Research Project - Investigation of Cybersecurity Challenges in Danish SMEs

Camilla Nadja Fleron {cafl@itu.dk}
Jonas Kofod Jørgensen {jkoj@itu.dk}
Supervisor: Oksana Kulyk {okku@itu.dk}

May 14, 2020

Course code: KIREPRO1PE

Abstract

Denmark is one of the most digitised countries in Europe. However, according to recent reports IT security in Danish companies has not followed along. This circumstance may be due to the many challenges associated with implementing IT security. We conducted interviews with four employees from four different organisations, asking about their companies IT security and what tool they need to become better protected. Our results show that the state of IT security in Danish small and medium-sized businesses (SMEs) is inadequate. The companies are lacking fundamental cyber protection. The participants indicated a need for basic security help and awareness of cyber threats in their organisations. These findings align with the report from Monitor Deloitte (2018), which claims that about two out of three SMEs have an IT security level inadequate to their risk profile [1]. Based on our findings and with the inspiration of the latest reports and international accepted security standards, we suggest a simple framework. The framework is meant as an option for SMEs that search for simplistic and straightforward IT security guidance.

1 Introduction and motivation

Over the past 20 years the risk of cyberattacks has increased significantly. This is not least due to the rise of internet usage as a means of doing business and gaining access to large amounts of data [2]. Lost, destroyed, stolen or unavailable information, may hurt the reputation of the company and the trust of its customers. Society and businesses are therefore facing considerable risks as more and more data is being digitised and thus dependence of IT systems has increased. Awareness of this increase in danger, as well as the primary management steps, are essential to becoming better protected. Lots of available help exist, but it may be difficult to navigate within the security field.

According to the European Commission's Digital Economy and Society Index (DESI) of 2019 [3], Denmark, Sweden, Finland, and the Netherlands are the most digitised countries in Europe. However, IT security in Danish companies has not followed the high digitisation degree. Monitor Deloitte (2018) has conducted an in-depth study of the IT security level in Danish Small and Medium-sized Enterprises (SME)[1] [1]. The report shows that 22% of Danish SMEs do not have basic IT security implemented, which includes: firewall protection, antivirus, backup of data and access control. The research also shows that 39% of SMEs have an IT security level that is considered inadequate to their risk profile [1].

A company's appropriate level of IT security depends on the individual situation. One cannot speak of a fixed standard of IT security measures that fit every business. Companies vary in both size, resources, business models, and the use of data and technology. Therefore, when assessing whether a company has sufficient IT security, one should look at the risk profile of the company and based on that assessment, decide what measures the company should aim for [5].

Monitor Deloitte (2018), claims that 70% of Danish SMEs have outsourced all or part of their IT security [1]. The reasons for IT outsourcing may be that the companies do not have the necessary competences in the field to be able to establish and operate the required security measures on their own hand. It can also be a resource issue where the time spent on implementing it on the their own may be more costly than having it outsourced to a supplier [1].

Focusing on risk profiles may be helpful, but perhaps the problem of low security level of Danish SMEs is based on something else. Investigation on what SMEs need to do in order become more secure could provide crucial information for businesses and society.

Research Question

For this paper we conducted interviews to gain knowledge about the current state of cybersecurity in Danish SMEs. We did this by analysing the findings and studying recent security papers with the aim of getting an understanding of

[1] SMEs is businesses having 1-249 employees or a turnover up to 50 million euro, representing 99% of all companies in the EU [4].

the cybersecurity challenges SMEs are facing, what security measures they have and what kind of help they might need. The goal of this investigation was to gain knowledge of what kind of help SMEs might need to improve their general security level.

2 Background

Managing security as well as deciding on security measures may be a difficult task without guidance. Thus, using a framework may easy the challenging process of implementing IT security. However, there exist plenty of standards, frameworks, badges and internet tools which may assist with the process of securing the business. To navigate between these guides and to decide on one may be the first challenge for SMEs in their first steps of implementing IT security measures.

2.1 Choosing a security guide

It can be overwhelming and difficult to navigate between all the available security sources. Some of the tools may not fit the risk profile of the SME, and some may be too complicated. To get an overview of some of the the national and international best practices we briefly present a handful of the available tools in the following.

The ISO27001
The ISO 27001 standard sets requirements for the establishment, implementation, maintenance and continuous improvement of an information security management system (ISMS). It is the standard that all public institutions in Denmark have to follow. The standard is also a good basis for dealing with the requirements of the General Data Protection Regulation (GDPR), which began in May 2018 in Denmark [2]. The core requirements of the security standard consists of 22 subjects and has 14 optional controls to choose from [6].

NIST
Another top-rated security best practice is from the National Institute of Technology (NIST). They have created a cybersecurity framework as a optional product to provide organisations with guidance on how to prevent, detect and respond to cyberattacks [7]. The framework is divided into five steps: *Identify* cyber risks of the organisation. *Protect* the organisation with safeguards. *Detect* cyberattack with monitoring. *Respond* to incidents and make a response plan. *Recover* and restore services that may be impaired due to a security breach [8].

Seven steps that work
A Danish take on a framework for businesses is from Center for Cybersikkerhed og Digitaliseringsstyrelsen, 2017 *Cyberforsvar der virker* [9]. This framework consists of seven steps and is meant as cybersecurity guidance for organisations

to help them be better protected [9]. The list includes the following steps: 1. Understand the cyber threats and support implementation of the cyber defence. 2. Delegate technical tasks to employees who posses the needed competencies. 3. Implement basic security. 4. Increase security awareness. 5. Develop a response plan and perform logging. 6. Have a continuous test of security. 7. Make technical controls, e.g. mobile device management and two-factor authentication.

