
9. Teie kogemuste põhjal - kuidas on Eesti avaliku sektori asutused COVID-19 ajal ja pärast seda teiste osapooltega koostööd teinud? Kas nad on seda üldse teinud?
10. Millised on olnud Teie peamised COVID-19 küberturvalisuse õppetunnid nii valmistumise kui reageerimise valdkonnas?
11. Teie arvates - Millised meetmeid peaksid Eesti avaliku sektori asutused oma küberturvalisuse taseme parendamiseks rakendama?
12. Kas Teil on mõned spetsiifilised tehnoloogiad või praktikad, mis Teie kogemuse põhjal on osutunud väga edukaks küberohtudele reageerimisel?

13. Kas Teie organisatsiooni vastu on COVID-19 ajal või järel toiminud märkimisväärseid küberründeid? Kuidas neile intsidentidele reageeriti? Mis olid intsidentidele reageerimisel suurimad väljakutsed?

14. Kas Teie organisatsiooni töötajaid on küberturvalisuse alal koolitatud kas COVID-19 ajal või pärast seda? Millist koolitust on Teie töötajad saanud ja mis on koolitussagedus?

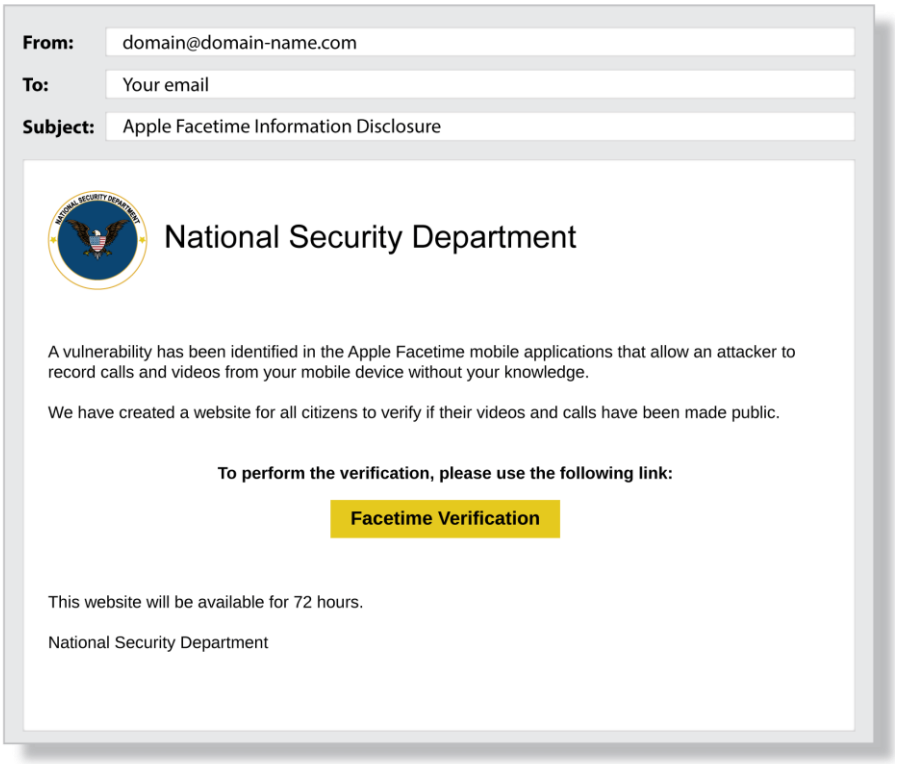
15. Kas Teil on esinenud potentsiaalseid ohuolukordi, mille on põhjustanud madal küberturvalisuse alane teadmine koolituse puudumise tõttu? Kuidas Te neile olukordadele reageerinud olete, nii protsesside alaselt kui tehniliselt?

16. Teie arvates - millised on parimad võimalused kaitsta töötajaid, kes on vähem küberohtudest teadlikud?

17. Kas Teie organisatsioonis on COVID-19 ajal või pärast eraldatud rohkem finantsressursse IT vahenditele või isegi küberturvalisuse tõstmiseks? Kui suur % või summa võrreldes varasema eelarvega?

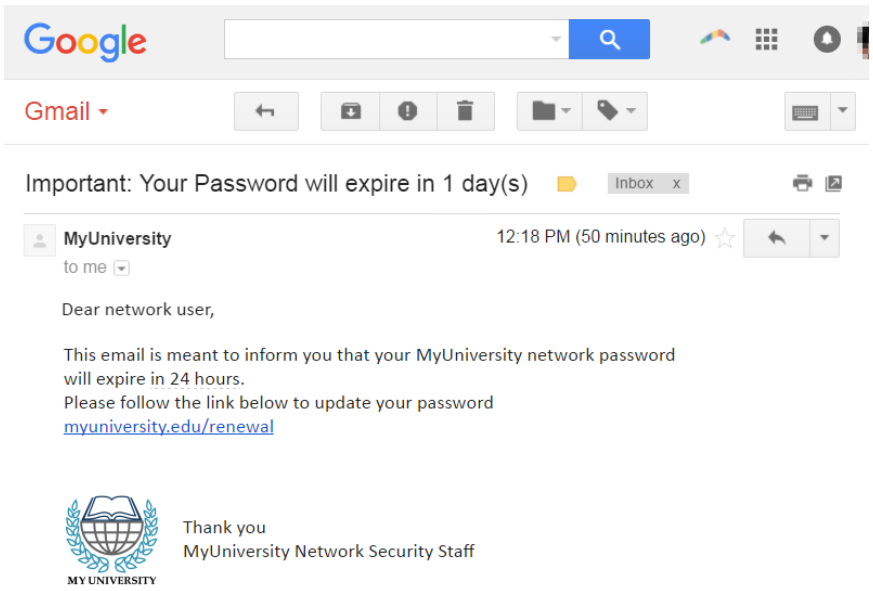
Appendix 4 – Phishing email examples

Example 1



Source: (Terranova Security, 2023)

Example 2



Source: (Imperva, Phishing attacks, 2023)