Falch, Morten; Olesen, Henning; Skouby, Knud Erik; Tadayoni, Reza; Williams, Idongesit

Conference Paper

Cybersecurity in SMEs in the Baltic Sea Region

31st European Conference of the International Telecommunications Society (ITS): "Reining in Digital Platforms? Challenging monopolies, promoting competition and developing regulatory regimes", Gothenburg, Sweden, 20th - 21st June 2022

Provided in Cooperation with:

International Telecommunications Society (ITS)

Cybersecurity in SMEs in the Baltic Sea Region

Morten Falch, Henning Olesen, Knud Erik Skouby, Reza Tadayoni, and Idongesit Williams
Dept. of Electronic Systems, Aalborg University Copenhagen

Introduction

In this paper we will explore and characterise the challenges and problems for SMEs in relation to cybersecurity. Firstly, we present an overview of the major cyber threats and attacks and the types of countermeasures that can be applied to prevent and detect cyber-attacks in organisations – with a particular focus on SMEs. Next, we will discuss and analyse what SMEs have been doing so far, based on published surveys and our own research, and how SMEs can prioritize their limited resources to address the challenges from cybersecurity. Finally, we will discuss how various policy initiatives can contribute to enhance cybersecurity in SMEs.

Cybersecurity has become a serious challenge for businesses around the world. Distributed Denial of Service (DDOS), ransomware and other kinds of cyberattacks are happening more and more frequently, and for businesses they can lead to severe consequences, e.g., interruption of work processes and customer services, loss and compromising of data, violation of data protection and privacy laws, a lot of time wasted, and large costs. The ongoing process of digital transformation is affecting all businesses and organisations, large and small, and this puts further focus on the challenges related to cybersecurity.

World Economic Forum has in 2019 recognized cybersecurity to be among the top 10 global risks (Heidt, Gerlach, & Buxmann, 2019). The EU has published a common strategy on cybersecurity (POLICY, 2020), and several major initiatives are being launched by the EU to increase awareness and protect critical infrastructure, e.g., the NIS2 (Network and Information Security 2) Directive (NIS2 Directive, 2020). In Denmark, research performed by PwC shows that business leaders see cybercrime as the most important challenge, more important than the pandemic and the climate change (Danish Business Authority, 2021).

The debate on cybersecurity tends to focus on attacks on large companies and critical infrastructures, but cybersecurity is also important for Small and Medium-sized Enterprises (SMEs). Even though the potential gain for attackers might seem smaller and hardly worth the effort, SMEs cannot neglect the growing threats and feel safe that they will not become the target of an attack. As mentioned above, digital transformation also affects SMEs, even the ones that have not traditionally been involved with the use and development of technology. Contrary to bigger enterprises, SMEs with typically 5-50 employees often lack the competences, resources, and capabilities to deal with cyber threats and protect their assets (Horn, 2017). Depending on the type of SME different measures may need to be applied, and SMEs need a better understanding of the attackers' motives.

Despite its importance, research on cybersecurity in SMEs specifically is still rather limited, as shown in a recent literature review (Tam, Rao, & Hall, 2021).

This paper is based on research carried out as part of the DINNOCAP project funded by the EU (DINNOCAP, u.d.). The objective of the project was to empower the use of ICT opportunities among SMEs, involving industry organizations and public sector authorities in the Baltic Sea Region (BSR).

We will use the following definition for cybersecurity: "*cybersecurity aims at protecting the cyberspace (which includes both information and infrastructures) from any cyber threat or cyber-attack",* following the suggestion of (Lezzi, Lazoi, & Corallo, 2018), who carried out a review of different alternative definitions. Cybersecurity is not just a technical issue, but should be addressed as an interdisciplinary issue, especially when it comes to implementation of security measures. According to (Sarri, Paggio, & Bafoutsou, 2021), recommendations on cybersecurity should address three different aspects, people, processes and technical.

Methodology

The paper is based on a combination of primary and secondary data. All primary and most secondary data are collected as part of the research activities carried out in the DINNOCAP project (DINNOCAP, u.d.) and its predecessor DIGINNO. Both projects are funded by the EU Interreg programme and address digital transformation of SMEs in the Baltic Sea Region (BSR).

Secondary data include a literature review of the kind of possible cybersecurity challenges, surveys on implementation of cybersecurity measures in SMEs, and suggested policy initiatives. We will draw on surveys on cybersecurity & SMEs mainly from ENISA (Sarri, Paggio, & Bafoutsou, 2021) and from the Danish Business Authority that have made several analyses in this area. These data and analyses are examined and compared with data from EUROSTAT and with information and primary data from the BSR countries. Input has been gained from discussions with industry organisations and from a survey done by the DINNOCAP (DINNOCAP, u.d.). The companies, who have participated in the survey are mainly based in Kaliningrad; however, the data and the information obtained support that the cybersecurity challenges to SMEs in the BSR countries are similar to challenges generally faced by SMEs.

Adoption of cybersecurity safeguards in SMEs is mainly about making changes in how organisations implement IT systems. Therefore, business process engineering and change management has been considered as a suitable framework for the analysis.

Cyber threats, guidelines, and countermeasures

ENISA

The European Union Agency for Cybersecurity, ENISA, is *"the Union's agency dedicated to achieving a high common level of* ***cybersecurity across Europe"***, as stated on their website. ENISA has published a number of reports on cybersecurity in SMEs, including *"Guidelines for SMEs on the security of personal data processing"* (ENISA, 2016) and *"Cybersecurity for SMEs - Challenges and Recommendations"* (Sarri, Paggio, & Bafoutsou, 2021).

In their recent report on the threat landscape, they have identified the following prime threats (ENISA threat landscape 2021, 2021):

- Ransomware
- Malware
- Crypto jacking
- E-mail related threats
- Threats against data

- Threats against availability and integrity
- Disinformation – misinformation
- Non-malicious threats

The NIST Cybersecurity Framework

The National Institute of Standards and Technology at the U.S. Department of Commerce (NIST) has developed a framework for what organisations should do in order to be protected (Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018). ISO has developed international standards (ISO 27001 and ISO 27002) based on the same principles. The NIST cybersecurity framework includes five core functions, which must be addressed by any organisation in order to address cybersecurity threats (Fig. 1).

Figure 1. The core functions of the NIST cybersecurity framework.