Cyber Essentials

Great Britain has created a badge called *Cyber Essentials* which is an IT security badge. It is a security standard for businesses and customers, which helps to secure the enterprises from cyberattacks and also to build a trust-based relationship to business partners and customers. The badge requires that all devices and software in the company must meet five technical security requirements. Some authorities require that companies must hold the badge to collaborate with public institutions [10]. The Government in Great Britain created the badge, especially for SMEs, but it is suitable for all organisations of any size in any sector [11].

In Denmark, a company called *Virksomhedsrådet for IT-sikkerhed* have suggested a similar badge [10]. The purpose of this badge is the very same as the British *Cyber Essentials* badge. Its purpose is to make it easier for businesses to structure their work with IT security and achieve a basic level of IT security, as well as guidance to consumers that priorities IT security. It is, however, still in the prototype phase [10].

Safety check

The SMEs in Denmark have a free and available internet tool for getting an overview of the state of their IT security. The name of this tool is *Sikkerhedstjekket* [12]. This tool is built as a survey asking questions about the company, and the output is a customised risk report. The investigation is split into three categories. First, they identify the risk profile of the company by asking questions about the company's size, turnover, the importance of the IT system and how they handle sensitive information. Then 17 questions are asked about the management and the current state of the IT security of the company. The topics range from management, security procedures, employees, technical security solutions and partners. The report provides an overview of how well the company is secured and where to focus. The tool also has a step by step guide on how to get aligned with the recommendations.

2.2 Challenges with security in businesses

Danish SMEs experience a wide range of challenges in working with IT security, where employees, management and knowledge of IT security in particular play a role. Many Danish companies do not adequately control their digital security, and the problem is significant among SMEs. Three barriers stand out, especially: the lack of management involvement to IT security, knowledge of employees and prioritisation of resources [1].

Human factors are the main challenges, and this includes human error (by employees and management) and decisions in terms of priorities. This leads to the three barriers, namely, employees, management and prioritisation of resources. Intuitively, one would think that the less tech-savvy are the sinners. Still, studies show that even users with technical skills such as system administrators and developers, often struggle to keep up with the complexity and workload created by the security mechanisms [13].

When employees and management possess knowledge of IT security, it becomes a driving force, which also applies to the IT managers in the SMEs. However, IT managers also find that it can sometimes be challenging to navigate the information in the area. This is often overcome by listening to and receiving advice from external collaborators such as an outsourcing partner or an IT security consulting firm [1].

Education of employees

Many Danish SMEs do not have a formalised approach to IT security when it comes to their employees. This is because they primarily use oral communication to make employees aware of IT security in opposite to using formalised measures such as training employees in IT security and measuring their awareness of same. In particular, smaller companies do not have formalised training aimed at employees [1]. The Monitor Deloitte (2018) study showed that 10 of the 14 companies perceive employees' actions and lack of knowledge about IT security as a barrier to the company's work with IT security. According to the companies, this is reflected by the employees lack of responsiveness to the changes that have been necessary to increase IT security, and which at the same time affect the employees' workflows. In addition, companies also find that employees are not able to identify IT security threats to a sufficient degree [1].

Lack of knowledge among the management

If management does not prioritise IT security sufficiently, it becomes a barrier as the resources needed are not allocated to implement security initiatives. The Monitor Deloitte (2018) study points out that several companies' management does not engage in IT security, it is because they focus more on the commercial and do not have sufficient knowledge of IT security to engage [1]. Therefore, top management is vital for implementing a good security culture in any SME. Beautement et al. (2008) present a paradigm called the compliance budget which is used as *'a means of understanding how individuals perceive the costs and benefits of compliance with organisational security goals'*. The more security minded an organisation is the fewer conflicts concerning compliance will appear. Weirich and Sasse (2001) report that behavioural norms strongly influences the security behaviour of individuals and that most people strive to fit in [14]. If the company builds a positive and robust security culture, it will most likely reduce the friction and perceived cost of compliance [13].

Security culture and priorities within the company
In general, a barrier for getting started with IT security is that the decision makers in the company does not possess sufficient knowledge of threats and relevant security measures. Lack of knowledge can be fatal, as a company's risk profile grows and eventually the company won't be able to respond to a threat as it occurs. Moreover, lack of knowledge is deprioritising security measures in general.

Informal communication is a tool for creating the necessary cultural change and 74% of Danish SMEs also use oral communication with the workers in their work with IT security. The informal communication creates an increased understanding of IT security. This increased understanding makes the employees better know the importance of IT security and the consequences of inadequate IT security for the company. It is fundamental for the SMEs that the employees understand what IT security is, and it is, therefore, necessary to make IT security very tangible and something which is discussed. However, oral communication is often not enough, and it may, therefore, be necessary to follow up with rules and policies so that IT security is also anchored in the company's processes and workflows [1].

3 The Study

In this paper we aimed to get an understanding of the cybersecurity challenges in SMEs. We conducted interviews to obtain an understanding of the current state of the cybersecurity. This investigation was made to understand what kind of help may be useful for SMEs to improve cybersecurity.

3.1 Study design

We decided to conduct semi-structured interviews which in many ways are similar to everyday conversations, though guided by an interview guide [15]. The meeting is a planned but flexible interview with some research questions. The purpose is to gather nuanced answers and an in-depth understanding of the interviewee's perceptions. In the semi-structured interview, it is possible to change the order of questions, and it offers an opportunity to ask follow-up questions. These opportunities give the interviewer control over the conversation while allowing the respondent to answer freely. The advantage of the semi-structured interview is that the approach provides the respondent with the freedom to pursue particularly exciting topics that may arise along the way [15].

Interview guide
We designed the interview guide to help us gain knowledge of how the state of cybersecurity was in different businesses and to make our respondents more comfortable with getting interviewed. The interview guide was sent to the respondents before the actual interview in order to make the respondents confident about the agenda and what kind of questions they were going to answer.

