TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Janno Arnek 182504IVCM

IMPROVING CYBERSECURITY LEVEL OF ESTONIAN SMALL AND MEDIUM SIZED ENTERPRISES THROUGH COORDINATION WITH NATIONAL LEVEL

Master's thesis

Supervisor: Sille Laks
MSc

Tallinn 2021

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Janno Arnek 182504IVCM

EESTI VÄIKE JA KESKMISE SUURUSEGA ETTEVÕTETE KÜBERTURVALISUSE TASEME PARENDAMINE RIIKLIKU TASANDIGA KOORDINEERIMISE KAUDU

Magistritöö

Juhendaja: Sille Laks
MSc

Tallinn 2021

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: Janno Arnek

14.05.2021

Abstract

Small and medium enterprises (SMEs) represent a significant role in Estonian society by making up 99.8% of all active enterprises registered in Estonia. Several of them are also an operator of essential services (OES) and subject to Estonian Cybersecurity Act (ECA) that came to force in 2018. In a world of rapid digitalization and intertwining services, the SMEs are no longer bound to operate in one small area but are free to operate on a global market. This also means becoming a target for cybercriminals from around the globe. Many SMEs tend not to acknowledge the possibility that they can fall victim of a cyberattack. The SME consider themselves an unattractive target for the cybercriminals because of their small size and seeming irrelevance to the society nor are they aware of the threats caused by systemic cyber risk.

This thesis explores possibilities to improve the cybersecurity level of Estonian SMEs through more efficient coordination with national level. In the scope of this work are Estonian SMEs whom the author believes to be unaware and unprepared of the risks of digital interconnected world.

This thesis aims to uncover methods that would enable SMEs to improve their cybersecurity capabilities of their organizations using existing limited resources and gaining a more systemic understanding of cyber risk through help of coordination with the national level.

This thesis is written in English and is 82 pages long, including 9 chapters and 2 figures.

Annotatsioon

Eesti väike ja keskmise suurusega ettevõtete küberturvalisuse taseme parendamine riikliku tasandiga koordineerimise kaudu

Väike ja keskmise suurusega ettevõtted täidavad kriitilist rolli Eesti ühiskonnas moodustades 99.8% kõikidest aktiivesetest ettevõtetest registreeritud Eestis. Mitmed neid on ka elutähtsa teenuse osutajad ja peavad lisaks täitma ka Küberturvalisuse seadusest tulenevaid kohustusi, mis jõustus 2018. aastal. Maailmas mida kirjeldab kiire digitaliseerimine ja läbipõimuvad teenused, ei ole VKE-d enam piiritletud tegutsema ainult regionaalselt vaid saavad oma teenust pakkuda klientidele ülemaailmselt. See toob endaga aga kaasa sihtmärgiks muutumise küberkurjategijatele üle maailma. Enamus VKE-sid ei taju, et nad võiksid langeda küberrünnaku ohvriks. Üheks põhjuseks on asjaolu, et VKE-d ei pea ennast piisavalt atraktiivseks ohvriks küberkurjategijatele kasumi teenimise eesmärgil, teiseks põhjuseks võib välja tuua, et ei tajuta süsteemse riski ohte oma ettevõttele.

Lõputöö uurib võimalike viise, kuidas parendada Eesti VKE-de küberturvalisust läbi efektiivsema koordineerimise riikliku tasandiga. Lõputöö käsitleb Eesti VKE-sid kes, autori arvates ei ole piisavalt teadlikud digitaalselt läbipõimunud maailma ohtudest.

Lõputöö eesmärk on leida meetodeid, mis võimaldaksid VKE-del parendada oma küberturvalisuse võimekusi kasutades olemasolevaid piiratud ressursse ning luua süsteemsem arusaamine küberriskidest tänu koordineerimisele riikliku tasandiga.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 82 leheküljel, 9 peatükki ja 2 joonist.

List of abbreviations and terms

IT	Information Technology
ICT	Information and Communication Technology
SME	Small and Medium-sized Enterprises
VKE	Väike ja keskmise suurusega ettevõtted
ECA	Estonian Cybersecurity Act
CERT-EE	Computer Emergency Response Team Estonia
CERT	Computer Emergency Response Team
AKI	Data Protection Inspectorate
PPA	Police and Border Guard Board
PPP	Public-private partnership
RIA	Estonian Information System Authority
OES	Operator of essential services
NIS	Directive on security of network and information systems
BEC	Business E-mail Compromise
EU	European Union
IR	Incident Response
CEO	Chief Operating Officer
GDPR	General Data Protection Regulation
ICC	International Chamber of Commerce
PC	Personal computers
VPN	Virtual private network
MaaS	Malware as a Service
WEF	World Economic Forum
CIS	Center for Internet Security
ISAC	Information Sharing and Analysis Center

Table of contents

List of figures

1 Introduction

Along with the growth of use and reliance on information technology (IT) also the involved risks are on the rise [1]. Even for the enterprises whose business focus is not on information technology, the reliance on information communication technology (ICT) is rapidly growing either to support teleworking options from the beginning of COVID-19 pandemic or the increased use of ICT methods to make work processes more efficient and cost beneficial. It has been emphasized by substantial number of cybersecurity experts that this situation creates a larger attack surface for the cybercriminals [2]. Cybercriminals have more internet connected devices and interconnected services as targets and are relying on carelessness and unawareness of people who have now been suddenly enforced to move all their work, school, and personal activities online creating a larger attack surface for the attackers [3]. Witnessing the complexity and potential impact that cyber-attacks can have on the enterprises and their customers can be seen from cyber incidents like NotPetya [4] that caused over $10 billion in damages around the globe that also serve as a proof that even large organizations are unable to respond to cyber incidents without external assistance.

National governments and entities like the European Union (EU) have made great strides in streamlining and implementing standards in form of national cyber security laws and various regulations like General Data Protection Regulation (GDPR) and Directive on Security of Network and Information Systems (NIS) in attempt of better safeguarding organizations but also society from cyber incidents. While significant effort has been made [5] there does still exist a gap where a substantial portion of enterprises are not obliged to follow any guidelines or laws regarding cyber security. In an interview with Estonian Information System Authority (RIA) lead analyst Lauri Tankler, he stated that "We have a situation where organizations that prioritize cybersecurity are rapidly moving forward with bigger and more involved investments. And those that might not have any inherent interest in cybersecurity are left even more behind and so the disparity between those that are proficient and those that are not, is constantly growing." There is a growing

problem that many enterprises are not being cybersecure, but they can also become a source of threat for those that do their best in hardening their cybersecurity [6].

Due to rapid digitalization and growth of borderless service provision, organizations can provide their services on a global market instead of servicing a standalone small region in one specific country. This also means that the effects of a possible cyber-attack can be experienced globally as could be witnessed during a DDoS attack that took DynDNS offline and thereby disrupted global online services like Twitter, Netflix, GitHub, etc [7]. It has been also seen on a smaller scale in Estonia that a service disruption of one service provider impacts the service of another and can even cause an imminent threat on life. One of the most relevant examples of such an incident is when for one day all end users using Estonian mobile operator Elisa were unable to dial the emergency number 112 from their phone because of a network error in Elisa's network [8]. This incident involved a large organization who is also listed as an operator of essential service (OES) and not a small or medium-sized enterprise (SME) nevertheless similar risks can be applied to smaller region-specific critical services, where a small city or village could be solely dependent on a singular service provider.

Going more into detail with Estonian Emergency Act and the information provided on the website of Ministry of Interior, we will find that there are several OES who are also an SME, for example providing snow removal services in a local municipality [9]. And while OES are subject to the Estonian Cybersecurity Act (ECA) it does not inherently make an organization any more secure. In many cases enterprises might even consider the cost of ensuring full or partial compliancy too expensive [10] and take the risk of fines or possible cyber-attacks. And in many cases the reason for not trying to reach proper compliancy is a lot more innocent than could be expected - enterprises have not been properly informed of their responsibilities or they might have never considered themselves as something critical for society. Along with the arrival of an updated EU-wide Directive on security of network and information systems (NIS 2.0) which is the basis for nation specific cybersecurity laws the idea of how responsibility is distributed can initially cause confusion [5] – unlike original NIS there is a drastic shift to sector based approach and that in itself is further split into essential and important entities with varying level of compliance requirements. That is not all either, enterprises have to take into account their employee count and also be ready for exceptions based on risk

assessments which may force them to comply with regulations no matter other if other requirements are fulfilled or not [5].

Enterprises are overall investing more in cybersecurity capabilities every year [11]. According to a survey conducted among Estonian SMEs at least 75% [12] of respondents are implementing an antivirus, keeping their software up-to-date, and back up their data. Global computer security firm McAfee estimates that the annual global cost of cybercrime reached $1 trillion [13] in 2020 and considering that cyber-attacks are becoming more sophisticated and frequent, using the abovementioned solutions are no longer sufficient to protect organizations and their assets. In many cases, organizations do understand the increasing need to invest more in cybersecurity but overlook the fact that many threats can be mitigated by inexpensive and easy to implement solutions like vulnerability patching policy and separation and limitation of access privileges [14]. While there is a place for layered defences the reality is that even those enterprises cannot always keep up with cybercriminals and that can hinder the motivation of small non-IT focused enterprises to address the cybersecurity matters. SMEs should be looking to coordinating their cybersecurity efforts not only among themselves but also with the public sector.

Another quite often overlooked matter is that many SMEs consider themselves too small and not a worthy target for cybercriminals and thereby have not seen the necessity for taking any steps to improve their cybersecurity level. It has been highlighted in the annual reports of RIA that the awareness level of the SMEs is low and that they are experiencing issues mitigating an ongoing cyberattack, lack procedures for IR and require external assistance [15]. From professional experience working 4 years at Computer Emergency Response Team Estonia (CERT-EE) the author believes that another problematic issue for SMEs is the lack of knowledge where to receive assistance in case a cyber incident that is currently occurring at the organization. This observation was also confirmed by the focus group interviews for IT-vaatlik when the focus group claimed to have no information on entities like CERT-EE where they can turn or assistance in case of a cyber incident despite all conducted awareness raising campaigns. Knowing where to turn for assistance in case of a cyber incident can minimize negative consequences for the SME and ensure an easier restoration of daily operations. The author also believes that there is a lot to be done concerning what kind of help could be given to the SMEs and how exactly the bilateral relationship between private and public sector could be conducted.

It must also be understood that organizations themselves do not realize the effect their business can have in society and on other enterprises [16]. The responsibility does fall on each organization to ensure that fundamental security solutions have been implemented, but only by working together, building common processes, and sharing information, can improve organization's knowledge of interconnected systems and complexity of societal dependencies [17].

1.1 Problem statement

The purpose of this master's thesis is to improve SME cybersecurity level through coordination with national level. It is not in the scope of this work to develop or significantly improve any existing IR procedures, management guidelines or cybersecurity frameworks. The work is novel as the cybersecurity landscape for Estonian SMEs has previously not been researched from the perspective of cooperation and coordination and has until now only been focusing on technical guidelines.

The author's experience from working at CERT-EE has led him to hypothesize that there are fundamental problems concerning SME cybersecurity:

- SMEs are not aware of their importance from cybersecurity perspective in society and connection to other stakeholders.

- Lack of awareness of cyber risks leads to SMEs not prioritizing cybersecurity and therefore to greater of risk cascading cyber incidents.

- Limited awareness of the importance of cybersecurity for SMEs stems partly from lack of efficient coordination between SMEs and national level.

This thesis will try to identify shortcomings, that are limiting the existing coordination between SMEs and national level. Solving the hypothesized problem does not only require fundamental change in understanding cyber risks but also more willingness from national institutions to assist with prevention and ongoing cyber incidents. As cyber-attacks are becoming more sophisticated, trying to defend from every type is too costly for most SMEs: "The ability of entities to prepare for the consequences of systemic risk and build common processes, capabilities and capacity to enhance their cyber resilience,

and ensure they are able to recover from a systemic cyber event, is therefore more important than ever." [17].

1.2 Research goal

Main goal of this thesis is to identify possible methods to improve SME cybersecurity level through more efficient coordination with national level and propose possible solutions that the awareness raising campaigns could be conducted more effectively and reach more members of the target group.

Additional goals of this research are to determine to what extent is cybersecurity prioritized in SMSs and the possible reasons why cybersecurity is not a more significant priority for the thesis. In addition, it is necessary to form an understanding which specific risks SMEs face, their interdependencies, and whether these are isolated risks to employees only or whether they could affect all stakeholders and third parties. After determining the risks to SMEs, a set of viable solutions for improvement can be proposed.

To determine the business risks and applicable solutions, a series of sub-questions need to be asked to gain a more thorough understanding:

1. What is the importance of SMEs in Estonia from the economic and employment perspective and how is their cybersecurity regulated?

2. What are possible coordination and collaboration options for SMEs and national level?

3. What are the possible methods for improving existing coordination between SMEs and national level?

With extensive understanding of the listed sub-questions, we can achieve a more appropriate understanding of the existing environment, its shortcomings and can propose viable solutions for SMEs to improve their collaboration with national level and thereby improve their cybersecurity resilience.

1.3 Scope

In the scope of this thesis paper are Estonian SMEs employing under 250 employees and their awareness of the importance of cybersecurity and coordination.

1.4 Limitations

There are three identified limitations for the thesis:

1. Technical and procedural measures of the organizations are business confidential, and the information can only be obtained from limited number of subjects willing to share information.

2. Cybersecurity is not a priority for SMEs and therefore it is harder to obtain relevant amount of data because of small number of responses.

3. Best effort basis for obtaining statistically relevant number of responses.

1.5 Research methods and structure

This thesis will be applying a mixed methods approach [18] that allows the use of both qualitative and quantitative research methods. The author believes that this approach enables reaching a better understanding of the fundamental risks and offer potential solutions. As the purpose of this research is to analyse the existing problem, determine potential shortcomings, and offer solutions for further research and possible preliminary practical solutions, the thesis follows an evaluation-based research model. Based on author's experience working on determining solutions to similar issues, most of the literature will be technical in nature and published by technology or cybersecurity organizations as white papers or reports. A great number of used literatures originates from the public sector who is responsible for cybersecurity matters on national level. The author has acknowledged that need to be extremely critical when proposing public sector approach and solutions to private sector.

The author will also conduct a survey among Estonian SMEs to determine their current level of cybersecurity as well as their experience responding to cybersecurity incidents and possible experience for incident coordination with national level or cybersecurity service providers from the private sector. Unfortunately, after conducting the survey it

became clear that the final number of respondents is too low to use as a reliable statistical benchmark for drawing fundamental conclusions. The author nevertheless believes that surveys are a useful tool in order to obtain a better overview of the cybersecurity level of the SMEs. As a qualitative research method, an interview with an expert from RIA was scheduled to obtain an adequate assessment from the national level on the cybersecurity level of Estonian SMEs, relevant parts of the interview will be referenced throughout the thesis. The expert also provided author with an additional focus group based research to complement the quantitative survey. Due to the extremely small number of responses, additional interviews were carried out to obtain an expert overview of the situation by interviewing both national level and SME experts who are directly involved with working with SMEs and provide assistance and guidance in case of cyber incidents. Two interviews with 2 representatives from SMEs have also been conducted to obtain an overview of the issues SMEs can encounter when suffering a cyber-attack and needing assistance.

The thesis has the following structure:

1. Chapter 2 gives a preliminary overview of some the main concepts discussed later in the thesis

2. Problem concept. The purpose of chapter 3 is to identify possible current cyber threats to Estonian SMEs and to identify the main reasons for those threats' realization into incidents and the possible impacts. This chapter will also provide a brief overview what is incident response and why it is not a focus in this thesis.

3. Literature review. Chapter 4 explores existing literature with focus on improving SME cybersecurity or coordination and also looks into literature about coordination, public private relations, and information sharing.

4. Chapter 5 provides an overview of the conducted survey, its results and makes relevant observations. Included will be the focus groups research provided by RIA.

5. Chapter 6 will be used validate some of the findings in this thesis.

6. In chapter 7 the theoretical understandings gained from previous chapters will be used to identify possible ways how to improve coordination between SMEs and

national level and potential preliminary solutions will be recommended including ideas for future research.

7. Chapter 8 will summarize the findings of the thesis, offers discussions and possible future research problems.

First this thesis will be developing a strong theoretical understanding of the problem statement. Consequently, the knowledge base will be used to start identifying specific problems and start synthesizing the gathered knowledge into potential solutions and preliminary practical suggestions.

2 Theoretical overview

Conveying information about cybersecurity to people or organizations who do not care, do not have IT as their business focus or just try not to rely on it as much as possible can be difficult. Trying to relay new ways on how and what enterprises or organizations should think about or do, can be even more taunting as majority of organizations are already feeling overwhelmed of the existing possibilities or possess a false sense of security. In a 2016 survey conducted among UK's small businesses 68% of respondents believe that there is little to no risk of them becoming a victim of a cyber-attack [70]. It can be estimated that the overall awareness has gotten better, drastic change however does not happen in such a short manner and that is reflected in a 2019 survey amongst enterprises with fewer than 500 employees showing that 66% of respondents believe that a cyber-attack is unlikely to happen to their organization [91]. A quote from the former FBI director Robert S. Mueller "I am convinced that there are only two types of companies: those that have been hacked and those that will be." [94] is well in place to describe the overall cybersecurity landscape.

