jamk.fi

Cybersecurity situation analysis

Survey in Central Finland 2016-2018

Jarmo Nevala

Master's thesis
November 2018
School of Technology, Communication and Transport
Degree Programme in Information and Communication Technology
Cyber Security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s)	Type of publication	Date
Nevala, Jarmo	Master's thesis	November 2018
	Number of pages 102	Language of publication: English
		Permission for web publication: x

Title of publication

Cybersecurity situation analysis

Survey in Central Finland 2016-2018

Degree programme

Master's Degree Program in Information Technology, Cyber Security

Supervisor(s)

Kotikoski, Sampo; Karjalainen, Mika

Assigned by

Jyväskylä Educational Consortium (2016), Personal subject (2017, 2018)

Abstract

The idea for the study arose during work on the project 'Secondary level cyber' ('Toisen asteen kyber') for the Jyväskylä Educational Consortium. The goal of the project was to find out what the educational needs of the small and medium enterprises and microenterprises in Central Finland are from the perspective of the secondary level education. The project included a survey for companies and the representatives of the participating schools. After the project, the survey was further developed and repeated. As a result, research data was gained from a three-year study on the cybersecurity of companies in Central Finland.

The survey focused on companies in Central Finland. The main goal was to find out about the state of cybersecurity in companies and the changes occurred in the timeline of three years. The goal was to study how the companies perceive cybersecurity and what kind of challenges they face when implementing procedures to help them to anticipate and survive different cyberthreats and their consequences.

The survey was carried out with an online questionnaire on three consecutive years. After the first year the questionnaire was modified based on the feedback from the respondents. However, the majority of the questions were kept the same so that the results would be comparable. The study was quantitative by nature.

Based on the results, the companies have a clear need to improve cybersecurity. Cyber-security means recognizing, preventing and preparing for disruptions in the electric and network systems. In the digital era, cybersecurity is a challenge for the companies, as in addition to the hardware and software, also the knowhow and motivation of the personnel has an effect on the cybersecurity of the companies.

Keywords/tags (subjects)

cybersecurity, small enterprises, research, statistical analysis, Central Finland

Miscellanous

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Nevala, Jarmo	Opinnäytetyö, ylempi AMK	Marraskuu 2018
	Sivumäärä 102	Julkaisun kieli Englanti
		Verkkojulkaisulupa myönnetty: x

Työn nimi
Kyberturvallisuuden tilanneanalyysi
Keski-Suomen tutkimus 2016-2018

Tutkinto-ohjelma
Master's Degree Program in Information Technology, Cyber Security

Työn ohjaaja(t)
Kotikoski, Sampo; Karjalainen, Mika

Toimeksiantaja(t)
Jyväskylän koulutustuntayhtymä (2016), Oma aihe (2017, 2018)

Tiivistelmä

Idea tutkimukselle syntyi tehtäessä hanketta "Toisen asteen kyber" Jyväskylän Koulutuskuntayhtymälle. Hankkeen tavoitteena oli selvittää Keski-Suomen pk- ja mikro yritysten kyberturvallisuusosaamisen koulutustarpeet toisen asteen koulutuksen näkökulmasta. Hankkeessa toteutettiin kysely yrityksille sekä oppilaitoksien edustajille. Hankkeen päätyttyä kyselyn kehittämistä jatkettiin ja kysely toistettiin. Lopputuloksena syntyi kolmena vuonna tehty kyberturvallisuuskysely keskisuomalaisille yrityksille.

Tutkimus keskittyi keskisuomalaisten yritysten toimintaan. Päätavoitteena oli selvittää, mikä on yrityksien kyberturvallisuuden tilanne ja millaisia muutoksia on tapahtunut kolmen vuoden aikajanalla. Miten yritykset näkevät kyberturvallisuuden, ja millaisia haasteita heillä on toteuttaa toimenpiteitä, joiden avulla voidaan ennakoivasti hallita ja sietää erilaisia kyberuhkia ja niiden vaikutuksia.

Tutkimus toteutettiin sähköisellä kyselylomakkeelle kolmena peräkkäisenä vuotena. Ensimmäisen vuoden jälkeen kyselyä muokattiin vastaajilta tulleen palautteen perusteella kuitenkin pitäen suurin osa kysymyksistä samanlaisina, jotta tuloksia pystyttäisiin vertailemaan keskenään. Luonteeltaan tutkimus oli määrällinen kyselytutkimus.

Tulosten perusteella yrityksillä on selkeitä tarpeita kyberturvallisuuden parantamiseen. Kyberturvallisuudessa tunnistetaan, ehkäistään ja varaudutaan sähköisten ja verkotettujen järjestelmien häiriöiden vaikutuksiin.

Kyberturvallisuus on digitaalisen aikakauden haaste yrityksille, koska laitteistojen ja ohjelmistojen lisäksi myös henkilöstön osaaminen ja motivaatio vaikuttavat yritysten kyberturvallisuuteen.

Avainsanat (asiasanat)
kyberturvallisuus, pienyritykset, tutkimus, tilastollinen analyysi, Keski-Suomi

Muut tiedot

Contents

Figures

Tables

1 Introduction

When the research began in 2016, Central Finland, especially Jyväskylä had an important role in cybersecurity. In 2012 the Ministry of Economic Affairs and Employment of Finland (2012) set up the Innovative Cities program (INKA). The Innovative Cities program 2014-2017 is a partnership between the state and the approved cities where the cities play an important role in creating new types of development environments and in developing new business ecosystems . By choosing the priorities for the program, instead of traditional technology or industry orientation, it is desirable to emphasize demand-driven, solution-oriented and multidisciplinary thematic choices combining several areas of expertise. The program focuses on Bio economy, Sustainable Energy Solutions, Cybersecurity, Future Health as well as Smart City and Renewable Industry. The cities responsible for developing the priority areas of the program are Joensuu (Bio economy), Vaasa (Sustainable Energy Solutions) Jyväskylä (Cybersecurity), Oulu (Future Health) and Tampere (Smart City and Renewable Industry). In addition to these five cities responsible for the thematic cooperation, seven other urban areas (Lahti, Lappeenranta, Kuopio, Turku, Seinäjoki, Pori and the Helsinki Metropolitan Area) participate in the program.

In the spring of 2016, the Ministry of Economic Affairs and Employment of Finland decided on the new main projects and cybersecurity was not included in them. Despite of this, a gread deal was accomplished within the program in Central Finland. The most important achievements of the program were the new training programs for cyber safety offered at JAMK University of Applied Sciences and at the University of Jyväskylä.

It is often stated that Finland's goal is to be the key factor in cybersecurity. According to current publications, Finland does not currently have an overall picture of the current state of cybersecurity or of the need for information. Cyber safety related activities for companies and corporate employees are mainly based on warnings and sad news. The need for cyber knowledge is increasing; it touches everyone and extends into all activities. Cybersecurity is every citizen’s responsibility. The best way

to adopt and maintain cybersecurity is education and training. Cybersecurity must be included in the civic competence of all the citizens.

According to the regional strategy of Central Finland (Regional Council of Central Finland 2014) cybersecurity is a key competitive factor in digitalization, whereby bits and data networks have become more and more commonplace and an integral part of products, services and practices. This enables to establish new customer relationships, earnings and markets. In Jyväskylä, the national focus on cybersecurity is a key factor in exploiting competitive advantages. Digital literacy also requires a new orientation to developing services and content. To succeed, Central Finland must be both a strong producer and utilizer of digital services and content. Utilization requires knowledge and understanding from citizens, as well as from ordinary microenterprises and small companies.

The disfunction of IT equipment and systems, inadvertently or because of a cyberattack, has negative impacts on business, public services and governance, and thus on the vital functions of society. However, a key player in cyber safety is the individual person. Even little or no awareness, ignorance or neglect can result into large losses that are not covered by any insurance. The cause of the damage is most often the lack of guidance, information, choice of equipment and / or training.

Research background

In the autumn of 2015, the Regional Council of Central Finland approved the project for cybertraining in upper secondary education (“Toisen asteen kyber”). The main facilitator was Jyväskylä education consortium. The aim of the project was to provide an overall picture of the role and importance of secondary education in the implementation of the cybersecurity strategy of Central Finland. (Regional Council of Central Finland 2017)

During the project, a survey aimed at companies in Central Finland was conducted in order to clarify how cybersecurity could be developed in education. The survey was implemented in the spring of 2016 and the results of the survey were published in the autumn of 2016 (Nevala & Aho 2016). The project ended in the autumn of 2016.

Although the project ended, the author decided to continue mapping cybersecurity in Central Finland personally. In the spring of 2017, a slightly altered survey was republished by leaving out questions dealing with education and focusing on some specific follow-up questions. The latest survey was conducted in the spring of 2018, which resulted in survey data gathered in three different years.

2 Theoretical framework

Every day people read news about the latest security breaches. They wonder whether they should shutdown their computer, tablet, smartphone and put them into a Faraday cage to avoid these breaches: The main answer is that it does not matter. Other people's computers can hurt a person as much as one´s own computer (e.g. computers used in banking services). On the other hand, there are many other devices, which are connected to the Internet and these devices are a bigger problem than one's laptop.

Gartner (2017) forecast that 8.4 billion connected devices will be in use worldwide in 2017. This figure has increased by 31 per cent from 2016, and will reach 20.4 billion by 2020. Usually, when the number of connected devices grows, the risks increase in the same relation. Unprotected devices are and will be one major problem in future.

2.1 Finland's vision for Cyber Security

The Security Committee (2013) published a strategy plan on Finland's Cyber Security on January 24, 2013. The Security Committee's vision of Finland's cybersecurity is:

- Finland can secure its vital functions against cyber threats in all situations.
- Citizens, the authorities and businesses can effectively utilize a safe cyber domain and the competence arising from cyber security measures, both nationally and internationally.
- By 2016, Finland will be a global forerunner in cyber threat preparedness and in managing the disturbances caused by these threats.

Figure 1. (The Security Committee 2013) presented below visualizes this vision of cybersecurity. When analysing this vision made five years ago, it is clear that progress

has been made. Cyber education and preparedness have grown. Finland is participating in international activities and the new military intelligence law is being prepared by the government.

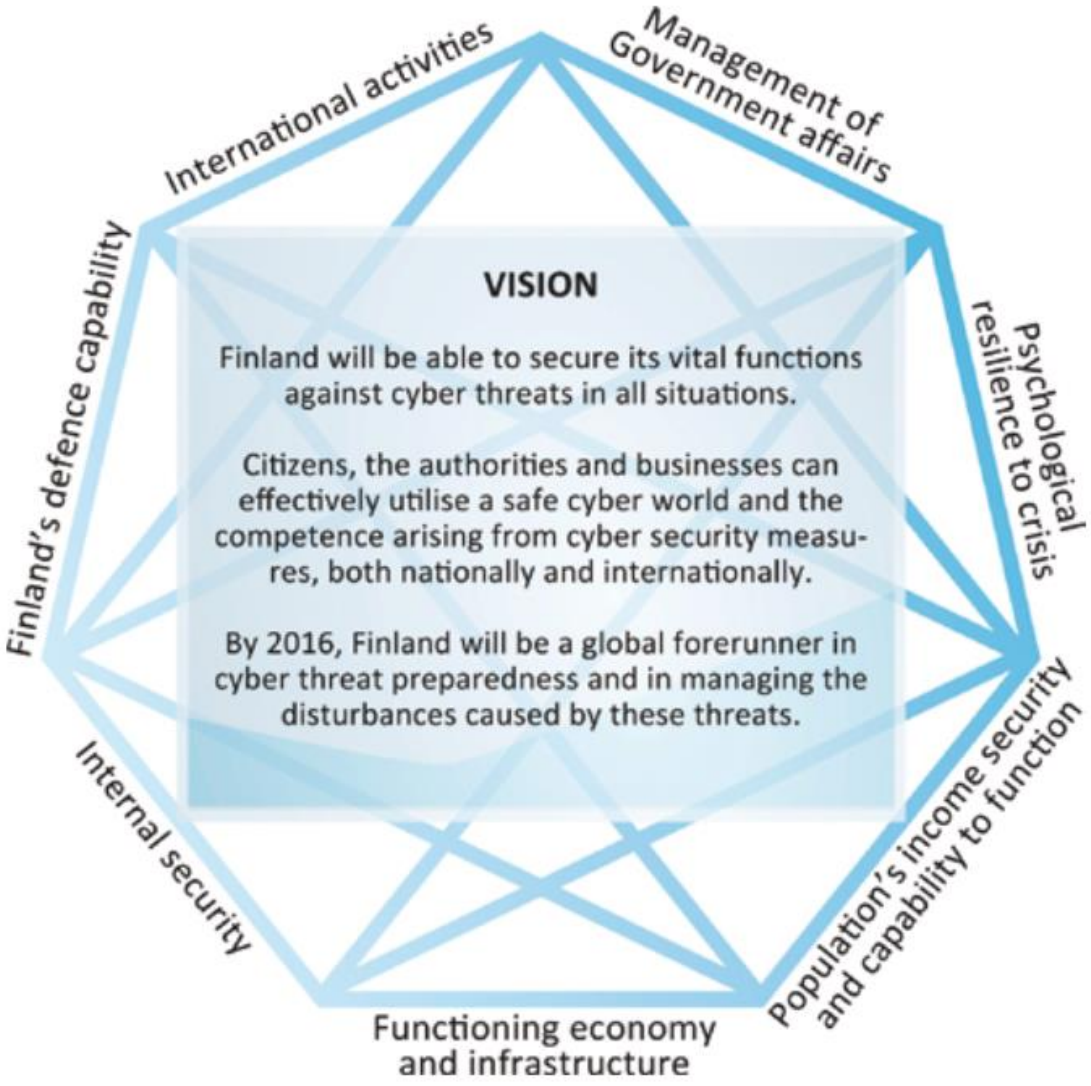


Figure 1. Vision for cyber security

2.2 Existing research

Currently, cybersecurity is a common conversation topic in the media. Usually every month some company releases restricted statements or informs about some cyberattacks against the government. These studies usually focus on problems, not

on the companies encountering these cyberattacks. The lack of research is one problem.

Helsinki Region Chamber of Commerce (HRCC) has conducted two reviews on the cybersecurity situation of companies in 2015 and 2016. The results of the latest research by Helsinki Region Chamber of Commerce (2018) mainly dealt with hybrid activity targeting. In the research on hybrid activity targeting, every tenth company participating in the survey recounts instances of being targeted with hybrid activity. Hybrid activity occurs most commonly among large companies; every fifth has been targeted with this type of activity. There is a considerable amount of activity targeting companies that can be classified as hybrid influencing. This highlights the need to expand and deepen cooperation between the business community and the authorities and to provide more resources as well. (Helsinki Region Chamber of Commerce 2018)

In chapter 5, the research results are compared to the review on cybersecurity situation published by Helsinki Region Chamber of Commerce in 2016.

2.3 Crime reporting statistics

The statistical service of the police (Helenius 2018) is maintained by Police University College. The statistics are public information and available on request from the statistical service (tilastopalvelu@poliisi.fi). Appendix 1 shows the number of cyber crimes reported to and solved by the police.

The Finnish law defines cyber crimes mainly in Chapter 39 Criminal Law. In addition, Chapters 35, Criminal damage (769/1990) and Chapter 39, Data and communications offences (578/1995) define different kinds of cyber crimes. Below is one example of the Finnish Law: 39. The criminal code of Finland (Ministry of Justice 2015)

Chapter 38, §8 - Computer break-in (368/2015).

> (1) A person who by using an access code that does not belong to him or her or by otherwise breaking a protection unlawfully hacks into an information system where information or data is processed, stored or transmitted electronically or in a corresponding technical manner, or into a separately protected part of such a system, shall be sentenced

> for a computer break-in to a fine or to imprisonment for at most two years.
>
> (2) Also a person who, without hacking into the information system or a part thereof,
>
> > (1) by using a special technical device or
> >
> > (2) otherwise by by-passing the system of protection in a technical manner, by using a vulnerability in the information system or otherwise by evidently fraudulent means unlawfully obtains information or data contained in an information system referred to in subsection 1, shall be sentenced for a computer break-in.
>
> (3) An attempt is punishable.
>
> (4) This section applies only to acts that are not subject to an equally severe or more severe penalty provided elsewhere in the law.

The Finnish law recognizes cyber crimes fairly well. However, there are also deficiencies in the law. For example, identity theft became punishable due to the law reform that came into effect on September 4, 2015. When identity theft was not recognized as a crime, the police was powerless. The new military intelligence law is also being reformed, which will grant the authorities more extensive rights to supervise and react to modern cyberthreats.

According to the statistics, cyber crimes are reported to the police every year. The number of occurrences varies from single to hundreds of reports. Table 1 (Helenius 2018) presents the number of reported and solved cyber crimes in the selected years. The figures clearly highlight that the number of solved cyber crimes is relatively small, as solving these crimes is always challenging. Detailed statistics on cyber crimes can be found in Appendix 1.

Table 1. Finnish Police crime report statistics on data and communications offences

	Notified 2016	Solved 2016	Notified 2017	Solved 2017	Notified 01-07 /2018	Solved 01-07 /2018
§3, Message interception	414	143	364	164	200	63
§5, Interference with communications	67	9	62	31	15	2
§7a, Interference in an information system	38	7	24	13	10	1
§8, Computer break-in	409	64	411	49	276	35
§9, Data protection offence	105	566	96	80	68	71
§9a, Identity theft	3 354	937	3 945	1 851	2 153	1 356

In reality, the number of cyber crimes is considerably larger. The problem is the difficulty in detecting security breaches and companies' reluctance to report these breaches to the police. This could be due to the belief that the breaches have a negative influence on the public image of the company. It also needs to be questioned whether the companies believe the police are capable of solving these kinds of crimes.

2.4 Cybersecurity auditing

The Security Committee's (2017) Implementation Programme for Finland's Cyber Security Strategy for 2017–2020 defines in their guide that the cyber security certificate model will be promoted and supported by the means of national action. A limited national cyber security audit with which organizations can ensure that they achieve the minimum security level will be prepared. The strategic guidelines of cyber security preparedness are: *7. Improve the cyber expertise and awareness of all societal actors. 9. Assign cyber security related tasks, service models and common cyber security management standards to the authorities and actors in the business community.* The FINCSC (Finnish Cyber Security Certificate) operating model, built in the Cyber Scheme Pilot in Finland at JAMK (Jyväskylä) University of Applied Sciences is particularly designed for SME cyber security assessment and accreditation and further development.

2.5 Security policy

Limnell & co. (2015, 182) define that the purpose of an information security plan is to identify the risks caused by the actions detailed in the enablement plan and to prepare for them in a suitable way. A security plan has three main parts:

- Situational awareness
- Effective information security management
- Prevention and rapid response

Situational awareness begins by creating a full picture of the company's systems and their links to each other and to the systems outside the company's network. Doing this is not easy, because usually there are quite many systems to inventory. When situational awareness is mastered, effective information security management can be performed. This means estimating risks and costs. For example, by making risk plans, it can be calculated how much money it is profitable to invest in these sections. If the risk is minimal, there is no need for maximum protection. Finally, prevention and rapid response starts. When there is a security breach, there is knowledge of what to do and how to react.

The Finnish Standards Association (2014) defines the policies for information security through control, implementation and how it should be created.

- Control: A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.
- Implementation guidance: At the highest level, organizations should define an "information security policy" which is approved by management and which sets out the organization's approach to managing its information security objectives.
- Information security policies should address requirements created by:
    - business strategy;
    - regulations, legislation and contracts;
    - the current and projected information security threat environment.
- The information security policy should contain statements concerning:
    - definition of information security, objectives and principles to guide all activities relating to information security;
    - assignment of general and specific responsibilities for information security management to defined roles;
    - processes for handling deviations and exceptions

Figure 2 demonstrates the lifecycle with the PDCA model. It is not enough that ~~we~~ policies are made. These also need to be implemented and checkpoints made to ensure that everything works and acts if necessary.