Furthermore, IT security policies within a company may be considered confidential by the company, which make it even more important to emphasise the anonymity of the interview. By sending an interview guide beforehand also makes the answers of the respondents more considered. The interview guide is included in appendix 1.1

Pilot test of interview
It is always good practice to test the questions before conducting an interview, which we also did on a student [16]. The pilot test was established to make sure that the questions where easy to understand and that the meeting did not take too long. The pilot test, combined with feedback from the test person gave us information to reduce the duration and improve the quality of the interview.

3.2 Designing the Interview

To obtain an empirical basis for our research, we conducted four in-depth interviews in four different organisations. The research questions of the interviews were exploring:

- The companies level of protection.
- What help they might need concerning security.
- The employees attitude toward security rules.

The interview questions was inspired by the article *The compliance budget: managing security behaviour in organisations* (2008) in the sense of having a focus on the organisation's security policies and the employee's behaviour toward these [13]. The Monitor (2018) study provided us with information about SMEs current state of security and with examples of interview questions [1].

Face-to-face interviews are to prefer due to possible hidden information in the mimic and gesticulation of the person [15]. However, due to the corona pandemic we were not able to conduct all the interviews face-to-face. Two of the interviews took place in person before the society shut down the last two were conducted remotely. The interviews duration ranged between 20-30 minutes.

The companies respective industries spanned from healthcare products, mobile games, virtual reality and IT security consulting. We found the four respondents through the two authors personal network. The interviewees had positions ranging from the part-time worker to the CEO of the company. We chose diversity in the posts to receive different thoughts, ideas and experiences within the IT security field. All participants had a university degree and at least one-year work experience.

3.3 Data Analysis

This study was conducted with respect for the participants privacy and anonymity. Thus, all collected recordings has been destroyed after transcription. Names of people and company has been anonymised. With respect to the participants privacy each participant was offered to review the transcript.

Transcription

We recorded the interviews and transcribed the them immediately after conducting them. The short time-span between the interview and transcription ensures that the interview is clear in memory. This approach aims to reduce errors in the transcription. This research works with a relatively simple level of transcription, for example; Tone pitch and count on pauses are not included in the transcripts, as it is the meaning of the essence that is essential in this study.

It is noteworthy to mention that all content used for the analysis has been translated from Danish to English, thus the quotations from interviews are not verbatim, but a translation.

Method for analysing

The methodology for analysing the collected data entails summarising the mass of the data collected and then presenting the results in a manner that offers the essential findings [17]. For this paper, we analysed the transcripts of the interviews through a process called content analysis. Content analysis involves coding and classification of data. The purpose of content analysis is to filter out essential messages from the mass of each interview. When conducting a content analysis, it is about continually revisiting the data and reviewing the categorisation of the data until a sense of certainty has been established about the findings ensuring truthful and accurate reflection of the data [17].

The analysis was initiated by reading through the transcribed interviews. When something notable was encountered, it was copied into a new document, and a note was made about the specific finding. Labelling every relevant item of information was done to distinguish and identify similarities between the data chunks. We approached the analysis looking for hits matching the research questions as defined in section 3. Afterwards, a list was compiled of the different types of hits found. The compiled list was analysed and compared between the participants. Finally, the original copies of the transcript were looked through again to see if we missed something that did not appear relevant the first time.

4 Results

The conducted interviews revealed many examples of companies that had problematic security flaws. Most of the interviewed participants indicated that there were limited to no security guidelines or policies in their company. Furthermore, the participants told that IT security was not something the employees were talking about at work, neither formal or informal. The only period where IT security was a topic was when the GDPR policy had to be implemented.

None of the interviewees had ever had any IT security training concerning cyberattacks. One example of missing awareness resulting from a lack of such training is the participants experience with passwords. One participant explained that they had the login-password for the business computer on a sticky note next to the device. We asked the participants if their company had provided them with any rules or guidelines concerning passwords. Here three out of four participants were indicating lack of guidance. We asked the participants about what they might think could help them towards becoming more secure. The participants all mentioned IT security guidance and some essential awareness of cyber threats. The one participating company with strong security indicated a need for an annual plan that would help them to revisit their security measures. Questions about workarounds concerning IT security policies were also asked, but due to the minimum security level in the interviewed SMEs, no noteworthy workarounds were reported.

We identified many different ways companies had tried to implement IT protection. Most of these were not successful. Due to the observed lack of knowledge within IT security in the SMEs, we argue that most of the interviewed organisations could increase their IT security level tremendously with just a little guidance. In the following section, we analyse some of the key questions from the interview.

4.1 Analysis of Key Questions

In this section we present a subset of questions and answers from the conducted interviews. They illustrate the participant's knowledge of their organisations IT security policies and how the company cope with cyber threats.

In response to the research question our study show that companies have minimal or no level of protection measures in place. For research question two: *employees attitude toward security rules*, we found that employees don't talk about security and don't have any training in place. In relation to the last research question our study suggest that the participants need guidance to recognise the assets and corresponding threats of the the company.

4.1.1 Is IT security something that you talk about in the company?

Our study shows that SMEs do not talk about security. This is in line with the Monitor (2018) study [1] that claims that SME's typically approach IT security with oral communication, in opposite to using formalised measures such as training of employees.

P2: 'Uhhmm, no .. it's not something we have talked to our team about.'

The respondent is the CEO of the company. This response shows, as mentioned before that more often, the motivation should come from above. Studies show that the lack of digital security is present in SME's due to the missing involvement from the top-level [5]. Deloitte Cyber Risk recommends that employees are always aware of IT security. It is not about the method but the frequency of communication [1].