Based on authors personal experience, the issue of reflecting one's understandings is very prevalent in cybersecurity, as knowledgeable and experienced cybersecurity experts reflect their own understanding and beliefs on those who might not have any inherent interest in cybersecurity. This is neither surprising nor inherently wrong as both of those worlds make decisions based on their own beliefs and backgrounds. But there can and should be a method that these two communities can work in a manner that is beneficial to both and this is where the necessity of coordination has to be addressed. Coordination is management of interdependent relationships that necessitates the exchange of information in order to align actors' intentions, goals, and actions. This definition perfectly encapsulates not only the fundamental problem this thesis tries to solve but also the solution. The definition originates from a 1988 article "What is coordination Theory?" by T.Malone [19] and is effectively used in a research addressing coordination issues between entities due to small and large organizational seams [96].

The author believes that that lack of financial resources and qualified experts form a part of overall problem, but the issue is deeper than the lack of abovementioned resources and begins from people's threat perception. As is supported by various surveys and reports

stating that small to medium enterprises do not consider themselves to be at risk from cyber-attacks [70] and this way of thinking is rather widespread and amplifies the impact of the attacks. Additionally, to limited resources and knowledge, the complexities of today's interconnected world make proper risk assessment and management even more complicated [93]. In a report by IBM that included 1000 global enterprises and 800 insurance providers, 32% had been affected by a digital interconnectedness incident that caused economic damage over the past three years and 60% believe that relative risks of digital interconnectedness will increase over the next ten years [93].

National level should not be thought about as any specific entity rather as a way for the government or the SMEs to communicate through various formats like private-public partnerships (PPP). What the exact parameters for that format could be will be explored later in this thesis along with a more thorough understanding of PPPs. While it is critical to clearly define stakeholders and their responsibilities within a public-private relationship, [20] in this thesis we will be focusing on potential directions and not so much on specifics of formats for PPP. When defining overall stakeholders between Estonian SMEs and national level coordination, SMEs have a critical role. Specific national stakeholders will be explored later in the thesis but overall, it is needed to understand that the national level will have the critical role of coordinating cross-sectoral focus as only the national level can possess a holistic overview of the nation's overall cybersecurity to which SMEs contribute significantly. It cannot be expected that national level can possess the capabilities to fundamentally understand and manage every sector's specific risks considering public sector's limited resources. National stakeholders should be held responsible for synthesizing information from SMEs, offering their own available expertise and providing those result to the rest of SMEs to ensure proper understanding of cyberspace, threats, risks, and necessary actions to take. SMEs have been addressed by national level actors like CERT-EE and Police and Border Guard through several awareness raising campaigns over the past years but as we explore the annual reports, we can see that this has had rather low effect as the costs of cybercrime in Estonia are raising, leading to a realization that a more efficient coordination method is required.

A paper by National Cybersecurity Coordinator G.Sharkov from Bulgarian Ministry of Defense states that it is important to move from simple cybersecurity to cyber resilience. Meaning that we should be preparing for the "unknown unknowns." [20] This in emphasizes the same idea that is discussed in this thesis – threat of systemic cyber risk

and cascading effect of cyber incidents. In many ways these are the unknowns, especially in a rapidly digitalizing and interconnecting world. The paper elaborates that resilience can only be achieved through a multi-stakeholder approach, including SMEs. While each stakeholder needs to be an active participant, the paper suggests that it should be the initiative of the government to develop necessary multi-stakeholder frameworks. This is something the author of this thesis agrees upon. The idea of government initiative is even more important when addressing SMEs, as these enterprises operate with limited resources and priorities than cybersecurity and cannot be expected to start developing proposals and frameworks for cooperation or coordination from their own good will, when their main purpose is to produce business benefit. Sharkov also highlights the need to find a balance between regulation and self-regulation. The author fully supports this idea and explores this idea further in this thesis, meaning that while national cybersecurity laws are a crucial tool these can also have adverse effects where over-regulation can lead to loss of trust rather than a two-sided beneficial relationship and can lead to a situation where the public sector tries to use the private sector to fulfil its own goals. This idea is reflected in a survey where 64% of respondents stated that governmental influence and regulations will not improve future risks [21].

3 Cybersecurity challenges for Estonian SMEs

Cybersecurity research company Cybersecurity Ventures has estimated that cybercrime will cost the world $6 trillion annually by 2021, raising by $3 trillion from 2015 [22]. That amount of money is mostly out of range of imagination for most enterprises but comparing it to the total cost of $210 billion worth of losses caused by global disasters in 2020 [23], it can provide a vivid example of the importance of information systems today. With cybercrime estimated to cost the organizations $10.5 trillion by 2025 [24] the trend is moving upwards, and enterprises have no choice but to prepare for the inevitable cyber incident. That does not necessarily mean that every enterprise, medium, small, and large, IT focused and not, should invest in the same solutions. Rather than trying to keep up with adversaries and prepare for every possible know cyber-attack, we should be investigating more efficient ways of improving existing capabilities, processes, and solutions.

3.1 Estonian SMEs

In Estonia, as well as overall in EU, an enterprise is considered a small to medium enterprise when employing under 250 employees, having annual turnover under €51 million or a balance sheet total of no more than €43 million [25] [26]. Based on 2017 statistics, small enterprises in Estonia employed 56.5% and medium sized enterprises 22.3% of people, totalling to employing 78.8% of Estonian workforce.

For overall EU statistics, large enterprises, employing over 250 employees, generated 44% of gross value added, in comparison, Estonian large businesses generated 21.7% of gross value added [27]. That figure itself is not surprising, considering that Estonia has 137808 SMEs that form 99.8% of all enterprises registered in Estonia [28]. These figures are significant to this thesis and Estonia. It can be clearly said that the SMEs are a crucial part of people's everyday lives in Estonia by offering jobs but also functioning of the country itself by generating almost 80% of the country's total gross value added.

3.2 Estonian national cybersecurity level

RIA reports that Estonian enterprises are losing over €1 million euros a year to cyber-attacks [29]. The report also specifies that this amount is only the beginning as it only consists of actual figures that are reported to the authority by the victims. Due to the small nature and the small region of Estonia, it is not unexpected to encounter "Nothing bad happens to us!" or "It won't happen to us" attitude because of the size or relevance of the business numbers, and because enterprises are people, it is not uncommon to find that attitude from enterprises themselves as well.

That attitude is also reflected in a recent survey conducted by Turu-uuringute AS, where 37% of questioned enterprises do not have anyone solely responsible for cybersecurity [30]. In a similar survey on the other hand shows that 75% of questioned Estonian enterprises consider their cybersecurity capabilities to be good or even exceptionally good [12], at the same time only having implemented consider basic security solutions, which could be seen as overconfidence.

It is important to consider today's society's interdependencies between services and organizations and keep in mind that it is not enough to only to build a strong fortress around your own organization. Enterprises need to be able to communicate and coordinate incident response in real time with all its stakeholders. It has been reported that half-way through 2020 the amount cyber-attacks had already doubled compared to the total amount of cyber-attacks identified in the entire of 2019 [31]. Cybercriminals do not let the potential opportunities to exploit vulnerabilities bypass to increase their potential income. One of the main reasons for such drastic increase in cyber-attacks is the uncertain situation caused by COVID-19. The worldwide situation caused by a life-threatening virus has not only created a situation where organizations have been forced to support unprepared teleworking in a short notice but also a larger attack surface that cybercriminals can use by exploiting people's fears and uncertainties to get them to click and download malicious content. While teleworking itself can be done safely, the transition process can cause various degrees of problems.

Estonia has established a cybersecurity ecosystem where there are multiple national level stakeholders that can be of assistance to individuals and enterprises in case of a cyber incident. The Estonian Information System Authority has many responsibilities from

fulfilling strategic cybersecurity and digital society's goals to protecting critical infrastructure, but also facilitates CERT-EE that is a national and international point of contact for all cybersecurity matters occurring in Estonian internet space. CERT-EE is also conducting awareness raising campaigns for both general population and technical personnel of the organizations and is sharing information of on-going widespread campaigns. Anther stakeholder on a national level is Police and Boarder Guard (PPA) who facilitates cybercrime unit (C3), that is concerned with reported cybercrime. Estonian C3 prosecutes criminal offences, while CERT-EE provides technical assistance and threat intelligence. Another initiative led by PPA is "Online constable" program where people can contact designated police officers in social media directly and report their cybersecurity and cyberbullying concerns. The third national stakeholder that has become very active after GDPR came into force in 2018 is the Estonian Data Protection Inspectorate (AKI) that ensures people's confidential information (personal data) is sufficiently protected, including supervision over GDPR [32]. AKI also offers different lectures and guidance materials for different data privacy matters that have found large coverage in media, in example questions regarding surveillance cameras in private and public estates. The three institutions are often collaborating to ensure a larger coverage of awareness raising campaigns. As can be explored later in this thesis, they have not reached all focus groups, nor have the campaigns or organizations been heard of which leaves space for improvement.

3.3 Threat landscape

This thesis will focus on the recent threat landscape as whole with a focus on threats most relevant to Estonia. Due to the extremely interconnected nature of the cyber domain, the trends describing the prevalence of specific cyber-attacks or threats commonly reflect global situation. There are of course region-specific vectors of how a certain kind of attacks can be carried out. For example, Estonia as a small country receives global cyber-attack campaigns most commonly with a certain delay as because of the small size and small population it is not the most attractive target for cybercriminals. For example, crafting mass phishing emails for 83 million Germans versus 1.3 million Estonians can without a doubt be financially more profitable. But that does not mean that cybercriminals would not be investing in abusing the underlying systems of Estonia's public electronic services and trust to carry out phishing attacks.

3.3.1 Phishing attacks

In Estonia, each citizen has a state issued ID card and on it also a digital identity. Additionally, to the ID card the citizens also have a possibility to obtain mobile-ID that is one the methods to authenticate one's identity without the ID-card and conveniently from the phone [33]. Logging into any service that requires authenticating, your electronic identity in Estonia, also requires PIN1 and to sign a document or to confirm an action legally requires PIN2. Additionally, to the government issued mobile-ID, there is an application called Smart-ID that similarly to mobile-ID allows Estonian citizen to use e-services for authentication and signing their documents [34]. Over the past few years, cybercriminals have used this Estonian specific attack vectors and have directed users to phishing sites to create a Smart-ID account on their behalf instead. This gives them an option to use legitimate services with the created Smart-ID and perform and sign actions on the actual user's behalf [35]. The attack itself nevertheless was exploiting human factor instead of technical aspects. This incident outlines that an organization cannot prepare themselves or their employees for every possible attack scenario.

As enterprises cannot be ready for every possible attack vector that cybercriminals can develop, especially considering regions, languages, culture, etc, there must be an active role in every enterprise that in addition to implementing proactive methods, makes sure that their organization is always, as much as possible depending on their specific capabilities, up to date with the latest changes in threat landscape regardless whether these are news, white papers, or reports on newly discovered security vulnerabilities. This is not something that every single enterprise or organization has to do themselves but is something that should be handled as a community - a community of enterprises themselves but also national organizations like computer emergency response teams (CERTs).

3.3.2 Business email compromise (BEC) and Chief Executive Officer (CEO) fraud

During the past 5 years Estonian organizations have fallen a victim to CEO fraud where only the unawareness of the accountant or finance department can be counted as a cause. The easiest and a working solution to protect against CEO fraud is to view the sender's and reply-to e-mail that unfortunately has been made technically more difficult after widespread of Outlook and mobile mailboxes. Over the last 2 years the CEO fraud has evolved into more advanced BEC scheme where the actual e-mail of the user has been

compromised, most commonly after a successful phishing attack. In April 2020 FBI released a public service announcement, stating that BEC have cost US businesses more than $2 billion [19] and between the period of June 2016 and July 2019 the losses to BEC reached over $26 billion worldwide [36]. BEC was also the costliest cyberattack for Estonian businesses and organizations in 2018, as CERT-EE had received reports totalling to over €600 000 in damages. Although reported damages were totalling lower, the trend of BEC attacks continued into 2019 with multiple enterprises loosing up to €70 000 [37].

BEC does not only result in monetary loss but also in personal identifiable information (PII), personal data and business confidential information being exposed to third parties. In EU states that also means violating the GDPR which protects every individual's right to privacy and confidentiality and security of their personal data [38]. While BEC is technically not a sophisticated attack, it can stay unnoticed and can be conducted over period of time in case e-mail logs are not being monitored for anomalies like logins from different countries. In multiple cases the BEC schemes have been uncovered through a business partner who is communicating directly to confirm the change of bank details. Of course, if these business partners do not have a high cybersecurity culture in their organization, the changes in bank account details will be easily made and the loss of money is inevitable.

CERT-EE has made significant efforts in ensuring that information about these BEC attacks is available to all who need it and advise any possible victims [39]. CERT-EE reports in RIA's annual 2020 report that most victims to BEC attacks were SMEs who are handling various imported good like tools, industrial equipment, and even medicinal supplies. As it can be concluded from the profile of the impacted businesses, typical victims are from SMEs whose main focus is not on IT and who are providing services and goods. With limited resources, both financial and personnel, the goal of the SMEs is to focus on their primary business for survival, especially under COVID19 conditions. An effective method of prevention would be notifying CERT-EE of a suspicious e-mail for validation before making a new transaction but quite often the knowledge of CERT-EE's existence is not present at SMEs.

3.3.3 Ransomware

Following the global trend, the Estonian SMEs have been impacted by ransomware for nearly a decade. A report in 2017 estimated ransomware to be generating $1 billion paid in ransom annually [40] and causing total damage of $5 billion [41]. In 2020 it was estimated that ransomware damages totalled to $20 billion [42]. In 2014 CERT-EE identified single cases of ransomware spreading in Estonia but by 2015 this number had already gone up to 150 [43], reflecting a similar growth as the rest of the world. March 2020, the first month of worldwide COVID-19 lockdowns, saw a 148% rise in ransomware attacks compared to February 2020 [44]. Ransomware can be delivered to the victim by abusing vulnerabilities in the system, improperly configured online services or social engineering. By abusing an already demanding situation created by the pandemic, the cybercriminals started abusing the unclear and unknown situation in order to maximize the chances of possible profit and tailored their ransomware campaigns to follow the trending COVID-19 rumours. Most commonly the users were targeted with e-mails offering free vaccine, testing and miracle cures, as well as advertising secret messages from health organizations [45].

Based on a report by cybersecurity company Sophos about the state of ransomware in 2020 it was surveyed that in 95% of cases when ransom money was paid, the victims were able to get back their files [46]. It is also in the interests of the criminal that victims do get their files back as that is good for their business reputation. And in a situation where an enterprise has lost their backups or quite often do not have any at all, they have a choice, whether not to support cybercrime and lose their files or support cybercrime by paying the ransom to restore their business operations. Considering that most enterprises targeted by ransomware have a median size of 62 employees and a successful ransomware attack causes an average of 15 days of downtime or that paying the ransom has a median cost of $44000 [47] without considering the extra costs that go into employees decrypting the files and rebuilding IT infrastructure. Since summer of 2020 it has been reported that new functionalities have been added to several ransomware that strains not only to lock the systems but also to extract the data and leaking or selling the corporate information on the black-market [48]. For all the organizations that must comply with GDPR this also means a possible fine of up to €20 million or 4% of their annual global turnover. This has created another efficient way for criminals to pressure organizations and enterprises into paying.

3.3.4 Supply-chain attacks

Supply-chain attacks are difficult to uncover and mitigate as the organization may be implementing sufficient countermeasures but can be attacked through a business partner or serve unknowingly as an attack surface to a business partner instead. By compromising the initial victim and the service they offer, the attackers, rather than having compromised one victim, have compromised multiple victims along the supply-chain.

One of the most famous recent examples is an attack against SolarWinds where the attackers compromised a US based company SolarWinds with the purpose of modifying their network monitoring software named Orion. The compromised software was used by 33000 clients, including many government agencies, many private companies, and even potentially NATO, [49] and at the time of the attack 18 000 clients had the vulnerable version of the software installed [50].
This attack may seem distant and unrelated to Estonian SMEs but the relevant learning aspect in this case is that there are possible attack vectors against the company that are beyond the company's control and defence capabilities. The true impact of SolarWinds attack is still unknown as companies are still investigating the impact on their own system [51]. Microsoft has stated that a small subset of Azure, Intune and Exchange components were accessed by the criminals [52]. Considering data about Microsoft's widely used email service Exchange was stolen, it is possible that knowledge can be used to target enterprises using Exchange. According to one source 29% of Exchange users are small enterprises under 50 employees and 47% are employing 50-999 people [53], making Exchange popular amongst SMEs.

In June 2017 Estonian enterprises using accounting software developed by Ukrainian company M.E Doc experienced the results of a supply-chain attack first-hand when the software developer was compromised. Malicious code was injected to be executed with the next update spreading NotPetya virus with no option to recover the files even though ransom note was included and restoration of files upon payment was promised. The total damage caused by NotPetya reached over $10 billion [4] globally. Three Estonian companies reported infections, multiple reported applying countermeasures in the form of disconnecting their systems and a hardware store was shut down for a week to build up their systems [54] [55].

The peculiarity of supply-chain attacks is that it can be clearly seen that communication, collaboration, and coordination between different stakeholders, especially with national level, is required. The organizations might be able to mitigate the attack but sharing this information with national level can serve as a benefit to other organizations. The national level has the means and communication channel to make a make a public statement on the attack vectors and mitigation measures, to offer assistance for the organizations impacted but not yet reported or serve as a warning to other organizations to implement countermeasures before the situation has escalated into an incident.