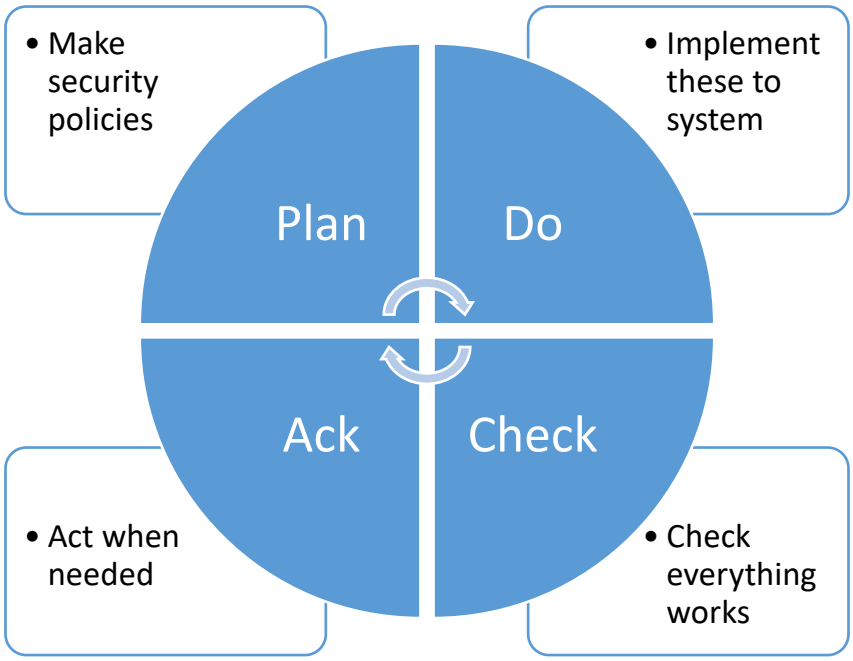


Figure 2. PDCA Model

There are many ways to form security policies, however, the main thing is to follow that everybody obeys these policies. The chain is as strong as its weakest link.

3 Research

This chapter presents the implementation of the research, the topic definition, the purpose of the research and the research questions. In addition, quantitative and qualitative research and research reliabilities and validity are reported. The chapter also presents the target group of the research, the chosen material collection method and the structure of the questionnaire.

3.1 Research objectives

In this thesis, the main goal is to find out what the state of cybersecurity is in Central Finland, what the main problems in cyber security are and how companies react to them. The main research goals are:

- Goal 1: To review the state of cybersecurity in Central Finland.
- Goal 2: To find out how the situation in cybersecurity has changed from 2016 to 2018.

3.2 Research method

The research method in this survey is mainly quantitative since the majority of the questions are made with Likert and are in check box format. There are some open-ended questions to define matters/issues? somewhat more; however, the main focus is on the quantitative analysis of the received data.

3.3 Qualitative and Quantitative research methods

Qualitative research is a method for understanding the phenomenon that is being studied. Edgar & Manz (2017) define this methods as follows. Qualitative research includes collection and analysis of descriptive data. Research involving humans often includes information about their emotional state and social characteristics. Qualitative data can be categorized and sometimes ordered but does not provide the ability to mathematically quantify the data. (Edgar & Manz 2017, 103)

Quantitative research refers to studies that often use statistical methods. Methods for collecting quantitative research material can be, for example, interviews or surveys. Edgar & Manz (2017) define these methods accordingly. Quantitative research involves the collection and analysis of numerical data. Quantitative research enables the quantification or statistical exploration and explanation of data. Quantitative provides the most flexibility in analysis and should be sought above qualitative when possible. (Edgar & Manz 2017, 103)

3.4 Survey population and sampling

The participants for the company survey have been selected randomly from the small and medium enterprises located in Central Finland. The survey was sent to the same target group on three consecutive years. Each year the survey included, however, some minimal changes. If the company had ceased to operate, new companies were chosen to replace these. Through the survey it was studied how the companies have prepared themselves for possible cyberthreats and whether the company had faced these kinds of threats.

Table 2 presents the answers received through the survey. The invitation to participate in the survey was emailed to the companies via the survey system. In addition to this, the survey was marketed in the newsletter of the Federation of Central Finnish Entrepreneurs (Keski-Suomen Yrittäjät) and of the Central Finland Chamber of Commerce.

Table 2. The answers, invitations and response rate

Year	Received answers	Sent invitations	Response rate
2016	201	2298	~8%
2017	101	2276	~4%
2018	78	2299	~3%

The invitation to the survey was sent in the spring, and the survey was closed at the beginning of the summer. Most answers were received in the spring and towards the summer the activity in answering the survey decreased.

3.5 Making the questionnaire

The first version of this survey was made at the beginning of the year 2016. At that time, the survey included two perspectives: the company and the educational institution. This was due to the fact that the view points of the companies on educational issues were also of great interest in the research. In the spring of 2017, the survey was republished with slight alterations by excluding questions related to

education and specifying some follow-up questions. The latest survey was conducted in the spring of 2018, which completed the survey covering three different years.

42 per cent of the questions were identical in all the three surveys, 37 per cent of the questions were supplemented with additional alternative answers and entirely new questions constituted 21 per cent of the questionnaire. The majority of these changes were made into the survey conducted in 2017. Appendix 2 presents the structure of the questionnaire and shows how the questions have been reformulated and supplemented from year to year.

In the previous years the feedback from the survey included reports on some questions being too sensitive and thus unanswerable (e.g. Do you believe that your organization will be able to detect cyberattacks?). It can also be assumed that some companies did not want to answer this survey because of the sensitivity of the questions. This is the reason why an alternative answer “I don't want to answer this question” was added into some questions in the last survey.

Figure 3 shows the survey structure. The survey was made on a survey program (based on a webpage). In Figure 1, the box surrounding the question numbers states which questions were simultaneously visible to the user. All these questions can be found in Appendix 2.

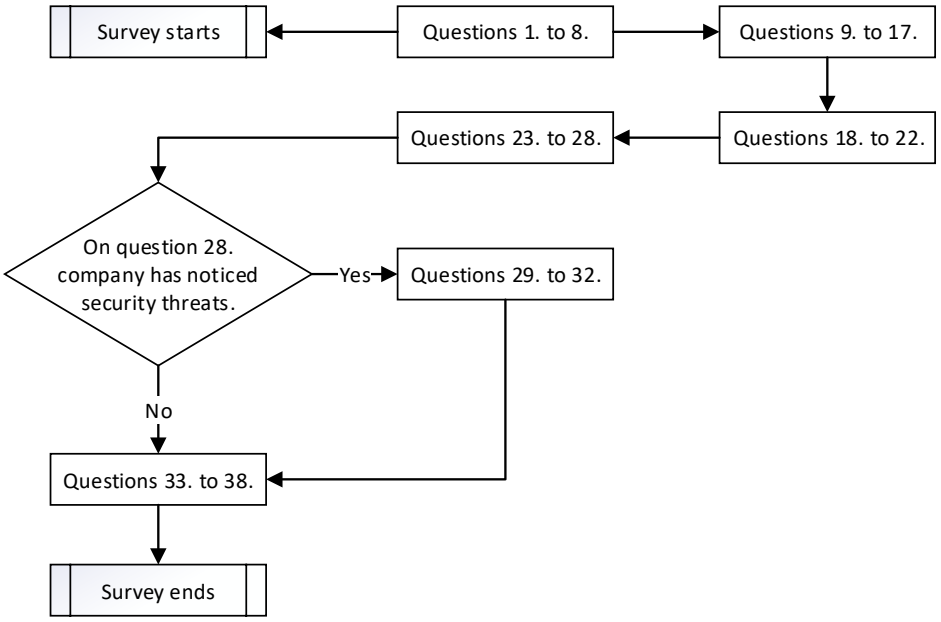


Figure 3. Survey structure

Since there were plenty of questions, they were grouped into six theme groups. These groups are described below.

Background information (Question 1. – Question 8.). These details were mainly background information such as the company name, number of employees, what kind of business the company does and where. The purpose of these questions was to categorize the companies taking part in the survey.

Observations on security (Question 9. – Question 17.). The purpose of these questions was to find out what devices the companies use on internet connections, whether the users use their own equipment, whether there is a security policy and whether the company controlled how the user follows these guidelines. There were also questions on how the company's security issues are resourced.

Attitudes (Question 18. – Question 22.). The questions on attitudes were mostly opinion questions on the Likert scale, e.g. how important is securing different parts of the company and which security issues concern the company most. There were also questions on what obstacles there are in making the business secure and what consequences the companies are afraid of.

Beliefs (Question 23. – Question 27.). These questions were mainly related to beliefs and preparedness (e.g. Do you believe that your organization will be able to detect cyberattacks?).

Actual threats (Question 28. – Question 32.). The questions in this section were probably the hardest questions to answer honestly, because the section included questions such as 'what kind security threats have occurred in your company'. This part is also the most interesting part because there was a question on whether the company notified the police or the customers on the security breach.

Education and needs (Question 33. – Question 38.). This part of the questionnaire was focused on training and the need for instructions on how to react in security issues. There was also a question whether the company follows FICORA's instructions and warnings.

3.6 Data collection and analysis

Data in this survey was collected by distributing unique links to the survey to the participants by email, and the software that was used recorded the answers for the researcher. The data were collected every spring from 2016 to2018.

The programs used for recording the answers were Digium Enterprise (2016, 2017) and Webpropol (2018). The program had to be replaced during the research as the license expired.

The data were analysed on SPSS statistics program (version 23). In the analysis, the percentages of the answers were used to calculate mean values and these two together were used to draw conclusions from the data. The general question of each topic was also compared to the more detailed ones to see if there was much difference and if so, where would the difference result from.

Furthermore, the data were also processed from the perspectives of correlations and cross tabulation. In cross tabulation the interdependence of two variables is studied and the distribution of different variables is compared with each other. The correlation matrix uses a correlation coefficient and its significance test to observe the linear dependence of the variables on the interval and ratio scale. Pearson's correlation coefficient was used to analyze the results of the survey, as it fit the variables on the ordinal scale. The correlation coefficient is between [-1,1] and the correlation is the stronger the further the coefficient is from zero. Huizingh (2007, 290) defines that correlation analysis provides information about the relationship between two variables. The analysis shows both the strength of the relation and its direction (positive or negative). Is there a relationship between age and the amount spent on tennis wear? Do people who play more often spend more money on court rental? Correlation analysis answers such questions. A higher correlation coefficient means a stronger relationship between two variables.

How to read correlation values

SPSS statistic program enables data processing. There are many ways to analyse data and calculating correlation values is one way to conduct statistics, for example

Pearsson correlation. The r value indicates the strength and direction (±) of the correlation. Bigger is better. The p value stands for the probability that one would see an r value of this size just by chance. Smaller is better.

Table 2 shows an example of this. It can be seen that the Pearson correlation coefficient, r, is 0.629, and that it is statistically significant (p = 0.000). The small n marks the sampling number.

A Pearson correlation was run to determine the relationship between the questions 'Has your organization been targeted by a cyber/information leak without anyone knowing about it' and 'Will your organization be subjected to a cyberattack in the next year'. There was a strong, positive correlation between these pretensions, which was statistically significant (r = .629, n = 78, p = .000).

Table 3. Example correlation table

Q27. How likely do you think that		Your organization has been targeted by a cyber/information leak without anyone knowing about it?	Your organization will be subjected to a cyberattack in the next year?
Your organization has been targeted by a cyber/information leak without anyone knowing about it?	Pearson Correlation	1	
	Sig. (2-tailed)		
	N	78	
Your organization will be subjected to a cyberattack in the next year?	Pearson Correlation	.629**	1
	Sig. (2-tailed)	0.000	
	N	78	78
**. Correlation is significant at the 0.01 level (2-tailed).			

The correlation analysis can be found in Appendices 4 - 16. In the table the questions with statistically significant correlation (at least 1% significance level) have been marked with two asterisks and the questions the correlation of which is somewhat significant (at least 5 % significance level) by one asterisk.

- *. Correlation is significant at the 0.05 level (2-tailed).
- **. Correlation is significant at the 0.01 level (2-tailed).

To make the tables easy to read, they have been color coded. All statistically significant (**. Correlation is significant at the 0.01 level (2-tailed)) have been marked

with a yellow color. The parts where Pearsson's correlation value exceeds 0,5 have been marked with a green color.

3.7 Validity and reliability

The key concepts in evaluating the reliability of the study are reliability and validity. Reliability indicates whether the measurement results are reproducible. Hayes (2008) explains reliability with a simple measurement example. A ruler could be used to measure the length of one particular part. The part could be measured five times, obtaining five scores, even though the part can be characterized by one true length, one would expect the five scores to be slightly different from each other. The deviation could be due to various random factors in the measurement process, such as variations in the ruler with each measurement or change in ruler length with each measurement. To the extent that random factors are introduced into the measurement process, any one score obtained may not reliably reflect the true score. (Hayes 2008, 35)

When developing a questionnaire that assesses customer perception of the quality of the service or product, one wants to be sure that the measurements are free from random error. That is, one wants to be sure the true underlying level of perception of quality or satisfaction is accurately reflected in the questionnaire score. When a random error is introduced into measurement, the observed score is less reliable in estimating the true underlying score. Errors of measurement are examined under the context of reliability. (Hayes 2008, 35)

As the results were examined, a mistake was detected in question 14. Which of the following things are covered in your company's security policy? In the years 2016 and 2017 this question was only visible to the respondents who reported having a cybersecurity plan in use in their company. In the last questionnaire in 2018 this modification was forgotten which resulted in this question being visible to all respondents. The problem was caused by the change in the survey platform. The questions being the same, this problem was solved with the help of the statistics

program by restricting the visibility of question 14 only to those who in the previous question had stated having a cybersecurity plan in use in their company.

4 Survey results and analysis

During the three years of the research, altogether 380 answers were collected as the survey data (2016 N=201, 2017 N=101, 2018 N=78). In the first phase of the survey, the response rate was approximately 7 percent, whereas towards the end of the survey it fell to about 2 percent. The survey was sent to around 2,300 companies in Central Finland in the spring. Some of the companies had ceased to operate, and thus, about 100 to 200 new companies were selected to participate in the survey each year. The main goal of the survey was to map the situation and needs of companies in Central Finland in relation to cybersecurity.

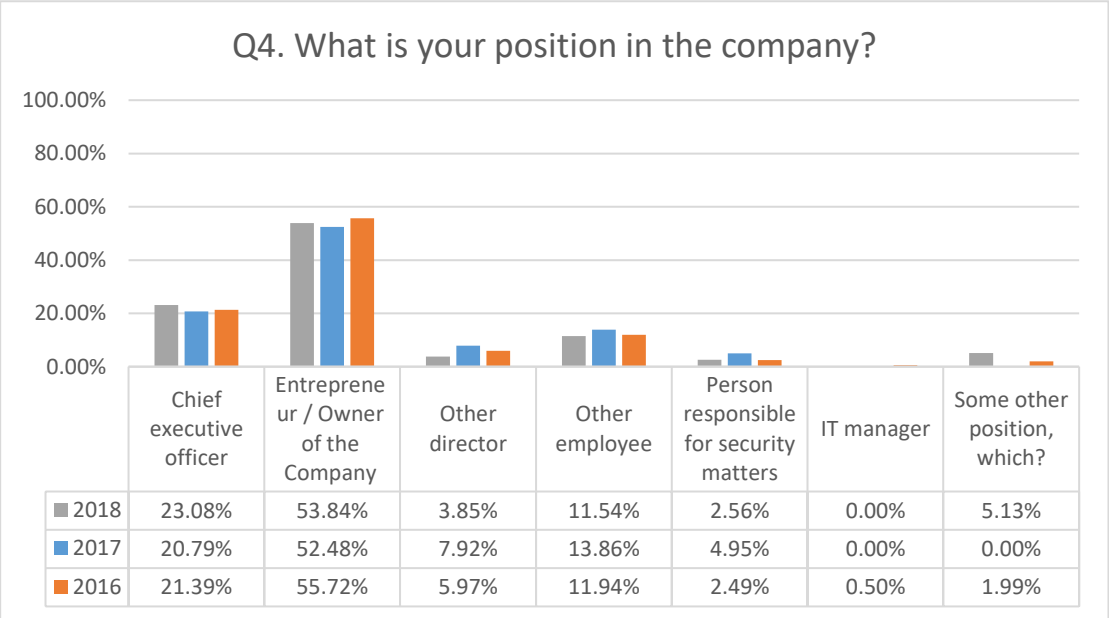
In questions 1. and 2. the participants were asked to (voluntarily) state the name and city of their company. These questions were intentionally marked as optional, as requiring an answer to these questions might have affected the results given by the following questions. It was assumed that most companies wish to answer the questionnaire anonymously. This assumption, however, was not true as more than 55 percent of the answerers filled in the questionnaire using their name. Most of the answers came from the area of Jyväskylä, however, also companies from smaller towns participated. Information about the participants will not be published as it is not relevant for the study.

4.1 Background information (Q1-Q8)

In question 2 it was asked whether the respondent was a member in an organization aimed at entrepreneurs. In the first year, 78 per cent of the answerers belonged to an organization whereas in the last year the rate dropped to 55 per cent. The average of all the three years was 65 per cent (average) In the timeline of three years, 42 per cent of the participants reported belonging to Suomen Yrittäjät (an organization for Finnish entrepreneurs). 10 to 14 per cent of the participants were

members of the Chamber of Commerce, with the average of 12 per cent within the three years.

In question 4 the purpose was to find out the respondents' position in the company. Figure 2 described the position of the respondent in the company. More than half of the respondents stated being the owner of the company (avg. 54%). This can be explained by the fact that more than half of the participants in the survey were small companies employing 1 to 4 persons (avg. 55%). All in all, 76 per cent of the respondents (avg.) were business executives (i.e. chief executive officer, entrepreneur, owner). People in charge of the information security of the company answered the questionnaire in 3.3 per cent (avg.) of the cases.



	Chief executive officer	Entrepreneur / Owner of the Company	Other director	Other employee	Person responsible for security matters	IT manager	Some other position, which?
2018	23.08%	53.84%	3.85%	11.54%	2.56%	0.00%	5.13%
2017	20.79%	52.48%	7.92%	13.86%	4.95%	0.00%	0.00%
2016	21.39%	55.72%	5.97%	11.94%	2.49%	0.50%	1.99%

Figure 4. Question 4. What is your position in the company?

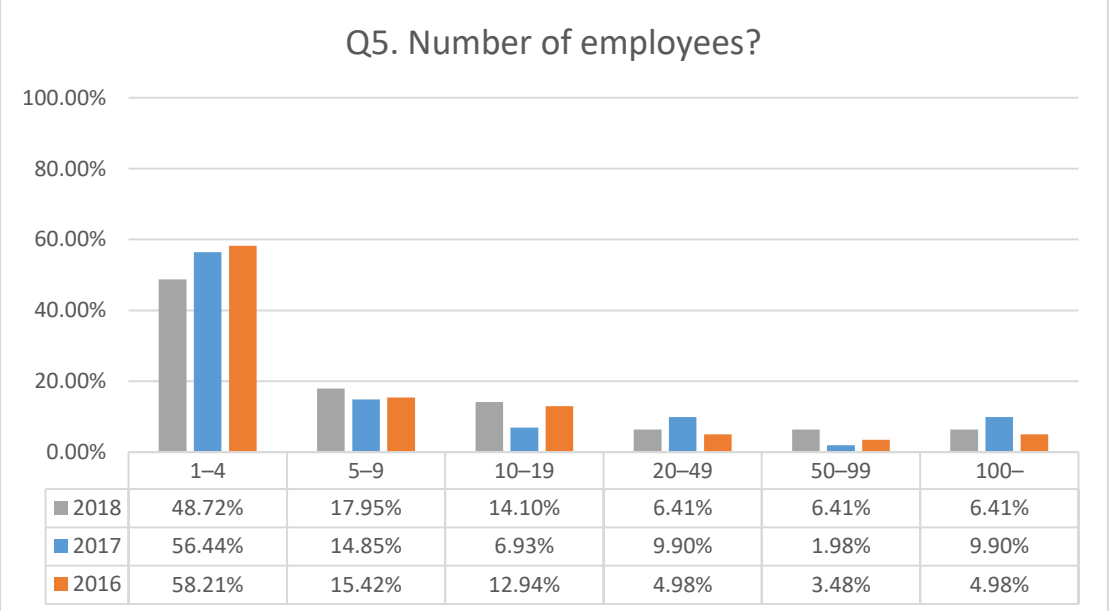
The employee classification has been compiled based on the classification used by Statistics Finland (size categories of the personnel, HS1). Most of the participating companies were small businesses employing 1 to 4 persons. Figure 5. presents the sizes of the companies. Microenterprises (1 to 4 persons) account for 55 percent (avg.) of the respondents. Regarding the research, this was a good sample, since the starting point for the survey was to find out what kind of challenges microenterprises

face when dealing with cybersecurity. It is the microenterprises that suffer from cybersecurity issues more often than the larger companies that have their own IT management responsible for these issues.