- **Identify** includes identification of the critical processes and resources. SMEs may not possess a lot of data that could be of interest to others, but if they are critical to the operations of the company they need to be protected. Moreover, GDPR demands that personal data – for instance customer data – must be protected.
- **Protect** includes protection of the sensitive data identified above. Much of the protection is built into the standard software applied by SMEs. Still the SME has an opportunity to implement additional measures such as long passwords and two-factor identification. Moreover, access to any system should only be allowed to those, who actually need it. SMEs do not always have an IT responsible, who make sure that security measures such as regular back-ups and updates are followed. It is therefore up to the individual employee to do this.
  Email filters with blacklisting or even whitelisting can help to avoid phishing and emails with harmful content to be opened, but awareness of employees is even more important in this respect.
- **Detect** includes monitoring of IT-systems in order to detect any cybersecurity events. Anomalies in data flows could be a sign of such an event. Maintenance of logfiles can be an important tool for detection of cybersecurity attacks.
- **Respond** includes guidelines for how to react if a cybersecurity attack is detected, and how to limit damages. This includes damages on the IT-system itself as well as damages on other operations of the company.

- **Recover** includes guidelines reestablishment of damages made by an attack, and reestablishment of data, systems, and business processes.

It follows that the controls to be implemented by SMEs include technical as well as organisational measures. Many SMEs have outsourced the responsibility of managing IT systems, but without an understanding of the importance of cybersecurity, they will not be willing to finance the necessary investments. Moreover, SMEs have less formal organisational structures than large companies, this implies that it is even more important to engage all employees in the organisation in the implementation of cybersecurity safeguards.

Countermeasures

When it comes to the most important ICT security measures to be applied, the Eurostat database includes the following categories:

- ICT security tests
- ICT risk assessment, i.e., periodical assessment of probability and consequences of ICT security incidents
- maintaining log files for analysis after security incidents
- use of VPN (Virtual Private Network extends a private network across a public network to enable secure exchange of data over public network)
- network access control (management of access by devices and users to the enterprise's network)
- data backup to a separate location (including backup to the cloud)
- user identification and authentication via biometric methods implemented by the enterprise
- keeping the software (including operating systems) up to date
- strong password authentication

Published results

ENISA survey

The ENISA survey from 2021 (Sarri, Paggio, & Bafoutsou, 2021) indicates an increasing dependence on IT in SMEs. The most used information services include teleworking, banking transactions, e-mail, and information services, while E-learning and e-commerce are less used. SMEs utilise the cloud for different kinds of information services and remote access tools of "various types, functionalities and security levels". Some of the findings are:

- 25% of the SMEs participating in the survey, who used remote access, have during the pandemic relied on cloud services that allow, as a minimum, access to and processing of e-mails, file processing and communication.
- However, over 90% of these SMEs "did not implement any new security measures, or any additional security measures, to ensure the security of these solutions".
- 80% of the SMEs process critical information, making cybersecurity a key concern.
- 70% of the companies participating in the survey take precautions like installing firewalls and anti-virus programs, making back-ups, and systematic update of software.
- Less than 30% of the companies that make use of removable media management, Information Security Management Systems (ISMS), or Cyber information, have appointed a security officer, have an incident report structure, or have a business continuity and disaster recovery plan.

According to the survey, the most common incidents in SMEs are (Sarri, Paggio, & Bafoutsou, 2021):

- Phishing (41%)
- Web based attack (40%)
- General malware (39%)
- Malicious insider (19%)
- Denial of service (12%)
- Social engineering (11%)
- Compromised/stolen device (7%)

The survey was supplemented with qualitative interviews with 16 SMEs in 14 EU countries, including Germany, Sweden, Estonia and Poland from the Nordic Baltic Region. Based on this, ENISA identifies seven types of challenges:

- low cybersecurity awareness of the personnel,
- inadequate protection of critical and sensitive information,
- lack of budget,
- lack of ICT cybersecurity specialists,
- lack of suitable cybersecurity guidelines specific to SMEs,
- shadow IT, i.e., shift of work in ICT environment out of SME's control,
- low management support.

Moreover, it is stated that 84% of the cyberattacks rely on social engineering.

Survey published by the Danish Business Authority

The Danish Business Authority (Erhvervsstyrelsen) recently published a report on digital security in Danish SMEs, based on 2 major surveys (Danish Business Authority, 2021):

- An annual survey from 2020 by Statistics Denmark, covering 3,947 SMEs with 10-249 employees, and
- A survey conducted by Epinion in the fall 2020 covering 1,806 Danish SMEs with 5-249 employees

The main findings – referring to the security measures mentioned above – were:

- 40% of the Danish SMEs have an insufficient level of digital security in relation to their risk profile.
- Only 76% of the Danish SMEs used both of the 2 essential security measures in 2019: **Keeping the software (including operating systems) up to date** and **doing backup of data**. This was at the same level as in 2018.
- Even among SMEs working with digital technologies (cloud, IoT and big data analysis), 15% do not use any of these 2 security measures.

Regarding the perceived challenges among the SMEs, 28% of the respondents mentioned

- uncertainty whether it pays off to invest (Digital sikkerhed i danske SMV'er (in Danish), 2021)in digital security,
- lack of IT knowledge and competences, and
- lack economic resources.

More than 70% of the SMEs expressed that their focus on digital security would be enhanced by having simple guidelines about IT security, receiving continuous information about current security threats, and having access to concrete tools.

10% of the SMEs had experienced security incidents, and they were mostly worried about potential loss of valuable data, shutdown of networks and systems, and loss of revenue. Finally, 74% of the SMEs answered that the management "to a high degree" was involved in decisions regarding the company's work with digital security.

Figure 2 shows an overview of the use of security measures in Danish SMEs, following the list suggested by ENISA (see above).