Systemic cyber risk as explained by World Economic Forum (WEF) is a realization of a certain cyber risk regarding an individual part of the cyber ecosystem which causes cascading effect that impacts other ecosystems causing adverse effects to public safety, health, finance, or even national security [56]. The presence of systemic cyber risk is caused by the issue that organizations focus on their own work and have forgotten that they are connected to the external stakeholders through connected services. Unless an organization is ISO (or some other framework) certified, the risk assessments, if they even exist, are created taking only the organization's internal factors into consideration.

3.3.5 COVID-19 threats

According to International Chamber of Commerce (ICC) SMEs and their employees are among the ones experiencing the hardest impact of COVID-19 pandemic [57]. While COVID-19 is not a cyber threat, it has changed many aspects of how the society functions and paved a way for a larger attack surface as people have been encouraged to move their lives online for the sake of their health. The main modus operandi for phishing attacks has been imitating actual service providers and attempting to lure the users to insert their credentials into a seemingly legitimate environment. COVID-19 has seen a new trend of inviting the users to insert their PII in order to receive critical information about the ongoing pandemic

The threat of cyber-attacks in COVID-19 times has seen a high rise in numbers as criminals have no moral issues in exploiting people’s fears for their own personal gain. A bigger issue for SMEs is the unprepared need of moving to teleworking that should not be confused with remote work. Remote work is mostly used to classify employees whose workplace for most of their time is away from the main offices no matter what. Teleworking is reserved for those employees who can conduct their tasks away from the

office but still need to be available to visit the office in a short notice or conduct regular meetings there [58]. An IBM 2020 survey found that 54% of respondents required their employees to start working from home [59] and cybersecurity company Carbon Black also reported an increase of 70% in remote work in the second quarter of 2020 [44]. More than a year has passed since enterprises and employees had to develop new ways to facilitate teleworking to their daily lives. Although there has been considerable amount of progress made to secure remote work, there are still several ways to increase the security of the teleworking employees in an environment that is not controlled by the IT-department of their employer.

Being prepared for the future does not just mean having mitigated the shortcomings brought forward by teleworking but also realizing that the way how people work, and enterprises behave has most likely changed for good [60]. Offices most likely will not stay empty but will develop a hybrid way, where enterprises will try to balance teleworking and the need for social interactions, is more than likely to become a trend after the end of pandemic. A survey by cybersecurity company MalwareBytes found that 31% of enterprises consider their teleworking cybersecurity level to be largely the same as when working from the office [61]. This can mean overconfidence in thinking that as all the employees are scattered, there is no centralized attack target, ignorance, or that an enterprise's existing cybersecurity level is extremely poor. In most of the cases it is highly likely that the cybersecurity status in the personal environment is at a lower level than it is at the workplace. This can involve managing software updates to ensure the security of the systems, security of the network, data security, but also third parties like family members or roommates having access to business confidential data when simply passing an unlocked device.

A troublesome aspect for enterprises at the time of teleworking is the use of non-audited devices used by employees to perform their daily tasks. The survey by MalwareBytes also found that 28% of respondents preferred using their own personal devices rather than the devices issued devices [61]. The large of amount personal devices that are now connected to the enterprise network through a virtual private network (VPN) can provide the attacker access to the corporate network and data, and to be used for lateral movement to corporate systems. The first results of this ad-hoc solution to teleworking are also noticeable, as enterprises are reporting 20% of security incident s have been caused by a teleworking employee using personal devices [61].

Unaudited laptops and personal computers (PC) for teleworking are not the only devices that are a cybersecurity concern as people connect to their home networks where they have other internet connected devices. Those devices can range from internet connected kitchen aids like smart fridges and kettles, children's toys, smart lights, security devices such as cameras or smart door locks, being classified as Internet of Things devices and create a larger attack surface for the attacker [62].

In a 2016 survey, the participants from various sized enterprises who are responsible for IT network technologies were asked if they knew about a security policy in their enterprise for IoT devices. Only 44% of the respondents knew about such policy [63]. Considering that the survey focused on participants who deal with IT and they were not aware of any security policies made it clear that employees that might not have any experience with ICT do not think about their smart kitchen appliance being a threat to their employer. Organizations also need to start focusing and allocating more resources not only securing and educating their employees about the dangers in the office but also from working from home environments. According to the Estonian law the employees must get the permission to perform work from home but also need to address the risks related to working from home environment, in example both the risks to health and to securing the company owned devices.

3.3.6 Data leaks

Data leaks or breaches are not referring to any specific attack but are generally a consequence of a successful attack. In a 2020 report Ponemon Institute in collaboration with IBM, states that the average cost of data breach has totalled globally to $3.86 million and that the average detection time is 280 days [64]. The report included 524 organization that had experienced a data breach. The report concluded that 54% of the data breaches were caused by a malicious attack, system glitches and human error following with 25% and 23%. In September 2020 RIA reported that malware known as Emotet had also started to harvest victims electronic address books [65]. Emotet is a malware originally developed with the purpose of stealing victims banking information but over time it was developed to serve as a malware as a service platform (MaaS). It is a trending situation where the cybercriminals do not only use malware for their own personal gain but also rent out the infrastructure to actors who can use it for their own gain by distributing more malware and only paying the original operators fee for using and renting the service.

Emotet botnet has been taken down as of 27.01.2021 by a collaborative effort of many authorities in Europe, US, UK, and Ukraine [66] and having operated since 2014, has been declared one of the most disruptive botnets. Emotet did not spread by sophisticated attack vectors, but rather through phishing and spam emails. Considering that in July 2020 RIA was reporting around a hundred infections of Emotet [67], it is clear that individuals and enterprises need to keep on focusing on basics of cybersecurity and follow best practices.

Many enterprises including SMEs are moving their data to the cloud as it can be more cost-effective than building, maintaining, and securing their own infrastructure. This can lead to a false sense of security and compliance. Technology company Oracle conducted a survey in 2019 including 456 participants, and while it mostly represents organizations employing 500-999 people, it does illustrate the importance of cloud services and hosting for enterprises as 49% of the respondents expecting to store majority of their data in the cloud by 2020 [68]. One critical aspect that the report highlights is the confusion regarding shared responsibility of securing the cloud. While cloud-based infrastructure and service hosting may inherently seem secure, in reality it depends on the model of cloud service an enterprise is implementing. The responsibility of securing several aspects like user access, data protection, application security etc falls on either the customer or the cloud service provider depending on the type of the cloud. And based on the survey carried out by Oracle, only 10% of chief information officers reported no confusion regarding the shared responsibility security model.

There have data breaches by Estonian enterprises that have led to GDPR violations and so far the consequences have resulted in fines of total amount of 408 euros [69]. This should not be an indicator not to work harder on securing your data but as a reminder that data breaches do happen, even in Estonia and at one point the data protection authorities will start enforcing the rules more harshly as is already shown by Estonian Ministry of Justice's plan to refine the existing regulations to allow more effective response to violation of the data protection law [70]. A survey conducted by analytical company Kantar Emor investigated Estonian enterprises' outlook on data breaches in the period of 2019-2020. In that period 6% of the participants had been affected by a data breach and 15% of enterprises reported no such incidents in their organization [71]. These statistics can be concerning, as the Estonian Ministry of Justice has proposed stricter financial punishments for data breaches following the lead of other EU member states [72]. In a

survey ordered by the US National Cyber Security Alliance (NCSA) in 2019 concluded that 10% of small enterprises declare bankruptcy after a data breach [73].

It is clear that enterprises must not only secure their organization's data, but also the data trusted to them by their customers. This is not a responsibility that can be taken lightly, especially considering the sustainability of the business as GDPR fines are becoming more prevalent and impactful. It should be noted that while a first offence of GDPR might be looked on more lightly, losing the trust of your clients can be worse to your business and unsurprisingly 10% of small enterprises have declared bankruptcy after suffering a data breach.

3.4 Impact of cyber-attacks on SMEs

Paying a fine due to a breach of GDPR or recovering from a ransomware attack by paying for the workhours required to restore systems and business functionalities are financially measurable and comprehensible for the enterprises. What are not so apparent are the hidden, also known as the beneath the surface costs, of a successful cyberattack. A report by Deloitte lists factors like investigation, customer notifications, public relations, various fees, and cybersecurity improvements among others but as well beneath the surface costs like insurance premium increases, value of lost customer relations, lost contracts, devaluation of enterprise name, and possible loss of intellectual property [74].

Beneath the surface costs of Estonian SMEs have not been clearly determined by any study but we are aware of some of them by the enterprises who are willing to share their experiences and information with national organizations like CERT-EE. It is not uncommon for the organizations to neglect to share the internal information about cyber-attacks they have suffered because of beneath the surface costs, in example the fear of reputation loss and trust of customers or fear that someone can uncover their business confidential information. Estonian organizations have been encouraged to share their information confidentially with CERT-EE for longer than a decade as the team has better tools for confronting and mitigating cyber threats and sees a larger threat landscape than any SME and might propose a solution that has already deemed efficient to another organization who has suffered a similar attack. RIA reports that Estonian businesses are losing over €1 million in a year due to cyber-attacks and that is only taking into consideration the costs that the organization has already managed to calculate [29]. Based

on Deloitte's risk assessment experience, the effects of the attacks can extend over years following the incident itself, whether it will be the restoration or exchange of infrastructure or media campaigns to win back the trust of the customers.

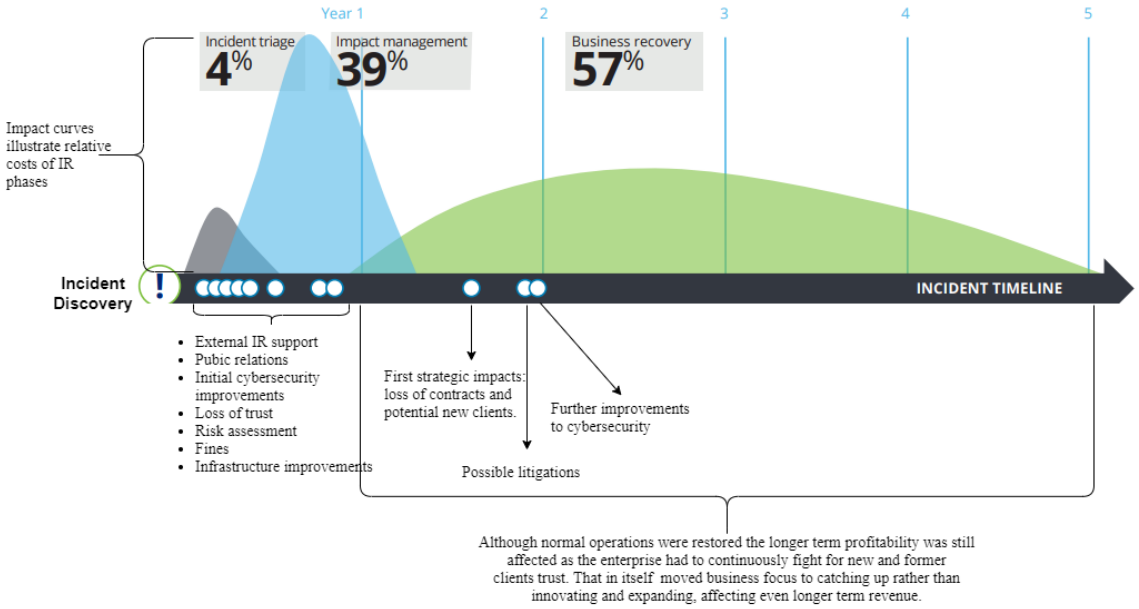

Figure 1. Incident response timeline. Adapted from [74]

Different SMEs have different thresholds on how much they can afford to lose to cyber-attacks or pay for ransom to get their files back. Many SMEs have also calculated whether it would be more beneficial to pay the ransom or to mitigate the attack as they have limited resources and mitigating the attack could cost them more than the requested ransom. In a survey by KPMG 89% of small businesses who had experienced a cyber-attack felt that the attack impacted their reputation [75]. Different cyber-attacks on enterprises can have varying results and entail different hidden costs. A business email compromise can potentially ruin a partnership between two long-term business partners as one could suffer substantial monetary loss because the other party has not implemented any cybersecurity measures. Data breach resulting in clients PII theft can not only lead to a GDPR fine but also clients losing trust in the brand and enterprise itself. A KPMG survey that included 1000 small enterprises across the UK found that 26% of enterprises that had suffered a cyber-attack reported being unable to develop as a company as a pre-attack growth plan foresaw [75]. As growth is critical for any business that wants to stay relevant and produce revenue, the idea that a cyber-incident could negatively impact their potential should be a worrying wake-up call. Not only is stunted growth worrying but also the impairment of

business functionalities as 93% of respondents to KPMG survey reported the businesses ability to operate [75] which led to customer delays as enterprises had to take down their website or pay a third party to fix their issues in response to dealing with the attack. Not being able to efficiently serve your clients according to the agreed service level agreement is not only an outward looking issue but also inward as the employees can lose their trust in the organization itself because it might also not be able to ensure its own employees safety in the digital world.

3.4.1 Interdependence of systems

Supply-chain attacks serve as a good example of cascading effects and interconnectivity not only among the information systems but society as a whole as no incident in 2021 will only impact only one organization or a single individual any longer. In a 2016 white paper "Understanding Systemic Cyber Risk" by WEF, the idea of a systemic cyber risk was introduced. It was described as a "risk that a cyber event (attack(s) or other adverse event(s)) at an individual component of a critical infrastructure ecosystem will cause significant delay, denial, breakdown, disruption or loss, such that services are impacted not only in the originating component but consequences also cascade into related (logically and/or geographically) ecosystem components, resulting in significant adverse effects to public health or safety, economic security or national security" [56]. This definition is suitable and will not be discussed in more depth in this thesis but rather the focus will be the cascading effects of the systemic cyber risk. One of the issues that WEF highlighted regarding systemic cyber risk was the fact that there were not any real-word examples but since 2016 a lot has changed, in example the NotPetya incident previously described under supply-chain attacks. The 2016 white paper accurately assessed the potential systemic cyber risk for the transportation sector as the risk when it materialized in 2017 when NotPetya ransomware caused the giant shipping company Maersk an estimated $300 million in total losses [76] [76]. That was just the total cost to Maersk without considering the impact to the global economy due to the cascading effect of Maersk being the world's largest shipping company and handling 20% of all goods along the world's busiest shipping routes [77]. It is estimated that NotPetya caused damages totalling to $10 billion, we can only assume at this point how much of that are the cascading effect damages caused by Maersk. It is important to remember that Maersk was not the point of origin for NotPetya, but another victim along the supply-chain attack path which in turn empowered the global cascading effect. What can be concluded as a

valuable lesson learnt from incident postmortem is that rather than isolating themselves to solve the ongoing incident, Maersk was open and professional in their communication with [78] external stakeholders and shared all their findings [78].

National legislation like ECA has made great progress in not only defining the specific critical enterprises and organizations, but also setting minimum cybersecurity standards for these entities in order to reduce the occurrence of cyber incidents and disruption of vital services. A law can serve as a legal basis to enforce organizations to achieve the minimum compliance in order to pass the audit and avoid fines. The ECA does not define any solutions or configurations that need to be implemented but outlines the security measures that the organizations are required to implement in order to "resist any action that compromises the availability, authenticity, integrity or confidentiality of data" [79] [79] leaving a lot open to interpretation for the organizations. For example - "§7. Security measures of service provider's system" outlines the need for security measures to be able to respond, resolve, prevent, and mitigate cyber incidents. ECA sets additional requirements for the organizations, such as a risk assessment, and compliancy controls among others [79]. It can be claimed that Estonia has been a visionary in the field for having a legally binding cybersecurity law, but the author wishes to highlight that even though the ECA sets minimum security requirements for the organizations it does not create a solid foundation for the real necessity of these requirements. Therefor many organizations find themselves from the situations where they have a law to comply with and list of requirements to implement and as per author's professional experience, the organizations are more concerned with compliance rather than finding a way for improving the organization's cybersecurity level. [5] and creating an understanding of cybersecurity relevance in daily operations and risks it poses [5]. Currently there is no available information on the number of SMEs that need to comply with the ECA, neither any number of SMEs who have been audited for the cybersecurity compliance nor the number of SMEs who have passed or failed. The low level of cybersecurity among SMEs has been highlighted in different reports by RIA and ENISA, but as per author's experience, the results of these reports do not reach the SMEs since they are focused on their daily operations and primary business goals and since they quite often lack a separate IT person, do not focus on the technology and cybersecurity section news, or reports since this is not their area of expertise and nothing that concerns them. "From one hand, we have the public sector who is concerned about the situation on the national level and is

reaching out to offer the SMEs an expertise they lack. On the other hand, we have the SMEs who do not see the hand and offer for help, since they are keeping eyes on their primary business area and rules and regulations that directly apply to them. For example, how much fish can they bring back or how long can the shifts of the employees be." [80]. In author's opinion, this not only summarizes the situation, but can also serve as a foundation for improving the cybersecurity level of the SMEs and cooperation between public and private sector. The national organizations like CERT-EE and Cybercrime unit of Estonian Police and Border Guard have the subject matter experts in cybersecurity and can offer them for awareness raising campaigns aimed at specific type of SMEs. The SMEs as experts in their own fields possess the communication channels to reach the target group and can provide valuable examples from their own area of expertise to bring cybersecurity closer to the SMEs [80].

3.5 Difficulties of coordination

Before approaching viable solutions to propose more efficient coordination, the difficulties of not only implementation but applying the solutions must be addressed.