4.1.2 Has the company faced a cyberattack?

IT security breaches usually have high costs for companies that are affected. When a company is hacked, it often requires direct expenses to IT specialists to repair and investigate the security breach. In addition, there are indirect financial losses, for example, in the form of failure to operate, lost business opportunities and loss of customer confidence [5].

We asked the participants if their company had experienced a cyberattack. Two of the participants did not know if their company had been attacked. The other two explained how they experienced cyberattacks elaborately. One of the companies had experienced an attack but did not take any measures to become more secure after. The boss would not pay the hacker and made it more difficult and time-consuming for the employees to do their work afterwards:

P1: 'Yes, it happened once before that someone hacked into the company's folders. With all information about products and product sheets and photos and photos located on the website. I am not .. it was before my time, so I do not know exactly what is in that directory, but it is often when I need, for example, a raw image of one of the products that I then have to take it myself, because some of the pictures on the website are not to find anymore due to the hacked folder. And my boss wouldn't pay the hacker for decrypting the files. So they are just lost. So it's extra work afterwards.'

Even though this company had experienced a cyberattack and still have very few security measures in place at the time of the interview, the interviewee could still see it happening again:

P1:'... Although the company is very small, we have a huge turnover. So, uhm. I could imagine that it might well happen again. It has happened before so why shouldn't it happen again?'

The other company that had experienced an attack witnessed a different kind of attack where it was the co-owner who was the target. However, the company was only affected at the time of the incident:

P2:'... we've had a single hmmm, incident where the co-owner became like the target of an attack.... where we just panicked for 24 hours and had to change all our codes and update our system of how we remember the codes and how we share them so that they are not in a spreadsheet and stuff like that. And there we also asked our employees to do a 2FA on a lot of things. Just so that if you have to access our drive, google drive then it's not that you just hack one person, or something like that.'

With this company, nothing about their security changed after the incident except their password management. Even though they did experience an attack they did not take any measures to become more secure in the long run:

P2: 'So with the ones we created it with (2FA) at the time, uhm, they clearly still have it .. I think.. It's not something we followed up on, but uhm, it's not something we kept doing when we have hired new employees. It is not like remember to put 2FA on this because our policy.. we have no policy on it. I guess it's something where if that happens again we'll probably panic again.'

4.1.3 Are there any password rules for your business computer?

Password management is a hard discipline to master, at the same time it is crucial because passwords provide an essential layer of protection. A policy about having strong passwords provides a layer of protection of a company's assets. But due to the mental capability of memory in humans, people tend to pick passwords that are easy to recall [18]. If the password is too difficult to remember, some may write them down. The participants were also indicating the challenge of mastering the password management discipline.

P1: '.. I think the password is still on one of the computers on a post-it next to the touch-pad on the computer.'

This quote is an example of a very problematic issue an organisation can have. They try to implement a layer of protection by forcing long and complicated passwords to their employees. But instead of raising the level of security in the company, they lower it.

P2: 'They use their own passwords to log in with ..'

It can be dangerous for the organisation trusting the employees to create their passwords without any training or guidance. Weak or reused personalised passwords could potentially be used in the company. Without the necessary security training or password guidelines, some employees may create an insecure password.

P3: 'We need to update them every third month — the password for our computers and systems ..'

One company had a security rule that required every employee to change all their passwords every third month. This practice has shown not to work because people are having difficulties of creating strong, unique and memorable passwords. People who are forced to create new passwords often tend to create passwords that follow a predictable pattern, such as incrementing a number or other changes that are easy to remember [19].

4.1.4 Are there any kind of IT security policies in the company?

Most of the interviewed participants indicated that there were no or minimal IT security guidelines in their company. Only one participant from an IT company mentions that they have several different policies in the company and did talk elaboratively and in-depth about it.

P4: 'We have many different things. We have something like you can't leave your computer without locking the screen. Then we also have some technical concerning one's laptop and mobile phones with a password and encrypted hard disk that must be turned on BitLocker on all Windows devices and firewall if it is Mac devices. Then we use MFA multi-factor authentication on anything possible. And then there are also some policies regarding lengths of passwords and yes, generally also how to store and use your IT equipment, don't put it in some car so you cannot see it and such.'

The company is an IT company which provide IT services for its clients, and this could be the natural reason for their proactive approach to IT security.

Another participant had signed an IT security policy paper but was not sure about the details in the signed document:

P3: 'there was some policy document when you signed the contract that required you to have an IT-safe behaviour such as updating and that you control the various systems yourself and that you do not share your password or save and send it and there are other things as well.'

This quote shows the importance of having a policy which has the right balance of details and length. Policies should not be so complex that the rules are not followed or omitted. A more detailed policy may be justified where risks are high and where the cybersecurity level is prioritised. However, a short policy has a much better chance to be assimilated [20].

The remaining two interviewed companies had no security policy. These findings align well with a 2018 study conducted by Monitor Deloitte for The Danish Business Authority on digital security in SME [1]. This study finds a clear trend of documented IT security policies as the size of the company grows. This shows that smaller companies have a lower degree of security measures.

4.1.5 Does the company have a response plan?

It is important to have a formalised plan that explains what should be done if an IT-related incident happens [21].

Only one out of four participants knew that there was a response plan in the company. However, the participant did not know what the plan entailed, only that such a plan existed in the company:

P4: 'Yes but uhm, it's actually not something I have much insight into what it is about, but it wouldn't really include me in the same way.'

The participant did mention that the response plan had not been updated recently and that it was created some years back and might need a revision:

P4:'Yes, but this is something that I think has a small leak compared to the fact that we have not had it tested recently, I mean done such a test. We really should do that because it would be really nice to drive it through.'

Having a response plan is not enough, maintaining the plan, training staff and keeping the plan updated is equally important. Thus, companies should pay attention and allocate resource to continually maintaining and developing a response plan and training staff accordingly [21].