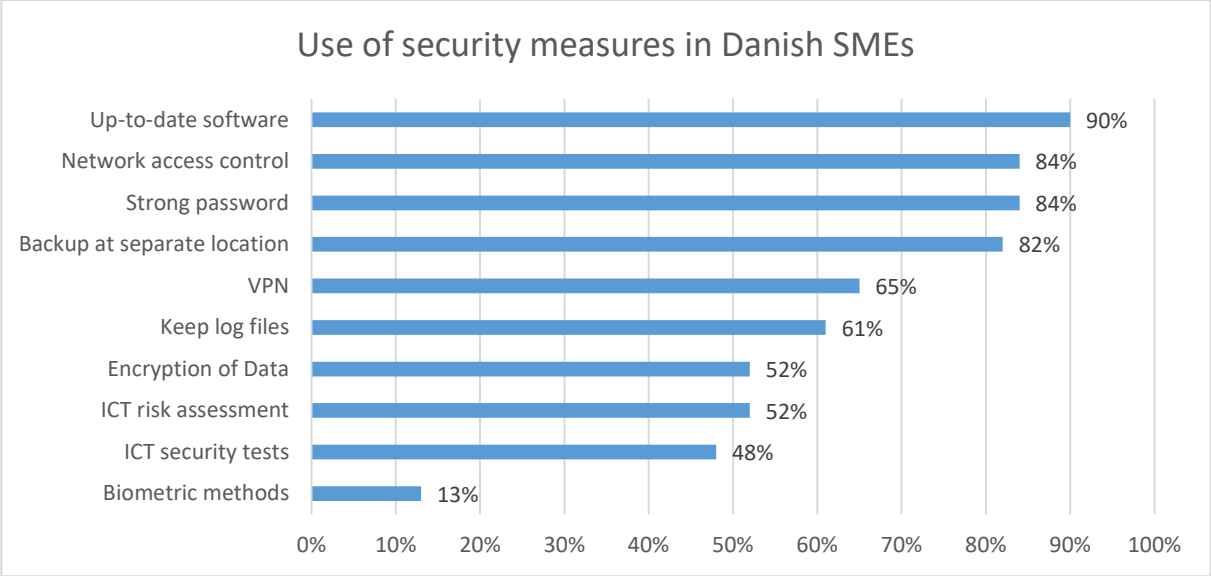

Figure 2. Use of security measures in Danish SMEs. The highest-ranking measures are systematic software updates, access control for networks, strong passwords for authentication, and backup of data. Source: Danish Business Authority.

The DINNOCAP project

This section is based on data from a report produced as part of the DINNOCAP project funded by EU. The objective of the project this project was to empower the use of ICT opportunities among SMEs, involving industry organizations, and Public Sector Authorities in the Baltic Sea Region (BSR).

In a forerunner of the project, DIGINNO, an overview of the level of ICT usage among SMEs in the BSR was obtained, including the state of the art of Industry 4.0 digitalization. Main drivers and barriers in the take-up of ICTs were identified, and it was among others concluded that there has been less take-up of ICT in the 'Eastern' area than in the 'Western' area (i.e., Denmark, Finland, Norway, and Sweden), and that there are some structural differences among the Eastern BSR countries in relation to the ICT take-up. However, for the BSR as a whole, there has during the last years been an increasing take-up due to awareness raising from industry organizations (including facilitation from DINNOCAP) and to the COVID-situation, leading to a growth in online-shopping and remote working. As reported by the OECD[1] and others, the increased take-up is a general development, exemplified in the increased use of online meetings[2]. Exchanges with industry

1 E.g., https://www.oecd.org/coronavirus/policy-responses/teleworking-in-the-covid-19-pandemic-trends-and-prospects-72a416b6/

2 E.g., the number of daily participants in Zoom video conferences were 10 million in December 2019; in April 2020 it was 300 million. IEEE Spectrum, Nov. 2021, p. 34.

associations have confirmed that this also covers the situation in the BSR. This amplifies the cybersecurity risk in SMEs and calls for initiative to protect SME against cyber-attacks.

The activities on cybersecurity within the DINNOCAP project included:

- State of the art based on data from EUROSTAT
- Stakeholder seminar on cybersecurity
- Survey among SMEs in the Baltic Sea region

State of the art (EUROSTAT)

The Eurostat database provides information on 41 different cybersecurity indicators. The indicators are available per country and per company type. At the time of writing (June 2022), most data are available for 2019 only. In the following these indicators are used to uncover the situation for SMEs in the Nordic Baltic region, to identify national differences, and to analyse how the conditions differ from EU as a whole.

The indicator "The enterprise's ICT security policy was defined or most recently reviewed within the last 24 months" can be used for representing the level of seriousness in different companies regarding cybersecurity. Looking at figure 3 it follows that SMEs in general are not as good as other companies to define their own security plans. This may not be surprising. More interesting is it to look at national differences. Here it follows that SMEs in Denmark, Sweden and Finland are much more up to date than companies from the rest of the EU, while companies from Estonia and Poland are below the EU average.

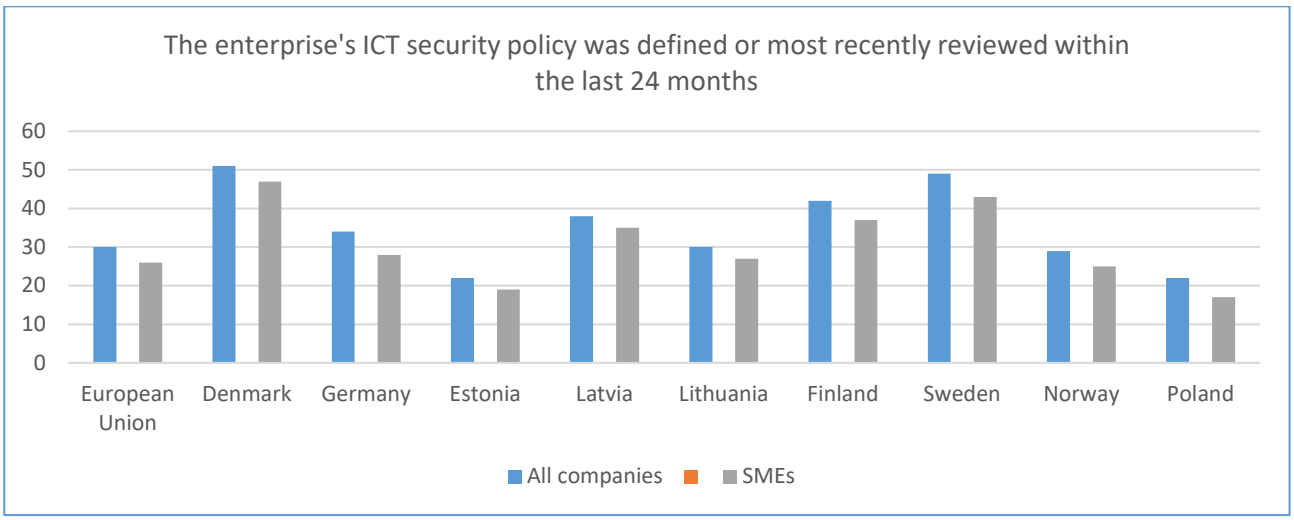

Figure 3. Percentage of enterprises for which the enterprise's ICT security policy was defined or most recently reviewed within the last 24 months. Source: Eurostat.

A comparison shows that the SMEs in the Nordic Baltic countries are close to the EU average (Figure 4). However, within the region there are considerable national differences (see the Table in Appendix A).