1. The quantitative problem. With 130000 SMEs in a country with a population of 1.3 million, the lack of cybersecurity workforce statistically stands out and taking into consideration that most Estonian SMEs employ under 15 people, hiring a cybersecurity expert is an unreachable requirement. The matter of trying to coordinate such substantial number of organizations has been very apparent ever since the implementation of ECA in 2018. As the author was responsible for CERT-EE's incident response procedures during the implementation period of ECA, it became apparent that determining the enterprises who have a legal obligation to comply with the ECA, was not so straightforward. Although the ECA itself clearly determines the critical infrastructure service providers, there are outliers that are harder to identify. For example, digital service providers, that manage online web stores, search engines, or cloud computing services can be SMEs [79] .

2. There are limits to the extent of the current ECA that is directly connected to the NIS directive itself. Laying a foundation to national standards with NIS, this has provided a solid foundation for obtaining suggestions for the improvement and

for the NIS 2.0 that is aimed at sector based approach and all businesses with over 49 employees within their respective sector will be considered subjects to the new directive [81]. The private sector establishments can be forced to comply with legal measures, but their employees cannot be enforced to make cybersecurity their main priority by any law or regulations. Estonia there are 6509 enterprises who employ between 10 to 49 people [28]. Among those 6509 enterprises are water suppliers, waste management, logistics, transport, chemical, and medical manufacturers, food, postal and courier services – sectors that are all subjected to the new NIS 2.0 and according to currently proposed legislation are not included as a vital service in Estonia.

3. Organizational interdependencies. The coordination requires at least two separate parties and is already difficult in case the parties have diverse backgrounds and focuses and lack of overall collective understanding of the matter as both parties view the matter from their personal and professional perspective [82]. The complexity of the situation increases by every party added to the coordination. This nevertheless is nothing cybersecurity specific but general communication theory. What makes the situation more complicated when solving a cybersecurity incident impacting different stakeholders is a specific knowledge required for the situation, a competent subject matter expert, and an unforeseen situation for the impacted parties who have been only focused on maximizing the efficiency of their main field of operation. Having the experience in solving cybersecurity incidents and leading coordination between different stakeholders, the national level, in example CERT-EE, has the necessary knowledge of how to address the known aspects that the stakeholders among SMEs are unaware of as this is not a focus of their daily operations, nor have they foreseen the necessity for preparedness for cybersecurity emergencies guidelines. Another problematic circumstance that has become apparent during COVID-19 times, is the difference in digital and technological advancement of the organizations where a situation has occurred where not only do the stakeholders have difficulties communicating because of different understandings, but also because of the variety of communication channels to interact and exchange information when face to face meetings are not encouraged [83].

3.6 Incident response

In simplest of terms incident response (IR) is directly involved in solving and mitigating a cyber incident and starts from the period before the detection until the final defensive measures have been implemented to prevent the reoccurrence of the incident. In larger organizations and on national level, incident response policies and procedures include the entire incident lifecycle from incident detection until final closure after restoration of the systems into their regular daily state. This approach is not anything that has been developed in the past decade. In 1988 a piece of malware known as Morris worm that was replicating itself impacted 10% of all computers connected to the Internet [84]. The incident led to the understanding that a need for a coordinated response to incidents in cyberspace is needed and the first computer emergency response team CERT-CC was established. IR has since then evolved alongside rapidly changing technology and threat landscape and no longer consists of sharing information in a mailing list as it was done to share knowledge of how to mitigate the spread of Morris worm. IR itself is not in the focus of the thesis but coordination is an important part of IR and the hypothesis that efficient coordination among stakeholders and national level that facilitate the subject matter experts who are the key factors in solving the incident without an SME having the implement expensive security solutions. Even though larger SMEs or ICT focused SMEs have established IR procedures and technical measures must address all internal and external stakeholders as well as establish coordination procedures as no organization alone is impacted by their incident any longer. The building where the SME operates is often rented, the logistics, and maintenance service are purchased from a third-party service provider and their systems lay outside the control of the SME. Even mature SMEs with an established IT-team can encounter incidents they lack knowledge to mitigate and require assistance from national subject matter experts who might have experienced a similar incident when assisting another organization or received information in form of an incident response, how the situation was mitigated. In today's interconnected world it is relevant for the organizations regardless of their size to acknowledge that they are part of a larger interconnected system in which the risk of cascading cyber incidents is two-fold - they can be both the cause of the incident or suffer a consequence of someone else's incident.

4 Literature review

Existing literature with the main focus on coordination between Estonian SMEs and national level is difficult to locate as most literature considering both SMEs and national level is focused on improving IR capabilities or risk assessment. Based on the author's experience from working at CERT-EE, establishing IR procedures, and conducting risk assessment is irrelevant and beyond the capabilities of SMEs [85] [86] [87]. Although there exists a possibility to implement many solutions to increase the resilience through better understanding of threat landscape, the most beneficial solution for the SMEs would be an established coordination procedures or frameworks with the national level.

The author believes that focusing specifically on coordination processes to improve SME cybersecurity resilience is novel approach. A large amount of existing literature is focused on technical aspects or risk assessments that do not consider the surrounding interconnected environment and national situation. RIA has done great work in providing SMEs with necessary guidelines for implementing technical solutions to protect their businesses and clients. At RIA's homepage the very first overall technical guideline is from 2007 but since 2017 the main focus has been on guidelines for enterprises in form of checklists that the enterprises can use as a foundation for setting up the security of their systems and validate their existing security measures.

Although individual recommendations and issues that are dissected during this thesis have been discussed in various publications and reports [56], a proper overview that consolidates them into concrete solutions for SMEs is missing in the author's opinion. Focusing more on the guidelines for enterprises, we can see that mainly technical aspects of cybersecurity have been prioritized, for example a document called "Brief cybersecurity guide for enterprises" [88] [88] consists of very concrete, easy to follow and simple changes or improvement recommendations that can benefit most every enterprise including some organizational and IR recommendations. There is also a document called "10+ recommendation for top managers in ensuring cyber security" [89] [89] which is mostly targeted towards top management in public sector but delivers useful recommendations that can also be adapted for use in private sector.

After publication of “Brief cybersecurity guide for enterprises” RIA launched the “IT-vaatlik” campaign for Estonian enterprises in 2020. This campaign was conducted to fulfil the strategic goals set by Estonian Cybersecurity Strategy 2019-2022 to improve low levels of responsibility and knowledge of cyber threats among public and private sectors [90]. The campaign consisted of a marketing campaign to bring attention to cybersecurity threats that enterprises are facing and additionally provided guidelines in form of cybersecurity measures called CIS Controls [91] that mainly include technical guidelines. CIS controls provide an easy-to-follow checklist and they have been developed by a non-profit organization Center for Internet Security (CIS) so that every enterprise regardless of their size can self-assess which of the offered controls are suitable for their business needs [92]. Since 2015 CERT-EE has also established a social media account to reach a wider audience and is sharing operational information regarding active threat campaigns and guidelines for mitigation [93].

“What is Coordination Theory and How Can It Help Design Cooperative Work Systems” by Thomas W. Malone [94]

Malone states that if there is no interdependence, there is nothing to coordinate. In the case of improving SME cybersecurity through coordination with national level, for example there must exist a prerequisite, a shared resource and simultaneity. These interdependencies translated to the real world could mean many things. But for the sake of an example a prerequisite could describe the need for overall better national cybersecurity and the coordination aspect could mean more focus from the national level to the SMEs. The shared resource could be as simple as a shared pool of knowledge which for the coordination aspect would mean established communication channels and procedures. Simultaneity can mean that both SMEs and national level are working towards a common goal at the same time and the coordination indicates synchronizing their activities to accomplish the goal. This example is solely for the purpose of illustration showing that there can be various methods of coordination, if only necessary interdependences are identified.

For any coordination to take place, necessary components need to be identified. First, we need to identify a goal, a set activities on how to achieve that goal, and then assign actors to carry these activities out. And most importantly manage interdependencies for without it, like already explained no need for coordination exists. Coordination itself consists of

different underlying processes. From the top we have coordination itself, that sets goals, activities, actors, etc. From there group decision making processes can begin, which means proposing alternatives, making choices either by authority or by voting, and conducting evaluation, as necessary. Third process would be communication, this does not only mean who or what are exactly communicating, but also includes agreeing the methods of communications. Finally, a perception of common objects is required, such as information, databases, documents, etc. Common objects can also hinder activities between actors. For example, the SMEs, without understanding what exactly NIS 2.0 entails from them, have challenging time proposing necessary alternatives to certain implementations that might serve the greater good.

An additional, more narrow definition for coordination is offered by the paper "Act of managing interdependencies between activities to achieve a goal." The author of the paper goes on to explain further that although many important coordination efforts involve multiple actors he is convinced that coordination can even be performed by a single actor. It is only required that multiple, interdependent elements of coordination be performed to achieve goals. While this definition will not play a significant role in this thesis, it is still beneficial to understand that the process of coordination can begin from a single actor as this, the author of this thesis believes, gives the opportunity of initiative. Author understands that the reviewed paper's purpose is to develop a theory and not offer any specific solutions. But it does offer great insights into the nature of coordination and what is required for it to be able to take place.

"Public–private partnerships in national cyber-security strategies" by Madeline Carr [95]

This paper by Madeline Carr consolidates many different topics, from coordination, and PPP to regulations with the purpose of analysing how nations are using the private sector to outsource national cybersecurity through PPPs. While this thesis does not focus on national security, SMEs still play a critical role in in ensuring availability of OES and so thereby it is possible to use this paper to gain a more thorough understanding into PPP and the necessary coordination required for improving and developing cybersecurity through PPP coordination and determine possible shortcoming or difficulties.

One of the issues the paper highlights regarding PPPs is the presumption that a partnership immediately means less regulation and oversight by the public sector or that it is possible to shift the responsibility of national cybersecurity to the private sector, to which the SMEs contribute to already. This understanding conflicts with private sector's cost/benefit ratio approach. If left to their own devices, private sector will most likely not recognize enough benefits from full compliance to the regulations enforced by the public sector. This should not been seen as something inherently malicious, rather private sector has stated that in many cases that full compliance is not achieved due to the simple fact that the government's cybersecurity strategy has not been convincingly explained to them and therefor they have not made any additional investments. The paper reinforces this idea with the fact that many national cybersecurity laws highlight the need to cooperate in improving cybersecurity for the "greater good," without realizing that greater good for the private sector is fundamentally different from the greater good to the public sector. For private sector cybersecurity is financial and reputational. The idea of needing to approach private sector in a way is understandable for them is also explored in this thesis.

M.Carr also explores what exactly is PPP. Consolidating various sources, the PPP can be categorized broadly into non-hierarchical arrangements or the opposite where a certain party is in a controlling position. It is argued that true partnership is culmination of both. While PPP is mainly seen as regard to large infrastructure projects, municipal issues, or the health sector, it can also play a significant role in cybersecurity while public sector has continuously stated that the private sectors is liable and responsible for its own cybersecurity and clarified that public sector does not have the authority nor capability to provide cybersecurity services to private sector. This although is clearly more of a controlling partnership and most likely will not achieve the efficiency that either parties wish in the long term. While it is clear that the public sector cannot be a cybersecurity administrator for the private sector both sides need to understand that there is much to gain from collaboration, as achieving desired objectives alone can be difficult. The paper states that this cannot be done in a robust partnership, but we should be thinking about a mutually beneficial relationship. This is an idea that the author of this thesis also subscribes to, as he believes that only through open and two-sided communication both sides can achieve satisfying results.

"Cybersecurity information sharing between public–private sector agencies" by Eric A. Kaijankoski [96]

Paper by E.Kaijankoski explores the reason why information sharing problems exist between government agencies and private companies. This paper takes a more general approach to what could be considered coordination and does not specifically explore the difficulties that SMEs face. The author does hypothesize that SMEs lack resources to participate in information sharing PPPs, but as the author himself states, not enough evidence of the issue is presented throughout the paper to draw underlying conclusions. The paper does highlight that while smaller private companies have received lower membership fees, for example in the Financial Services Information Sharing and Analysis Center (FS-ISAC) it has not improved the actual participation rates as was expected. Author of this thesis believes that this is due to lack of understanding of threats and focus on other business priorities for smaller enterprises who are already limited on available resources.

This paper offers a few use cases for PPP, but the underlying theme is a relationship in which both public and private sector share the risks, resources, and costs in achieving a goal benefitting the public. We have discussed possible shortcoming in such a relationship between private and public previously, it still serves as platform from which to build further efficient variations of PPPs. The paper references sources stating that PPPs have become the preferred solutions for critical infrastructure protection, but solutions on how to improve horizontal cooperation among PPPs is yet to be determined. The author of this thesis believes that horizontal collaboration is extremely important for the issue of improving SMEs cybersecurity and is something that should be tried to avoid from the ground up. To avoid a described situations in the paper, various sector based ISACs have become closed and established communities that are unapproachable to smaller and new enterprises. The paper also highlights that PPPs help increase the efficiency in achieving goals, reduce costs for taxpayers, and improve compliance with regulations. While author of this thesis agrees on these points, he still wishes to emphasize that full compliance to regulations can only be achieved through a PPP that does not try to control the other side or attempt to shift entirety of responsibility and liability. PPP is only efficient as a relationship if both sides understand what the other one wishes and can gain from the relationship and work together to help each other fulfil these goals.

5 Survey

The author conducted an anonymous survey among Estonian SMEs. The purpose of the survey is to establish a baseline understanding of the participants existing cybersecurity and uncover their experiences with coordinating responses to cyber incidents or attacks. While similar surveys have been carried amongst Estonian SMEs previously, their focus has been mostly on the generalized level of cybersecurity [97] and their implemented technical solutions. As there have been similar surveys conducted in other countries [75], the author expected to obtain a more detailed overview for Estonia. Due to exceedingly small number of participants, the survey can be used for observations only and for future research only and cannot be used for drawing conclusion that could describe the situation among majority of Estonian SMEs

The survey was published in the news section of Estonian Chamber of Commerce and Industry webpage, distributed among the members of Estonian Defence League's Cyber Defence Unit, and in several Estonian information security experts' group in social media. Estonian Association of Small and Medium-sized Enterprises was also contacted, but as per their response "they had received too many survey requests already and did not want to overwhelm their members with survey requests" they had to decline the author's request for distributing the survey. In total 13 participants submitted their answers out of which 4 had to be removed from the sample, as 3 were classified as large enterprises and one respondent requested to have the response removed, leaving 9 valid submissions. In the Coordination section, the 9 valid submissions are being described. The survey questions have been listed in the appendix in Estonian. Due to the exceptionally small number of responses, additional interviews were carried out to obtain an expert overview of the situation by interviewing both national level and SME experts who are directly involved with working with SMEs and provide assistance and guidance in case of cyber incidents. Two expert interviews with 2 representatives from SMEs have also been conducted to obtain an overview of the issues SMEs can encounter when suffering a cyber-attack and needing assistance.

5.1 Maturity of SMEs

In total 67% of the participants were medium sized enterprises and 37% employed less than 10 employees. Micro enterprises employ less than 10 people and are included in thesis with small to medium enterprises. The number of employees among the respondents' ranged from 17 to 40. Eight of the nine responders held a leading positions within the enterprise and one respondent did not wish to disclose their position. Four of the respondents were conducting businesses in IT sector, the rest were employed in agriculture, manufacturing, accounting, and counselling sectors.

Due to exceedingly small number of participants, the survey can be used for observations and for future research only and cannot be used for drawing conclusion that could describe the situation among majority of Estonian SMEs. First the cybersecurity maturity of the respondents was determined by investigating which security measures have they implemented in their organization. All 9 respondents had backups from their data. 7 respondents had implemented logging solutions, backup protection, firewall, change management, and updated antivirus solutions that makes them over average secure compared to regular SMEs who have already been better defended from cyber-attacks than 75% of Estonian SMEs who have only implemented antivirus, software updates and backups [98]. 6 respondents have also set up a corporate VPN solution and e-mail filtering and monitoring solution and 5 respondents had set up the minimum rights principle, provided employees with cybersecurity trainings, and had implemented different network security solutions. 4 out of 9 respondents had set up incident response processes at the SME and that is a high percentage even from such small number of respondents as has been highlighted in several reports by RIA that SMEs are experiencing issues setting up their incident response procedures and policies or do not see the necessity to do so. Based on the responses, only one SME had implemented antivirus on gateway level and multifactor authentication in the corporate systems. As the reason behind many cybersecurity incidents has been the lack of multifactor authentication and as the necessity of multifactor authentication has greatly been covered in media it was an unfortunate response among respondents who have more security measures implemented then average SMEs [99].

5.2 Coordination

As previously mentioned, due to the small sample size, this dataset cannot be used to come to any analytical conclusions. The uncovered information should be taken as observations.

The overall readiness to address IT related issues is moderate, as 44% responded that they either have their own IT department or are purchasing IT support from a third party service provider. One respondent stated that they do everything on their own, as it is a one-person enterprise. 55% state that they are addressing IT and cybersecurity issues separately. This is promising, as having functioning IT solutions does not mean having any acceptable level of cybersecurity, quite opposite, it can easily introduce vulnerabilities. Only 1/3 of the respondents answered that their enterprise have workstation guidelines which includes instructions for mitigating cyber threats or have received briefing on that topic. At the same time only one respondent replied that they have not received phishing emails or email containing malware. Considering that 55% of respondents were from outside IT sector and it can be estimated that their overall knowledge of cybersecurity is lower and at the same time having not received any briefing on cybersecurity threats nor having any resources to look up on that matter is concerning. This can nevertheless mean that the participated organizations are overall well educated in the matters of cybersecurity and do not find it necessary to invest resources in basic cybersecurity. It could also mean that they have set their spam filters to maximum defence settings and are using Google or Microsoft based e-mail accounts, that send all suspicious e-mails to spam filter for manual review. Some of the next answers although shine some light to the fact that the situation might not be as positive as it first seemed to be.

