CYBERSECURITY AND SMES IN THE BALTIC SEA REGION

Knud Erik Skouby, Idongesit Williams, Morten Falch, Henning Olesen

AALBORG UNIVERSITY, COPENHAGEN

Interreg Baltic Sea Region
EUROPEAN UNION
EUROPEAN REGIONAL DEVELOPMENT FUND
DINNOCAP

Cyber security and SMEs in the Baltic Sea Region

Knud Erik Skouby, Idongesit Williams, Morten Falch and Henning Olesen
Aalborg University Copenhagen

The report is produced by the DINNOCAP project. An EU Interreg BSR finances the project.

Table of Contents

The objective of the project DINNOCAP is 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, 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 associations have confirmed that this also covers the situation in the BSR.

Cyber security challenges

With the increased take-up of ICT-based solutions in industry activities generally, discussions on cyber security have developed. It seems obvious that with more ICT-based activity, cyber security must become a bigger concern. Within the project this was reflected in an online seminar on 16 Sept. 2021 on 'Cyber security and SMEs in a transnational context'. Among the main conclusions at the seminar were that

- The biggest and most manifest attacks have been on 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 cyber security for SMEs by organisations in the BSR has generally been limited so far.

In this paper we will explore and characterise the challenges and problems for SMEs in relation to cyber security. We will draw on surveys on cyber security and SMEs mainly from the EU, incl. data extracted from the Eurostat database and from the Danish Business Authority that have made several analyses of this area. These data and analyses are compared with information and data from the BSR countries. Input has been gained from discussions with industry organisations and from a survey done by the project. The survey has mainly resulted in responses from Kaliningrad; however, the data and the information obtained support that the cyber security challenges to SMEs in the BSR countries are similar to challenges generally faced by SMEs.

[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.

Below we characterize these challenges based on the above-mentioned sources. The report concludes with some policy recommendations for macro-regional actions.

ENISA results

ENISA – the EU agency responsible for cyber security within EU – has in 2021 published a survey[3] on cyber security issues in SMEs. The survey 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".

- 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 cyber security 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.

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

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

Data from Eurostat

The Eurostat data provide information on 41 different cyber security indicators. The indicators are available per country and per company type. 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 with

[3] "Cybersecurity for SMEs – Challenges and recommendations", ENISA, June 2021.

regard to cyber security. Looking at figure 1 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.

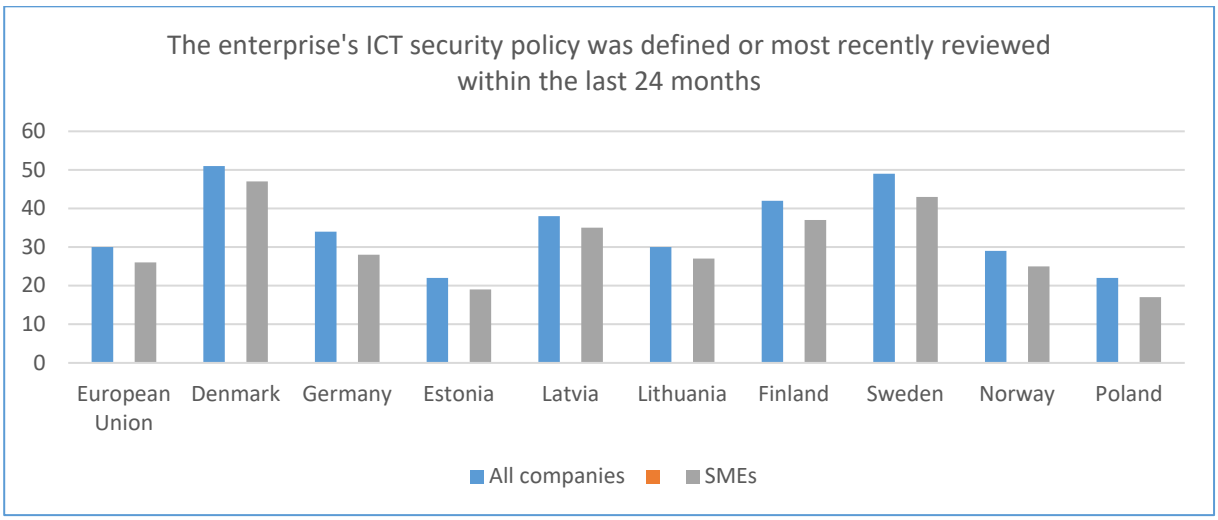

Figure 1. Percentage of enterprises for which the enterprise's ICT security policy was defined or most recently reviewed within the last 24 months. Source: Eurostat.