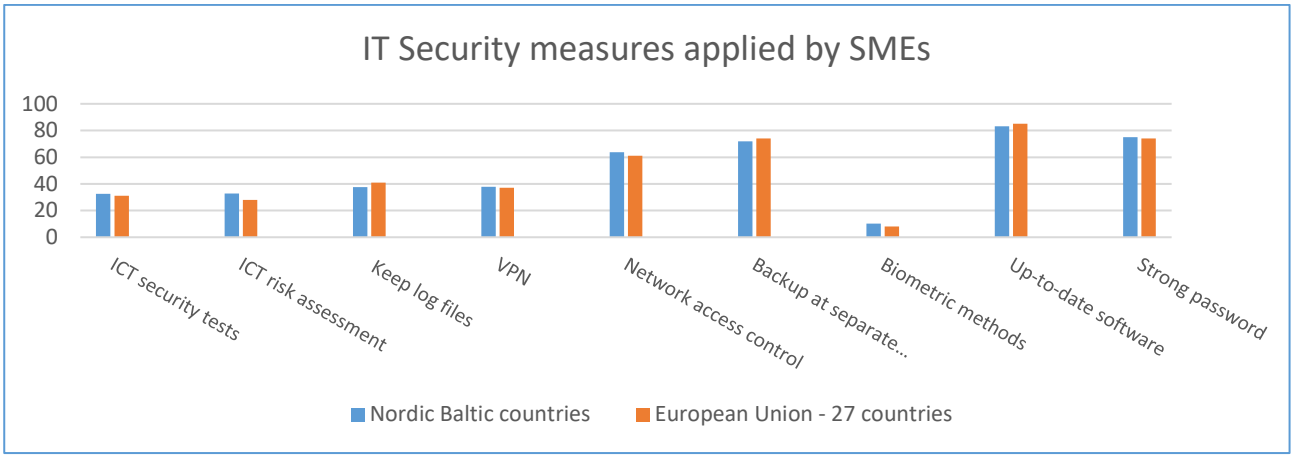

Figure 4. IT Security measures applied by SMEs (2020). Source: Eurostat.

Figure 5 illustrates the percentage of SMEs' access to security expertise, grouped by internally, externally, and in total.

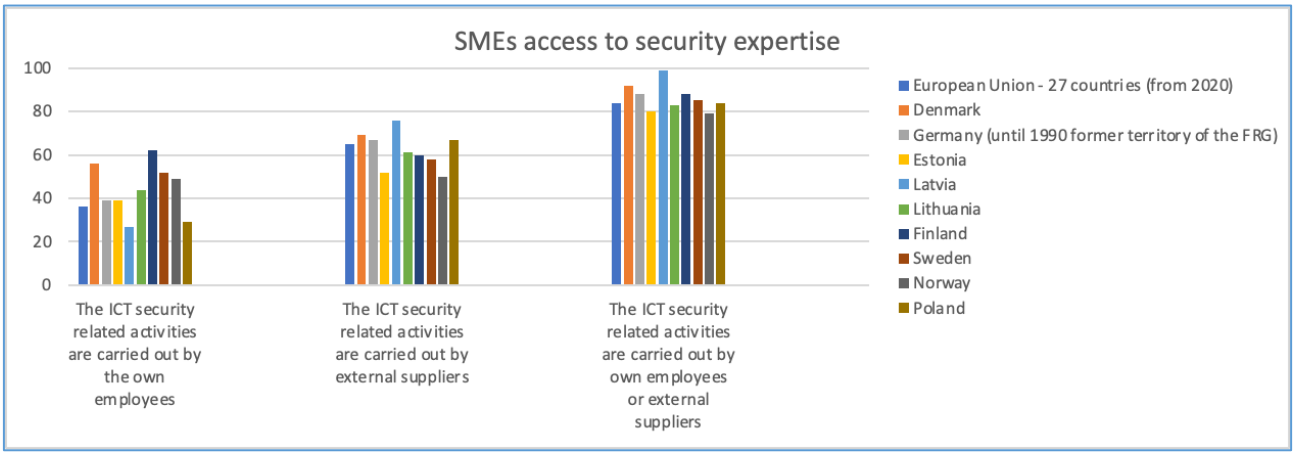

Figure 5. SMEs access to security expertise. Source: Eurostat.

Stakeholder seminar

Within the project this was reflected in an online seminar on 16 Sept. 2021 on 'Cybersecurity and SMEs in a transnational context'. Among the main conclusions of the seminar were that:

- The biggest and most manifest attacks have targeted bigger companies (such as Sony, Google, Maersk …), but it is also a problem for SMEs.
- The guidance and solutions offered by public and international organisations are in reality directed towards – and only useful for – bigger companies.
- The awareness raising on cybersecurity for SMEs by organisations in the BSR has generally been limited so far.

Survey among SMEs in the Baltic Sea region

Based on the outcome from the seminar, a questionnaire was sent to industry organizations participating in the DINNOCAP and distributed to relevant industries in each country. Data from the survey were provided by 33 respondents representing 33 SMEs. The respondents were from Russia (Kaliningrad) (24), Poland (5), Latvia (2), Lithuania (1) and Estonia (1), respectively. The positions held by the respondents were: Director (16), CEO (4), Head of IT (2), Head of technical department (2), managers (2), IT practitioner (3), IT specialist (1), Technical Director (1), Accountant (1), and Business development manager (1). The sectors represented were Education (8), Service (7), Manufacturing and production (7), Information Technology (6), Automotive (1), Shipping (1), Research and development (1), and the Financial sector (1). Although Kaliningrad is highly overrepresented, and Kaliningrad is somewhat behind some of the Baltic countries, the data are considered to be fairly representative for the region.

The breakdown of the number of employees for companies represented in the survey is shown in Fig. 6.