Five of the respondents stated that their main concerns for cyber threats are more sophisticated cyber-attacks and cyber threats that can escalate quickly. 4 respondents also outlined the lack of necessary human resource and knowledge. When exploring possible restrictions for the SMEs that prevent improving their cybersecurity level - lack of financial resources and personnel as well other corporate priorities were mentioned. 4 respondents stated that there is no need for improving their cybersecurity level. One respondent shared that their main restriction is that the SME has multiple offices in different countries, and this prevents the harmonization of cybersecurity level throughout the company.

66% of the respondents claimed that they have not experienced a cyber-attack, the rest not knowing if they have experienced one or not. It could be confirmation that the respondents might be knowledgeable enterprises regarding cybersecurity and have been able to avoid any incidents or it can also mean they have not been able to identify one yet. There is also a lot of conflicting information as 66% have taken into consideration that their enterprise could be a target for cybercriminals. They also rate their readiness mainly average, with 8 respondents giving a rating of 3 or more to their enterprises ability to react to a cybersecurity incident (on a scale of 1-5 with 5 being the highest score). Yet only 33% had guidelines or were conducting briefings on the matter of cybersecurity threats. It might be questionable to rate your response capability high in case you have not provided basic cybersecurity training or have established basic cybersecurity guidelines. It has been uncovered that the enterprises and organizations who have not experienced a cyber-attack also do not perceive the threat of a cyberattack as realistic as those who have had negative experiences [100]. When asked whether the enterprise would be able to manage a cyber incident on their own, 55% of the respondents answered that they could manage the incident on their own and 33% were not sure. One respondent clearly stated that they do not have the capability to respond to cyber incidents on their own. When examining the reasons behind need of assistance for solving cybersecurity incidents, the lack of knowledge, designated personnel, and missing processes for incident response were provided as most frequent reasons. 2 of the respondents stated honestly that since they do not have the capability to detect any cyber incidents in the system, they would just be unaware of the ongoing incident before any visible consequences that would hinder their daily operations.

As several of the respondents were employed in IT sector, their professional skillset would give them a possibility to better respond to cyber-attacks to those working in agriculture. Taking into consideration the complexity of all possible cyber-attacks it can be estimated that the respondents from the IT sector would be able to respond to most common cyber-attacks but might need to coordinate their response with national level in case of a large scale cyberattack or previously unencountered attack vector.

Although none of the participants reported having been a victim of a cyber-attack, 3 out of 9 respondents stated that they had to ask for assistance solving a cybersecurity matter. One of the participants did specify the need for coordination and information exchange which does not necessarily mean that the SME suffered a cyberattack but might have

received a suspicious e-mail or discovered a suspicious process and was exchanging information with cybersecurity community or national level to gain insight if this is something known and confirmed malicious, something unknown so far, or regular spam or another default process in the system. In 2 cases the SMEs sought technical assistance and information about the severity of the situation along with further mitigation guidelines.

The survey inquired whether the enterprises have an appointed position that is responsible for cybersecurity matters. Three of the respondents claimed having a designated position and one respondent replied that they have necessary skills within the company, but no separate position has been created. The main tasks of the person responsible for cybersecurity generally include incident handling, information exchange, and in one case also being responsible for network monitoring. In one case it was clearly outlined that the person responsible for cybersecurity must send the information about the incident to CERT-EE immediately and then notify the management over the phone. The SMEs without a designated cybersecurity position brought out the SME's different priorities, no need for a separate position or some other reason that was unfortunately not specified. None of the respondents stated that the absence of the position is in any way connected to financial resources.

The survey also inquired whether the enterprises would be willing to ask help for solving a cybersecurity incident to which 88% replied that they would be willing to request assistance, and only one respondent said that even in the most extreme incidents they would still manage on their own without any external assistance. The respondents were asked to choose all the organizations whom they have heard of that could be of assistance for solving a cyber incident and were given an option to list their own solution. 8 respondents were aware that they could turn to CERT-EE for assistance, 7 knew that they could seek assistance from the Police and Border Guard and 5 respondents said that they would seek assistance from an acquaintance with IT knowledge. 3 respondents stated that they are aware that they could turn to Data Protection Agency for assistance and one respondent stated that they would turn to a private sector consultant in case of a need for assistance. 8 out of 9 respondents said that they could assign a dedicated person who would serve as the main point of contact for incident coordination.

6 Validation

Due to the small number of responses received for the survey and to also validate the results, additional expert interviews were carried out with 2 subject matter experts and 2 SME representatives, who turned to the Author of the work for assistance to solve a cybersecurity matter.

6.1 IT-vaatlik campaign

The details of the survey carried out for IT-vaatlik campaign have not been made public but have been provided by RIA upon request for this thesis. The survey consisted of two focus groups of 16 representatives from Estonian SMEs. The focus groups were split into Estonian and Russian speakers, both groups had to include male and female participants. The group consisted of people in leading positions in the SMEs. Only details relevant to this thesis will be covered.

Both focus groups received identical questions and discussion topics. During cybersecurity concerns discussions, a common concern for both groups was possible reputational damage that can lead to loss of trust and clients and results in termination of business. Examining the opinions of potential causes of the attacks revealed that the most common cause is human factor, more specifically the low awareness on cybersecurity matters. When different cyber threats were introduced CEO and BEC frauds, one of the threats that have found large media coverage and caused great losses, had not reached the participants [29]. Neither of the focus groups reported not having experienced any evident incidents like ransomware, data breach, or denial of service attacks. This also confirms the claim that in case the SME has not experienced a cyberattack, it something that is irrelevant to them and no risk is seen.

When cybersecurity responsibilities within the SME were explored, the most common answer was either the CEO or that every employee is responsible for their own online actions. This is a common stance in many SMEs as they have limited resources and employees have been hired to perform specific tasks needed for the daily operations of the primary business. From one perspective, the management is overall responsible and should create a clear policy and will be held liable for all corporate actions. From another perspective assigning responsibility to employees who have expertise in their specific

field but might be inexperienced computer users without any understanding of online threats can create additional attack surface as the devices and environments are maintained on best knowledge basis. Due to size and workflows of SMEs one single solution cannot be recommended to work in all SMEs. One possible proposal for improving the cybersecurity level are guidelines for cyber risk assessment and creation of coordination plan and minimum level of threat awareness when performing any actions online. Rather than implementing expensive technical solutions that employees have no experience nor will they be trained for it, creating an awareness of where to turn for assistance in case of a cyber-attacks, could be proposed.

When asked about cyber risk mitigation, the resounding answer was that those would be dealt with when the need arises. As the SMEs are occupied with their own daily operations and cybersecurity matters are of secondary priority, it was declared, that the enterprises are rather expecting manuals prepared for them or trustworthy sources they could turn to in an emergency rather than develop the risk assessments and security manuals customized for their own special needs. The participants also highlighted the need for public information sharing from the public sector as would be appropriate for a country that prides itself on being digitally innovative, nevertheless as previously highlighted, many awareness raising campaigns that were aimed at general public had gone without notice for the participants. Multiple participants explained that a change in fundamental thinking is needed, the risks in physical world are understood more easily than the risks in the digital world, even when many physical systems are controlled from the cyber domain. One participant compared the need for occupational safety training with the need for a cybersecurity safety training stating that it would be beneficial for the users themselves to acknowledge the risks and that cybersecurity is a shared responsibility.

As a contrast to the survey conducted for this thesis, none of the IT-vaatlik target group participants mentioned having any knowledge of CERT-EE and only one participant mentioned turning to the police because of a cyber incident. From the results of focus group interviews it can be concluded that the knowledge about existence of organizations like CERT-EE is low and that cyber incidents are commonly also not reported to the police, but the participated SMEs have clearly brought out the need for a public awareness raising campaign or creation of a 24/7 operational hotline that can be contacted in case of a cyber emergency. As such possibility has already been put into work in 2015,

developing a more effective solution, like a national information line 1247, or conducting an awareness raising campaign is easily justified. Not only were the focus group participants unaware of a national support hotline, but also unaware of trustworthy national organizations and institutions where they could seek assistance in case of a cybersecurity matter.

According to RIA's leading analyst Lauri Tankler, who led the "IT-vaatlik" campaign "It is too early to know what long term-effect of the campaign is going to be. But considering that we have also conducted campaigns targeting individual and even the elderly on raising their cybersecurity awareness, we assume and hope that in culmination of these various campaigns in a few years' time we will see positive change in statistics in terms of the individuals and enterprises impacted by cyber-attacks." Although due to COVID-19 many of the planned workshops and seminars targeting SMEs had to be cancelled, Lauri hopes that in 2022 when the focus of the awareness raising campaign is once again on SMEs, they can make up for the missed chances and start seeing the effects of the campaign. CERT-EE has also aimed several awareness raising campaigns on different specific issues, like Wi-Fi security or ransomware prevention and infection [101].

6.2 Expert interview – hosting service

In order to obtain more relevant data on the topic, a subject matter expert on cybersecurity from one of Estonian hosting service providers was interviewed by the author for his professional experience and long-term experience in the field. The interview results confirm the current findings but also introduce surprising new findings when it comes to insurance providers. The interview questions and responses are being published in full below and have been included without the name of the expert.

Question: One of the hypothesis of the thesis is that cybersecurity is still a low priority and a background issue for most small to medium sized Estonian enterprises. What is your experience (if possible please add relevant statistics)?

Answer: Interest in security is minimal – with over 40000 clients we have had ca 10 sign Data Processing Addendum from May 2018 to May 2021 (during entire period GDPR has been in force), mostly clients providing services to larger companies and needing to provide proof of having evaluated their service providers.

Question: What has been you experience regarding Estonian SMEs' knowledge of available national institutions for assisting with their cybersecurity related matters (e.g. CERT-EE, PPA)? Have you had any feedback from the SMEs whether it was easy or difficult finding a point of contact for their cybersecurity problems?

Answer: We have directed clients to report their incidents to CERT / PPA but having not heard back about any success stories we consider that “for statistics only”. We usually suggest they hire an IT-support provider as there is no possibility to “just give a couple of good ideas” if the problem is lack of IT management.

Question: If possible how would you rate SMEs 's awareness of availability of organizations like CERT-EE and PPA C3 to turn to in case of a cyber incident.

Answer: Awareness in the form of “we need to let somebody know” is high, perhaps the most common question after BEC / compromised web is “should we report to police or somewhere?”.

Question: When SMEs turn to you for help, can you describe if they have the necessary resources or know-how to properly assess the issue and receive and implement help in resolving the incident?

Answer: Nope. Most common answers are “we don’t have IT person”, “we do not know who developed our web / don’t have support contract” etc. As most incidents we hear are related to compromised websites the next tier of problems is their web developer (presuming they have one) not having skills to perform cleanup, doing development work on live site (meaning there is no copy or version managed repo of custom components), no experience with log analysis etc.

Question: In your opinion, could that be one of the mains reasons for low levels of cybersecurity or are there other more important aspects. If so like what?

Answer: I think the main problem for most SME is no risk assessment at all. The only solution I see is via state procurement / larger companies starting to require some basic (self)assessment from their (sub)contractors. This would create a “need chain” and put a monetary value to dealing with cybersecurity.

Question: How has Estonian Cybersecurity Act impacted Estonian SME-s cybersecurity?

Answer: Until spring-2021 insurers have done dis-service by offering coverage (incl paying ransom) without need to improve security posture. I do not see any effect of Cybersecurity Act. We could say, that GDPR made some companies think about security, but even that was mostly paper-shield.

Question: Do you believe that cybersecurity law is sufficient going forward or should more focus be on coordination with the national level (abovementioned examples) and if so, in what way?

Answer: Until there is no requirement in public procurement there will be no change. Money talks.

6.3 Interviews - SME representatives

2 representatives from Estonian SMEs agreed to be describe their experience with cyber incidents for this thesis. The answers from both employees will be summarized along with a brief description of the SME.

SME1 works as an accountant for an SME employing 16 people offering consulting services. They do not have a separate person for IT services, their website is maintained by an acquaintance of the CEO, they use an Estonian small service provider for hosting service and get assistance from them in case of any issues with their e-mail server. Every employee has a designated laptop and they do not have a domain account, every employee is also responsible for the wellbeing of their own devices. The company does not use any VPN or multifactor authentication. In August 2020 one of the employees noticed that there is a ransom note, demanding bitcoins to restore access to the data. As something like this had not happened before, there was a lot of confusion on what to do. The accountant described that he saw the note and converted the sum into euros and found it too big of a price to pay and it being cheaper to buy a new laptop. The employee received a new laptop in a matter of hours and was able to continue working. The accountant as the most technologically savvy received the task of finding a solution what to do with the encrypted laptop. He started calling IT people he knew and received different recommendations from restarting the system to restoring from backups, the backups were not present in this case. He was referred to call a friend of an IT friend who has experience in malware infections, who had heard from another IT specialist who was interested in

security matters, that there is a page called NoMoreRansom that has been set up by Europol. He turned to the page and followed the instructions and found himself in a lucky situation where the ransomware in question could successfully be decrypted. It took over a week to reach the page in question thanks to a friend of a friend and as the source of infection could not be determined, it was also not clear which mitigation measures to implement to prevent the incident happening again. When he was asked whether they have now taken any measures to avoid such situations, the response was that this was the first time in 20 years such thing has happened in the SME and unless it happens again, this is a one time problem and does not need any further assistance. When he was informed of the option of turning to CERT-EE for assistance during the interview he said that he has not heard of such team and has not read anything concerning any cyber threats from the media because "this is outside my area of expertise.".

SME2 works at a medium enterprise with around 100 employees, and they offer technical services in Estonia. The employee is responsible for product design and testing but has IT background from previous work. In spring of 2021 they discovered that two domain machines have been encrypted by ransomware. He called an acquaintance whether he has any knowledge of such ransomware and how to behave in this case. With the assistance they managed to restore the machine from a backup copy. He was referred to CERT-EE for further assistance to determine the initial infection vector and for advice on measures to implement to prevent this incident from reoccurring in the future. He also mentioned during this interview that they are now working on establishing procedures for cyber incidents and hope to finish their cyber security manual aimed for all employees by the end of summer.

In both cases it can be observed that the persons involved in solving the cyber incidents called an acquaintance first to receive advice. This was also mentioned as a frequent answer in the survey conducted for this thesis. Although they experienced a similar situation the outcomes and lessons learnt by the two SMEs vary greatly where one has started addressing cybersecurity matters to save the SME from future losses and the other one sees the situation as a one time situation that does not have to be addressed before it happens again.

6.4 Estonian cybersecurity program

Estonian cybersecurity program for 2021-2024 aims to implement Estonian information society development strategy with purpose of making Estonia the most cybersecure digital country. As one of the program goals it has been highlighted that Estonia will be able to effectively deal with cybersecurity issues by relying on the joint capacity of public authorities and on informed and involved private sector [102]. This program also supports one of the outlined problems, that society can no longer defend against cybersecurity threats in an isolated manner. The cybersecurity program highlights seven challenges and risks that Estonia faces regarding national cybersecurity and states that because Estonia is one the most digitally dependent nations in the world various risks involving cybersecurity are therefore that much more critical compared to most other nations [102].

It is important to highlight the seven risks and challenges in the Estonian cybersecurity program, as they are critical to understanding the problems we will be facing moving forward and that the thesis set out to find solutions to from the beginning.

1. The first issue we uncover is that being a small country has provided Estonia with tight-knit expert communities and personal relations [102] but as IT systems and emerging threats are becoming more complex and interconnected, these fragmented groups will not be enough to manage risks posed by systemic cyber risk. To efficiently respond to systemic cyber risk, a coordinated approach is needed and that cannot be done if various smaller groups of experts that are all trying to find their own solutions to their own or to problems of a small groups. A coordinated effort between private and public sector is necessary and for that coordinated effort a more systemic way of approaching systemic cyber risk is needed.

2. Several highlighted risks in the program are focusing more on the public sector. The second issue addresses the lack of unified leadership, as much of the public sector planning has been left to individual institutions and no single strategy or entity to coordinate the entire public sector has been appointed [102]. This thesis would like to extend this issue to Estonian private sector as well. Once a proper authority has been selected with a clear strategy, it could be easier to focus the public sector compared to the private sector. Without a single central entity, both

public and private sector can lose the benefit of efficient situational awareness, information exchange, and defence solutions and measures that can be built with consolidated resources. s.

3. The third issue in the program focuses on the lack of understanding of cybersecurity threats, impact of incidents, possible interconnections, and cross dependencies in infrastructure as been highlighted by the public sector [102] . An insufficient understanding of cyber threats and possible interconnections as well as the impact of systemic cyber risk is not just an issue for the public sector but greatly for the private sector as well. Since ECA came into force in 2018 issues like insufficient understanding of the threat landscape and systemic cyber risk are still current. This backs up the claim that an implementation of the law will not make our society or nation more secure by itself. What is needed, is a more fundamental change in how cybersecurity is perceived by both public and private sector.

4. As another issue, it has been highlighted that a sense of ownership among public and private sector management is lacking when addressing cybersecurity matters. This has led to a situation where cybersecurity is not seen as one of the main concerns for enterprises or organizations and as such, necessary funding to keep up with rapidly changing and complex technologies is missing as a result [102].