4.1.6 Could you think of a scenario in your workflow where security policies have been a little too cumbersome so instead of following the IT security policy you have looked through it to be able to finish your tasks?

This question was asked to understand if the participants had done any workarounds in their organisation. But, due to the minimum security level in the interviewed organisations, not many workarounds had been made.

P1: 'The only thing I can think of is about post-its.'

Due to the lack of security rules of P1s organisation, not many workarounds were made. The participant was indicating that the CEO of the company had no interest in implementing security.

4.1.7 Does the company have any IT security training programs?

None of the companies had a formalised approach to the employee's awareness and knowledge in relation to IT security training. The participants all provided very short answers to the question:

P1: 'Not at all.'

P2: 'No, not at all. Nothing.'

P3: 'No, now you're talking to a start-up, it's probably not there. So we have to do it ourselves, but there are no resources.'

P4: 'Not specifically IT security but I have been on quiet few courses on GDPR *but it has mostly been a legal approach to it. Um so no, not like that.'*

The findings show that none of the companies has training programs. The concise answers indicate a lack of awareness of assets and threats. By informing and training employees, the company helps itself staying secure, as the employee becomes aware and up-to-date of potential cyber risks.

4.1.8 What would you think could help you as a company be more secure?

We asked the participants to think of anything they could need in their work-life to be better protected. The question was asked to get an understanding of the needs in SMEs concerning IT security. One participant was not sure about what was needed, but the three other had precise demands. Two of the participants were mentioning an awareness-guide of basic IT security or a brief explanation of common gaps.

P1: 'It should be a very brief explanation may be a poster, and it should not be very costly - or cost anything at all. At least I don't think my boss would invest in a course for employees ..'

The quote from P1 indicates the importance of making a very cheap product. The product may be excellent, but if it is costly, the organisation will not invest in it.

P2: '.. So a kind of a guide like. Hey, these are the common gaps you have in such a business, here's what you can do to secure them. And why it's important ... just to get a security check or something like that. It could certainly be very good.'

This quote is from the CEO of the company, and it shows the need for a tool to gain awareness. What the participant cries for here is some guidance to recognising the assets and the corresponding threats of the company. And to get an understanding of the cyber threats in the company and how to secure them.

The last company which had great security culture were mentioning a demand for a plan for when to revisit the existing security measures.

P4: '.. It could be great to have that kind of thing like having a year wheel in the business where there are those things you do every year, so having such a plan for when it makes sense to check up on IT security and incident plan and IT policies and so on.'

They already had comprehensive IT protection so the thing they wanted was a tool to remember to revisit the measures.

5 Discussion

In section 4.1, we mentioned one SME which stood out from the rest. This company were similar in size and resources but had well-defined security policies and good security culture. It may be due to the companies focus and knowledge as the company provides security guidance to other SMEs. The outstanding level of protection may also be due to the danger of a bad reputation. A bad reputation could be devastating for a company which are helping other companies with IT protection. If well-protected companies were a general competitive factor, perhaps more SMEs would prioritise security higher as it is for some companies in Great Britain with their *Cyber Essential* badge.

As mentioned before top management is the key for implementing strong security. If the CEO and other important company leading people are prioritising the safety, the rest of the company will most likely follow along [9]. The company in our study that stood out from the rest had arguably a good security culture. This may be driven from the focus on security from above.

None of the interviewees had ever received any security training concerning cyber threats. This lack of cybersecurity awareness may hurt the company as a small mistake from an employee could result in a cyberattack, e.g. a phishing attack. This information aligns with the findings from the Danish Business Authorities report from 2019 on digital security in SMEs. In this study, they found that 2 out of 3 SMEs has not provided any training or education for their employees in IT security nor data protection [5].

6 A simplistic framework

Choosing to implement IT security may be an overwhelming task for many SMEs. Monitor Deloitte (2018) claims that 70% of SMEs have outsourced all or part of their IT security [1]. However, there are a lot of critical security steps which, with a little guidance, could be implemented without professional help.

Based on our findings, all companies except for one had no or very limited IT protection. Another conclusion was that there was a need for essential security guidance. Therefore, we decided on a simple go-to framework with focus on the very basics.

Based on our findings and the previously explained standards, we have tried to come up with a framework that could work for any SME based on the level of security they may need. The framework could have been much more substantial like the ISO 27001 standard, but we aimed to narrow it down to at most five steps for simplicity and ease implementation. However, if one of the steps seems too overwhelming there exist plenty of external support.

As stated earlier top management is key to a successful implementation of IT security, it is, however, not explicitly included in the framework as it focuses on the concrete steps toward protection. When using a framework like this, we cannot stress the importance of including the employees in the implementation process. If employees are involved, they will gain awareness of the importance of security and will most likely also communicate it, which again will raise the security level.

In the following, a complete description of the five steps is presented. These five steps describe a concrete, prioritised plan for how SMEs can decrease the risk of cyberattacks. The step by step guide focuses on initiatives that can directly reduce the risk of cyberattacks.

1. Cyber Essentials

- *Use a firewall.* It is essential to turn on the firewall on the computer. Turning on this basic security standard in the computer settings allows for analysing the incoming traffic and decide whether or not it should be allowed onto your network [22].

- *Turn on anti-malware system.* Anti-malware systems are software that prevents viruses and malware from infecting IT systems. Anti-malware measures are often included for free with the operating system.

- *Choose the most secure settings for your devices.* Enabling the most secure environment includes several small changes for your device. Some of these settings include: Strong passwords, automatically log off when the user has been passive for a certain period, and encrypting of private or confidential information.

- *Patching.* As vulnerable applications and operating systems are the targets of most common cyberattacks patching should be a top priority [23]. Patching not only adds new features but also fix newly discovered security vulnerabilities. Programs, apps, phones and operating systems should all be set to update automatically. If programs or operating systems no longer can be updated, the organisation should prepare a plan for phasing out or isolating them. Continual use of non-updatable systems involves high-security risk.