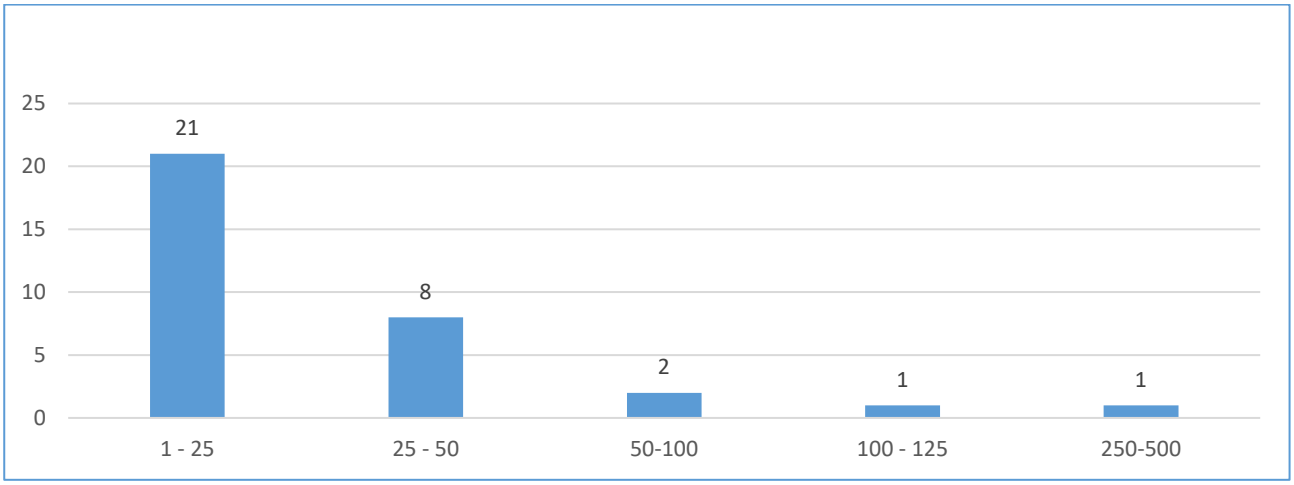

Figure 6. Number of employees in the SMEs, who responded to the DINNOCAP survey.

The trend on how SMEs use security measures in Fig. 7 (DINNOCAP survey) and figure 2 (ENISA survey) are similar, but with minor differences. Although the sample size used for the ENISA survey is larger and it covers more countries, the outcome of the DINNOCAP survey corresponds to the outcome of the ENISA survey.

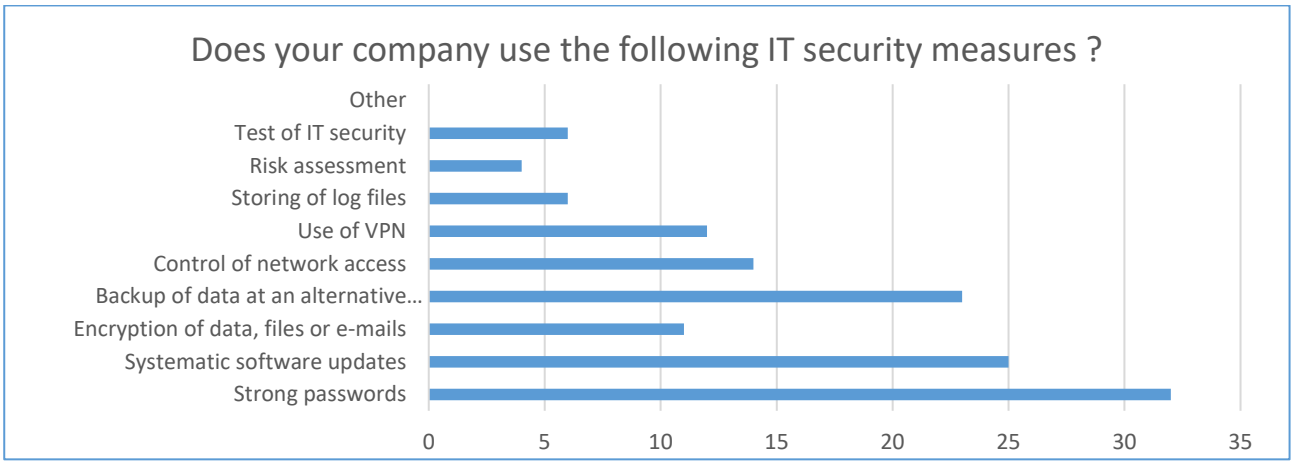

Figure 7. Number of SMEs using different security measures in the DINNOCAP survey.

Analysis

Our goal is to provide recommendations to SMEs that can help them to address the challenges and threats from cybersecurity. How can SMEs and their employees become better informed, and how should they prioritize their efforts, given their limited manpower and capabilities? They need to have a clear picture of how exposed they are to cyber-attacks, what the hackers' motives and incentives are, and what could make their business attractive for cyber-attacks (risk assessment). Based on this understanding, they will be in a better position to target their efforts and countermeasures in the most efficient way. As a part of this they must also decide whether they are able to cope with the challenges themselves, or they need to involve external resources.

In the following we first discuss the hacker types and incentives and how these relate to SMEs. Next, we review the classification of SMEs introduced by the Digital SME Alliance. Here, e.g., it is important for SMEs to understand how dependent they are on parts of their business processes being outsourced. Finally, early theoretical work on Business Process Reengineering (BPR) is reviewed in order to investigate, whether elements of BPR could inform and support the decision on measures to be applied in SMEs. In our context, SMEs are facing a continuously evolving threat of cybersecurity and a constant need for monitoring, risk assessment, and prioritisation of resources.

Hacker types and incentives

If we look at the attackers doing the attacks, it is important to be aware that hackers can have different motivations for hacking into IT-systems, and the harm they are doing differ. The way they are working depend on both motives and competences. A large number of categorizations of hackers have been developed. They define from 3 (black, white, and grey) up to 14 different categories (black, white, grey, script kiddies, green, blue, red, state sponsored, insiders, hacktivists, elite, crypto hackers, gaming hackers, and botnet hackers) (14 Types of Hackers to Watch Out For, 2022).

(Chng, Lu, Kumar, & Yau, 2022) offers the most comprehensive overview of hacker types and motivations applied in the literature. The paper identifies 13 different types of hackers with seven different types of motivations.

Hacker Types	Motivations						
	Curiosity	Financial	Notoriety	Revenge	Recreation	Ideology	Sexual Impulses
Novices	✓	–	✓	–	✓	–	–
Cyberpunks	–	✓	✓	✓	✓	–	–
Insiders	–	✓	–	✓	–	✓	–
Old Guards	✓	–	✓	–	✓	✓	–
Professionals	–	✓	–	✓	–	–	–
Hacktivists	–	–	✓	✓	✓	✓	–
Nation States	–	✓	–	✓	–	✓	–
Students	✓	–	–	–	–	–	–
Petty Thieves	–	✓	–	✓	–	–	–
Digital Pirates	–	✓	–	–	–	–	–
Online Sex Offenders	–	–	–	–	–	–	✓
Crowdsourcers	–	–	✓	✓	✓	✓	–
Crime Facilitators	–	✓	–	–	–	–	–

Table 1 Hacker types and their motivations.

Some hacker types share motivations and can first of all be distinguished by their levels of skills. Here it suffices to make a distinction among following groups and purposes.