5. A major highlighted problem is the limited availability of highly specialized workforce. Both private and public sector are in high need of qualified specialists, and they are not only competing against each other but also cross-border demand for specialists from Estonia [102]. The fundamental issue of competing over a single pool of highly qualified specialists needs a serious approach from the government, as the already small and aging population [103] will not help alleviate the fundamental problem.

Based on available literature which in the case of this thesis are mostly technical documents, whitepapers and governmental publications, the attitude towards unification and coordination of both public and private sector has gained popularity over the last decade. The author of this thesis believes that there is still space to improve in understanding the importance of SMEs in the context systemic cyber risk and by paying

more attention to public sector unification, we should in parallel be thinking about how to involve SMEs more efficiently as they form the largest part of national economy and therefore and also the largest group of users of ICT and are the biggest target group for cybersecurity matters. The Estonian cybersecurity program does highlight the need to understand the rapidly growing interconnection and complexity of IT systems and services better and that is something from where to build future solutions and research on.

7 Improving cybersecurity through coordination

SMEs form 99.8% of all Estonian enterprises and it is not difficult to understand the significance of SMEs based on the given percentage. While the necessity for cybersecurity matters to be addressed by SMEs' is finding wide coverage there are 37% of enterprises who do not have anyone assigned responsible for cybersecurity matters [30]. Another survey even estimates the percentage as high as 60% [104] that is not problematic only because of large amount of SMEs who have not assigned anyone to be responsible for cybersecurity matters but also because the number of cyber-attacks has almost doubled within a year and the cost of cybercrime has gone up to $6 trillion in damages [105] [24].

7.1 Proposals for improvement

Proposals for improving the coordination between SMEs and national level will be presented in this chapter. It cannot be expected that a universal manual can be produced to improve the coordination rather a set of recommendation to be implemented in coordination with national level for reducing cyber risk.

7.1.1 Systemic approach to risk

Systemic approach to risk is defined as acknowledging the complex, interconnected, changing, and unpredictable nature of the environment [106]. R. Barber and M. Burns point out that even though they might believe it, individuals cannot recognize nor understand the risks they are facing and assume that risks can be managed in independent pipelines while ignoring complex relationships between risks [106].

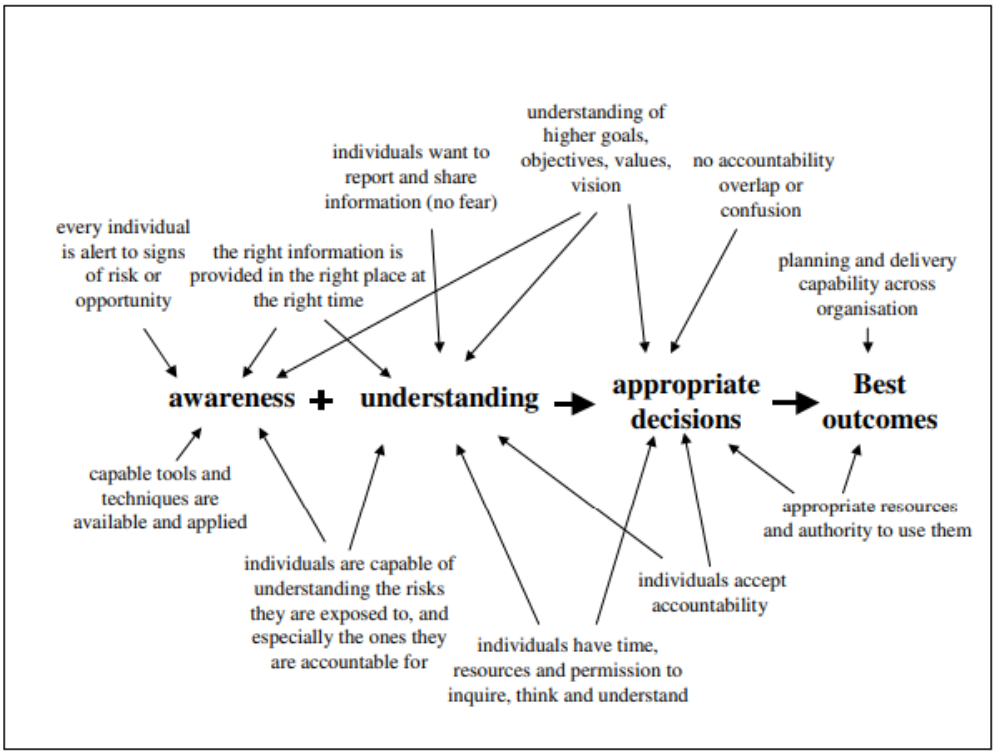

Figure 2 Systemic approach to risk [106]

NIS 2.0 proposal foresees that all subjects to the new directive must conduct risk assessments and implement basic cybersecurity measures. Proposal also assigns focus on addressing cybersecurity risks in supply-chains and supplier relationships [81]. The author of this thesis is glad that the focus is shifting more towards to systemic approach to cyber risk rather than isolated risks in not only national, but also EU level. Nevertheless, a problem of transferring understanding of such necessity to SMEs remains. Lauri Tankler has suggested that "Understandably we cannot approach sectors like agriculture, forestry, or smaller shops like car mechanics, barbers, etc with the same narrative as for example large IT enterprises. We must carefully choose in what manner to approach and which narrative to convey. The most beneficial would be if the input would come from the same sector and from those who have the necessary experience explaining the given sector specific risks and threats. Or as the time goes by, inevitably there will be more examples from which to learn from, even for even SMEs."

An important aspect regarding improving or helping enterprises move into a more systemic approach to cyber risk assessment is cyber insurance. Cyber insurance is not a defensive measure per se, rather it provides necessary resources to recover from a cyber incident. Cyber insurance was introduced in Estonia after WannaCry and NotPetya cyber-

attacks but is not very widely known or purchased [107] [15]. Cyber insurance is more widely purchased in USA since mid-2000s and has achieved an estimated global market size of $4-5 billion by 2020 [108]. In 2016 it was estimated that the cyber insurance market could more than double from $3 billion by 2020 due to GDPR coming to force in 2018 [109] but did not achieve the estimations which somewhat reflects attitude towards regulations and the need for cybersecurity. The Organisation for Economic Co-operation and Development highlights that misunderstanding of insurance coverage and knowledge of potential cyber threats are some of the main reasons behind the slow implementation among policyholders [108]. This opinion is partially applicable to Estonian Cybersecurity strategy 2019-2022 as well, as one of the goals is to mitigate private sector cyber risks by coordinating the communication effort between stakeholders by sharing information and risk assessments [110].

Communication between enterprises and insurance providers for the public sector offering coordination and making sure that the collected and analysed information reaches all interested parties is what makes cyber insurance important regarding having organizations move towards a systemic cyber risk assessment and higher level of cybersecurity. Lauri Tankler stated that “Enterprises will be looking at the benefit-cost ratio and if cyber risk is not measurable, they are also not willing to make the investment on insurance or demand higher level of cybersecurity from their service provider.” This means that cyber risk must become something that has a measurable monetary value for SMEs. Enterprises need to see that if they make these smaller investments in the form of cyber insurance, they can avoid the greater expenses which a cyber incident can cause. While the amount of incident reports that CERT-EE receives from enterprises has grown over time it is still only a small number of all incidents Estonian SMEs are experiencing [29]. According to Tankler Estonian insurance providers still have a better overview than CERT-EE of the enterprises that have suffered cyber incidents and the involved costs. Bringing together insurance providers, Estonian enterprises and the public sector would not only benefit from cooperation but through a coordinated approach to cyber risk, the SMEs can begin to comprehend the risk and threat landscape better, insurance providers can attract new clients, and the public sector can efficiently fulfil the national cybersecurity strategy by bringing together these stakeholders and improve the overall level of national cybersecurity. In a research paper from 20178 one of the leading cybersecurity experts in Estonia, Peeter Marvet stated on the topic of ‘Cybersecurity

awareness on the example of companies offering e-commerce services and belonging to Estonian E-Commerce Association' that "One of the possible ways to approach how smaller enterprises would better acknowledge cyber risk is through cyber insurance. Enterprises could be offered more favourable insurance premiums by having previously raised their cybersecurity level." [111].

Introducing systemic approach to cyber risk throughout enterprises is an extensive undertaking. While the concept is simple – create awareness and understanding, it does require rewiring of how people and therefore enterprises think about cybersecurity and risk. Most likely there does not exist a solution that could improve these fundamental issues, rather small steps over an extended period of time that are focused on the idea that SMEs are not just the subjects of national cybersecurity strategy, but also have a chance to contribute to finding better solutions for the future. This understanding of systemic cyber risk can only come from bilateral trust and cooperation, focusing on making enterprises understand the necessity of systemic approach to risk. It is also relevant to understand that more efficient coordination will not be achieved through enforcing laws, but only through working together where all sides show initiative and effort in finding the best solutions.

7.1.2 National level

NIS 2.0 brings with itself Cybersecurity Competence Centre and Network, which will consist of a Cybersecurity Competence Centre and Network of National Coordination Centres. While the Cybersecurity Competence Centre will allow the EU to implement a longer and more proactive strategy concerning the future and build upon the shared pool of resources so that the EU can move towards a more secure cyber domain in a unified manner. The Nation Coordination Centres will be located in every EU member state and function as a single point of contact on how the resources and competence of the Networks shared pool will be managed within the state itself [112]. While the new EU Cybersecurity Strategy for 2021-2027 poses many meaningful goals, one stands above the rest in the context of this thesis: "Additional measures will include dedicated support to SMEs" [5]. What exactly is meant by this goal or how the SMEs would benefit from this in reality is yet to be discovered, as no public data on specifics of this goal is available at this moment.

Although these are great advancements forward and will grant EU member states a greater variety of tools and assists the EU member states to focus on work toward unified goals, it might still take years to implement. One of the most problematic issues can be a greater involvement of SMEs in taking up the use of the provided tools and fair distribution of available resources. The NIS directive was approved in 2016 [5] and implemented in Estonia in 2018 as Cybersecurity Act and as explored in the thesis, a law itself does not make anything more secure, but a change in fundamental understanding is required. We can expect that there will be improvement after the implementation of Competence Centre and Network but must also acknowledge that in case the SMEs do not acknowledge the existence of systemic cyber risk and how to mitigate it, this will not be an immediate solution to risk reduction.

7.1.3 Improvement of coordination

When asked whether RIA has planned on establishing any additional security measures that would specifically be made available for SMEs Tankler stated that "At this moment RIA has no plans developing sector specific computer security incident response teams or similar entities. The focus will rather be on developing CERT-EE's overall capabilities to be able to respond to cyber incidents." He also added that "In many ways it would not be reasonable for cybersecurity funding for specific private sector initiatives to come from the public sector, as private sector itself is responsible for their own business continuity. In addition, there is also the question of resources regarding the number of SMEs in Estonia and all their specific needs. It would not be feasible for the public sector to have or be an expert in every specific sector and its needs.". In the end Tankler added that "Sector based ISACs that are organized and led by the private sector itself, are a feasible solution.".

Based on available information and expert interview the previously discussed National Coordination Centres which are part of the planned NIS 2.0 directive, are still a concept and a political direction set by the EU cybersecurity strategy for 2021-2027 rather than very concrete goals and methods by which national authorities will be supporting SMEs [5]. It is understandable that private sector is the one that must show initiative and provide the necessary funding if considering developing new collaborative entities like CERTs or ISACs. Based on the analysed surveys and overall situation regarding SME cybersecurity awareness, there is a lot that could be done by the public sector. While global reach, like

for example FI-ISAC (Financial Institutions-ISAC) is important, it is not the first concern for Estonian SMEs when it comes to cybersecurity. The format in which to bring together Estonian SMEs does not have to be in the form of ISAC, it can be a simple workgroup or representation entity with established goals and means of coordination.

No matter the established format, it is important that the entity would not exist in isolation and coordinates with national level to solve the cybersecurity matters of its members. The effort must be collaborative as only through unified and focused coordination and sharing of information the public and private sector evaluate and understand the real depth of cyber risk. For example, CERT-EE has the capacity to understand cyber risks on a technical level and does it by monitoring the Estonian cyber domain 24/7. The insurance providers can provide their statistics of cybersecurity insurance claims of SMEs and the representatives from SMEs can elaborate on that information and bring the matter closer to other SMEs operating in a similar field. This can only take place in case of efficient coordination, that allows us to align actors' intentions, goals, and actions [113] in hopes to combat systemic cyber risk and therefore improve cybersecurity.

8 Findings and discussions

By analysing the cyber threat landscape, it was identified that the threats SMEs are facing are no longer just isolated cyber incidents but risks that without mitigation realized can have serious negative effects on business functions not only for the victim but to all stakeholders. These stakeholders can vary from clients whose PII is now in danger because of a data breach, cooperation partner that will not receive a paid cargo shipment due to the victim being unable to deliver the goods because of a malware infection that has disrupted their systems or a malware that is spreading itself to everyone who is using a specific software – this cascading effect is all a part of systemic cyber risk. These incidents do not only cause costly damages but also hidden costs which can surface years later, when the victim comes to a realization that they have not only suffered significant monetary losses but lost the trust of their stakeholders.

In order to identify to what extent Estonian SMEs are prioritizing cybersecurity matters a survey was conducted for this thesis. For additional references additional interviews were conducted and interviews with a focus group for IT-vaatlik campaign interview was shared. The two data sets were compared with additional similar surveys and research that has previously been carried out. A similar situation can be perceived from the survey and interview results is that when an enterprise has not experienced a cyber incident themselves, they also do not acknowledge the possible risk or impact on their enterprise. Due to no perceivable risk SMEs also do not have any inherent interest in cybersecurity, which can also been seen from their low level of knowledge of current cyberthreats that are impacting Estonian organizations and have also received extensive media coverage.

Cyber risks that enterprises face today are evolving rapidly and becoming too complicated for SMEs to solve on their own considering their limited resources. The author hypothesized that the national level could assist in fulfilling the knowledge cap and offer assistance for the SMEs to solve their cybersecurity concerns by fulfilling the coordination role and offer the help of subject matter experts. Although it is the responsibility of every private sector establishment to ensure their business continuity and profitability, there is inherent interest for national level to ensure that SMEs that form 99.8% of enterprises in the country, are actively acknowledging cyber risks and mitigating them to avoid escalation. This interest is directly tied to the successful

functioning of society and although national security is not a focus of this thesis, many SMEs inherently contribute to it as several SMEs are also operators of essential services and subjects to the ECA.

Although both EU and national level have acknowledged a need for a greater unified focus on cybersecurity and related issues, it is yet to be seen what exact methods will be implemented to assists SMEs in improving their cybersecurity level. There have already been campaigns like "IT-vaatlik" that was focused on raising awareness and introducing potential cybersecurity controls to SMEs after a determining the needs and existing shortcomings of the target audience to launch a more efficient campaign that would also reach the target group in the channels they are observing. The author believes that awareness campaigns like "IT-vaatlik" and information sharing by CERT-EE are not only crucial to improving the cybersecurity level but can only achieve their full potential if the SMEs acknowledge the need of cybersecurity in their daily operations and recognize that it is not only necessary to do so in order to comply with the law.

The author suggests that the cybersecurity level can be improved through more efficient coordination with national level like CERT-EE. In order to determine the factors that are hindering the improvement process, it was first important to identify those factors to start working on possible suggestions. As highlighted by Lauri Tankler having over 130 000 SMEs in Estonia, coordinating all of them is a challenging task and requires more resources than the public sector could provide.

Since 2018 the ECA and the EU NIS directive have done significant work on focusing the attention of member states to improving cybersecurity matters and creating a deeper understanding of cyber risk. Based on the findings in this thesis the author concludes that cybersecurity law has not had a relevant effect on cybersecurity level of Estonian SMEs as the laws set requirements that must be implemented but do not impact the way people whose main task is not ensuring cybersecurity behave.

Based on the findings in this thesis the author suggests that the most crucial aspect for the SMEs to be able to counter systemic cyber risk is to shift into a systemic approach when assessing cyber risk. In its nature systemic approach to risk is simple to understand and implement – take all stakeholders not only your own organization into consideration when conducting risk assessment. The environment is constantly changing and complex, and

no individual or an SME can mitigate or identify every risk alone, it must be a collaborative effort. The author suggests that one of the methods to improve the rooting of systemic approach to cyber risk is through a collaboration of SMEs, insurance providers, and national level. Combining the capabilities of the three stakeholders makes it possible to comprehend a wider overall threat landscape other than the specialized area of expertise and to reach the shared goal of raising the cybersecurity on a national level. As the initiative from SMEs is of high importance in moving forward, the public sector can greatly contribute by providing SMEs the assurance that they can request assistance from national level to coordinate their awareness raising and receive assistance for cyber incidents. One of the suggestions by the author is to form a sector or location based SME representation entities for coordination of cybersecurity efforts.

8.1.1 Future research

This thesis offered potential preliminary solutions on how to improve the cybersecurity level of Estonian SMEs trough coordination with national level. As these have been only preliminary recommendations based on the fundamental issues explored in this thesis, the future research based on this thesis can take different routes and create a more in-depth view into these specific recommendations. The future research can focus on:

1. How to bring together insurance providers, private, and public sector with the purpose of understanding systemic cyber risk better and developing more efficient methods to approach insurance premiums with the purpose of improving SMEs cybersecurity?

2. How can data sharing among insurance providers, public, and private sector be conducted and how cyber incidents can be registered and reported to all impacted parties simultaneously?

3. How will NIS 2.0 affect Estonian SMEs and highlight potential shortcoming and improvements?

4. Investigate systemic cyber risk with the purpose of building a framework or guidelines aiding SMEs to understand and implement systemic cyber risk?