- *Access control.* To minimise the potential damage if an account is misused or stolen, employees should only have access to areas of the company that are necessary for performing their tasks. Extra permissions should only be given to those who need them. Accounts with minimum privileges must be used as a standard. Thus, an attacker with unauthorised access is far more dangerous with administrative privileges.

2. Data Protection

- *Software whitelisting.* The organisation should choose which software to use while blocking all others. Whitelisting helps to prevent malicious software and unapproved programs from running. A simple and effective way of doing this is only to use software from official sources such as software centers and app stores [22].

- *Backup your data.* Inadequate backup is one of the most common reasons why companies lose their data [24]. The company should start with identifying what types of data the company need to back up, then address the backup task to one or more employees. The backup could be on a remote server e.g. cloud or on an external drive.

3. Security Policies

- *Define security policies.* Define and write down a security policy that everyone in the company understands, follows and actively supports. A security policy should have defined all of the company's assets and all the potential threats to those assets. The employees should be kept updated on the company's security policies. Some of the procedures could be concerning employees as well as physical and network security. There exist many websites providing security policy templates, one such is SANS. They provide a wide range of free security policy templates [25]. Communicating security measures of the company among and with employees may assist the process of gaining awareness of cyber threats. The security policy should circulate everyone in the company and be relied on and updated regularly [26].

- *Response plan.* Another critical aspect of security policies is the response plan. There should be a plan for the procedure of an unusual situation, for example, a suspicious mail. The list should also include procedures for when a hacker has succeeded in breaking through the security measures. The response plan must clearly outline responsibilities and tasks in an unusual situation and contain contact information on the support that can be used if necessary. The digital security website for Danish SMEs *sikkerdigital.dk* provides free templates and guidance for implementation [27]. If however, such a model is too overwhelming, the company should choose an employee that should function as the go-to person if any anomalies or incidents occur. This person should have technical skills or know which IT security supplier to contact.

4. Risk Assessment

- *Identify the company's level of risk.* It is vital to know the vulnerabilities and threats to identify the company's level of risk. The Danish survey tool called *Sikkerhedstjekket* is an excellent tool for getting a risk profile. It gives an idea of where to focus and the need for additional security measures [12]. A method called SWOT which stands for Strengths, Weaknesses, Opportunities and Threats could be another tool for SMEs to identify the risks of the company [28]. The goal in risk assessment is to get a comprehensive picture of the dangers facing the security of the organisation.

5. **Security Training**

- *Awareness and training.* Every employee should be aware of the assets and threats of the company. By informing and communicating IT security with the employees helps to stay secure. The employees should know the most elementary cyber risks and keep up to date on the area throughout their carrier. In addition to communicating security in the company resources on professional security training such as rules for storing data and passwords and knowledge about ransomware and phishing-attacks is excellent. Based on the risk profile and the need for security, the individual business should consider investing money in security training for their employees.

6.1 Illustration of the five-step framework

The diagram is sketched as a circle which indicates the need for revisiting the steps. How often the security steps are visited is up to the individual organisation.

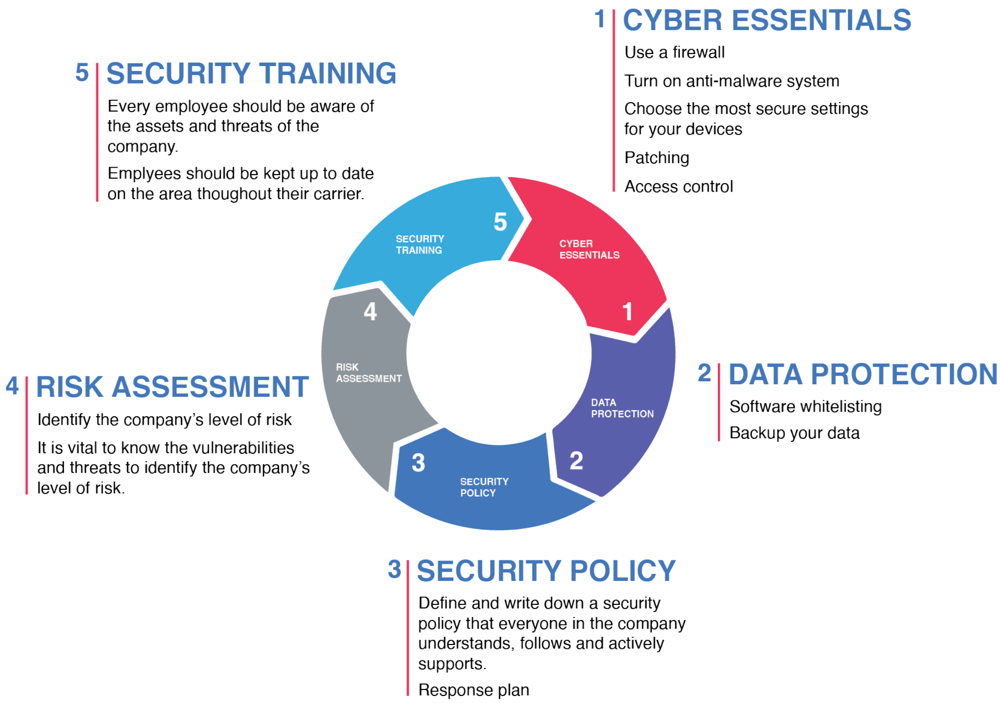
1 CYBER ESSENTIALS
Use a firewall
Turn on anti-malware system
Choose the most secure settings for your devices
Patching
Access control
5 SECURITY TRAINING
Every employee should be aware of the assets and threats of the company.
Emplyees should be kept up to date on the area thoughout their carrier.
5
SECURITY TRAINING
CYBER ESSENTIALS
1
4
RISK ASSESSMENT
DATA PROTECTION
2
3
SECURITY POLICY
2 DATA PROTECTION
Software whitelisting
Backup your data
4 RISK ASSESSMENT
Identify the company's level of risk
It is vital to know the vulnerabilities and threats to identify the company's level of risk.
3 SECURITY POLICY
Define and write down a security policy that everyone in the company understands, follows and actively supports.
Response plan