(Myrup, 2022) uses a simpler framework and distinguishes between following types of hackers:

1) Insiders (people working inside the organization)
2) Cybercriminals (hackers with financial motives)
3) Script kiddies (hacking for fun, and to impress others)
4) Hacktivists (using their skills for political purposes)
5) Foreign states
6) Gray hats (just for fun hackers)

These six groups vary according to both purposes and skill levels. Looking at the purposes, it is important to distinguish between financial purposes and purposes with financial implications, and those driven by curiosity and recognition. The relation between hacker types and purposes are illustrated in

1) Curiosity and recreation: Include the mere retrieval of information. This may be the innocent motives of students and novices as suggested by (Chng, Lu, Kumar, & Yau, 2022) but information retrieval can also be a motive of foreign states and industrial spies, and it may have financial or political implications even though the IT system itself is not affected.
2) Recognition (correspond to notoriety in table 2): Some hackers do it just for fun and recognition among their peers. They don't hack to do any harm, but just to prove they can. They can be very skilled but will often be so-called script kiddies using hacker tools developed by others. They will not necessarily do any harm to the systems they are attacking.
3) Financial motives: Cybercriminals include highly skilled and well-organized hackers. The market for cybercrime includes hackers as well as crime facilitators developing the tools, which are necessary for performing the hacking. Cybercriminals can either make profit by misuse of for instance financial information or they can lock it-systems and demand a payment for unlocking them again. Also, digital pirates, who want access to information protected by copyright have financial motives.
4) Revenge is not a directly financial motive, although it can have severe financial implications, as may lead to permanent destruction of data and IT systems. Revenge can either be political motivated by foreign states, hacktivists or insiders.

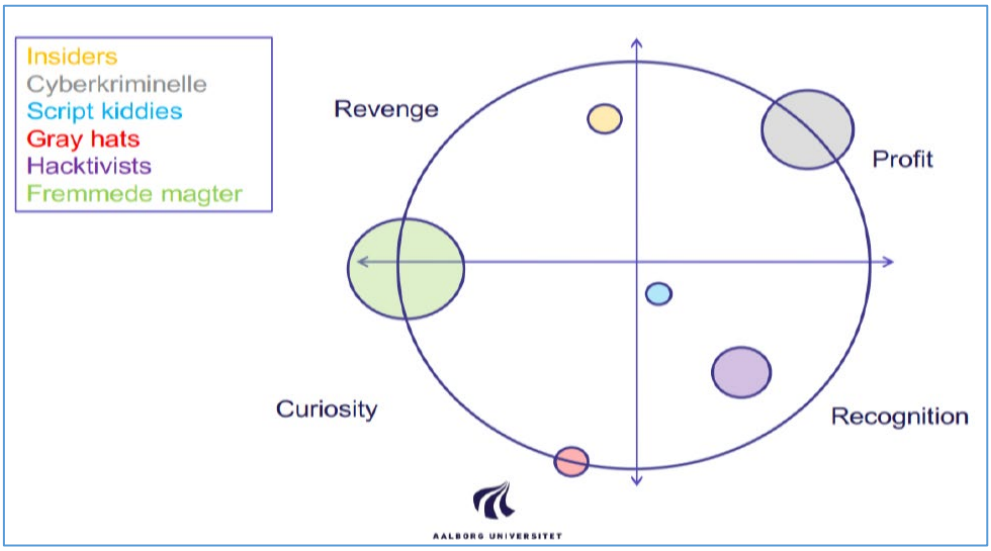

Figure 8. Hacker types and their motivations.

It can be argued that SMEs first of all should take precautions against cybercriminals. Just for fun hackers are less harmful and hacking an SME is not something that will create much recognition among experienced hackers. Few SMEs will be of interest of nation states or political motivated hackers. However, SMEs may suffer from attacks by different types of hackers, as they may be affected even though they are not their primary target. Moreover, their systems may be used as a remedy for attacks on other organisations.

Different types of SMEs

It is necessary to make a distinction between different types and sizes of SMEs and for role in the digital ecosystem in order to make sure that solutions are tailored to them (DIGITAL SME Alliance 2020).

The (DIGITAL SME Alliance 2020) study distinguishes between

- *digital enablers*, providing software and services,
- *'digitally based' SMEs*, which are connected to digital enablers via clusters and value chains, and where the businesses do not have digital or cyber as a core but are highly dependent on digital solutions, and finally,
- *'End user'* or *'digitally dependent' SMEs* that use regular ICT for running their businesses.

Furthermore, the paper indicates that the size and maturity level of the company should be considered; "Micro-enterprises (up to 10 employees) are less likely than larger SMES (10-250 employees) to implement security measures. For smaller SMEs, complexity needs to be reduced as e.g., micro-enterprises are likely to lack the internal resources to deal with complex standards and guidelines' (DIGITAL SME Alliance 2020).

Most SMEs, especially end user SMEs, have either outsourced their ICT activities or rely on standard solutions offered on the market. This implies that their cybersecurity to some extent depends on the security offered by their network and IT providers. Still, the SMEs need to take their own precautions as well.

Some of the conclusions are that *"less digitally mature SMEs are perhaps the most vulnerable to cybersecurity threats of all organizations"* (van Haastrecht, et al., 2021) and that *"A highly specialized 'digital enabler' that provides IT security solutions will be more fit to adopt a complex IT-security standard and should assist 'digitally based' companies in doing so. 'End user' SMES on the other hand may require secure-by-design solutions and a set of basic standards with relevant certifications they can follow to make sure they meet the basic level of cybersecurity 'hygiene'"* (DIGITAL SME Alliance 2020).

Change management in SMEs

Cybersecurity is not only about technology. It is also about people and business processes. This is reflected in the ENISA report, where recommendations to SMEs are given in all of these three areas. This implies that SMEs must implement a complete business process re-engineering (BPR) of all processes involving IT. When BPR was introduced by Davenport (1993), the focus was on altering business processes, organisational structures, and employee responsibilities in order to improve cost, quality, service and speed (Hammer & Champy, 1993). Even though BPR has been on the table for more than three decades, and that digitalisation is implemented in many European companies, the concept is still relevant for many SMEs and its implementation is just as important as it is in large organisations (Aziz, 2019).

Also today, the remedy for BPR is digitalisation. This includes both hardware and software as well as people (Edoun, 2018).Today the objective is however slightly different. For companies, which have been digitalised already, the task is to take up the cybersecurity challenge created by increasing use of technologies like cloud

computing and web-based service solutions. Therefore, performance indicators applied in BPR must be modified in order to take this new challenge into account. Still the concept BPR is relevant in this context as business processes, organisational structures, and employee responsibilities need to be modified in order to meet this new challenge.