According to Suomen Yrittäjät, companies employing fewer than 10 persons are defined as microenterprises and companies employing 10 or more people are called small enterprises. This classification results in the following samples.

- In 2016, companies employing less than 10 people accounted for 73 percent (148 companies) and companies employing more than 10 people 27 percent (53 companies) of the participants.
- In 2017, companies employing less than 10 people accounted for 71 percent (72) and more than 10 people 29 percent (29).
- In 2018, companies employing less than 10 people accounted for 67 percent (52) and more than 10 people 33 percent (26).

The sample was evenly distributed every year and thus, the results can be considered comparable.

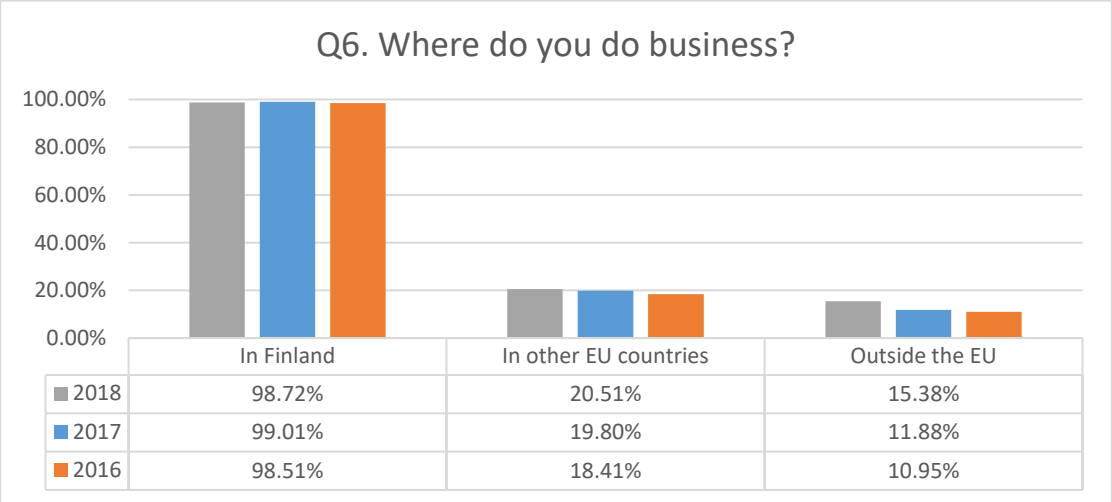


	1–4	5–9	10–19	20–49	50–99	100–
2018	48.72%	17.95%	14.10%	6.41%	6.41%	6.41%
2017	56.44%	14.85%	6.93%	9.90%	1.98%	9.90%
2016	58.21%	15.42%	12.94%	4.98%	3.48%	4.98%

Figure 5. Question 5. Number of employees?

The majority of the participants (Figure 6) operates on the Finnish market (avg. 99%). Some of the participants do business also in other EU countries (avg. 20%) and outside the EU (avg. 13%). Some companies operate in all the areas mentioned

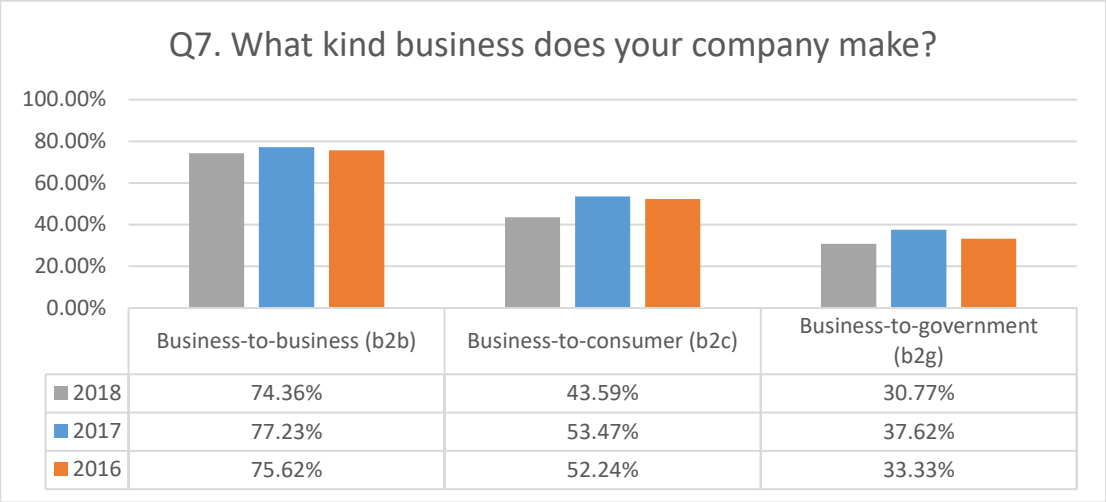
above. Nowadays cybersecurity has become an important factor in doing business. Companies choose secure companies as their business partners. Therefore, cybersecurity auditing will be increasing in the future.



	In Finland	In other EU countries	Outside the EU
2018	98.72%	20.51%	15.38%
2017	99.01%	19.80%	11.88%
2016	98.51%	18.41%	10.95%

Figure 6. Question 6. Where do you do business?

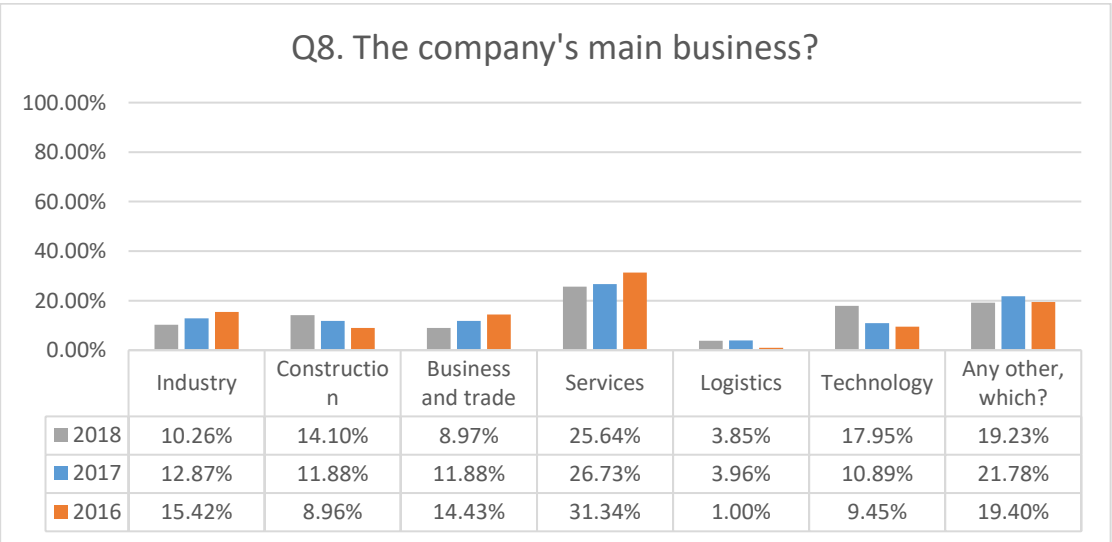
The types of businesses the companies operate in are fairly evenly distributed on every area as described in Figure 7. Business-to-business arises as the largest area of business (avg. 76%). The proportion of business-to-consumer operations is slightly smaller (avg. 50%) and business-to-government is the area covered the least in the business operation of the companies (avg. 34%). Part of the companies do business in all the areas mentioned above, which is why the combined percentages exceed 100 per cent. Doing business with the public administration accounts for a surprisingly big share of business areas in the survey results.



	Business-to-business (b2b)	Business-to-consumer (b2c)	Business-to-government (b2g)
2018	74.36%	43.59%	30.77%
2017	77.23%	53.47%	37.62%
2016	75.62%	52.24%	33.33%

Figure 7. Question 7. What kind business does your company do?

The main business of the participating companies is evenly distributed to all the areas mentioned in the questionnaire (Figure 8). Service is the largest area of business operations (avg. 28%). Other areas of business mentioned in the alternative 'Any other, which?' were public administration, electrical engineering, expert services, consulting, security and accommodation.



	Industry	Construction	Business and trade	Services	Logistics	Technology	Any other, which?
2018	10.26%	14.10%	8.97%	25.64%	3.85%	17.95%	19.23%
2017	12.87%	11.88%	11.88%	26.73%	3.96%	10.89%	21.78%
2016	15.42%	8.96%	14.43%	31.34%	1.00%	9.45%	19.40%

Figure 8. Question 8. The company's main business?

As a summary, the majority of the participants in this survey are small enterprises, whose operations focus on doing business in Finland. They mainly work in the

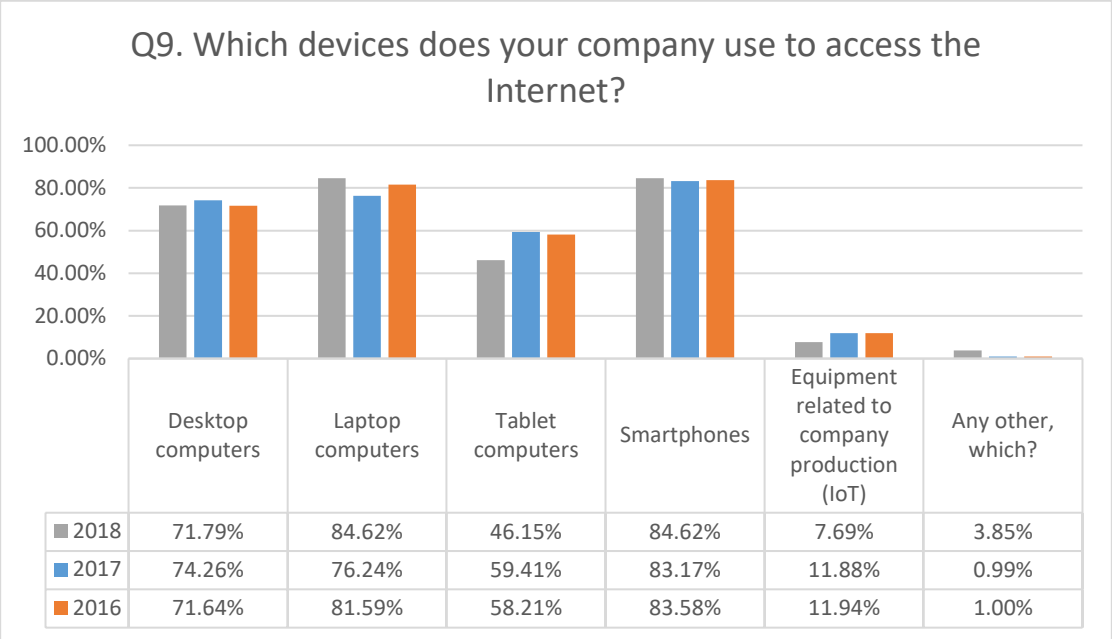
business-to-business and service industry. When comparing the results from the three years of the study, it can be stated that the target group has stayed the same from year to year. Even though the response rate decreased every year, the sampling stayed the same. Therefore, the results from each year are comparable with each other.

4.2 Observing security (Q9-Q17)

Questions 9-17 were set to clarify how the companies take cybersecurity into consideration. This means, for instance, which devices have access to the network and whether the company has guidelines for cybersecurity or whether the forthcoming EU data protection regulation has been paid attention to.

Figure 9 presents the equipment, with which the company is connected to the network. Previously only desktop computers were used to connect to the Internet, however, as technology has advanced also the devices and equipment used have diversified. As shown in Figure 9, companies are active users of smart phones (avg. 84%) in their work today. In addition to this, tablet devices account for as much as 55 per cent (avg.) of all the devices used. These two types of devices pose one of the largest cybersecurity risks to the companies as these devices most often are not protected; in some cases due to the lack of skills needed to perform this. Tablets and smart phones are usually taken along on business trips and connected to the first open wireless network without further consideration on the security of the network. This poses a threat because several user names and passwords have usually been saved in the smart phone applications or in the device itself.

Based on the answers, it can also be stated that the share of laptop computers seems to be increasing and the share of tablet devices decreasing. Previously many workers preferred carrying tablet devices on business trips because of the light weight of the device. However, working on tablet devices proved out to be slow, which led to the increasing use of laptop computers while traveling for work. Other devices mentioned to be used when connecting to the Internet were servers.



	Desktop computers	Laptop computers	Tablet computers	Smartphones	Equipment related to company production (IoT)	Any other, which?
2018	71.79%	84.62%	46.15%	84.62%	7.69%	3.85%
2017	74.26%	76.24%	59.41%	83.17%	11.88%	0.99%
2016	71.64%	81.59%	58.21%	83.58%	11.94%	1.00%

Figure 9. Question 9. Which devices does your company use to access the Internet?

26 per cent (avg.) of the respondents use their own personal devices for work (Figure 10). This can mean for example using their own personal smart phone or tablet computer for reading their company email. The share of personal devices has, however, dropped from the year 2016. The underlying reason for this could be the desire to make a clear distinction between work and freetime.

A personal device always causes a risk situation since it is a new device in the company systems and possibly has no protection. From the perspective of risk management, it is also relevant to notice that the personal device might also be used by family members. Therefore, there is a risk the family members have access to classified materials.

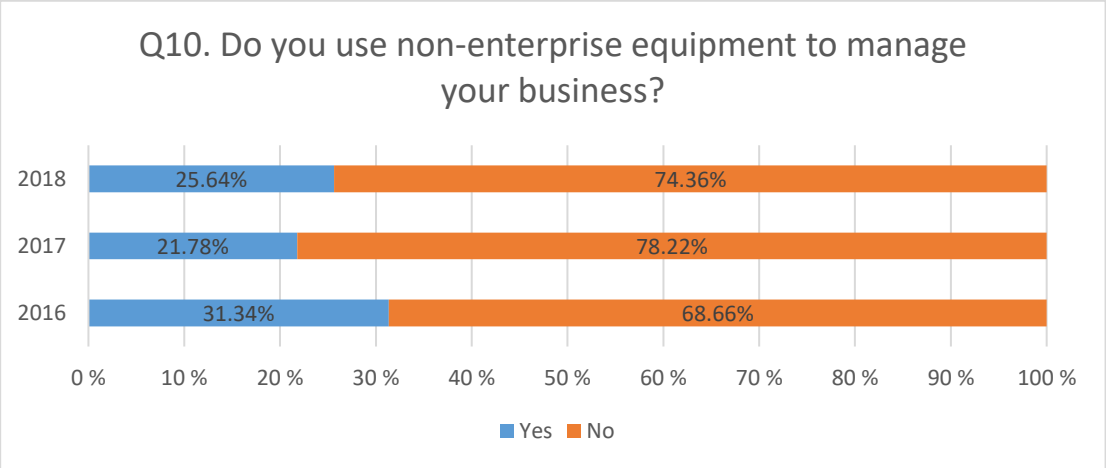


Figure 10. Question 10. Do you use non-enterprise equipment to manage your business?

Cybersecurity guidelines are mostly a company procedure determining, for example, the rules and regulations on what devices can be connected to the company network and on how to react of one suspects a security breach. As shown in Figure 11, 35 per cent (avg.) of the companies had drawn a cybersecurity policy. Compared to the results of the previous year, there has been a positive increase in this area. The companies want to be capable of reacting to cybersecurity issues.

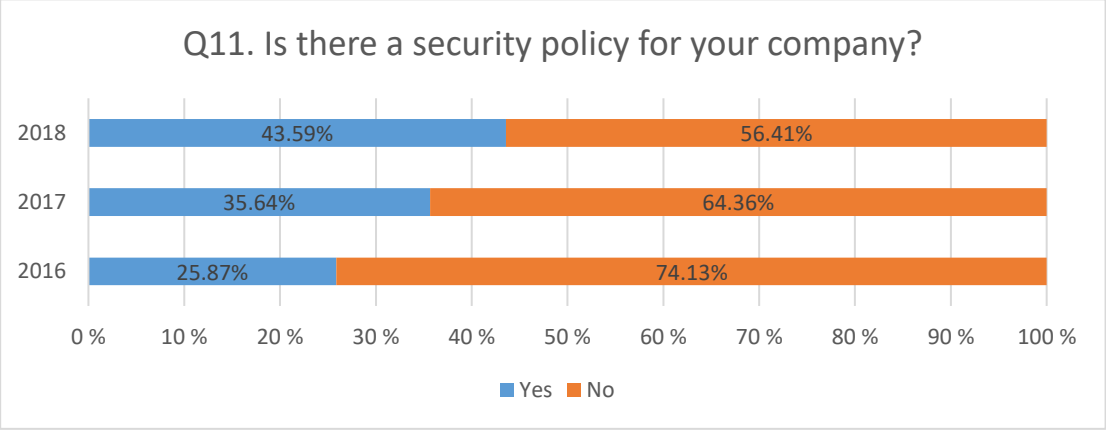


Figure 11. Question 11. Is there a security policy for your company?

The EU data protection regulation was approved of in the spring of 2016. This regulation is going to be implemented after the two-year transition period. The EU data protection regulation affects, in principle, all processing of personal information

in EU countries. According to the guidelines drawn by the Ministry of Finance (2016), this redulation affects information collected of both clients and the personnel of the company. As it is an EU regulation, the sanctions given for violating it are equally extensive. The regulation has set the sanctions to 4 per cent of the company's global turnover.

Only 32 per cent (avg.) of the respondents were aware of the EU data protection regulation (Figure 12). The research question may in this case have misled the respondents because not everyone was able to combine this question with the EU data protection regulation. It is positive, however, to notice the increase in the knowledge of the participants because the awareness increased by 55 per cent after the regulation came into force in 2018. Even though the total is somewhat large, it is still alarmingly small compared to the big picture. The increase in awareness is mostly a result from the media activity and increased education on behalf of the entrepreneur organizations.

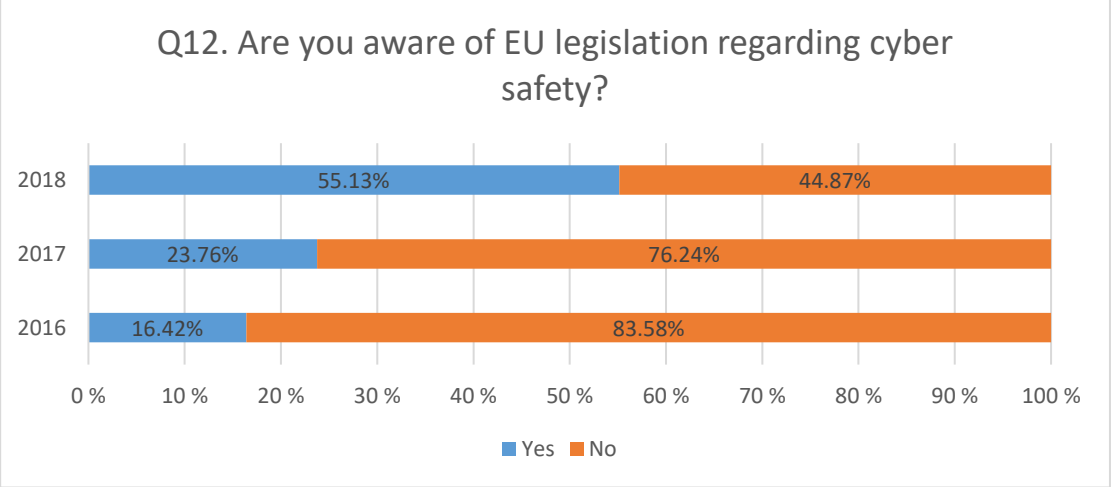


Figure 12. Question 12. Are you aware of the EU legislation regarding cyber safety?