Figure 1: The five step framework for SMEs

6.2 The three security levels

The ability to categorise the level of security need in an organisation is crucial. Having too weak defence may have consequences of a security breach, deciding on a too comprehensive security framework may also fail. A security implementation too large can be overwhelming for some companies and may end up incomplete. A categorisation on the level of security needs in SMEs is therefore essential. The report *Digital sikkerhed i danske SMV'er* from Erhvervsstyrelsen distinguish between three levels of security needs depending on how digitised the organisation is [5]. This categorisation of the need of IT security may help to clarify the aim for an SME.

In addition to the five-step framework, we have decided to split it into three categories. A similar categorisation is done in the report *Digital sikkerhed i danske SMV'er* from Erhvervsstyrelsen [5]. Figure 2 illustrates the three split and explains which steps each category holds. Each group builds upon each other. Some organisations may only need *Basic Security* to fit their risk profile; some may require additional security measures. The framework is split into these three different levels:

- The *Basic Security* level is as defined the basic security settings. This category suits every SME that uses digital devices. This category only involves step one, but have many minor technical changes. We concluded on our findings that there was a demand for the most critical security measures and that it should be easy to implement. For this criterion, we got inspired by the British badge *Cyber Essential.* They claim that these measures could prevent up to 80% of all cyberattacks [29]. We think that most companies most likely will be able to do these security settings without any particular help. That is the reason for having these as the core basis for strong IT security in our framework.

- The *Organisational Security* level combines the *Basic Security* settings, with data protection and policies for the organisation. This level of protection may fit most SMEs, that have employees primarily working on devices. It concerns the process of doing backups and defining and communicating policies. We chose to put these measures at the second level of security because they provide an opportunity for organisations to communicate and collaborate on rules and procedures. Our findings showed the importance of money, as for some companies, the implementation of safety should not be costly. We assume many SMEs can execute the *Organisational Security* level themselves if they are aware of the free and great tools available like *Sikkerhedstjekket* [12] and *sikkerdigital.dk* [27].

- The *Extended Security* level is more comprehensive and contains two additional security steps. This level of protection may be relevant for Danish SMEs, which are highly digitised and depend heavily on IT systems. We have chosen to include security training at the *Extended Security* level because it is costly and the company have to dedicate time to it. We think that security training is precious for a company, but according to our findings, many companies may not value the need for security training for their employees. If however, a company decide to invest in security training, we think that it will help the security level in the organisation tremendously.

6.3 Illustration of the three security levels

The three splits of the security framework are visualised as three circles which built upon each other. This visualisation shows that the *Basic Security* level is the core and more steps can be added on top of it.

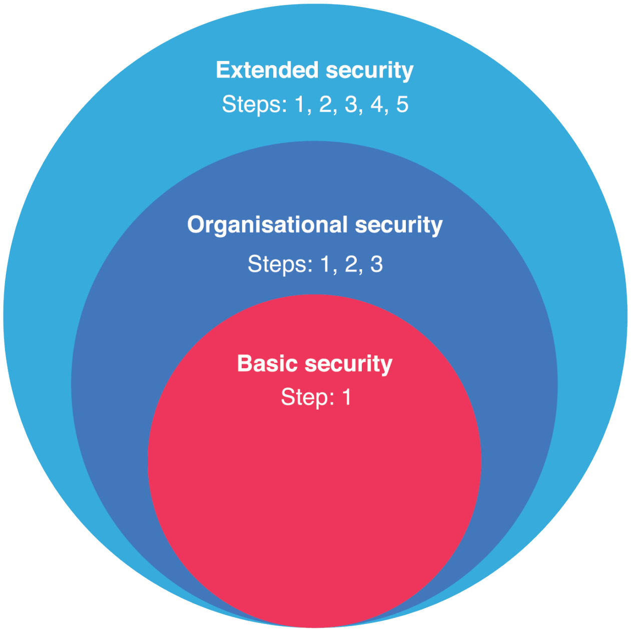

Figure 2: The frameworks three security levels

7 Conclusion

A company may face various cybersecurity challenges and barriers toward good security culture. One of these challenges is to have the directing team of the company to prioritise IT protection. Without top management, a business will have a difficult time implementing strong security. Employees' actions and lack of knowledge about IT security is related, as limited awareness of cyber threats results as a barrier to the company's work with IT security. The same problem concerns the decisionmakers in companies. Without awareness about threats and knowledge of the available security-assistance, some companies may not think there is a need for protection.

The security frameworks and standards like *ISO27001*, *NIST* and *Seven Steps* may work for some companies, but we think, based on our study, that they may be too comprehensive and overwhelming. Basic and straightforward steps to strong security may be the answer.

Our findings indicated that there is a lack of basic security and that they would benefit from simple, free and concrete help. Such help already exists in some degree for Danish SMEs. One tool called *Sikkerhedstjekket* [12] gives a risk profile in combination with tips for securing the gaps. Another tool is to use a framework like the one we have put together, which prioritise the essential security standards as a core with an opportunity to extend for SMEs that may need it. This tool may give an overview of an implementation that is to overcome.