There are different options for organising a BPR process: It can be done without having any formal structure, by creating a separate committee or department, or even a separate business unit, or it can be outsourced to a separate operating company (Chaffey, 2011). SMEs have less capacity to address issues such as cybersecurity, and it is likely that it will be addressed either without any formal structure, or that it will be outsourced to a consulting company. However, even if cybersecurity is outsourced, or if it is built into the standard software applied by the SME, it is necessary for the employees to become aware of security issues. "People are a major weakness in cybersecurity, but when engaged and correctly trained they can become a first line defence against attacker" (Ponsard, Grandclaudon, & Bal).

When defining public policies for supporting SME in redesign of their business processes in order to become cybersecure, it is important to be aware of how changes in business processes are made.

Several models have been developed with the purpose of preparing a prescription for how changes or innovations should be implemented in an organisation (Galli, 2018) (Stouten, Rousseau, & De Cremer, 2018). Although most of these focus on large organisations they offer some take-aways for small companies as well.

Lewin's change model includes three phases: unfreeze, change, and re-freeze. There needs to be a motivation before an organisation is ready for a change. The employees are at the heart of the change, as they need to discontinue past practise adapt to new routines. Even if goals are desirable there will often be resistance towards change.

Kotter's model includes 8 steps an organisation must go through in order to make a successful implementation of a change. The model emphasizes on the need for a clear vision, which has to be communicated to the employees, and generation of motivation through creation of short-term wins for the employees. The model represents a top-down approach, which may not be suitable for implementation in small companies. It is however relevant for policy makers in their formulation of initiatives in the area of cybersecurity. Here it will be important to set out clear visions and to communicate and motivate the companies. However, visions are not enough. It follows from the surveys presented above that the awareness of using standard protection measures built into the software is high. This indicate that an unfreeze of present routines is possible, as a sense of urgency of the management in most SME are created. Still, it is necessary that implementation of safeguards protecting against cybersecurity threats must involve all employees in the organisation not just the management and the IT people. The vision must be shared, and employees must be empowered to act on the vision.

Finally, the ADKAR model is worth to mention, as it opposed to the previous focuses on changes in people's behaviour, which is a key for achieving a higher level of cybersecurity. In addition to awareness motivation, which also is included in the previous model, this model also pay attention to the required knowledge and skills among the employees, so they can participate and act as ambassadors for implementation of a change.

Table 2 shows an overview of the 3 models.

Lewin	Kotter	ADKAR
1. Unfreeze 2. Change 3. Re-Freeze	1. Create a sense of urgency 2. Create a core coalition 3. Develop and form a strategic vision 4. Communicate and share vision plans 5. Empowering employees to act on the vision 6. Generate short-term wins 7. Consolidate gains and produce more change 8. Initiate and set new changes	1. Awareness 2. Desire 3. Knowledge 4. Ability 5. Reinforcement

Table 2. Overview of 3 models for change management.

Defining implementation strategies of cybersecurity measures in SMEs must take the limitations of SMEs into account. (Heidt, Gerlach, & Buxmann, 2019) represents one of the few studies, which explicitly dealing with security issues in SMEs. Based on an extensive review of IS literature on the subject, they formulate conceptual framework of SME constraints in relation to IT security. The framework includes a following constraints:

- Limited Resources
- Small Asset Base
- Low Formalization level
- Ingrained culture
- Geographical insularity

These constraints interact with leadership characteristics such as managerial skills, IS/IT knowledge, attitude and values, and strategic outlook. The framework is tested in a qualitative study. Limited resources such as finance, time and know-how were among the most important constraints. The small asset base did not seem to play an important role. Low formalization was also important. This implies that that many processes are undefined and undocumented. This will complicate introduction of new cybersecurity measures. Business relations are often based on a trust-based relationship among employees and business partners. Finally, many SME were constrained by access to IT based expertise – especially if located in rural areas.

Discussion

In the paper titled 'A Threat-Based Cybersecurity Risk Assessment Approach Addressing SME Needs ' (van Haastrecht, et al., 2021) a framework for assessment in combination with means for motivation of SMEs is presented. The approach of the paper is that it is not enough to come with solutions that manages SME's cybersecurity risks but also motivate them to take actions

Recommendations

Awareness and how to raise awareness is addressed in (Ponsard, Grandclaudon, & Bal) (Benz & Chatterjee, 2020). (Benz & Chatterjee, 2020) argue that senior management don't see themselves as likely targets for cyber-attacks. SME IT leaders may be aware of the threat, but they don't have enough information on how to reduce the risk. Therefore, a combination of awareness creation and empowerment is needed.

It follows from the surveys presented above that the awareness of using standard protection tools is generally high among SMEs, while there is less focus on the other parts of the NIST framework.

Based on a review of other reports on cybersecurity in ENISA has prepared a checklist for SMEs in three different areas: People, process, and technology and there are also detailed recommendation in the ENISA report (Sarri, Paggio, & Bafoutsou, 2021). The people related checks involve *responsibility; involvement/ buy-in; awareness; cybersecurity training; cybersecurity policies; third party management*. The process related checks concern *audits; incident planning and response; passwords; software patches; data protection*. The technology checks are *network security; anti-virus; encryption; security monitoring; physical security; secure backups*. Whereas some of the checks simply are generally relevant (e.g., awareness, passwords and backups), other (e.g., third party management and security monitoring) and especially the extent of checks are dependent on the type and size of an SME.

Based on the activities in DIGINNO and DINNOCAP we have suggested activities to be developed in the BSR and most of these are well-suited to be developed as macro-regional activities in collaboration between at least the three Baltic states; but possibly involving support from other countries in the region, e.g., involving the already established digitalization training programmes offered by RISE in Sweden.

Suggested activities are:

- Awareness raising programmes targeting SMEs and based mainly on illustrative examples on problems and solutions. The examples should address difference in sizes and types of SMEs.
- The programmes should be
    - integrated into the activities of European Digital Information Hubs (EDIHs)
    - promoted by sector regulators such as business registers, and
    - promoted by industry associations
- Developments of training programmes resulting in a pool of experts able to assist SMEs in the region
- Development of certified, 'automated' procedures that SMEs can implement for typical/ common activities
- Financial incentives to develop cybersecurity infrastructure in SMEs – e.g., via EU projects
- Incorporate the NIST Cybersecurity Framework into the e-delivery standards developed as building blocks by CEF (Connecting Europe Facility) such as eID[3] and EBSI[4]. When SMEs adopt these building blocks, they can automatically consider and also implement the cybersecurity framework as well.
- Industry associations should adopt tools that enable SMEs to measure and upgrade their cybersecurity readiness
- Industry associations should guide SMEs to understand how to take advantage of the cybersecurity financing and technical possibilities developed by ENISA

The suggestions would imply that eDIHs and industry associations, themselves, possess the cybersecurity competence to assist the SMEs.