5. How to develop a representation entity for SMEs that would coordinate the unified cybersecurity view of the SMEs with national level and involved stakeholders?

9 Summary

The purpose of this thesis was to discover methods that can help to improve cybersecurity level of Estonian SMEs through more efficient coordination with national level. It was hypothesized that SMEs are not aware nor interested in the cyber risks that they are exposed to in today's digital interconnected world. Being unaware of the risks leads to neglecting cybersecurity as SMEs perceive no threat that would require taking notice of cybersecurity and integrating these questions to their daily operations or making any cybersecurity investments. It was additionally hypothesized that the lack of knowledge is partially caused by inefficient coordination between private and public sector.

To prove the stated hypothesis' the author followed evaluation-based research model and carried out both qualitative and quantitative research. It was important to identify what are the threats that Estonian SMEs are facing and statistically prevalent cyber threats and impacts available from national reports were analysed. By developing a better understanding of the current threat landscape and its potential impacts, it was possible to identify the underlying threat that the SMEs are facing and introduce the concept of systemic cyber risk.

To understand the preparedness of Estonian SMEs in managing cybersecurity related matters better, a survey was conducted among SMEs. Although the number of participants was too low to draw statistically relevant conclusions, a combination with a focus group survey conducted previously by RIA among SMEs and expert interviews were added to obtain more adequate overview of the situation. Overall, these observations confirmed a similar finding to published reports and surveys. In case enterprises have not had negative experiences concerning cyber incidents, they also recognize no reason to invest in cybersecurity or manage cybersecurity matters. Although enterprises might not acknowledge cyber risk, it does not prevent it becoming more complex and cause more damage to more stakeholders due to interconnected systems. This means that SMEs who are already operating on limited resources are facing threats that cannot be mitigated on their own. The complexity and the interconnected nature of systemic cyber risk requires coordinated approach not only to comprehend the risk but to find possible mitigation measures.

It is recommended that SMEs show initiative in the context of improving their cybersecurity level and therefore coordinate with other stakeholders, including public sector, but on the other hand, based on the findings in this thesis, it is apparent that cyber risk is not something SMEs are prioritizing in their daily operations. Due to unawareness of the risks and waiting for the cyber incident that would create a situation where the SME is already forced to seek assistance, the author suggests the public sector to take the first step and introduce to the SMEs the concept of systemic cyber risk. The public sector can raise awareness what impact systemic cyber risk can have to business continuity and how systemic approach to risk could assist enterprises for more efficient preparation and mitigation of cyber risk. It needs to be taken into consideration that in order to carry out such awareness raising campaign more efficiently, it has to be designed together with all stakeholders and representatives from the focus group.

The author also suggests collaboration between insurance providers, public, and private sector to create a better situational awareness and determine the real effects of systemic cyber risk in Estonia and provide better insurance premiums to SMEs based on their existing cybersecurity level. For the last proposal, the author recommends the Estonian SMEs to develop a representation entity for cybersecurity matters that would focus on the needs and requirements of NIS 2.0 and updated ECA and would have the necessary knowledge of SMEs' daily concerns and operations.

References

[1] Deloitte, „Managing Risk in Digital Transformation,“ 2018.

[2] Ministry of the Interior, „The Future of Cybercrime in Light of Technology Developements,“ 2020.

[3] S. Laks, „THREAT LANDSCAPE - C19 RED EDITION,“ 22 October 2020. [Võrgumaterjal]. Available: https://www.first.org/resources/papers/africa-arab-regions2020/Sille-Presentation-materials.pdf.

[4] WIRED, „The Untold Story of NotPetya, the Most Devastating Cybercattack in History,“ 22 August 2018. [Võrgumaterjal]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[5] European Commsion, „New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient,“ 16 December 2020. [Võrgumaterjal]. Available: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391.

[6] Palo Alto, „NIST Highlights Palo Alto Networks Supply Chain Best Practices,“ 26 June 2020. [Võrgumaterjal]. Available: https://blog.paloaltonetworks.com/2020/06/policy-supply-chain-best-practices/.

[7] The Atlantic, „How a Bunch of Hacked DVR Machines Took Down Twitter and Reddit,“ 22 October 2016. [Võrgumaterjal]. Available: https://www.theatlantic.com/technology/archive/2016/10/how-a-bunch-of-hacked-dvr-machines-took-down-twitter-and-reddit/505073/.

[8] „Geenius Meedia OÜ,“ 13 Veebruar 2018. [Võrgumaterjal]. Available: https://digi.geenius.ee/rubriik/uudis/elisa-vea-tottu-ei-saanud-paev-otsa-112-helistada-firma-jattis-sellest-teavitamata/.

[9] Ministry of the Interior, „Elutähtsad teenused,“ 21 December 2020. [Võrgumaterjal]. Available: https://www.siseministeerium.ee/et/eesmark-tegevused/kriisireguleerimine/elutahtsad-teenused.

[10] InformationAge, „Cyber security industry believes GDPR is ‘stifling innovation’,“ 12 July 2017. [Võrgumaterjal]. Available: https://www.information-age.com/cyber-security-industry-believes-gdpr-stifling-innovation-123467262/.

[11] Cybersecurity Ventures, „Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021,“ 10 June 2019. [Võrgumaterjal]. Available: https://cybersecurityventures.com/cybersecurity-market-report/.

[12] Turu-uuringute AS, „Uuring: ettevõtted hindavad oma küberturbe taset liiga optimistlikult,“ 13 January 2021. [Võrgumaterjal]. Available: https://digitark.ee/uuring-ettevotted-hindavad-oma-kuberturbe-taset-liiga-optimistlikult/.

[13] McAfee, „The Hidden Costs of Cybercrime,“ 2020.

[14] Deloitte, „Cyber crime: a clear and present danger. Combating the fastest growing cyber security threat,„ 2010. [Võrgumaterjal]. Available: https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/ZA_RA_CyberCrime_CombatingFastestGrowingCyberSecurityThreat_2015.pdf.

[15] Information System Authority, „Küberturvalisus 2018,“ 2017.

[16] Estonian Information System Authority, „Riigi Infosüsteemi Ameti küberturvalisuse teenistuse 2016. aasta kokkuvõte,“ 2017.

[17] World Economic Forum, „Understanding Systemic Cyber Risk,“ October 2016. [Võrgumaterjal]. Available: http://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf.

[18] C. Williams, „Research Methods,“ *Journal of Business & Economic Research,* kd. 5, nr 3, 2007.

[19] T. W. Malone, „What is coordination theory and how can it help design cooperative work systems?,“ September 1990. [Võrgumaterjal]. Available: https://dl.acm.org/doi/abs/10.1145/99332.99367.

[20] G. Sharkov, „From Cybersecurity to Collaborative Resiliency,“ October 2016. [Võrgumaterjal]. Available: https://dl.acm.org/doi/10.1145/2994475.2994484.

[21] IBM Institute for Business Value, „Cyber and beyond,“ 2016.

[22] S. Morgan, „Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021,“ Cybersecurity Ventures, 26 October 2020. [Võrgumaterjal]. Available: https://cybersecurityventures.com/annual-cybercrime-report-2020/.

[23] Munich Re, „Record hurricane season and major wildfires – The natural disaster figures for 2020,“ 07 January 2021. [Võrgumaterjal]. Available: https://www.munichre.com/en/company/media-relations/media-information-and-corporate-news/media-information/2021/2020-natural-disasters-balance.html#1105489295.

[24] S. Morgan, „Cybercrime To Cost The World $10.5 Trillion Annually By 2025,“ Cybersecurity Ventures, 13 November 2020. [Võrgumaterjal]. Available: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

[25] EAS, „VKE määratlemine,“ 2015. [Võrgumaterjal]. Available: https://www.eas.ee/wp-content/uploads/2015/12/VKE_definitsiooni_selgitus_-_EK_mrus_651-2014_alusel_-_2015.pdf.

[26] Eurostat, „SMALL AND MEDIUM-SIZED ENTERPRISES (SMES),“ [Võrgumaterjal]. Available: https://ec.europa.eu/eurostat/web/structural-business-statistics/small-and-medium-sized-enterprises.

[27] Eurostat, „How many people work in small enterprises?,“ 27 June 2018. [Võrgumaterjal]. Available: https://ec.europa.eu/eurostat/web/products-eurostat-news/-/WDN-20180627-1.

[28] Statistikaamet, „Majandusüksused,“ 2020. [Võrgumaterjal]. Available: https://www.stat.ee/et/avasta-statistikat/valdkonnad/majandus/majandusuksused.

[29] Estonian Information System Authority, „Eesti ettevõtted kaotavad aastas küberrünnakutele üle miljoni euro,“ 11 September 2020. [Võrgumaterjal]. Available: https://www.ria.ee/et/uudised/eesti-ettevotted-kaotavad-aastas-kuberrunnakutele-ule-miljoni-euro.html.

[30] Turu-uuringute AS, „Uuring: ligi 40% ettevõtetes ei tegele küberturbe teemaga otseselt keegi,“ 12 February 2021. [Võrgumaterjal]. Available: https://digitark.ee/uuring-ligi-40-ettevotetes-ei-tegele-kuberturbe-teemaga-otseselt-keegi/.

[31] L. Kaljundi, Digitark, 22 October 2020. [Võrgumaterjal]. Available: https://digitark.ee/kuberrunnakute-arv-on-aastaga-pea-kahekordistunud/.

[32] The Data Protection Inspectorate, „Inspektsioonist,“ 29 June 2022. [Võrgumaterjal]. Available: https://www.aki.ee/et/inspektsioon-kontaktid/inspektsioonist.

[33] e-estonia, „e-identity,“ [Võrgumaterjal]. Available: https://e-estonia.com/solutions/e-identity/mobile-id/.

[34] Information System Authority, „Smart-ID,“ [Võrgumaterjal]. Available: https://www.id.ee/en/article/smart-id/.

[35] Information System Authority, „RIA aprillikuu raport: kurjategijad lõid inimeste teadmata Smart-ID kontod,“ 14 May 2019. [Võrgumaterjal]. Available: https://www.ria.ee/et/uudised/ria-aprillikuu-raport-kurjategijad-loid-inimeste-teadmata-smart-id-kontod.html.

[36] FBI, „Business Email Compromise The $26 Billion Scam,“ 10 September 2019. [Võrgumaterjal]. Available: https://www.ic3.gov/Media/Y2019/PSA190910.

[37] Information System Authority, „Riigi Infosüsteemi Ameti Aastaraamat 2020,“ Information System Authority, 2020.

[38] European Union, „General Data Protection Regulation,“ *Official Journal of the European Union,* 2016.

[39] Information System Authority, „Küberkurjategijad on sihikule võtnud ettevõtted,“ 16 December 2018. [Võrgumaterjal]. Available: https://www.ria.ee/et/uudised/kuberkurjategijad-sihikule-votnud-ettevotted.html.

[40] The United States Department of Justice, „Deputy Attorney General Rod J. Rosenstein Delivers Remarks at the Cambridge Cyber Summit,“ 4 October 2017. [Võrgumaterjal]. Available: https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-cambridge-cyber-summit.

[41] Cybersecurity Ventures, „Ransomware damages rise 15X in 2 years to hit $5 billion in 2017,“ 23 May 2017. [Võrgumaterjal]. Available: https://www.csoonline.com/article/3197582/ransomware-damages-rise-15x-in-2-years-to-hit-5-billion-in-2017.html.

[42] PurpleSec, „2020 Ransomware Statistics, Data, & Trends,“ 2021. [Võrgumaterjal]. Available: https://purplesec.us/resources/cyber-security-statistics/ransomware/.

[43] Information System Authority, „Mullu kasvas Eestis hüppeliselt lunavara levik,“ 19 October 2016. [Võrgumaterjal]. Available: https://www.ria.ee/et/uudised/mullu-kasvas-eestis-huppeliselt-lunavara-levik.html.

[44] vmWare, „Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted,“ 15 April 2020. [Võrgumaterjal]. Available: https://www.carbonblack.com/blog/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/.

[45] S. Laks, „THREAT LANDSCAPE - C19 RED EDITION,“ 22 October 2020. [Võrgumaterjal]. Available: https://www.first.org/resources/papers/africa-arab-regions2020/Sille-Presentation-materials.pdf.

[46] Sophos, „THE STATE OF RANSOMWARE 2020,“ 2020.

[47] Coveware, „Ransomware Payments Up 33% As Maze and Sodinokibi Proliferate in Q1 2020,“ 2020.

[48] Information System Authority, „Lunavararünnakutega kaasneb üha sagedamini,“ 2020.

[49] UNITED STATES SECURITIES AND EXCHANGE COMMISSION, „SOLARWINDS CORPORATION,“ 14 December 2020. [Võrgumaterjal]. Available: https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm.

[50] Eesti Rahvusringhääling, „NATO kontrollib pärast USA-d tabanud küberrünnakut oma süsteeme,“ 19 December 2020. [Võrgumaterjal]. Available: https://www.err.ee/1213720/nato-kontrollib-parast-usa-d-tabanud-kuberrunnakut-oma-susteeme.

[51] CBSNews, „SolarWinds: How Russian spies hacked the Justice, State, Treasury, Energy and Commerce Departments,“ 14 February 2021. [Võrgumaterjal]. Available: https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-02-14/.

[52] Microsoft, „Microsoft Internal Solorigate Investigation – Final Update,“ 2021, 18 February. [Võrgumaterjal]. Available: https://msrc-blog.microsoft.com/2021/02/18/microsoft-internal-solorigate-investigation-final-update/.

[53] Enlyft, „Companies using Microsoft Exchange,“ 2021. [Võrgumaterjal]. Available: https://enlyft.com/tech/products/microsoft-exchange.

[54] Information System Authority, „Petya või… NotPetya,“ 28 June 2017. [Võrgumaterjal]. Available: https://blog.ria.ee/petya-voi-notpetya/.

[55] Postimees, „Ehituse ABC maadleb jätkuvalt küberrünnakuga,“ 3 July 2017. [Võrgumaterjal]. Available: https://majandus24.postimees.ee/4165669/ehituse-abc-maadleb-jatkuvalt-kuberrunnakuga.

[56] World Economic Forum, „Understanding Systemic Cyber Risk,“ October 2016. [Võrgumaterjal]. Available: http://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf.

[57] International Chamber of Commerce, „COVID-19 CYBER SECURITY THREATS TO MSMEs,“ 2020.

[58] Wrike, „What Is the Difference Between Remote Work and Telework?,“ 2021. [Võrgumaterjal]. Available: https://www.wrike.com/remote-work-guide/faq/remote-work-vs-telework/.

[59] IBM Security, „Cost of a Data Breach 2020,“ 2020.

[60] BBC, „Coronavirus: How the world of work may change forever,“ 23 October 2020. [Võrgumaterjal]. Available: https://www.bbc.com/worklife/article/20201023-coronavirus-how-will-the-pandemic-change-the-way-we-work.

[61] MalwareBytes, „Enduring From Home,“ 2020.

[62] Mordor Intelligence, „INTERNET OF THINGS (IOT) MARKET - GROWTH, TRENDS, COVID-19 IMPACT, AND FORECASTS (2021 - 2026),“ 2020. [Võrgumaterjal]. Available: https://www.mordorintelligence.com/industry-reports/internet-of-things-moving-towards-a-smarter-tomorrow-market-industry.

[63] Webtorials, „The Internet of Things isn't coming. It's here.,“ 2016.

[64] IBM Security, „Cost of a Data Breach 2020,“ July 2020. [Võrgumaterjal]. Available: https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf.

[65] Information System Authority, „Emoteti pahavaraga kaasneb ka andmevargus,“ 28 September 2020. [Võrgumaterjal]. Available: https://www.ria.ee/et/uudised/emoteti-pahavaraga-kaasneb-ka-andmevargus.html.

[66] Europol, „WORLD’S MOST DANGEROUS MALWARE EMOTET DISRUPTED THROUGH GLOBAL ACTION,“ 27 January 2021. [Võrgumaterjal]. Available: https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action.

[67] Information System Authority, „Olukord küberruumis – august 2020,“ 18 September 2020. [Võrgumaterjal]. Available: https://www.ria.ee/et/uudised/olukord-kuberruumis-august-2020.html.

[68] Oracle Corporatiion, „ORACLE AND KPMG CLOUD THREAT REPORT,“ 2019.

[69] DLA PIPER, „DLA Piper GDPR fines and data breach survey: January 2021,“ 2021.

[70] Estonian Ministry of Justice, „Justiitsministeerium toob Eesti õiguskorda uue trahviliigi,“ 6 June 2020. [Võrgumaterjal]. Available: https://www.just.ee/et/uudised/justiitsministeerium-toob-eesti-oiguskorda-uue-trahviliigi.

[71] Kantar Emor, „43% Eesti firmadest kardab, et andmeleke võib nende äri oluliselt kahjustada,“ 12 February 2020. [Võrgumaterjal]. Available: https://www.ituudised.ee/uudised/2020/02/12/43-eesti-firmadest-kardab-et-andmeleke-voib-nende-ari-oluliselt-kahjustada.

[72] Endpoint Protector, „A Look at Data Breach Statistics in 2020,“ 11 December 2020. [Võrgumaterjal]. Available: https://www.endpointprotector.com/blog/a-look-at-data-breach-statistics-in-2020/.

[73] National Cyber Security Alliance, „NCSA Survey Summary – Small Business,“ 2019.

[74] Deloitte, „Beneath the surface of a cyberattack,“ 2016.