One of the research questions was drawn to ask whether the company supervises if the cybersecurity policy is abided by (Figure 13.). Most companies do supervise this, and yet 21 per cent of the participants reported not to supervise the abiding of the regulation. The underlying reason for this may be ignorance or the fact that the employees are not informed about the policy. Alternatively, it may be thought that

the security policy has been drawn to hinder normal working. The significance of the document might not have been entirely understood. In this question only 'yes' answers to Question 11 have been taken into account.

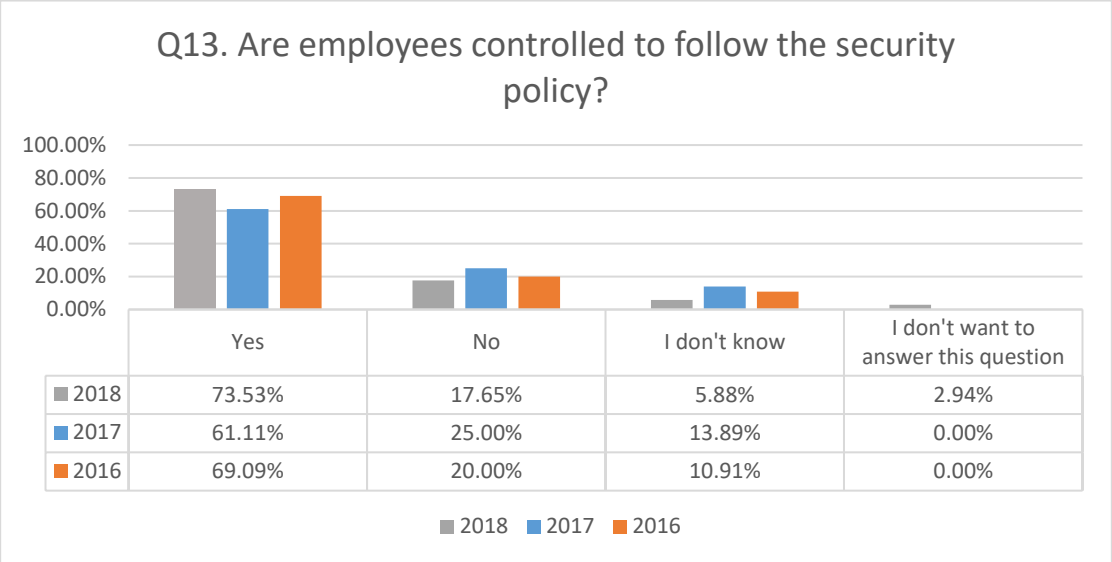


Figure 13. Question 13. Are employees controlled to follow the security policy?

Figure 14. presents the areas which are dealt within the company security policy. This question takes into account the 'yes' answers to Question 11.

Based on the results, it can be stated that the companies follow the guidelines to drawing traditional security policies. All the areas of the security policy got the response rate of 50 per cent in this question. Additional areas involving the company security policy were oral instructions and agreed practices.

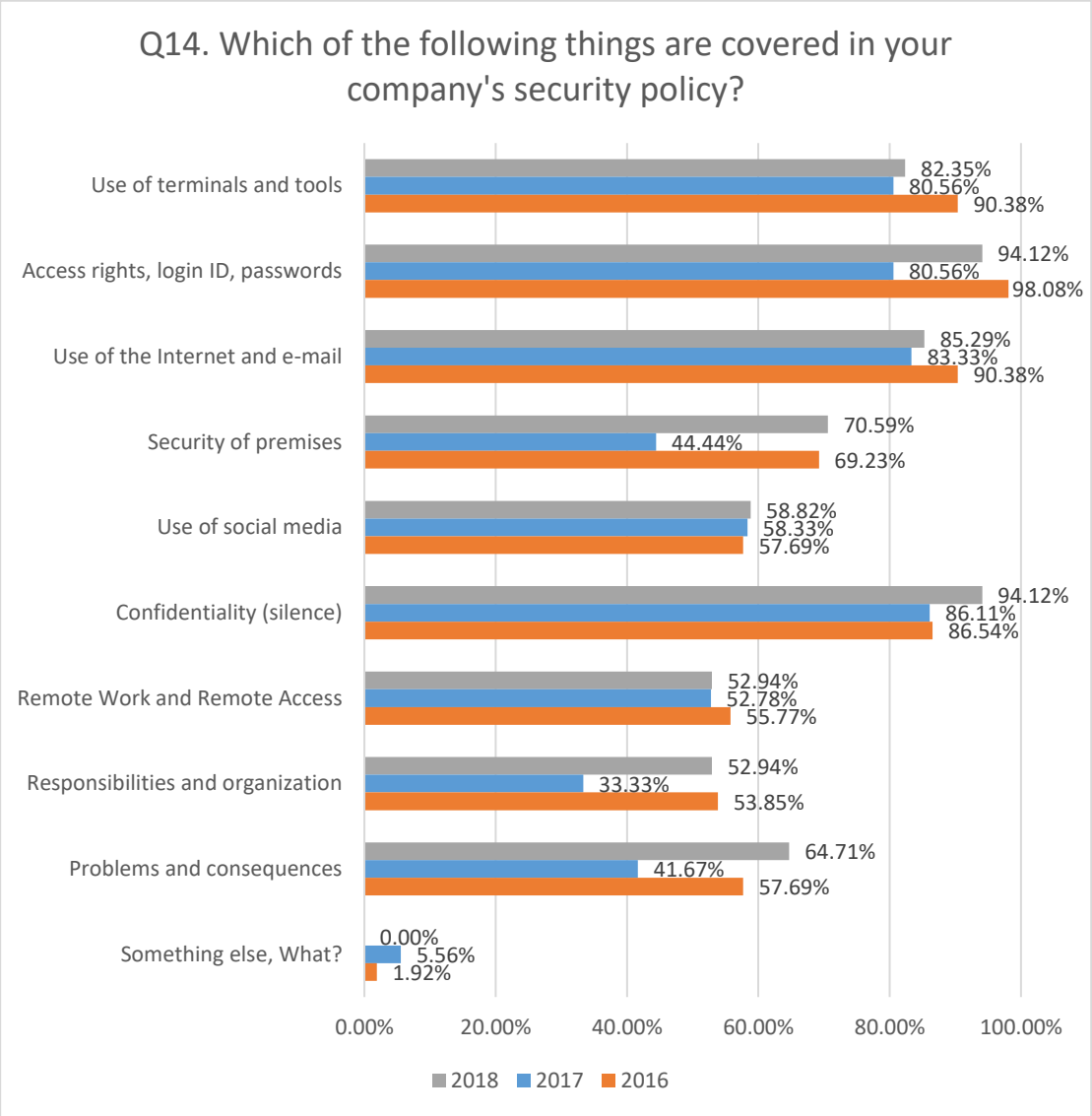
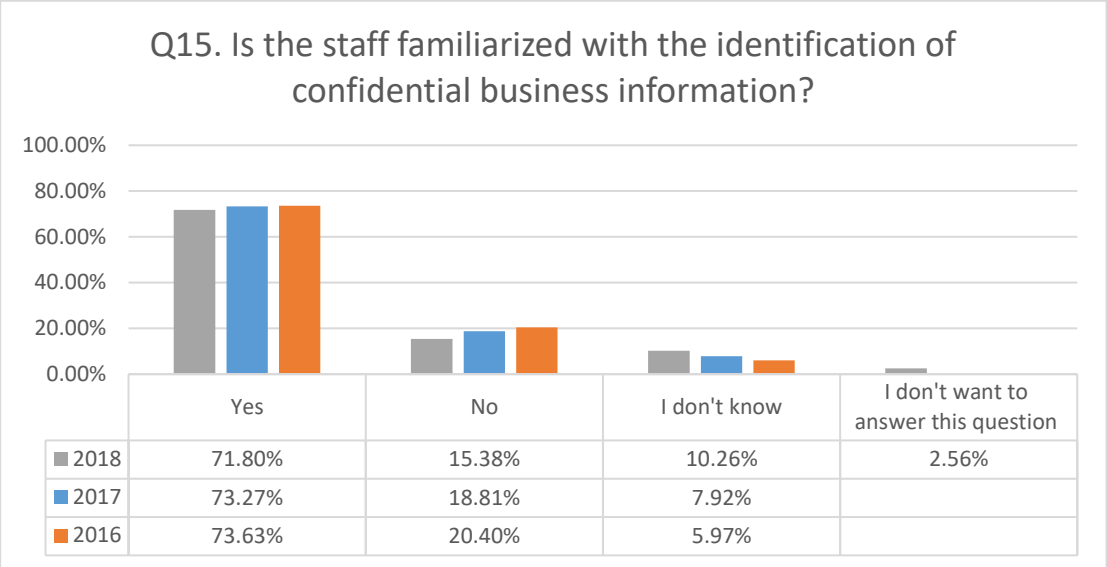


Figure 14. Question 14. Which of the following things are covered in your company's security policy?

While conducting the study, the general assumption was that small enterprises did not have a defined security policy. This was the reason behind the desire to find out whether the personnel had been advised to recognize confidential issues. As Figure 15 indicates, the majority of employees had been taught to recognize confidential issues, however, 18 perc ent (avg.) of the respondents did not know which issues were classified information. When answering Question 11, 35 per cent of the participants reported the company having a security policy. In relation to Question 11. it can be seen that confidentiality was considerably better taken care of.

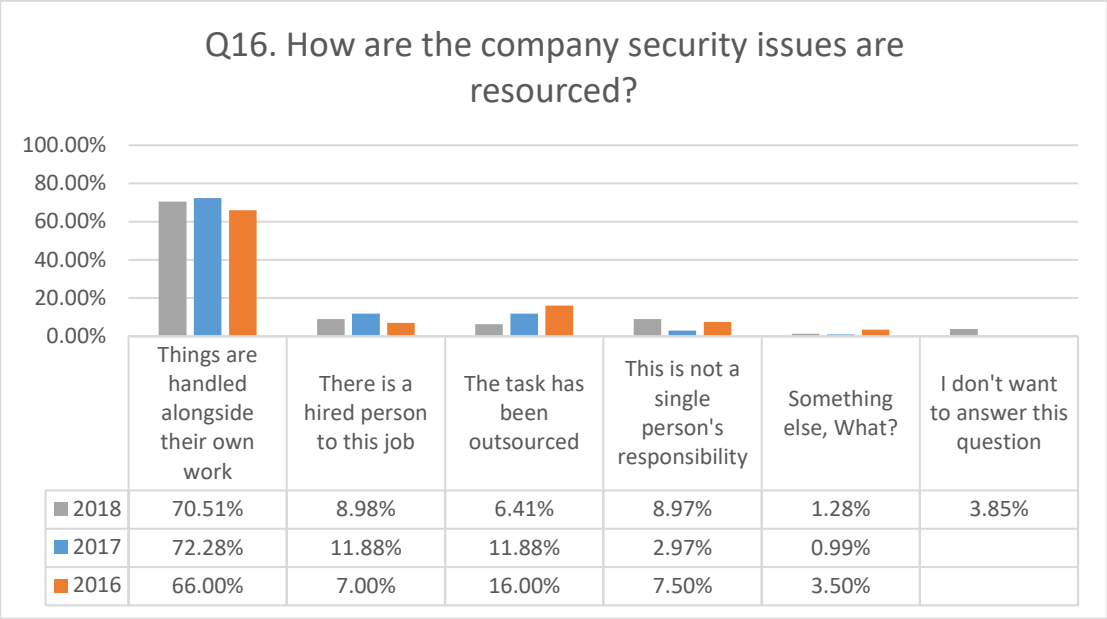


	Yes	No	I don't know	I don't want to answer this question
2018	71.80%	15.38%	10.26%	2.56%
2017	73.27%	18.81%	7.92%	
2016	73.63%	20.40%	5.97%	

Figure 15. Question 15. Is the staff familiarized with the identification of confidential business information?

As Figure 16 shows, 70 per cent (avg.) of the respondents reported taking care of the company security issues in addition to other duties. Most participants are small enterprises or entrepreneurs, which means that the company does not have the chance to hire a separate employee to take care of the cybersecurity issues and needs to be able to take care of all this by themselves. As the size of the company grows, cybersecurity will also be more resourced. Bigger companies have a hired employee responsible for cybersecurity issues. It can also be interpreted that bigger companies have their own IT management to take care of the functionality of devices and systems. Other actors helping with IT management were spouses.

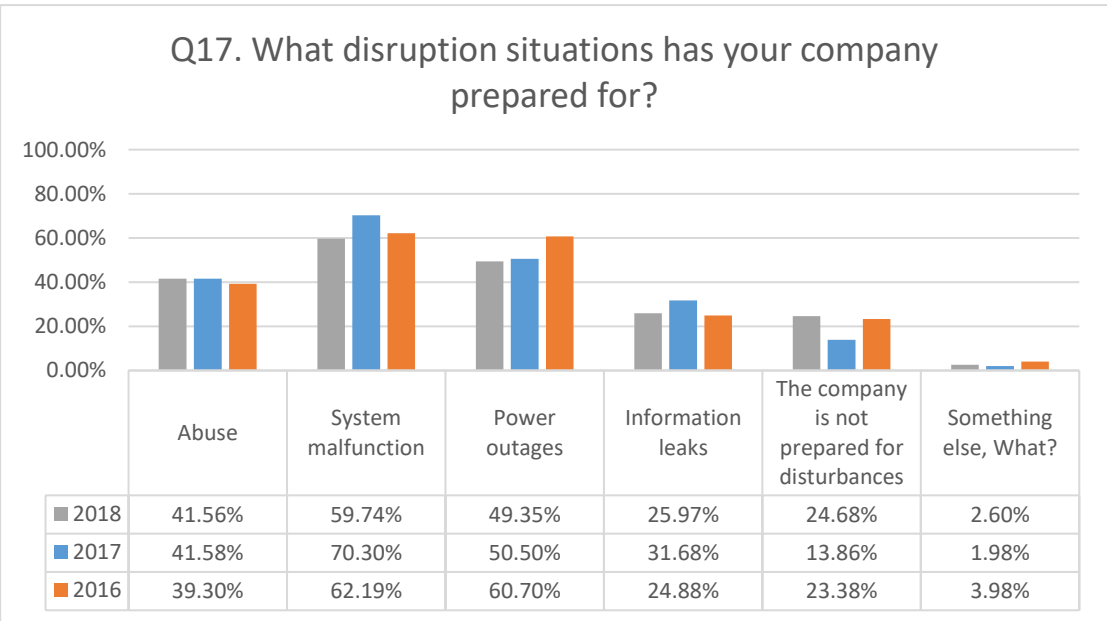
If the results are compared to the 2018 target group and only companies with security policies are regarded, the results are surprising. 67 per cent of the participants report handling things alongside their own work. Only 18 per cent stated that the company has a hire person to do this job.



	Things are handled alongside their own work	There is a hired person to this job	The task has been outsourced	This is not a single person's responsibility	Something else, What?	I don't want to answer this question
2018	70.51%	8.98%	6.41%	8.97%	1.28%	3.85%
2017	72.28%	11.88%	11.88%	2.97%	0.99%	
2016	66.00%	7.00%	16.00%	7.50%	3.50%	

Figure 16. Question 16. How are the company security issues resourced?

The results in Figure 17 show that the companies are prepared for system malfunctions and power outages. These are traditional disruptions that occur most often, but cybersecurity has been forgotten. 21 per cent of the participants are not prepared for disruptions. Other problems mentioned in the answers were thefts.



	Abuse	System malfunction	Power outages	Information leaks	The company is not prepared for disturbances	Something else, What?
2018	41.56%	59.74%	49.35%	25.97%	24.68%	2.60%
2017	41.58%	70.30%	50.50%	31.68%	13.86%	1.98%
2016	39.30%	62.19%	60.70%	24.88%	23.38%	3.98%

Figure 17. Question 17. What disruption situations has your company prepared for?

In conclusion, it can be stated that taking cybersecurity is at a reasonable level; however, there are still challenges. The share of smart phones is on a slight increase and this is a challenging area when it comes to protection. These devices do not always have installed security software and another problem involves the applications installed on the phone. Companies often look for applications that can help them make their business more effective, but they do not stop to consider the security of these apps. The share of personal devices is fairly small but yet a risk factor to the company in case the device is used in the freetime.

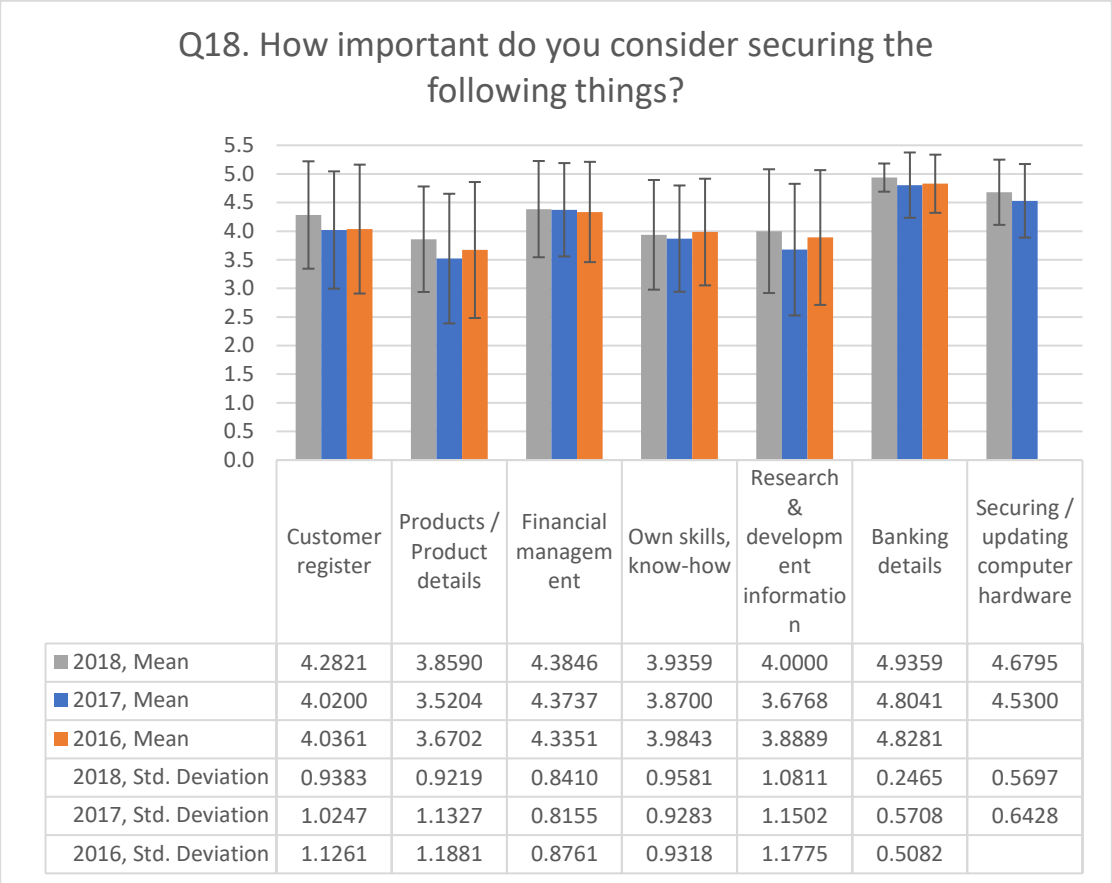
The number of companies having a security policy was surprisingly high when considering this included small enterprises with limited resources. This is also the reason why cybersecurity issues are mostly handled alongside the regular work-related duties. The cybersecurity policy is luckily not only a document in the company as following the company guidelines is also controlled. Recognizing confidential data also arose as a key issue in the survey.

4.3 Attitudes (Q18-Q22)

It all comes down to the attitudes and how the company desires to act. It is up to the company to decide whether they want to react to cybersecurity issues and consider them important. The company's attitude to their employees is important and they can be regarded as threats or possibilities. Breaking into the company network often starts by exploiting single employee's actions. The workers should understand that a cyberattack is not always a malware accessing the company network via the Internet but can also come via a phone call or a insignificant email. For example, emailed links and attachments containing a malware have also often been warned about. Yet, people open these messages without hesitation. Chapter 4.7 deals with the correlation of attitudes.