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

- 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

A comparison shows that the SMEs in the Nordic Baltic countries are close to the EU average (figure 2). However, within the region there are considerable national differences (see the Table in Appendix A).

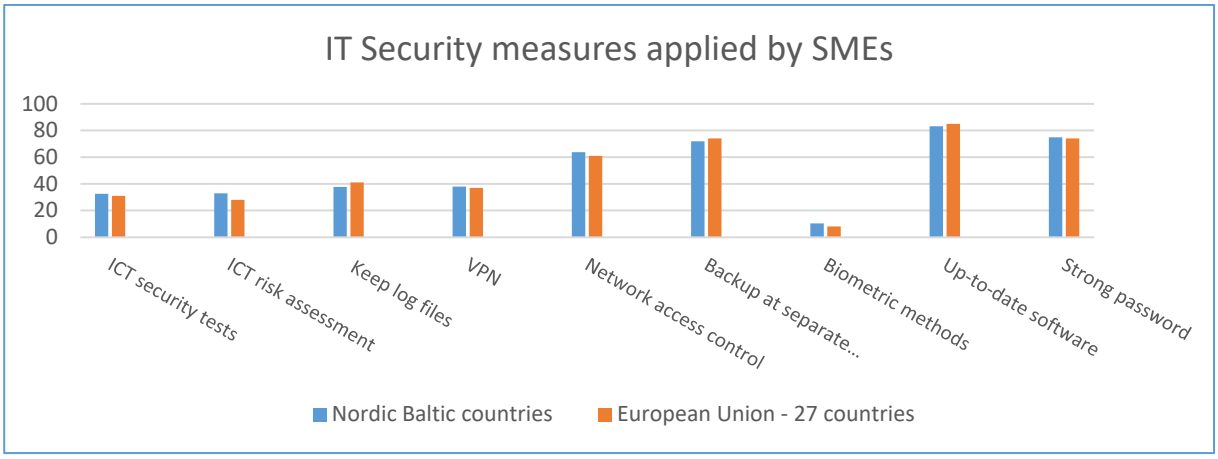

Figure 2. IT Security measures applied by SMEs (2020). Source: Eurostat.

Figure 3 illustrates the percentage of SMEs' access to security expertise, grouped by internally, externally, and in total.

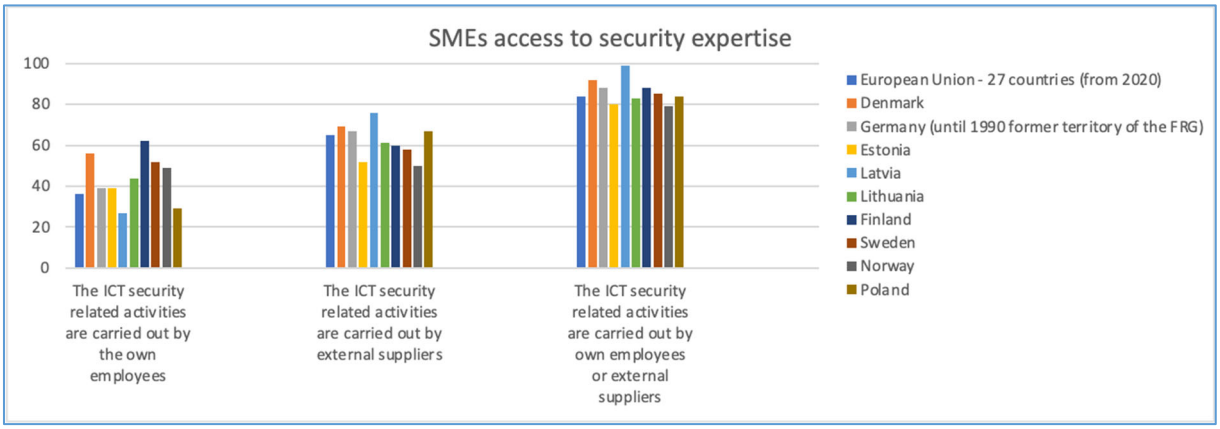

Figure 3. SMEs access to security expertise. Source: Eurostat.