There exist several tools for Danish SMEs. However, there may still be a need for promotion on these as they are spread out to various sites. A solution may be to combine the available tools on a straightforward website, which the only purpose was to guide SMEs with the implementation of IT security. Having a framework like the one we suggest combined with the free available tools, templates, and a badge like *Cyber Essentials* could maybe be a solution to the issue we have with inadequate cyber protection in Denmark. The framework could possibly work for some SMEs by providing them with an overview of the steps to take toward implementation strong IT security.

References

[1] Monitor Deloitte for Erhvervsstyrelsen. *It-sikkerhed og datahåndtering i danske SMV'er*. Apr. 2018. URL: https://erhvervsstyrelsen.dk/sites/default/files/2019-03/it-sikkerhed_og_datahaandtering_i_danske_smver.pdf.

[2] Anders Linde. *ISO/IEC 27001 Informationssikkerhed*. 2019. URL: https://www.ds.dk/da/om-standarder/ledelsesstandarder/iso-27001-informationssikkerhed.

[3] European Commission. *The Digital Economy and Society Index (DESI)*. URL: https://ec.europa.eu/digital-single-market/en/desi.

[4] European Commission. *What is an SME?* URL: https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en.

[5] Erhvervsstyrelsen. *Digital sikkerhed i danske SMV'er*. Nov. 2019. URL: https://erhvervsstyrelsen.dk/sites/default/files/2019-11/Analyse%20af%20digital%20sikkerhed%20blandt%20SMV%27er%202019.pdf.

[6] ISMS.online. *The Requirements Annex A Controls of ISO 27001*. URL: https://www.isms.online/iso-27001/requirements-controls/.

[7] Kate Brew. *NIST Cybersecurity Framework Compliance with AlienVault USM Anywhere*. Apr. 2020. URL: https://cybersecurity.att.com/resource-center/solution-briefs/nist-compliance-usm-anywhere?utm_source=google&utm_medium=cpc&utm_term=kwd-338808096181&utm_campaign=728621670&source=EBPS0000000PSM00P&WT.srch=1&wtExtndSource=&wtpdsrchprg=AT.

[8] National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*. Apr. 2018. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[9] Center for Cybersikkerhed og Digitaliseringsstyrelsen. *Cyberforsvar der virker*. Jan. 2017.

[10] Sikkerhedsrådet. *En mærkningsorden for it-sikkerhed*. Dec. 2018. URL: https://em.dk/media/12881/anbefaling-om-et-maerke-for-it-sikkerhed-2.pdf?fbclid=IwAR0P0stPl08GMMeJkT3pewUEBXIqC-6T7jVFhMbX0EEn4NGj4XEM3P8R1d4.

[11] gov.uk. *Cyber Essentials Scheme: overview*. Jan. 2018. URL: https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

[12] Virk. *Sikkerhedstjekket*. URL: https://startvaekst.virk.dk/sikkerhedstjekket/testen.

[13] Adam Beautement, Angela Sasse, and Mike Wonham. "The compliance budget: managing security behaviour in organisations". In: (Jan. 2008). DOI: 10.1145/1595676.1595684.

[14] Dirk Weirich and Martina Sasse. *Pretty Good Persuasion: a First Step Towards Effective Password Security in the Real World.* 2001. DOI: 10.1145/508171.508195.

[15] Steinar Kvale Svend Brinkmann. "Interview - det kvalitative forskningsinterview som håndværk". In: (2009).

[16] Arthur Cropley. *Introduction to Qualitative Research Methods.* Dec. 2015.

[17] Beverley Hancock. *An Introduction to Qualitative Research.* 1998. URL: http://faculty.cbu.ca/pmacintyre/course_pages/mba603/mba603_files/introqualitativeresearch.pdf.

[18] Angela Sasse Awais Rashid. *Human Factors Knowledge Area.* Oct. 2019. URL: https://www.cybok.org/media/downloads/Human_Factors_issue_1.0.pdf.

[19] Lorrie Cranor. *Time to rethink mandatory password changes.* Mar. 2016. URL: https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes.

[20] Alasdair Taylor. *Cyber security policy templates as small business tools.* Aug. 2018. URL: https://seqlegal.com/blog/cyber-security-policy-templates-small-business-tools.

[21] Nationale Cyber Crime Center. *Forholdsregler - Ved brud på it-sikkerhedssystemer.* URL: https://sikkerdigital.dk/media/10263/forholdsregler-ved-brud-paa-it-sikkerhedssystemer.pdf.

[22] National Cyber Security Center. *Cyber security for your organisation starts here.* URL: https://www.ncsc.gov.uk/cyberessentials/advice#section_1.

[23] Canadian Cyber Incident Response Centre. *Top 4 Strategies to Mitigate Targeted Cyber Intrusions.* Nov. 2015. URL: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/tp-strtgs-en.aspx.

[24] Sikkerdigital. *Invester i en it-sikkerhedspakke med back up.* URL: https://sikkerdigital.dk/virksomhed/fem-gode-raad-der-styrker-din-virksomheds-it-sikkerhed/invester-i-en-it-sikkerhedspakke-med-backup/.

[25] SANS. *Information Security Policy Templates.* URL: https://www.sans.org/security-resources/policies/.

[26] Techopedia. *Security Policy.* Jan. 2017. URL: https://www.techopedia.com/definition/4099/security-policy.

[27] Sikkerdigital. *Skabeloner og værktøjer.* URL: https://sikkerdigital.dk/virksomhed/saadan-beskytter-du-din-virksomhed/skabeloner-og-vaerktoejer/.

[28] Fred Wilson. *How to do a SWOT Analysis for Risk Identification and Risk Management.* Nov. 2018. URL: https://www.ntaskmanager.com/blog/how-to-do-a-swot-analysis-for-risk-identification/.

[29] IT Governance. *The Cyber Essentials Scheme*. URL: https://www.itgovernance.co.uk/cyber-essentials-scheme.