Most respondents (Figure 18) considered it to be most important to protect bank records, financial management and customer registers and to secure and update computer hardware. Traditionally, the physical goods of the company are regarded as important, however, it needs to be discussed whether the products of the

company do not form an equally important part. If there is no product, there is no turnover. When the figures are compared to the previous years, the outlines are the same. This section included a new question on updating and securing hardware and the results attracted large attention when comparing the company attitudes. Companies have recently started to understand to importance of installing updates.

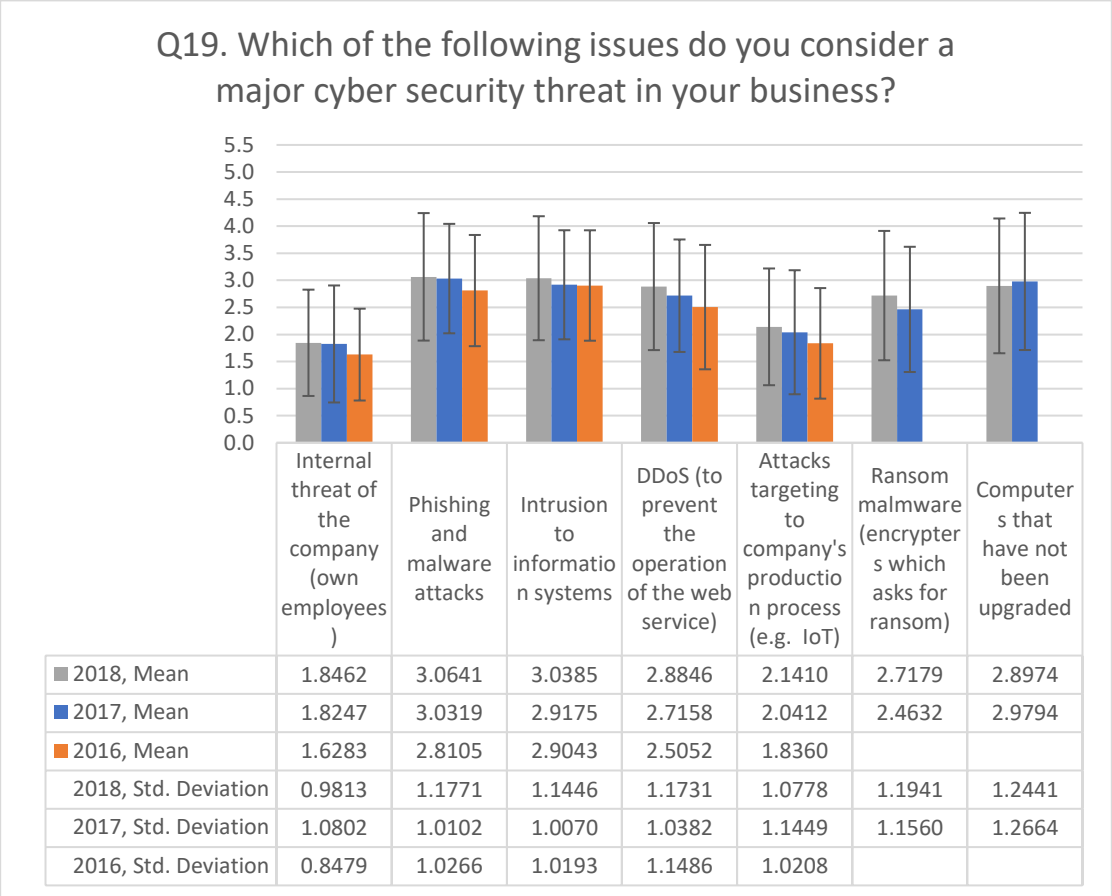


	Customer register	Products / Product details	Financial management	Own skills, know-how	Research & development information	Banking details	Securing / updating computer hardware
2018, Mean	4.2821	3.8590	4.3846	3.9359	4.0000	4.9359	4.6795
2017, Mean	4.0200	3.5204	4.3737	3.8700	3.6768	4.8041	4.5300
2016, Mean	4.0361	3.6702	4.3351	3.9843	3.8889	4.8281	
2018, Std. Deviation	0.9383	0.9219	0.8410	0.9581	1.0811	0.2465	0.5697
2017, Std. Deviation	1.0247	1.1327	0.8155	0.9283	1.1502	0.5708	0.6428
2016, Std. Deviation	1.1261	1.1881	0.8761	0.9318	1.1775	0.5082	

Figure 18. Question 18. How important do you consider securing the following things?

Helsinki Region Chamber of Commerce (2016) published a study on the cyberthreats companies face in 2016 (‘Yrityksiin kohdistuvat kyberuhat 2016’). In this study, the employees of the company were considered a great internal threat. However, as Figure 19 shows, the employees were no longer regarded as a great threat in this survey. There has either been a change in the attitudes, or the question was misunderstood.

When asked about the opinions on threats, computers that have not been upgraded, phishing, malware and break-ins into the information systems were thought to be the biggest threats. On the other hand, the entry 'attacks targeting the company's production processes' contradicts with the previously mentioned ones. A question arises whether the company is aware of these risks and what they can cause to the company in the worst case scenario.

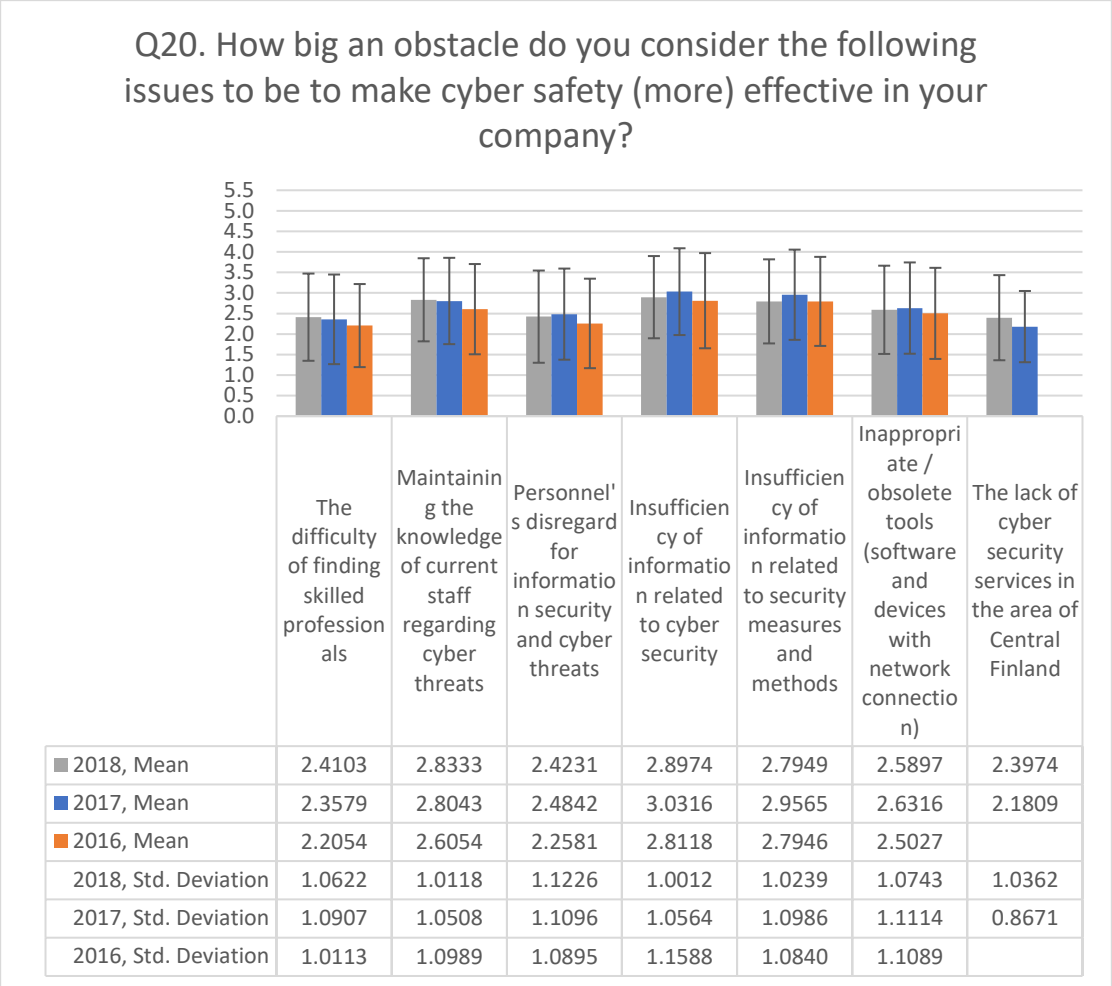


	Internal threat of the company (own employees)	Phishing and malware attacks	Intrusion to information systems	DDoS (to prevent the operation of the web service)	Attacks targeting to company's production process (e.g. IoT)	Ransom malmware (encrypters which asks for ransom)	Computers that have not been upgraded
2018, Mean	1.8462	3.0641	3.0385	2.8846	2.1410	2.7179	2.8974
2017, Mean	1.8247	3.0319	2.9175	2.7158	2.0412	2.4632	2.9794
2016, Mean	1.6283	2.8105	2.9043	2.5052	1.8360		
2018, Std. Deviation	0.9813	1.1771	1.1446	1.1731	1.0778	1.1941	1.2441
2017, Std. Deviation	1.0802	1.0102	1.0070	1.0382	1.1449	1.1560	1.2664
2016, Std. Deviation	0.8479	1.0266	1.0193	1.1486	1.0208		

Figure 19. Question 19. Which of the following issues do you consider a major cyber security threat in your business?

As Figure 20 shows, the companies see no hindrance to improving the company's cybersecurity. A small percentage of the respondents had stated that the lack of knowledge is the biggest obstacle in developing the company's cybersecurity. This contradicts, however, with Figure 22, which presents what the most important areas for developing the company's cybersecurity are. As many as 70 per cent (avg.) stated that the most important area for development is the knowledge about cybersecurity.

'The lack of cyber security services in the area of Central Finland' was added as a new alternative into this section. Based on the answers, the companies feel that there are enough cybersecurity services on offer. Small enterprises can see this part as an extra expense, which is why these services are not very often used yet.

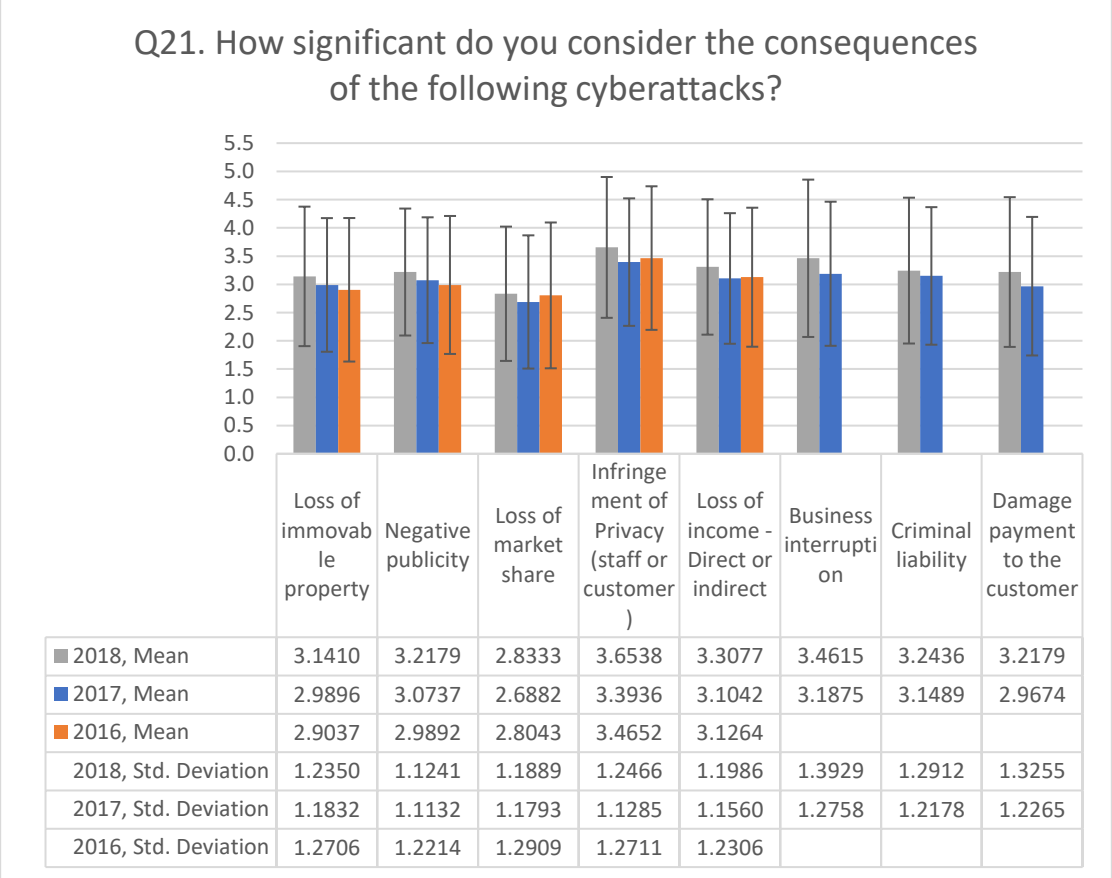


	The difficulty of finding skilled professionals	Maintaining the knowledge of current staff regarding cyber threats	Personnel's disregard for information security and cyber threats	Insufficiency of information related to cyber security	Insufficiency of information related to security measures and methods	Inappropriate / obsolete tools (software and devices with network connection)	The lack of cyber security services in the area of Central Finland
2018, Mean	2.4103	2.8333	2.4231	2.8974	2.7949	2.5897	2.3974
2017, Mean	2.3579	2.8043	2.4842	3.0316	2.9565	2.6316	2.1809
2016, Mean	2.2054	2.6054	2.2581	2.8118	2.7946	2.5027	
2018, Std. Deviation	1.0622	1.0118	1.1226	1.0012	1.0239	1.0743	1.0362
2017, Std. Deviation	1.0907	1.0508	1.1096	1.0564	1.0986	1.1114	0.8671
2016, Std. Deviation	1.0113	1.0989	1.0895	1.1588	1.0840	1.1089	

Figure 20. Question 20. How big an obstacle do you consider the following issues to be to make cyber safety (more) effective in your company?

When asked about the consequences caused by cyberattacks (Figure 21.), the companies considered the most severe consequences to be the infringement of privacy and interruptions in business, i.e. if information on the personnel or the clients ends up in the wrong hands or if there are disruptions in the company operations because of computer problems.

Compared to previous years, the percentages on all the consequences have grown, which can lead to a conclusion that the participants are concerned about these issues. A year ago it seemed like there was a change in the attitudes for example regarding negative publicity. Previously, information leaks were considered to be negative but the more recent survey shows this might not be the case anymore. The companies should think of the consequences if they do not inform the public about the security breaches the company has encountered. The attitudes can also be affected by the fact that there are news reports on security breaches almost weekly.



	Loss of immovable property	Negative publicity	Loss of market share	Infringement of Privacy (staff or customer)	Loss of income - Direct or indirect	Business interruption	Criminal liability	Damage payment to the customer
2018, Mean	3.1410	3.2179	2.8333	3.6538	3.3077	3.4615	3.2436	3.2179
2017, Mean	2.9896	3.0737	2.6882	3.3936	3.1042	3.1875	3.1489	2.9674
2016, Mean	2.9037	2.9892	2.8043	3.4652	3.1264			
2018, Std. Deviation	1.2350	1.1241	1.1889	1.2466	1.1986	1.3929	1.2912	1.3255
2017, Std. Deviation	1.1832	1.1132	1.1793	1.1285	1.1560	1.2758	1.2178	1.2265
2016, Std. Deviation	1.2706	1.2214	1.2909	1.2711	1.2306			

Figure 21. Question 21. How significant do you consider the consequences of the following cyberattacks?

The most important areas for development (Figure 21.) are the knowledge of information security (avg. 70%) and creating backups (av 47%) as well as improving the competence of the personnel (avg. 47%).

In comparison to the previous years, no significant change has arisen. Only the rate related to creating backup systems had decreased a bit. Technology ages fast and most backup systems create only extra costs to the company.

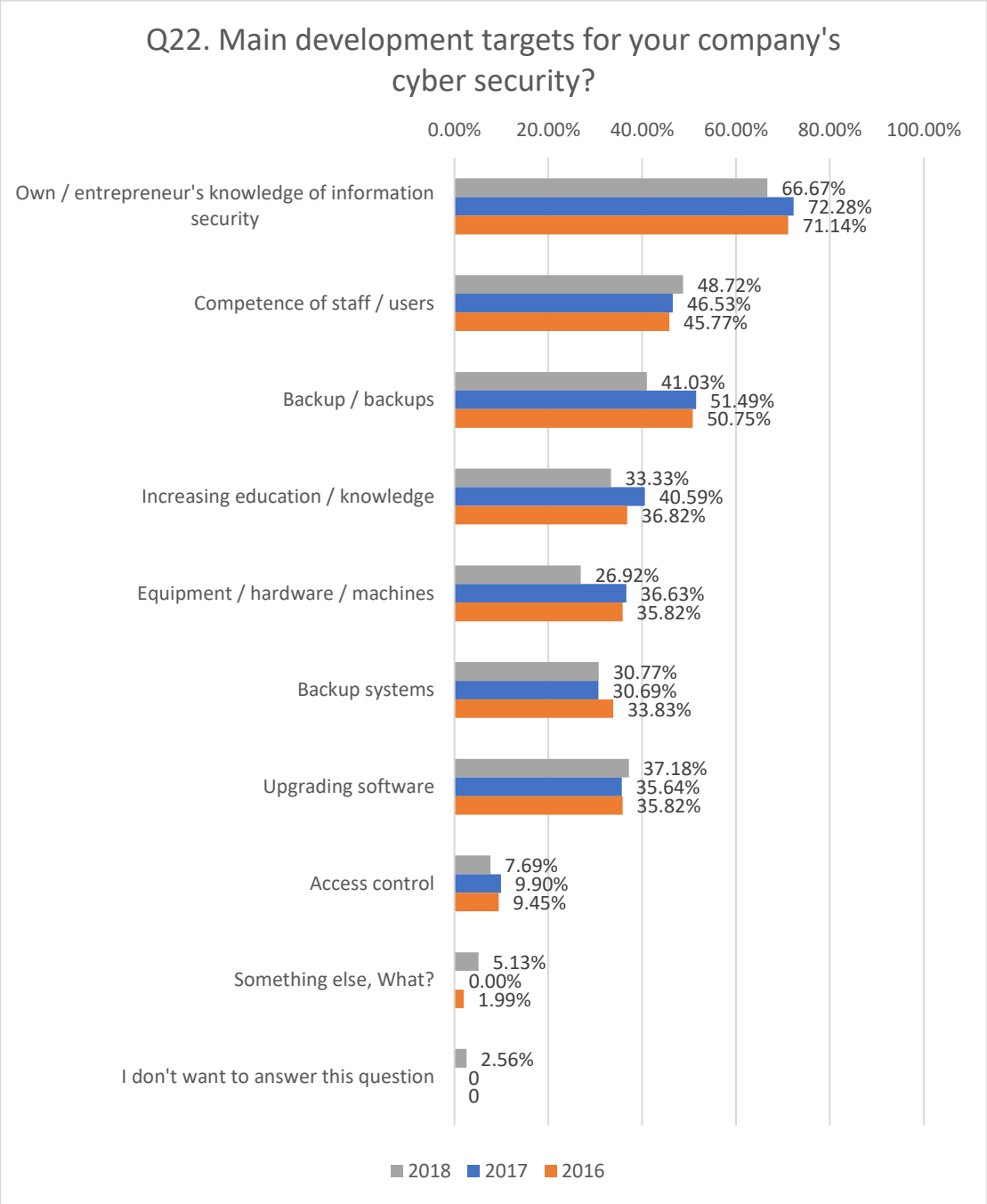


Figure 22. Question 22. Main development targets for your company's cyber security?

In conclusion, it can be stated that attitudes have increased; however, are otherwise in line with the previous years. Cyberattacks and threats are still considered the biggest risks together with the lack of knowledge. Further education is needed but the problem of time management needs to be solved too as the employees hardly ever have time to focus on these issues. If the main industry of a company is e.g. selling flowers, it is understandable that understanding cybersecurity can be a challenge. Small enterprises might not have the funds to invest in preventing threats.