Danish results from 'Digital sikkerhed'

The Danish Business Authority (Erhvervsstyrelsen) recently published a report[4] on digital security in Danish SMEs, based on 2 major surveys:

- 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

[4] "Digital sikkerhed i danske SMV'er", Erhvervsstyrelsen, Sept. 2021 (in Danish).

The main findings were:

- 40% of the Danish SMEs have an insufficient level of digital security in relation to their risk profile.
- 24% of the Danish SMEs did not use 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.

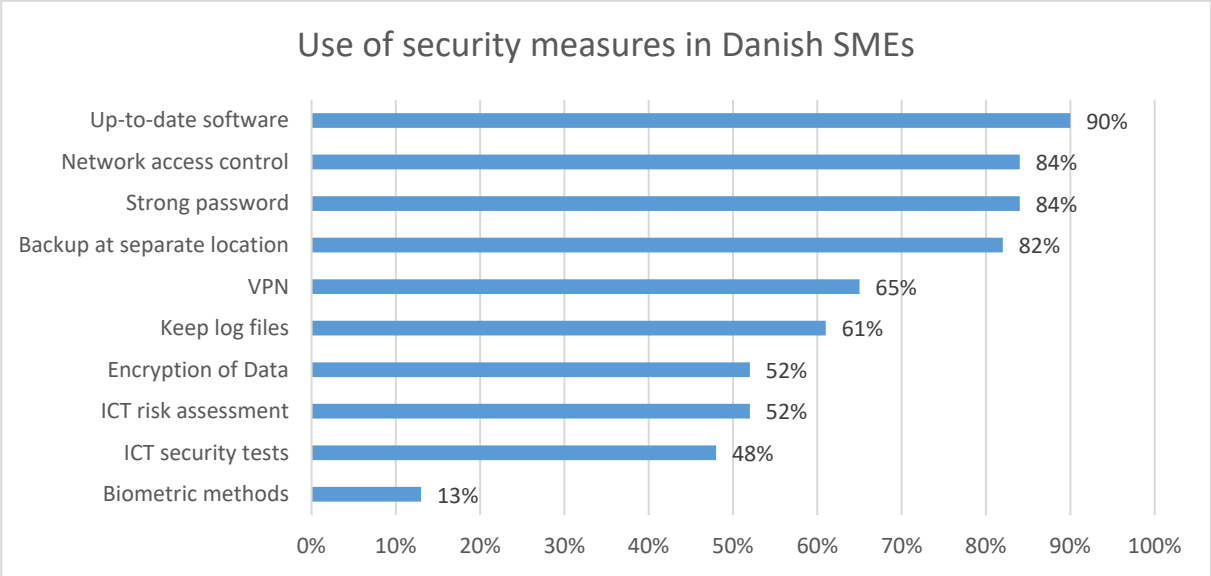

Figure 4. Use of security measures in Danish SMEs. The highest-ranking measures are systematic software updates, access control for networks, strong passwords for authentication, and backup of data. Source: Danish Business Authority.

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

- uncertainty whether it pays off to invest 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.

Results from the DINNOCAP survey

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 (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).

The breakdown on the number of employees in each company represented in the survey is presented figure 5.