3 Electronic Identity

4 European Blockchain Services Infrastructure

Conclusion

From the findings cited above it is quite clear that SMEs are vulnerable to cyber-attacks and that there is a need for upgrading the cybersecurity among SMEs. This is in line with the EU cybersecurity policy[5], under which substantial investments are provided via the Digital Europe programme, the recovery funds, and the Horizon Europe programme. Further, technical support is planned to be provided to SMEs, e.g., via the European Digital Information Hubs.

However, it appears that there is an even greater need for upgrading cybersecurity measures among countries in the Baltic Sea Region compared to the EU countries in general. It appears from our findings that the security activities and awareness generally – even if there are differences between the countries - are at a lower level. Further, it is our conclusion that this situation is a barrier for the digitalization process. In our initial surveys of the digitalization process, cybersecurity was not mentioned as an important issue by companies and organizations. During a workshop and associated interviews in 2021 it was clear that cybersecurity is now seen as a serious problem. This calls for measures in the BSR that are organized and coordinated as macro-regional activities.

5 See, e.g., The EU's Cybersecurity Strategy for the Digital Decade, Joint Communication to The European Parliament and the Council, Brussels 16.12.2020; and https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391.

Bibliography

14 Types of Hackers to Watch Out For. (2022, 5 10). Retrieved from Panda Mediacenter: https://www.pandasecurity.com/en/mediacenter/security/14-types-of-hackers-to-watch-out-for/

Aziz, W. A. (2019, 33(4)). Business process reengineering impact on SMEs operations: evidences from GCC region. *International Journal of Services and Operations Management*, pp. 545-562.

Benz, M., & Chatterjee, D. (2020, 63(4)). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, pp. 531-540.

Better Business Bureau. (2017). 2017 state of cybersecurity among small businesses in North America. *Better Business Bureau*. Retrieved from https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf

Chaffey, D. (2011). *E-business &E-commerce Managemnt.* London: Prentice Hall.

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022, 5, 100167.). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*.

Danish Business Authority. (2021). *Digital sikkerhed u danske SMV'er (Digital Security in Danish SMEs.* Copenhagen: Danish Business Authority.

(2021). *Digital sikkerhed i danske SMV'er (in Danish).* Danish Business Authority.

DIGITAL SME Alliance 2020. (n.d.). . *European Digital SME alliance 2020. The EU cyber security Act and the role of standards for SMEs- Position paper. Technical report.* Brussels.

DINNOCAP. (n.d.). Retrieved from https://www.diginnobsr.eu/dinnocap

Edoun, E. I. (2018). (2018, April). Business Process Reengineering: An Evaluation of Soft versus Hard. In *Proceedings of the 2018 International Conference on Internet and e-Business* (pp. 90-93).

ENISA. (2016). *Guidelines for SMEs on the security of personal data.* ENISA.

(2021). *ENISA threat landscape 2021.* ENISA.

European Union Agency For Network and Information Security (ENISA). (2019). *ENISA threat landscape report 2018: 15 Top Cyber-Threats and Trends.* Heraklion: ENISA.

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (2018, April 16). Retrieved from NIST Cybersecurity Framework: https://www.nist.gov/cyberframework

Galli, B. J. (2018, 46(3). Change management models: A comparative analysis and concerns . *IEEE Engineering Management Review*, pp. 124-132.

GEIGER consortium. (2020). *GEIGER project web site*. Retrieved from https://project.cyber-geiger.eu

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019, 21(6)). Investigating the security divide between SME and large companies: How SME characteristics influence organizational IT security investments. *Information Systems Frontiers*, pp. 1285-1305.

Horn, A. (2017). Why cybersecurity should be a top concern for middle-market companies. *SmallBizDaily*. Retrieved from https://www.smallbizdaily.com/cybersecurity-middle-market-companies/

Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry*, pp. 97-110.

NIS2 Directive. (2020, Dec. 16). Retrieved from EUR-Lex: https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF

POLICY, H. R. (2020). *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: The EU's Cybersecurity Strategy for the Digital Decade.* Brussels: European Commission JOIN(2020) 18 final.

Ponsard, C., Grandclaudon, J., & Bal, S. (n.d.). Survey and Lessons Learned on Raising SME Awareness about Cybersecurity. *ICISSP*, pp. 558-563.

Sarri, A., Paggio, V., & Bafoutsou, G. (2021). *CYBERSECURITY FOR SMES - Challenges and Recommendations.* Heraklion, Greece: European Union Agency for Cybersecurity, ENISA.

Stouten, J., Rousseau, D. M., & De Cremer, D. (2018, 12(2)). Successful organizational change: Integrating the management practice and scholarly literatures . *Academy of Management Annals*, pp. 752-788.

Tam, T., Rao, A., & Hall, J. (2021, 109, 102385.). The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. . *Computers & Security*.

van Haastrecht, M., Sarhan, I., Shojaifar, A., Baumgartner, L., Mallouli, W., & Spruit, M. (2021). A Threat-Based Cybersecurity Risk Assessment Approach Addressing SME Needs. In *The 16th International Conference on Availability, Reliability and Security.*

Wainwright, H., & Kettani, P. (2019). On the Top Threats to Cyber Systems. In *IEEE 2nd International Conference on Information and Computer Technologies (ICICT)* (pp. 175-179).

Appendix A

	ICT security tests	ICT risk assessment	Maintaining log files for analysis after security incidents	Use of VPN	Network access control	Data backup to a separate location	User identification and authentication via biometric methods	Keeping the software up-to-date	Strong password authentication
Denmark	45	44	55	57	83	84	11	86	81
Germany (until 1990 former territory of the FRG)	33	28	55	50	68	88	9	95	83
Estonia	23	18	30	34	54	60	7	68	58
Latvia	28	25	18	21	52	57	10	72	86
Lithuania	24	19	18	21	48	65	14	77	62
Finland	40	56	44	48	74	80	15	93	90
Sweden	47	47	53	50	69	81	9	89	71
Norway	32	39	44	36	69	79	12	90	70
Poland	21	20	22	24	56	53	6	78	73
Nordic Baltic Union	33	33	38	38	64	72	10	83	75
European Union - 27 countries (from 2020)	31	28	41	37	61	74	8	85	74

Table A.1: Security measures applied by SMEs by country in the Nordic Baltic Region (2020). Source: Eurostat.