4.4 Beliefs (Q23-Q27)

Questions 23-27 were asked to find out what kind of beliefs the companies have related to cybersecurity. These questions were not included in the 2016 questionnaire but were added into the most recent questionnaires in 2017 as these beliefs were regarded as an essential part of this research.

Figure 23. shows that approximately half of the participants (avg. 55%) believe to be capable of detecting the cybersecurity threats targeted at the company. Only 17 per cent think they are not aware of the cybersecurity threats. It is great news that the companies have the right attitude to cybersecurity, however, it still needs to be questioned whether they are overestimating the knowledge they have about the matter. Detecting cyberthreats is always challenging.

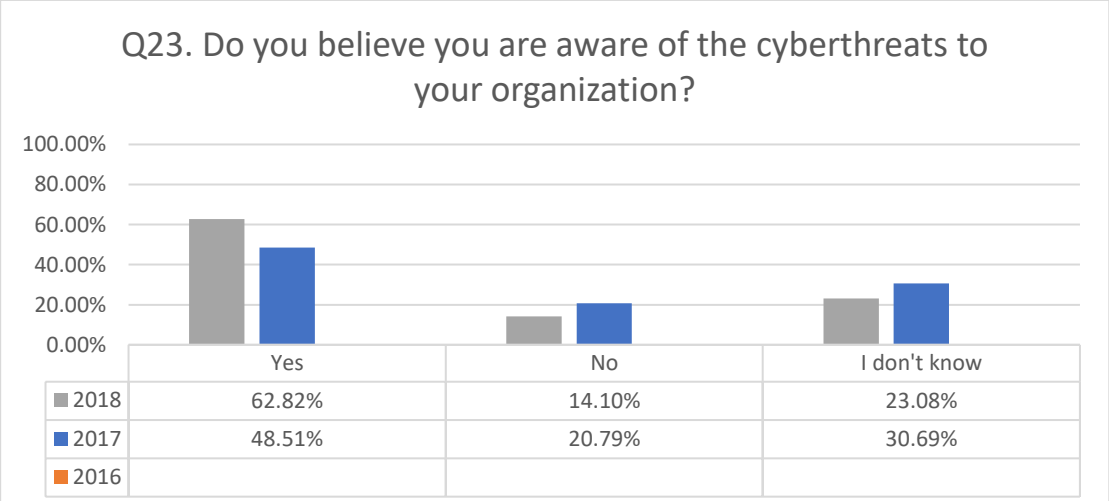


Figure 23. Question 23. Do you believe you are aware of the cyberthreats to your organization?

Figure 24. shows that the companies are aware of cybersecurity threats but as can be seen in Figure 23., they are not necessarily always detected. 32 per cent of the respondents do not believe they are able to detect cyberattacks and 36 per cent cannot tell whether they are or are not. Therefore, it can be said that 68 per cent do not think they can detect cyberattacks.

The reason for this awareness can be the active media coverage and the press releases by the Finnish Communications Regulatory Authority on cybersecurity threats, which makes the companies believe they are aware of the threats. Compared to the results from the previous years, uncertainty about the matter has increased a little. It is known that there are threats; however, the skills to prevent them are not necessarily available.

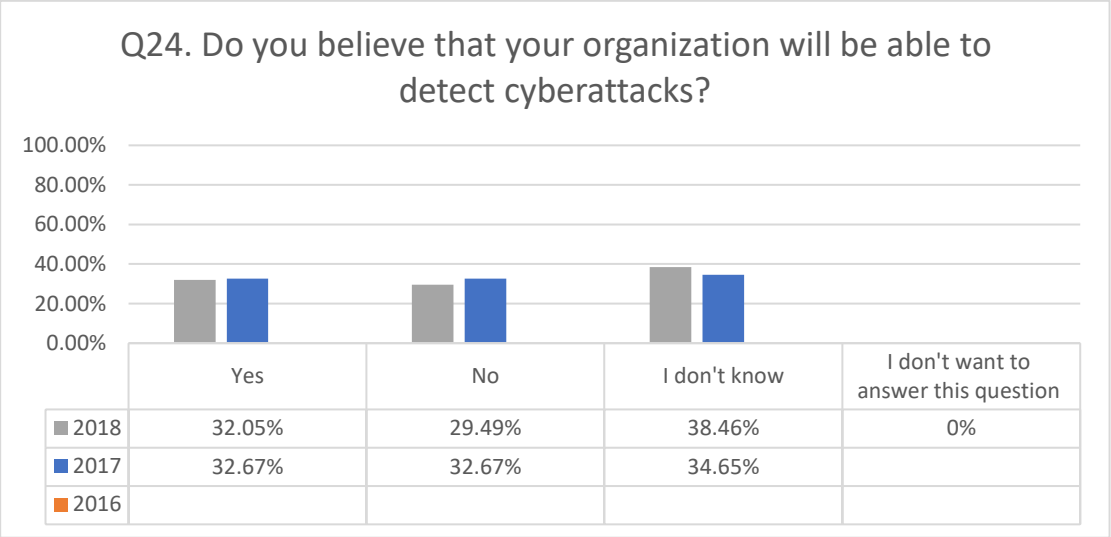


Figure 24. Question 24. Do you believe that your organization will be able to detect cyberattacks?

46 per cent of the answerers (Figure 25) think that the risk for cyberattacks has grown in the past year. The answers are distiributed roughly in the same proportion as in the previous questions. It is beneficial that the companies are aware of the risk and uncertainty about the matter is on the decrease. As a result of this, the companies may more easily ask for help from an external partner in order to solve the situation.

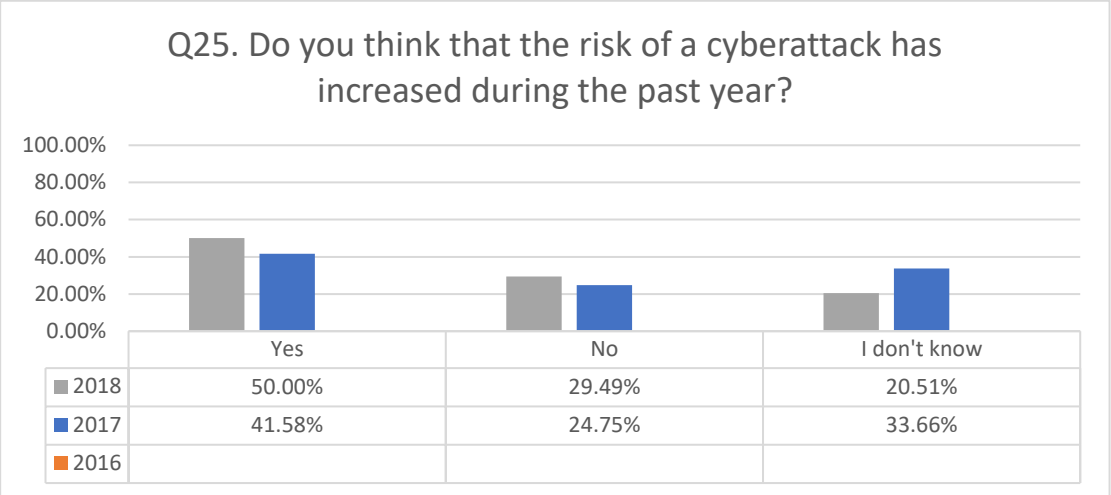


Figure 25. Question 25. Do you think that the risk of a cyberattack has increased during the past year?

A year ago almost half of the participants (Figure 26) thought that there is no need to prepare themselves for cyberthreats or that the need for preparedness had not increased or decreased within the past year. According to the latest survey, the need for preparedness has almost doubled. Still, most companies neglect creating backups and therefore, there might be a total disruption in the business in case the company encounters a cyberthreat.

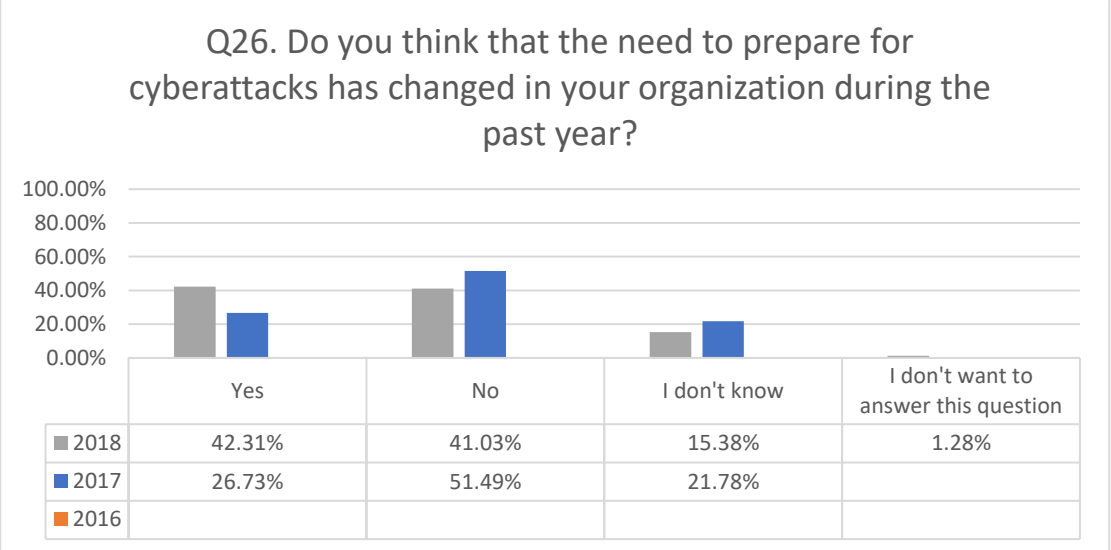
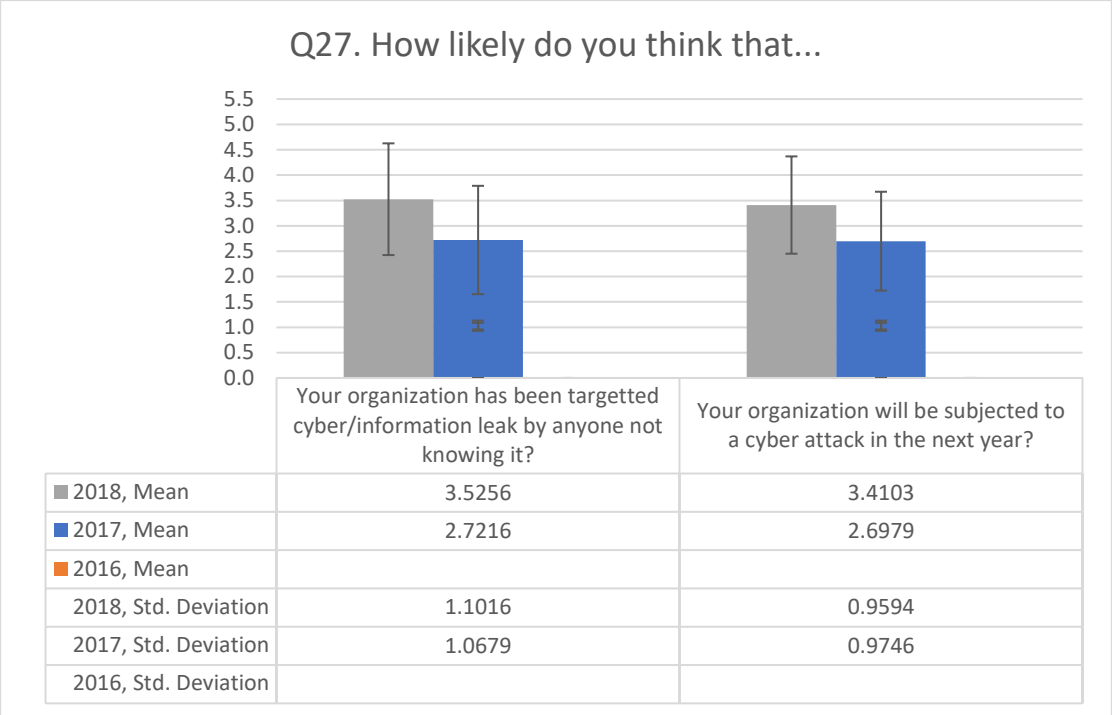


Figure 26. Question 26. Do you think that the need to prepare for cyberattacks has changed in your organization during the past year?

The results shown in Figure 27 confirm the results presented in the previous figures. The threats are considered to be real and from the future perspective the company may be targeted by a cyberthreat within the following year. Compared to the previous years, the increase is considerable.



	Your organization has been targetted cyber/information leak by anyone not knowing it?	Your organization will be subjected to a cyber attack in the next year?
2018, Mean	3.5256	3.4103
2017, Mean	2.7216	2.6979
2016, Mean		
2018, Std. Deviation	1.1016	0.9594
2017, Std. Deviation	1.0679	0.9746
2016, Std. Deviation		

Figure 27. Question 27. How likely do you think that…

As a summary, it can be pointed out that companies consider the threats realistic. Awareness has increased most likely due to the extensive media coverage, however, it is still noticeable that many companies believe they are incapable of detecting these threats. Future is frightening to many companies and they think that in the worst case scenario a cyberattack could cause a disruption in the business and create a negative public image for the company.

4.5 Actual threats (Q28-Q32)

Though the attitudes have changed, the occurred security threats are a sensitive issue to many companies. Large companies in particular, operating in the areas of B2B or B2G, do not or cannot publicly admit a security breach unless it is absolutely

unavoidable. On a worldwide scale, Hunt (2018) brings these kind of cases into public knowledge on his website. The case of Dropbox is an example of this: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Up to 58 per cent (avg.) of the companies reported that the company has not encountered a cybersecurity attack (Table 4.). Therefore, it can be interpreted that 42 per cent of the companies have experienced some kind of security breach or attack of similar sort. In comparison with the previous years the percentages are approximately the same as in 2018. Alternative 2. 'Ransomware has locked a computer' was not included in the 2016 questionnaire. The cases mentioned in part 'Something else, what?' were, for example, phishing, email scam and ordinary theft.

Three respondents were not willing to answer this question. Even thought the survey was answered anonymously, some participants do not dare to comment on this part as it would be considered an internal information leak in the company. The obligation to be loyal to the employer requires the employee to consider the company's interest and the employee is not, for instance, allowed to harm the employer's reputation.

What makes the table interesting is the fact that almost every threat mentioned – from stealing credit information to ransomware - has occurred. Email scams and misconfigured servers were also mentioned as threats in addition to the ones listed in the table.

Table 4. Question 28. Which of the following security threats have occurred in your company?

		2018, N=78		2017, N=101		2016, N=201	
		N	%	N	%	N	%
1.	User IDs and passwords have been stolen and have been misused	2	2.74 %	4	3.96 %	6	2.99 %
2.	Ransomware has locked a computer	4	5.48 %	4	3.96 %	-	-
3.	There have been attempts to spy on work related information	10	13.70 %	7	6.93 %	18	8.96 %
4.	Identity has been stolen and has been misused	1	1.37 %	2	1.98 %	4	1.99 %
5.	The organization has lost money because of online scams	0	0 %	2	1.98 %	6	2.99 %
6.	Company data has leaked	5	6.85 %	3	2.97 %	1	0.50 %
7.	The company has lost important information due to hardware failure	4	5.48 %	12	11.88 %	26	12.94 %
8.	A terminal (phone, computer, etc..) has been stolen or lost	4	5.48 %	4	3.96 %	9	4.48 %
9.	An employee has been exposed or has become aware of the confidential information he or she has not been entitled to	7	9.59 %	7	6.93 %	7	3.48 %
10.	The workplace credit card has been misused	2	2.74 %	3	2.97 %	7	3.48 %
11.	A security breach / denial of service has been targeted to the company	5	6.85 %	11	10.89 %	15	7.46 %
12.	The company has not been exposed to a security breach	44	60.27 %	56	55.45 %	118	58.71 %
13.	Something else, What?	6	8.22 %	17	16.83 %	21	10.45 %
14.	I don't want to answer this question	3	4.11 %	-	-	-	-

Question 29. ’How did you find out about the security threat referred to in the previous question?’ was only addressed to the respondents who stated that a security breach or similar incident had occurred in the company. In Table 5, parts 1 and 3 refer to the company’s own means to detect cybersecurity threats. In 2018 the companies had detected 40 per cent of the attacks. In the previous years, this percentage had been higher.

Every fifth cybersecurity threat was informed to the company by a client. In Table 3., additional ways to find out about a threat were information from the client, observing an employee and an anonymous report.

Table 5. Question 29. How did you find out about the security threat referred to in the previous question?

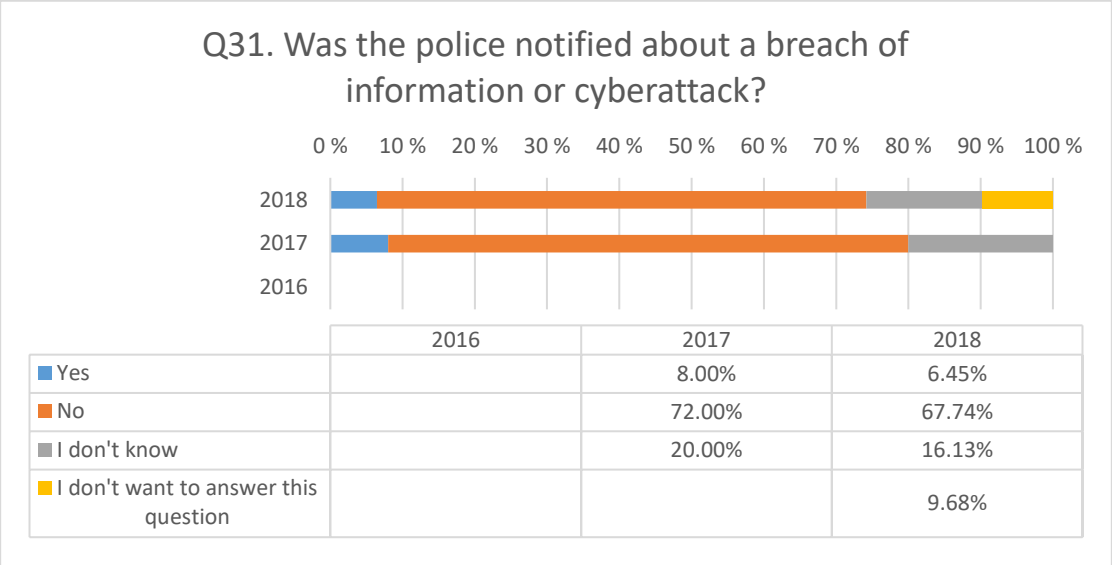
		2018, N=78		2017, N=101		2016, N=201	
		N	%	N	%	N	%
1.	We detected it ourselves using our own prevention and intrusion detection systems	7	25.93 %	19	38.00 %	38	41.76 %
2.	Our users recognized it and reported it	5	18.52 %	11	22.00 %	22	24.18 %
3.	We recognized it by ourselves because we checked and analyzed our logs	4	14.81 %	9	18.00 %	13	14.29 %
4.	Law enforcement/intelligence organizations warned us	0	0 %	2	4.00 %	4	4.40 %
5.	Third party, such as an internet operator or service provider, informed us	4	14.81 %	6	12.00 %	14	15.38 %
6.	Something else, What?	7	25.93 %	15	30.00 %	17	18.68 %
7.	I don't want to answer this question	3	11.11 %	-	-	-	-

When asked about what kind of information the intruders might be looking for (Table 6), there is variation in the answers. As many as 50 per cent reported not knowing this, which in itself is a good answer since in most cases it is impossible to say why the network has veen broken into and what the intruders are looking for. They are often trying to take control of the system in order to use it to break into the next system. 24 per cent of the respondents thought the intruders were looking for confidential information on the products or services of the company. 13 per cent suspected the intruders were trying to find information on the company's clients and partners. Other information the intruders might try to get was credit card information that could be turned into money, employees' information and any kind of information that could be used to blackmail the company.

Table 6. Question 30. What kind of information do you think intruders are looking for?