[75] KPMG, „SMALL BUSINESS REPUTATION & THE CYBER RISK,“ 2015.

[76] DigitalGuardian, „THE COST OF A MALWARE INFECTION? FOR MAERSK, $300 MILLION,“ 7 August 2020. [Võrgumaterjal]. Available: https://digitalguardian.com/blog/cost-malware-infection-maersk-300-million.

[77] „The law of unintended consequences,“ 2020.

[7 Red Goat Cyber Security, „Maersk Incident Response,“ [Võrgumaterjal].
8] Available: https://red-goat.com/cyber-exercise/why-you-should-test-your-incident-response-a-review-of-the-maersk-incident.

[7 Riigiteataja, „Cybersecurity Act,“ 9 May 2018. [Võrgumaterjal]. Available:
9] https://www.riigiteataja.ee/en/eli/523052018003/consolide.

[8 Finnish-Estonian Chamber of Commerce, „Küberturvalisuse seminar,“ 8 October
0] 2019. [Võrgumaterjal]. Available: https://fecc.ee/kuberturvalisuse-seminar/.

[8 European Commision, „Proposal for directive on measures for high common level
1] of cybersecurity across the Union,“ 16 December 2020. [Võrgumaterjal]. Available: https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union.

[8 E. Jones, B. Watson, J. Gardner ja C. Gallois, „Organizational Communication:
2] Challenges for the New Century,“ *Journal of Communication,* 2004.

[8 S. Morrison-Smith ja J. Ruiz, „Challenges and barriers in virtual teams: a literature
3] review,“ 20 May 2020. [Võrgumaterjal]. Available: https://link.springer.com/article/10.1007/s42452-020-2801-5.

[8 The Cornell University, „The Cornell Commission: On Morris and the Worm,“ kd.
4] 32, nr 6, 1989.

[8 ENISA, „Incident Response Plan,“ 2021. [Võrgumaterjal]. Available:
5] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience/bc-plan/incident-response-plan.

[8 KPMG, „10 Common cyber incident response mistakes,“ 2016. [Võrgumaterjal].
6] Available: https://assets.kpmg/content/dam/kpmg/pdf/2016/04/cyber-incident-response.pdf.

[8 UK NCSA, „Incident management,“ 2021. [Võrgumaterjal]. Available:
7] https://www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes#plan.

[8 Estonian Information System Authority, „Ettevõtte küberturvalisuse lühijuhend,“
8] 2019. [Võrgumaterjal]. Available: https://www.ria.ee/sites/default/files/content-editors/kuberturve/lisa_5._ettevotte_kyberturvalisuse_lyhijuhend_eesti_keeles.pdf.

[8 Estonian Information System Authority, „10+ soovitust tippjuhile küberturvalisuse
9] tagamisel,“ 2019. [Võrgumaterjal]. Available: https://www.ria.ee/sites/default/files/content-editors/kuberturve/10_soovitust_tippjuhile_2019.pdf.

[9 Majandus- ja Kommunikatsiooniministeerium, „KÜBERTURVALISUSE
0] STRATEEGIA,“ 2018. [Võrgumaterjal]. Available: https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf.

[9 Estonian Information System Authority, „MIS ON CIS MEETMED?,“ 2020.
1] [Võrgumaterjal]. Available: https://www.itvaatlik.ee/meetmed/.

[9 Center for Inernet Security, „CIS Meetmed,“ 1 April 2019. [Võrgumaterjal].
2] Available: https://www.ria.ee/sites/default/files/content-editors/kuberturve/cis20_meedet_eesti_keeles.pdf.

[9 C. Estonia, „CERT Estonia,“ [Võrgumaterjal]. Available:
3] https://twitter.com/cert_ee.

[9 „What is Coordination Theory and How Can It Help Design Cooperative Work
4] Systems,“ October 1990. [Võrgumaterjal]. Available: https://crowston.syr.edu/sites/crowston.syr.edu/files/10.1.1.92.4445.pdf.

[95] M. Carr, „Public–private partnerships in national cyber-security strategies,“ 2016. [Võrgumaterjal]. Available: https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf.

[96] E. A. Kaijankoski, „Cybersecurity information sharing between public–private sector agencies,“ March 2015. [Võrgumaterjal]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a620766.pdf.

[97] Postimees, „Uuring: enamikul ettevõtetel on tagatud vaid algeline küberturvalisus,“ 12 January 2021. [Võrgumaterjal]. Available: https://majandus.postimees.ee/7153539/uuring-enamikul-ettevotetel-on-tagatud-vaid-algeline-kuberturvalisus.

[98] AS Äripäev, „Uuring: ettevõtted hindavad oma küberturbe taset liiga optimistlikult,“ 25 January 2021. [Võrgumaterjal]. Available: https://www.aripaev.ee/sisuturundus/2021/01/25/uuring-ettevotted-hindavad-oma-kuberturbe-taset-liiga-optimistlikult.

[99] ESET, „Microsoft: 99.9 percent of hacked accounts didn’t use MFA,“ 9 March 2020. [Võrgumaterjal]. Available: https://www.welivesecurity.com/2020/03/09/microsoft-99-percent-hacked-accounts-lacked-mfa/.

[100] Turu-Uuringute AS, „UURING: ÜLE POOLE ETTEVÕTETEST ON AASTA JOOKSUL KOKKU PUUTUNUD KÜBERÜNNAKUTEGA,“ 10 December 2020. [Võrgumaterjal]. Available: https://www.telia.ee/uudised/uuring-ule-poole-ettevotetest-on-aasta-jooksul-kokku-puutunud-kuberunnakutega.

[101] Estonian Information System Authority, „Juhendid,“ 2021. [Võrgumaterjal]. Available: https://www.ria.ee/et/ametist/juhendid.html.

[102] State Information Systems Department, Communications and Undersecretary of State Information Systems, „KÜBERTURVALISUSE PROGRAMM AASTATEKS 2021-2024,“ 2020.

[103] Statistikaamet, „Eesti rahvastikuprognoos 2040: neli positiivset stsenaariumi,“ 6 October 2016. [Võrgumaterjal]. Available: https://www.stat.ee/et/uudised/2015/10/06/eesti-rahvastikuprognoos-2040-neli-positiivset-stsenaariumi.

[104] Keeper Security, „Cyber Mindset Exposed: Keeper Unveils its 2019 SMB Cyberthreat Study,“ 24 July 2019. [Võrgumaterjal]. Available: https://www.keepersecurity.com/blog/2019/07/24/cyber-mindset-exposed-keeper-unveils-its-2019-smb-cyberthreat-study/.

[105] Telia Eesti AS, „Küberrünnakute arv on aastaga pea kahekordistunud,“ 22 October 2020. [Võrgumaterjal]. Available: https://digitark.ee/kuberrunnakute-arv-on-aastaga-pea-kahekordistunud/.

[106] R. Barber ja M. Burns, „A Systems Approach to Risk Management,“ 10 December 2002. [Võrgumaterjal]. Available: http://manex.com.au/wp-content/uploads/2013/08/A-Systems-Approach-to-Risk-Management.pdf.

[107] Geenius Meedia OÜ, „Eestis pakutakse nüüd küberkindlustust, mis näib tänavuste suurte rünnakute järel üha vajalikum,“ 1 August 2017. [Võrgumaterjal]. Available: https://digi.geenius.ee/rubriik/uudis/eestis-pakutakse-nuud-kuberkindlustust-mis-naib-tanavuste-suurte-runnakute-jarel-uha-vajalikum/.

[108] The Organisation for Economic Co-operation and Development, „Encouraging Clarity in Cyber Insurance Coverage,“ 2020.

[109] OECD, „SUPPORTING AN EFFECTIVE CYBER INSURANCE MARKET,“ 2017.

[110] Ministry of Economic Affairs and Communications, „KÜBERTURVALISUSE STRATEEGIA 2019-2022,“ 2019. [Võrgumaterjal]. Available: https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf.

[111] A. Aljas, „Küberturvalisuse teadlikkus e-kaubandusega tegelevate Eesti E-kaubanduse Liitu kuuluvate ettevõtete näitel,“ 2018.

[112] European Commision, „Commission welcomes political agreement on the Cybersecurity Competence Centre and Network,“ 11 December 2020. [Võrgumaterjal]. Available: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2384.

[113] J. J. M. S. P. B. Tarun Chaudhary, „Patchwork of confusion: the cybersecurity coordination problem,“ kd. 4, nr 1, 2018.

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

I Janno Arnek

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Improving Cybersecurity Level of Estonian Small and Medium Sized Enterprises Through Coordination With National Level” supervised by Sille Laks
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

14.05.2021

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 – Survey questionnaire in Estonian

***** Kohustuslik
1. Mis on Teie ettevõtte põhitegevusala? *

2. Milline on Teie positsioon ettevõttes? *

3. Kui palju on Teie ettevõttes töötajaid? *

4. Kas Teie ettevõttes on eraldi IT-juht ja/või IT-osakond või Te ostate teenust sisse?*
Märkige ainult üks vastus.
a) IT-juht
b) IT-juht ja IT-osakond
c) IT-teenus on sisse ostetud
d) IT-teenuse eest vastustav isik puudub ja IT-teenust sisse ei osteta
e) Ma ei tea
f) Muu:

5. Kas Teie ettevõttes eristatakse küberturvalisuse ja IT-teemasid? *
Märkige ainult üks vastus.
a) Jah
b) Ei
c) Kumbki pole oluline
d) Muu:

6. Kas Teie ettevõtte arvutikasutuse juhendis või tööandja poolses juhendamises tööle asumisel on välja toodud tegevused küberrünnete ennetamiseks? *
Märkige ainult üks vastus.
a) Jah
b) Ei
c) Ettevõttes puudub arvutikasutamise juhend ja juhendamist ei tehta
d) Ma ei tea

7. Kas Teie ettevõtte postkastidesse on jõudnud erinevaid õngitsuslinke ja pahavara sisaldavaid kirju? *
Märkige ainult üks vastus.
a) Jah
b) Ei
c) Ma ei tea
d) Ettevõtte töötajatel ei ole e-maile

8. Kas Teie ettevõte on kunagi langenud küberrünnaku ohvriks? Küberrünne on intsident, mille tagajärjel on mõjutatud süsteemide terviklus, käideldavus või konfidentsiaalsus ja/või on Teie ettevõte kannatanud otsest finantskahju *
Märkige ainult üks vastus.
a) Jah
b) Ei *Liikuge küsimuse 13 juurde*
c) Ma ei tea *Liikuge küsimuse 13 juurde*

9. Millise küberrünnaku ohvriks on Teie ettevõte või ettevõtte töötaja/d langenud? *

10. Millal viimati Teie ettevõte langes küberrünnaku ohvriks? *
Märkige ainult üks vastus.

a) 2021
b) 2020
c) 2019
d) 2018
e) 2017
f) 2016
g) Ma ei tea
h) Muu:

11. Mitu korda on Teie ettevõte küberrünnaku ohvriks langenud? *
Märkige ainult üks vastus.

a) 0
b) 1-4
c) 5-9
d) 10-14
e) 15-19
f) >19
g) Ma ei tea
h) Muu:

12. Millised olid küberründega kaasnenud tagajärjed? *
Märkige kõik sobivad.

- Töötaja meililt saadeti õngitsus- ja spämmikirju
- Ettevõtte koduleht näotustati
- Ettevõtte kodulehe kaudu jagati pahavara
- Ettevõtte meiliserveist läksid tundmatud kirjad välja
- Ettevõtte kõik süsteemid olid teenustökkeründe tulemusena kättesaamatud
- Ettevõtte arvuti/d olid lunavaraga krüpteeritud ja neile puudus ligipääs
- Ettevõtte töötaja tegi rahalise ülekande
- Ettevõtte töötaja kasutas ettevõtte finantsvahendeid oma internetikallima toetamiseks
- Ettevõtte ressursse kasutati krüptoraha kaevandamiseks
- Ettevõtte (klientide) andmed olid kolmandatele osapooltele kättesaadavad
- Muu:

13. Kuidas hindate oma ettevõtte võimekust reageerida küberintsidendile? *
Märkige ainult üks vastus.

(väga halb) 1 2 3 4 5 (väga hea)

14. Kas Teie ettevõttel on rakendatud meetmeid kaitsmaks ettevõtet võimalike küberrünnakute eest? *
Märkige ainult üks vastus.

a) Jah *Liikuge küsimuse 16 juurde*
b) Ei *Liikuge küsimuse 17 juurde*
c) Ma ei tea
d) Muu:

15. Kas Teie ettevõttes on olemas küberintsidendi korral käitumise juhend või suunised? *

Märkige ainult üks vastus.

a) Jah
b) Ei
c) Ma ei tea

16. Millised meetmed on Teie ettevõttes rakendatud kaitsmaks ettevõtet küberrünnete eest? *

Liikuge küsimuse 18 juurde

17. Miks ei ole rakendatud meetmeid kaitsmaks võimalike küberrünnakute eest? *

18. Kas arvate, et Teie ettevõte võiks olla sihtmärgiks küberkurjategijatele? *

Märkige ainult üks vastus.

a) Jah
b) Ei

Liikuge küsimuse 19 juurde

19. Kas Teie ettevõttes on keegi, kelle eesmärgiks tegeleda infoturbeintsidentide lahendamisega? *

Märkige ainult üks vastus.

a) Jah *Liikuge küsimuse 20 juurde*
b) Ei *Liikuge küsimuse 21 juurde*
c) Muu:

20. Millised on mõned tema peamised ülesanded? *

Liikuge küsimuse 22 juurde

21. Miks puudub töökoht, mis tegeleb infoturbeintsidentide lahendamisega *

Märkige kõik sobivad.

- Ettevõtte prioriteedid
- Rahalise ressursi puudujääk
- Puudub vajadus
- Teised prioriteedid
- Midagi muud

22. Millised on Teie ettevõtte peamised murekohad seoses küberohtudega? *

Nt - ettevõte ei ole võimeline soetama uut tarkvara ja riistvara? Ei tea millist turvalahendust kasutada? Finantsvahendite kaotuse kartus?

23. Millised piirangud Teie ettevõttes takistavad küberturvalisuse taseme parendamist? *

24. Kas Teie ettevõte on võimeline iseseisvalt küberintsidendi lahendamisega toime tulema? *

Märkige ainult üks vastus.

a) Jah *Liikuge küsimuse 26 juurde*
b) Ei *Liikuge küsimuse 25 juurde*
c) Ma ei tea

d) Muu:

Liikuge küsimuse 26 juurde

25. Miks puudub Teie ettevõttel Teie hinnangul võimekus küberintsidendi lahendamisega iseseisvalt toime tulla? *

Märkige kõik sobivad.

- o Puudub oskusteave
- o Puudub rahaline ressurss
- o Puudub inimressurss
- o Puuduvad protsessid küberintsidendi lahendamiseks
- o Puudub ülevaade võimalikust toimunud küberintsidendist
- o Ei oska öelda, ei ole selle peale mõelnud
- o Muu:

26. Kas oleksite valmis vajadusel küberintsidendi lahendamiseks abi küsima? *

Tõenäoliselt oleks tegemist Teie ettevõtte jaoks aegkriitilise intsidendiga. Märkige ainult üks vastus.

a) Jah *Liikuge küsimuse 28 juurde*

b) Ei *Liikuge küsimuse 27 juurde*

Liikuge küsimuse 28 juurde

27. Miks Te ei oleks valmis küberintsidendi lahendamiseks abi kaasama? *

28. Juhul kui Teil tekib vajadus küberintsidendi lahendamiseks abi kaasata, kas teate kelle poole abi saamiseks pöörduda? *

Märkige ainult üks vastus.

a) Jah *Liikuge küsimuse 29 juurde*

b) Ei *Liikuge küsimuse 30 juurde*

Liikuge küsimuse 30 juurde

29. Märgi kõik asutused, kellelt on Sinu teadmist mööda võimalik küberintsidendi korral abi saamiseks pöörduda. *

Märkige kõik sobivad.

- o Andmekaitse Inspektsioon
- o Politsei ja Piirivalveameti Küberkuritegude Büroo
- o CERT-EE
- o Tallinna Tehnikaülikooli Küberkriminalistika Keskus
- o Ma ei tea, pöördun alati tuttava IT-inimese poole.
- o Pole teadlik antud valikutest
- o Muu:

30. Kui Teile pakutakse abi küberintsidendi lahendamisel, kas Teie ettevõttes oleks, keegi, kes tegeleks ainult antud probleemiga ja oleks ettevõtte poolne intsidendilahenduse kontakt? *

Märkige ainult üks vastus.

a) Jah

b) Ei

c) Muu:

31. Kui olete palunud abi küberintsidendi lahendamisel, kas Teie palvetele on vastatud? *

Märkige ainult üks vastus.

a) Jah *Liikuge küsimuse 33 juurde*
b) Ei *Liikuge küsimuse 32 juurde*
c) Ei ole abi palunud

Liikuge küsimuse 35 juurde

32. Kui oskate, siis palun kirjeldage, miks ei vastatud Teie abipalvele? *
Liikuge küsimuse 35 juurde

33. Kas Te suutsite tänu osutatud abile küberintsidendi lahendada? *
Märkige ainult üks vastus.

a) Jah
b) Ei
c) Muu:

34. Millist abi Teie ettevõttele pakuti? *

Tänan, et leidsite aega küsimustikule vastamiseks!

35. Kas Teil on ettepanekuid või soovitusi parendamaks väike ja keskmise suuruse ettevõtete ning riiklike asutuste/organisatsioonide vahelise küberintsidentide lahendamise koordineerimiseks?