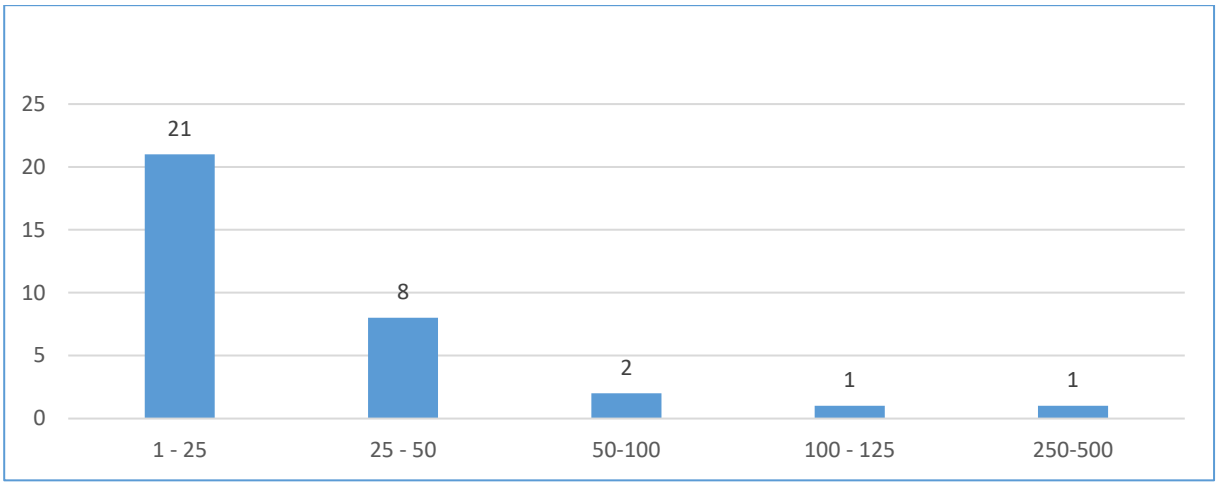

Figure 5. Number of employees in the SMEs, who responded to the DINNOCAP survey.

The trend on how SMEs use security measures in figure 6 (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.

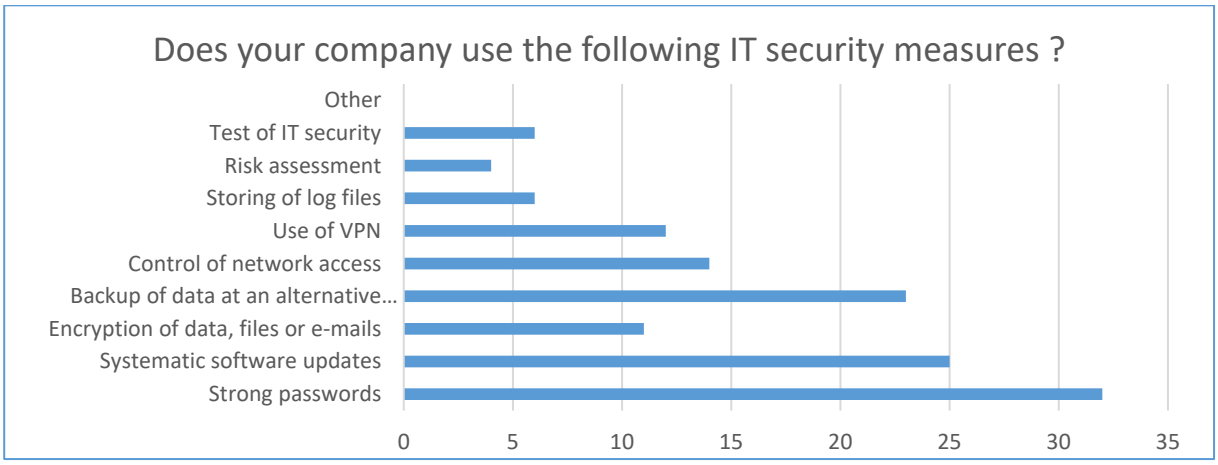

Figure 6. Number of SMEs using different security measures in the DINNOCAP survey.

Policy recommendations

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 (EDIH).

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. This calls for measures in the BSR that are organized and coordinated as macro-regional activities.

Suggested activities are:

- Awareness raising programmes targeting SMEs and based mainly on illustrative examples on problems and solutions
- The programmes should be
    - integrated into the activities of 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 cyber security 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, EBSI, CEF. When SMEs adopt these building blocks, they can automatically consider and also implement the cyber security 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 cyber security competence to assist the SMEs.

[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.

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.