		2018, N=78		2017, N=101		2016, N=201	
		N	%	N	%	N	%
1.	Personal information of senior management	4	14.81 %	1	2.00 %	8	8.79 %
2.	Personnel information such as names, responsibilities and units	5	18.52 %	1	2.00 %	5	5.49 %
3.	Information of subcontractors, partners, suppliers, or customers	3	11.11 %	7	14.00 %	13	14.29 %
4.	Confidential information about our products or services	9	33.33 %	9	18.00 %	18	19.78 %
5.	Network related information, such as network structure and other devices on your company network	1	3.70 %	7	14.00 %	9	9.89 %
6.	I don't know	12	44.44 %	26	52.00 %	49	53.85 %
7.	Something else, What?	3	11.11 %	10	20.00 %	14	15.38 %
8.	I don't want to answer this question	0	0 %	-	-	-	-

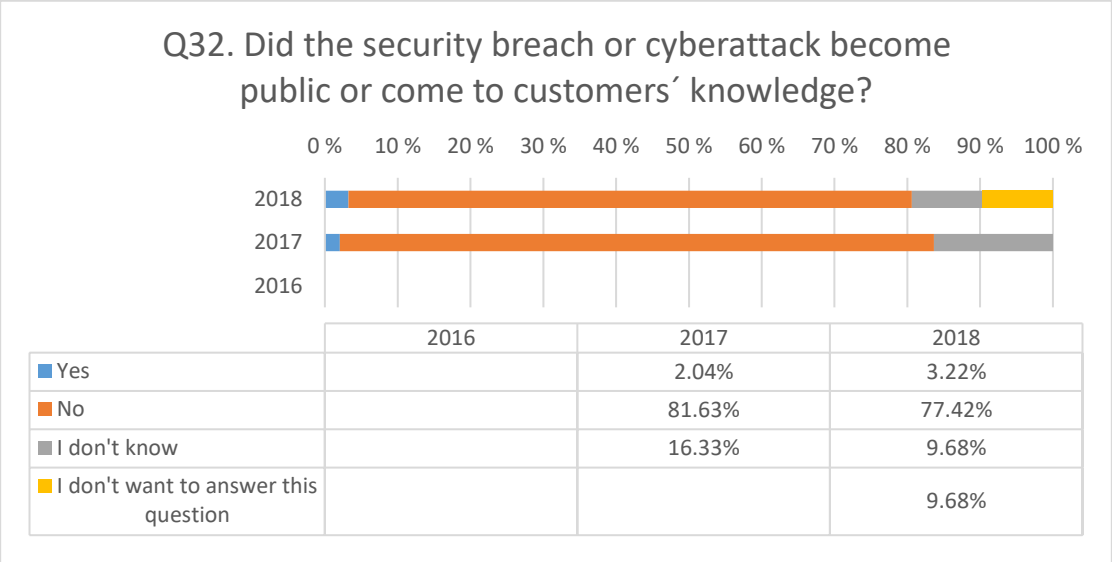
Questions 31 and 32 were new to the questionnaire. Cases where a company has encountered a security breach are often discussed; however, the actions taken after the breach are rarely negotiated. Only 7 per cent of the cases are reported to the police (Figure 28). This number sounds extremely low but can partly be explained by the nature of a security breach. In some cases, for example, the company had been sent scam emails. Additionally, these cases could be reported to the police; however, the report most likely would not lead to any results. Based on the results, it can be noted that very rare cases are reported to the authorities.



	2016	2017	2018
Yes		8.00%	6.45%
No		72.00%	67.74%
I don't know		20.00%	16.13%
I don't want to answer this question			9.68%

Figure 28. Question 31. Was the police notified about a breach of information or cyberattack?

When going through the results it can be seen that the attitudes of the companies have changed toward more open and security breaches have more often been told about in the media. As Figure 29 shows, the clients are not often informed about the security breaches in fear of the breach affecting the business with the clientele. Only 3 per cent of the cases were told to the clients and 80 per cent of the participants reported not informing the clientele about any security threats. The new EU data protection regulation which obligates othe companies to inform the people about security breaches that concern them. This is a positive step since it is not only disadvantageous to conceal information but also frightening from the company's perspective when considering how it will affect the company's business. It remains to be seen whether the companies' image will withstand a security breach and the negative publicity that follows.



	2016	2017	2018
Yes		2.04%	3.22%
No		81.63%	77.42%
I don't know		16.33%	9.68%
I don't want to answer this question			9.68%

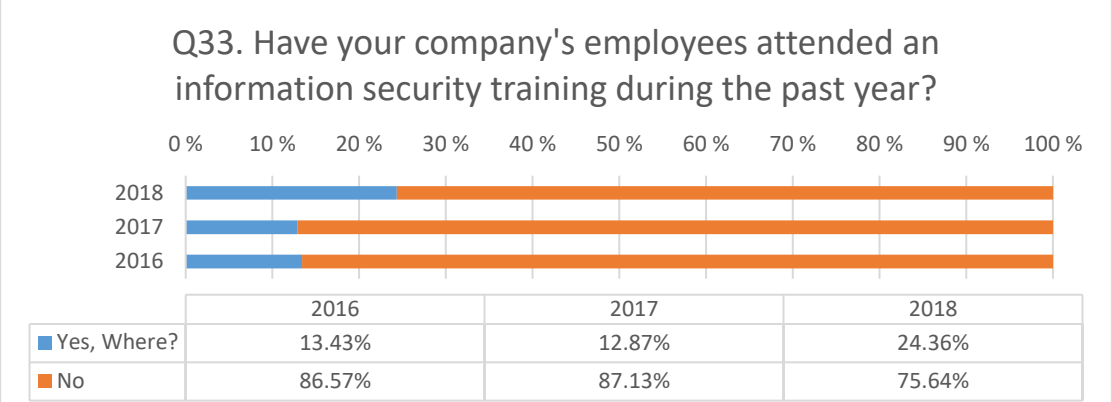
Figure 29. Question 32. Did the security breach or cyberattack become public or come to customers´ knowledge?

To summarize, the occurred threats are real and the customers are rarely informed about them because it is thought to affect the company's business in a negative way. It is worrying that only a few cases are reported to the police. It remains to be clarified whether the reason is the desire to conceal the matter or the distrust in the police forces' capability to solve these kinds of offences. On the other hand, the latter reason is reality because of the lack of resourcing in the police forces. Appendix 1 presents the cases reported to and solved by the police. For example, in the case of security breaches, the police were able to solve only 10 per cent of the cases in a year. A digital breach is challenging to solve due to the inexistence of physical elements.

4.6 Education and needs (Q33-Q38)

The educational background of the employees often plays a big role when talking about cybersecurity. Training the personnel to increase their knowledge of cybersecurity can nowadays be seen in education and these issues are taught to some students already in undergraduate studies. Today's students are more aware of these issue, but the working generation should not be forgotten either.

FIgure 30 shows that there is little training on cybersecurity offered to the personnel by the company. Only 17 per cent of the employees have participated in cybersecurity training. Even though the number is small, it is a start and according to the statistics, education is becoming more common. The increase in training in 2018 is most likely a result from the GDPR (EU General Data Protection Regulation) training that the companies were forced to react to. When asked where the training had taken place, employees mentioned internal training by the company, seminars and GDPR training.



	2016	2017	2018
Yes, Where?	13.43%	12.87%	24.36%
No	86.57%	87.13%	75.64%

Figure 30. Question 33. Have your company's employees attended an information security training during the past year?

The study tried to clarify how strongly the companies follow Ficora (Finnish Communications Regulatory Authority). As Figure 31 shows, almost half of the participants were aware of the services and information offered by Ficora. It is a significant step towards enhancing cybersecurity if companies follow official sources. The media occasionally inform about new instructions but also highlight wrong issues because of ignorance.

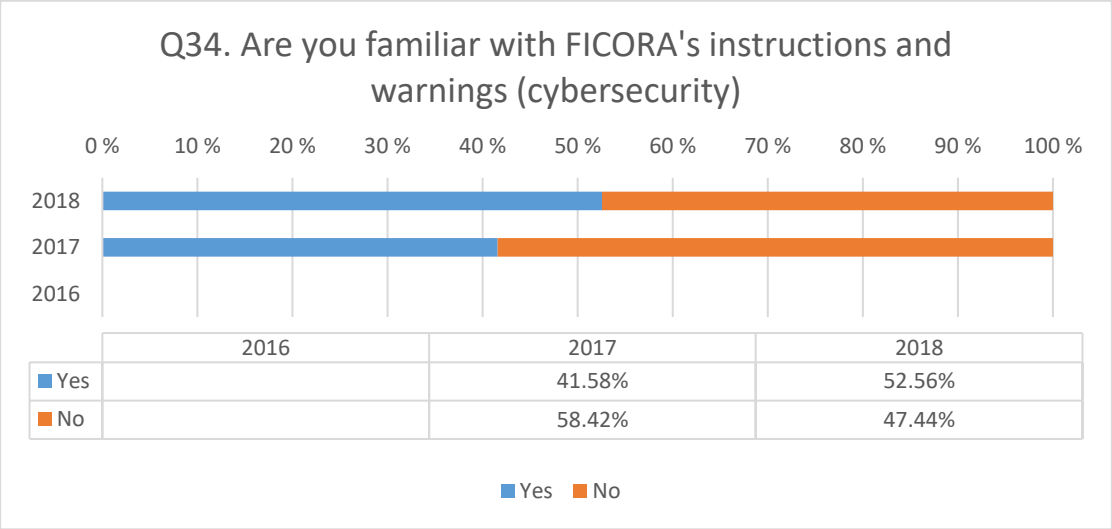


Figure 31. Question 34. Are you familiar with FICORA's instructions and warnings (cybersecurity)

Figure 32 presents the areas which the participating companies would be interested in getting training on. Based on the answers, the need for training is constantly growing and companies are increasingly interested in these issues. The problem may often be, however, the financial pressure as the training always costs something and the time spent on training the employees is taken from the time spent on the actual work that generates the company's turnover.

Software security arose as one of the most interesting areas and this can be seen as the right direction to take. Most often, it is exactly the outdated software through which the malware can spread on the the employees' computers.

Hardware security, the security of data files and telecommunications security were also issues that often came up in the answers. Other issues mentioned in this question were going through basic things and providing checklists for the owner-managers of small enterprises.

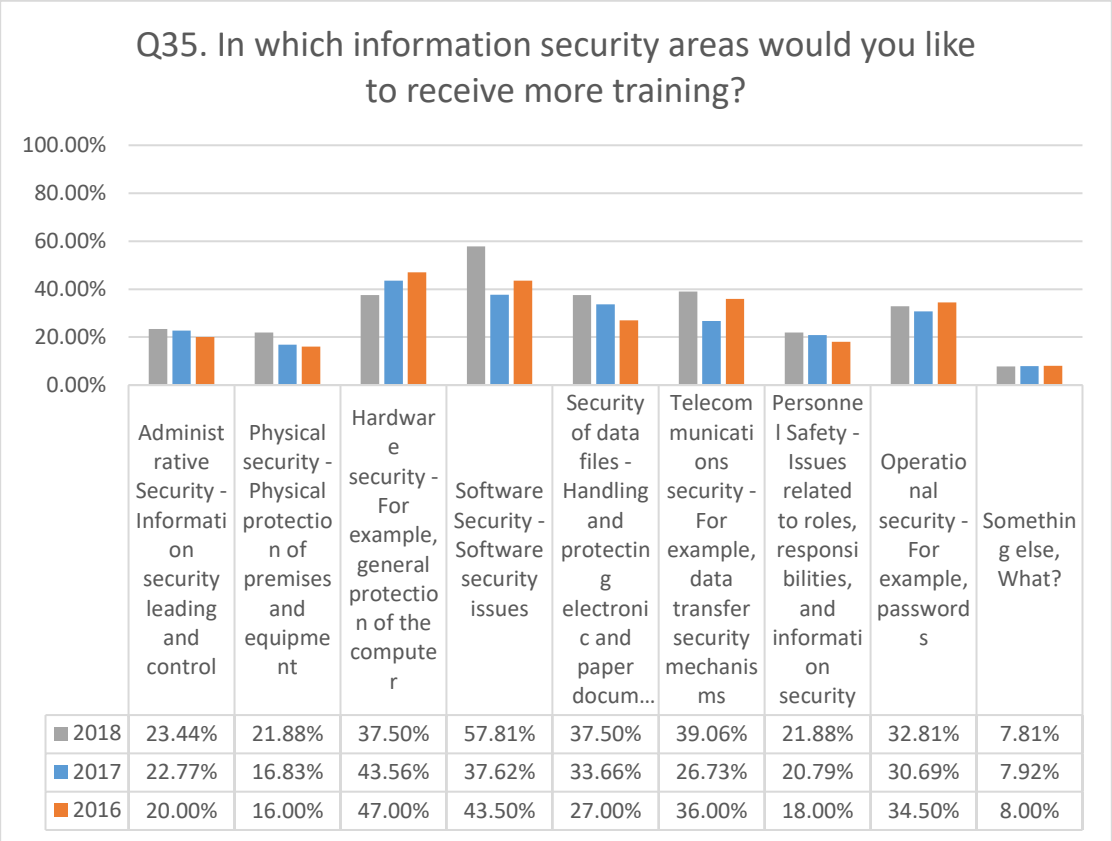
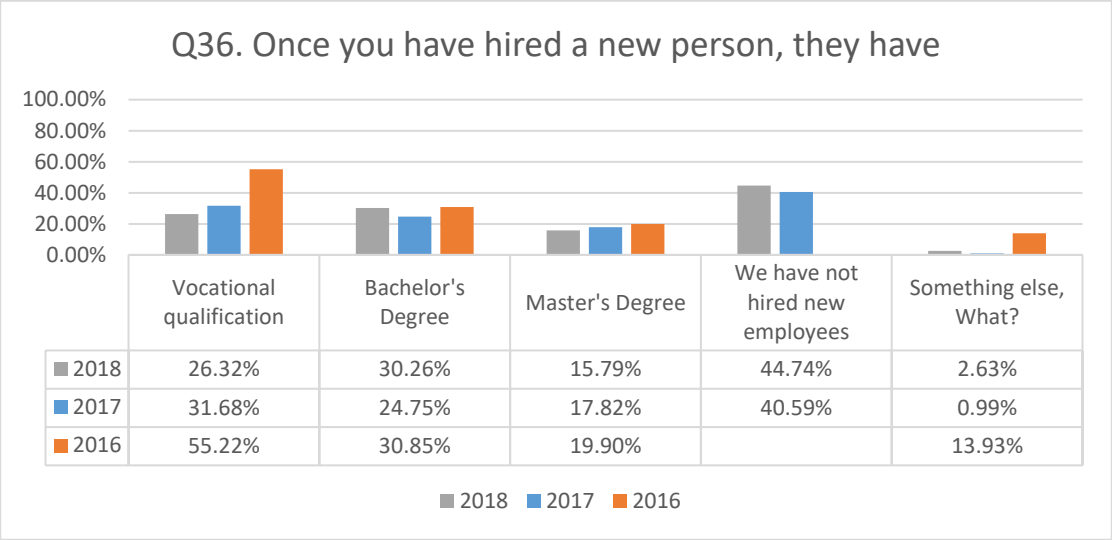


Figure 32. Question 35. In which information security areas would you like to receive more training?

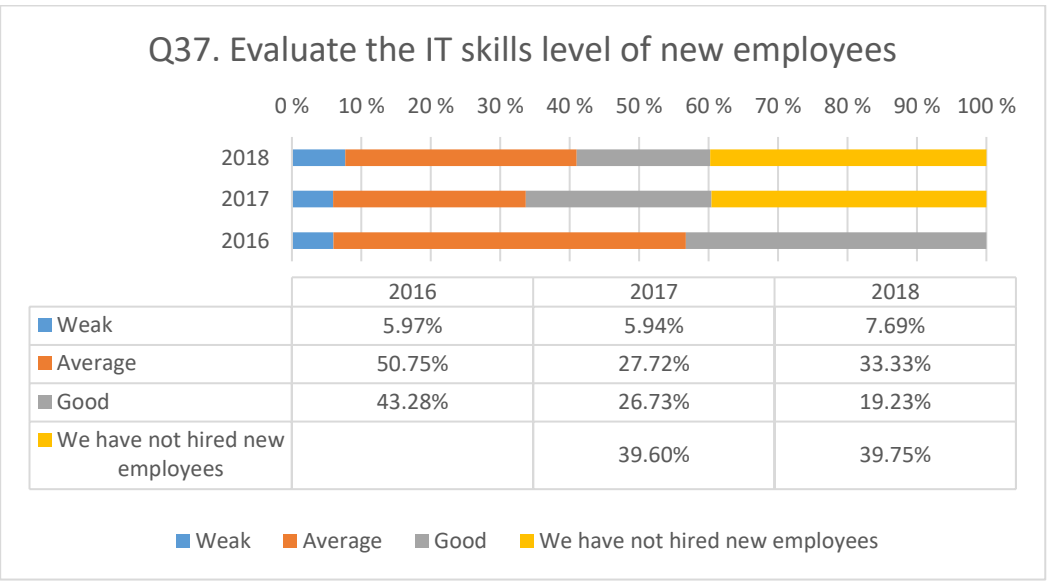
Figure 33 was drawn to highlight what kind of educational backgrounds the employed people have. As seen in the answers, all the levels of education have been an alternative. Approximately 43 per cent stated not having hired new personnel. In these cases the answerer may have been an owner-manager, whose resources to hire new employees are always small.



	Vocational qualification	Bachelor's Degree	Master's Degree	We have not hired new employees	Something else, What?
2018	26.32%	30.26%	15.79%	44.74%	2.63%
2017	31.68%	24.75%	17.82%	40.59%	0.99%
2016	55.22%	30.85%	19.90%		13.93%

Figure 33. Question 36. Once you have hired a new person, they have

The respondents were also asked to evaluate the IT skills of their employees. Based on the answers in Table 3., most companies estimated their employees' skills to be average.



	2016	2017	2018
Weak	5.97%	5.94%	7.69%
Average	50.75%	27.72%	33.33%
Good	43.28%	26.73%	19.23%
We have not hired new employees		39.60%	39.75%

Figure 34. Question 37. Evaluate the IT skills level of new employees

In conclusion, it can be stated that companies have educational needs and they view training necessary these days. Most respondents have been able to estimate in their previous answers that the cybersecurity threats can disable the company's business.

A question arises why the curricula in degree programs has not been developed to react to these issues more precisely. In higher education, the basic studies contain only a little content on cybersecurity. On secondary level, the training on cybersecurity is minimal. For example the study programs in social services only contain some training on data protection, not on cybersecurity. These people are, however, the ones who deal with confidential materials in their work, which makes it very important for their training to respond to today's threats better.

4.7 Correlation analyzing with SPSS

In order to analyze the data, SPSS statististics application (version 23) was in use. With the help of the application, it was possible to make statistical conclusions on the data. A correlation analysis was performed on questions 18, 19, 20, 21 ja 27 that consisted of the Likert scale. All the correlations in the questions mentioned above were positive.

Correlation tables can be found in the Appendices 4 – 16. The tables show that statistically significant correlations can be found in the questions that have been marked with two asterisks (**). Statistically somewhat significant correlations can be found in some questions. These correlations can be recognized from one asterisk (*).

4.7.1 Q18. How important do you consider securing the following things?

Question 18 was asked to find out the respondents' opinions on how important they consider securing the things mentioned in the questionnaire. The question arguments can be found in Appendix 1 and correlation tables in Appendices 4 – 6 There are three pages because the tables are separated into years 2018, 2017, 2016.

Based on the results from 2018, there are statistically significant correlations in several parts. The most significant correlations can be found in the following parts: Research & development information; Products / Product details; Financial management; Own skills, know-how. There was a strong, positive correlation between these pretensions, which was statistically significant ($r > .429$, $n = 78$, $p = .000$).

In the results from 2017, the strongest correlations can be found in the following parts: Customer register; Securing / updating computer hardware and Research & development information; Products / Product details ($r > .555$, $n = 97$, $p = .000$).

In 2016, the most significant correlations are found in ‘Own skills, know-how’, Research & development information’ and ’Products / Product details’ ($r > .532$, $n = 187$, $p = .000$).

To summarize, it can be stated that the parts ‘Research & development information’ ’Products / Product details’ correlate in the results of all the three years. In every year’s correlations more than half of the parts correlate statistically significantly with other parts.

4.7.2 Q19. Which of the following issues do you consider a major cyber security threat in your business?

In Question 19, the aim was to ask about the issued the respondents regarded as major security threats in their business. The question arguments can be found in Appendix 1 and the correlation tables in Appendices 7 – 9. There are three pages because the tables are, again, separated by year (2018, 2017, 2016).

In the results of the year 2018, there are statistically significant correlations in several parts. The biggest correlations can be found in the following parts: Intrusion to information systems; DDoS (to prevent the operation of the web service); Phishing and malware attacks. There was a strong, positive correlation between these pretensions, which was statistically significant ($r > .532$, $n = 78$, $p = .000$).

When compared to the results of the year 2017, the biggest correlations are found in the following parts: Phishing and malware attacks; Intrusion to information systems; DDoS (to prevent the operation of the web service); Attacks targeting to company's production process (e.g. network-connected production equipment or device (IoT)) ($r > .515$, $n = 92$, $p = .000$).

In 2016, the most significant correlations can be found in the following parts: Phishing and malware attacks; Intrusion to information systems; DDoS (to prevent the operation of the web service) ($r > .573$, $n = 186$, $p = .000$).

All in all, it can be stated that the parts 'Phishing and malware attacks', 'Intrusion to information systems' and 'DDoS (to prevent the operation of the web service)' correlate in every year's results. Half of the parts in the results every year correlate statistically significantly with other parts.

4.7.3 Q20. How big an obstacle do you consider the following issues to be to make cyber safety (more) effective in your company?

Question 20 asked for opinions on which issues hinder effective cybersecurity most. The question arguments can be found in Appendix 1 and the correlation tables in Appendices 10 – 12. There are three pages because the tables are separated by year (2018, 2017, 2016).

Examining the results from 2018, statistically significant correlations can be found in every part. Only one part contains a statistically somewhat significant correlation. The biggest correlations can be found in the following parts: Insufficiency of information related to cyber security; Insufficiency of information related to security measures and methods; Maintaining the knowledge of current staff regarding cyberthreats. There was a strong, positive correlation between these pretensions, which was statistically significant ($r > .637$, $n = 78$, $p = .000$).

In 2017, there were statistically significant correlations in all the parts. The biggest correlations can be found in the following parts: Insufficiency of information related to cyber security; Insufficiency of information related to security measures and methods ($r = .831$, $n = 92$, $p = .000$).

Based on the results of the year 2016, there are statistically significant correlations in all the parts. The biggest correlations are found in the following parts: Insufficiency of information related to cyber security; Insufficiency of information related to security measures and methods ($r = .835$, $n = 184$, $p = .000$).

In conclusion, it can be stated that the parts ’Insufficiency of information related to cyber security’ and ’Insufficiency of information related to security measures and methods’ correlate significantly in every year’s results. In every year’s results, all but one part correlates statistically significantly with other parts.

4.7.4 Q21. How significant do you consider the consequences of the following cyberattacks?

Question 21 asks: ’How significant do you consider the consequences of the following cyberattacks?’ The question arguments can be found in Appendix 1 and the correlation tables in Appendices 13 – 15. There are three pages because the tables are separated by year (2018, 2017, 2016).

In the results of 2018, there are statistically significant correlations in every part. The biggest correlations are found in the following parts: Loss of income Direct or indirect; Business interruption; Criminal liability; Damage payment to the customer. There was a strong, positive correlation between these pretensions, which was statistically significant ($r > .636$, $n = 78$, $p = .000$).

In 2017, there were statistically significant correlations in all the parts. The biggest correlations are found in the following parts: Loss of income Direct or indirect; Business interruption; Loss of market share. There was a strong, positive correlation between these pretensions, which was statistically significant ($r > .613$, $n = 91$, $p = .000$).

Based on the results of the year 2016, there are statistically significant correlations in all the parts. The biggest correlations are found in the following parts: Loss of market share; Negative publicity; Loss of income; Direct or indirect ($r > .449$, $n = 179$, $p = .000$).

To summarise, it can be stated that ’Loss of income Direct or indirect’ and ’Loss of market share’ correlate significantly in the results of all the three years. All the parts of all the years correlate statistically significantly with others.

4.7.5 Q27. How likely do you think that

Question 27 is ’How likely do you think that?’ The question arguments can find in Appendix 2 and the correlation tables in Appendix 16. This question was present in the survey only in 2018 and in 2017.

There were only two choices, which were: Has your organization been targeted by a cyber/information leak without anyone not knowing about it? – Will your organization be subjected to a cyberattack in the next year?

Based on the results of 2018 (r = .835, n = 78, p = .000) there was a strong, positive correlation between these pretensions, which was statistically significant. The 2017 results was also a strong. There was a positive correlation between these pretensions, which was statistically significant (r = .552, n = 96, p = .000).

4.8 Crosstabulation analyzing with SPSS

The covariation between two variables can be examined with the help of crosstabulation. This procedure enables a more detailed processing of the desired records. Chapter 4.2 dealt with security policy and EU legislation, which have been analyzed through crosstabulation. Table 7 describes the crosstabulation for questions ‘Is there a security policy for your company?’ and ‘Number of employees’.

When analyzing the results, a question arose about whether the respondents have misunderstood the question. Through crosstabulation, it can be noted that the security policy is mainly existent in big companies. Also smaller companies have drawn these policies but in a smaller scale than the bigger enterprises.

Table 7. Crosstabulation: Is there a security policy for your company? * Number of employees?

Is there a security policy for your company? * Number of employees? Crosstabulation								
		Number of employees?						
Survey 2018		1–4	5–9	10–19	20–49	50–99	100–	Total
Is there a security policy for your company?	Yes	8	7	7	3	5	4	34
	No	30	7	4	2	0	1	44
Total		38	14	11	5	5	5	78
		Number of employees?						
Survey 2017		1–4	5–9	10–19	20–49	50–99	100–	Total
Is there a security policy for your company?	Yes	12	7	2	4	1	10	36
	No	45	8	5	6	1	0	65
Total		57	15	7	10	2	10	101
		Number of employees?						
Survey 2016		1–4	5–9	10–19	20–49	50–99	100–	Total
Is there a security policy for your company?	Yes	17	14	5	2	4	10	52
	No	100	17	21	8	3	0	149
Total		117	31	26	10	7	10	201

Table 8 presents the crosstabulation of questions ‘Are you aware of EU legislation regarding cyber safety’ and ‘Number of employees’. The table shows that also the awareness of the EU legislation is higher in bigger enterprises. As chapter 4.2 stated, it is positive that the awareness of the EU legislation has increased among the companies. GDPR came into effect in the spring of 2018, which explains the weaker figures in 2016 and 2017.

Table 8. Crosstabulation: Are you aware of EU legislation regarding cyber safety? * Number of employees?

Are you aware of EU legislation regarding cyber safety? * Number of employees? Crosstabulation								
		Number of employees?						
Survey 2018		1–4	5–9	10–19	20–49	50–99	100–	Total
Are you aware of EU legislation regarding cyber safety?	Yes	16	10	6	4	3	4	43
	No	22	4	5	1	2	1	35
Total		38	14	11	5	5	5	78
		Number of employees?						
Survey 2017		1–4	5–9	10–19	20–49	50–99	100–	Total
Are you aware of EU legislation regarding cyber safety?	Yes	12	0	2	6	2	2	24
	No	45	15	5	4	0	8	77
Total		57	15	7	10	2	10	101
		Number of employees?						
Survey 2016		1–4	5–9	10–19	20–49	50–99	100–	Total
Are you aware of EU legislation regarding cyber safety?	Yes	18	4	3	3	1	4	33
	No	99	27	23	7	6	6	168
Total		117	31	26	10	7	10	201

From Tables 7 and 8 one can draw the conclusion that bigger companies are more active. One facilitator to this is the IT management of the company. Considering the next survey, it would be useful to find out what the company's size usually is for them to have an IT management of their own.

Table 9 shows the crosstabulation of questions 'How company security issues are resourced?' and 'Number of employees?' As previously assessed, small enterprises do not have a separate person hired to take care of security issues. What makes the table interesting is the question on outsourcing. In 2016 and 2017, surprisingly many companies had oursourced this area. Percentage-wise the figures follow the percentages of the results in 2018.

Table 9. Crosstabulation: How are company security issues resourced? * Number of employees?

How company security issues are resourced? * Number of employees? Crosstabulation								
		Number of employees?						
Survey 2018		1–4	5–9	10–19	20–49	50–99	100–	Total
How company security issues are resourced?	Things are handled alongside their own work	32	10	7	3	2	1	55
	There is a hired person to this job	0	0	1	1	2	3	7
	The task has been outsourced	0	2	2	0	0	1	5
	This is not a single person's responsibility	5	1	1	0	0	0	7
	Something else, What?	0	0	0	0	1	0	1
	I don't want to answer this question	1	1	0	1	0	0	3
Total		38	14	11	5	5	5	78
		Number of employees?						
Survey 2017		1–4	5–9	10–19	20–49	50–99	100–	Total
How company security issues are resourced?	Things are handled alongside their own work	46	11	5	8	1	2	73
	There is a hired person to this job	3	1	1	0	0	7	12
	The task has been outsourced	5	2	1	2	1	1	12
	This is not a single person's responsibility	2	1	0	0	0	0	3
	Something else, What?	1	0	0	0	0	0	1
Total		57	15	7	10	2	10	101
		Number of employees?						
Survey 2016		1–4	5–9	10–19	20–49	50–99	100–	Total
How company security issues are resourced?	Things are handled alongside their own work	86	22	15	4	3	2	132
	There is a hired person to this job	1	2	0	2	1	8	14
	The task has been outsourced	14	4	9	2	3	0	32
	This is not a single person's responsibility	9	3	1	2	0	0	15
	Something else, What?	6	0	1	0	0	0	7
Total		116	31	26	10	7	10	200

Table 10 focuses on the occurred threats. The crosstabulation was made on parts ‘User IDs and passwords have been stolen and have been misused’ and ‘Number of employees’. According to the results, the size of the company does not play a role here as stealing the user IDs is tied to the users’ knowhow.

Table 10. Crosstabulation: Which of the following security threats have occurred in your company?:User IDs and passwords have been stolen and have been misused * Number of employees?

Which of the following security threats have occurred in your company?:User IDs and passwords have been stolen and have been misused * Number of employees? Crosstabulation								
		Number of employees?						Total
		1–4	5–9	10–19	20–49	50–99	100–	
User IDs and passwords have been stolen and have been misused	2018	0	0	1	0	0	1	2
	2017	1	0	1	1	0	1	4
	2016	4	0	1	1	0	0	6

The occurred threats are mentioned in Table 11. Crosstabulation was made on parts ‘Ransomware has locked a computer’ and ‘Number of employees’. The results show that the size of the company is irrelevant.

Table 11. Crosstabulation: Which of the following security threats have occurred in your company?: Ransomware has locked a computer * Number of employees?

Which of the following security threats have occurred in your company?: Ransomware has locked a computer * Number of employees? Crosstabulation								
		Number of employees?						Total
		1–4	5–9	10–19	20–49	50–99	100–	
Ransomware has locked a computer	2018	0	0	0	1	1	2	4
	2017	3	0	0	1	0	0	4
	2016	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Bigger companies often have their own IT management that takes care of maintaining the functionality of the devices. IT management cannot, however, prevent the employees from opening a harmful file. As the tables presented previously show, these kinds of events occur in companies of all size.

5 Research discussion

The goals of the research were defined in chapter 3.1. This section deals with the results of the survey from the perspective of the goals.

While going through the statistics, a question arose on why the response rates were so small (< 7%) and got smaller all the time. Many of the company representatives said there was a steady flow of surveys of this kind and no time to respond to all of them. Spring is the busiest time for many companies as summer is approaching. Another reason for decreasing response rates was the media writing about the phishing attempts by criminals. One company representative commented, 'It is great that research is being conducted but we do not want to respond to the questionnaire as it could be connected to the business of our company'. On the other hand, it is also a positive thing that the companies carefully consider which questionnaires are worth answering. Even though the survey was advertised as anonymous and the respondents were not required to give out any personal information, some of the participants were reserved about this study.

5.1 Comparison of results with previous research

There are not many current and comprehensive studies on cybersecurity in Finland. Companies working in cybersecurity have published reports but these mostly inform the public about the findings they have made, e.g. what kind of malware their software detects and averts, or how a detected malware functions.

From the existing studies, the one conducted in 2016 by Helsinki Region Chamber of Commerce (HRCC) on the cyberthreats companies face is of special interest because it resembles this survey.

The study by HRCC covers all of Finland and is based on answers given by 754 companies (companies employing 1-4 persons n=206; 5-49 persons n=357; 50-199 persons n=100; over 200 persons n=91). The sample in the HRCC study is considerably larger than that of this study; however, the results are still comparable with each other.

On a general level, similarities and differences can be found in these studies. The results of the HRCC study show that companies have faced similar problems to the ones mentioned in chapter 4. A comparison was made on five parts where the

questions are of the same sort. The study by HRCC asked the respondents to choose different alternatives whereas this study used the Likert scale.

In this study Question 19 was ‘Which of the following issues do you consider a major cyber security threat in your business?’ According to the study by HRCC the three biggest threats are Phishing and malware attacks (47%), Intrusion to information systems (36%) and Internal threat of the company (own employees) (27%). In this study, the two first ones are in line with the HRCC study but the third Internal threat of the company (own employees) does not correspond to the results in this study, where this was rated as the smallest threat every year. Ransom malware (20%) placed fifth in the HRCC study, whereas in this study, it was placed in the top end of the spectrum. The reason for this can be the increased market share of these ransom malware.

Question 20 was ‘How big an obstacle do you consider the following issues to be to make effective cyber safety (more) effective in your company?’ According to HRCC, the three biggest obstacles are Personnel's disregard for information security and cyber threats (42%), Insufficiency of information related to cyber security (34%) and Maintaining the knowledge of current staff regarding cyber threats (33%). The results of the HRCC study correspond to the results of this study in this question.

In Question 21 ‘How significant do you consider the consequences of the following cyber attacks?’, HRCC states that the three biggest concerns are Loss of income, Direct or indirect (45%), Infringement of Privacy (staff or customer) (40%) and Loss of immovable property (37%). Additionally, in this sense the results of both studies are in line with each other.

Question 29 ‘How did you find out about the security threat referred to in the previous question?’ clarified that, according to HRCC, the three most common ways to detect security threats are the following: Third party, such as an internet operator or service provider, informed us (40%); We detected it ourselves using our own prevention and intrusion detection systems (36%) and We would probably not notice an ongoing intrusion (32%). Option ’We would probably not notice an ongoing intrusion’ was not present in Question 29 but a similar question can be found in

Question 24 in this study (‘Do you believe that your organization will be able to detect cyber attacks?’). Here the participating companies estimated being able to recognize cyberattacks at the likelihood of 32 per cent.

In Question 30 ‘What kind of information do you think intruders are looking for?’, HRCC names the following as the three most common answers: I don't know (40%); Confidential information about our products or services (40%) and Information of subcontractors, partners, suppliers, or customers (33%).

In conclusion, it can be said that based on the chosen questions, this study focusing on Central Finland is in line with the HRCC study. There are several similarities, as well as some disparities.

5.2 Analyzing the cybersecurity state view

The main goal of the study was to determine the state of cybersecurity in Central Finland. Chapter 4 deals with the results of the study and states that the results from the three different years of the survey are comparable with each other. Even though the sample diminished yearly, the results are similar and no significant variation occurred in them from year to year.

The target group of the survey was microenterprises that operate in the business-to-business branch mainly in Finland. The main business of the companies participating was the service industry and thus, it is logical that the most common devices used are laptop computers and smart phones. Regarding the devices, it can also be stated that the use of personal devices is still very common. 26 per cent of the respondents reported using their own devices for work but it is reasonable to assume that, in reality, this figure is larger even though the figure dropped by 10 per cent from 2016. The target group consisted of entrepreneurs of small enterprises, which leads to the fact that the devices are also in personal use; sometimes also used by family members.

The number of cybersecurity policies in companies is on the increase. The rate has increased by up to 18 per cent from the year 2016 to 2018. The underlying cause for this is most likely the EU data protection regulation as also this figure is now three

times larger than previously. A question arises whether the participants confused the GDPR and a cybersecurity plan. As a rule, companies follow these quidelines and consider them important. The main content of a cybersecurity policy is usually confidentiality, which is also tied to the EU data protection regulation.

Data protection is often taken care of alongside the regular work and less than 10 per cent of the respondents report having a hired person to take care of these issues in the company. When placing the results from 2018 into a crosstabulation grid, it was noticed that companies with more than 10 employees most often have hired a person to take care of the IT management. Disruptions are prepared for but yet, 25 per cent of the participants think they do not have the preparedness to anticipate possible disruptions.

Attitudes correlate strongly with each other and these were dealt in Chapter 4.7 and in Appendices 4 – 16. The companies are worried about their knowhow and the company property. The modern cyberthreats are slightly better understood and considered real in today's world. The biggest obstacles in dealing with the threats are lack of knowledge about cybersecurity and insufficient personal information. In addition, the lack of cybersecurity services arises. The companies are also scared of the consequences of a cyberattack as losing their privacy and getting negative publicity create substantial risks for the business.

Though the companies are concerned, over 60 per cent believe to be aware of the cyberthreats targeted at the company, and half of the respondents think cyberthreats are on the increase within the next year. The companies are aware of the risks but only 32 per cent think they are capable of preventing the attacks. The answers suggest that the companies would like to raise the level of preparedness but see the lacking knowhow as a challenge here. All the respondents were, in principle, unanimous when answering the statement 'Your organization has been targeted by a cyber/information leak without anyone knowing about it?' and 'Your organization will be subjected to a cyber attack in the next year?' The future is frightening because IT is a critical part of the business of many companies.

Although the attitudes have become more positive, the occurred threats are still a sensitive issue to many companies. They are afraid of violations in the protection of personal data and privacy, as well as of negative publicity. It is concerning to notice how many companies have encountered cyberthreats in the form of e.g. stolen user IDs and ransomware. For example in 2018, there were 29 different cases that can be categorizes as cyberattacks. Also, the number of denial-of-service attacks was large. It needs to be questioned whether this part was correctly understood. The companies might, for example, think that a disruption in the Internet connection can be interpreted as a denial-of-service attack.

In the case of cyberattacks, the companies had recognized approximately 40 per cent of the situations themselves, which is result-wise a large number. In reality, most of the cases are undetected as the personnel may not have the skills to recognize the attacks. According to the companies, most cyberattacks are related to collecting information.

What was most worrying was that only a few of the detected security attacks were reported to the police. This may be because the companies regard the police forces as powerless in solving these cases because they have a fear for sanctions. Although the company has not done anything wrong, negative publicity can directly lead to the loss of turnover and clients. Based on the answers, it can be stated that the companies are unwilling to discuss these issues in public.

The companies are willing to get more training and some of them have already increased the amount of training offered to their employees from the previous years. The reason for this is likely the EU data protection regulation (GDPR) which forced the companies to create data protection policies. Over 50 per cent of the participants stated being aware of the FICORA's instructions and warnings (on cyber security). This was a positive surprise as relying only on the media may mislead the companies or give them false images of the situation. The results show that the companies would like to receive more training on software security, protecting information and general protection examples. The IT skills of new workers were estimated to be better than average.

To sum up, cyberthreats are real and companies are aware of them. The fact that they are recognized or detected is concerning, and so are the losses that result from them.

5.3 Analyzing the change

The second goal of the study was to find out how the state of cybersecurity has changed from the year 2016 to 2018 and whether the results from these three years show any changes in the company's abilities to detect issues regarding cybersecurity.

The target group of the company has remained similar each year. The survey has involved companies that differ in size and line of business they operate in. Even though the number of respondents decreased every year, the sample population from each year can be compared with each other.

The results point out several similarities in the answers but also disparities between the years. The biggest changes appear in Questions 18 - 21 as they ask for opinions by focusing on the respondents' attitudes.

When considering cybersecurity, the companies have started to pay more attention to the security of the devices. The companies are more and more on the move, which can also be seen in the quality and number of the devices. The share of tablet devices has decreased and the share of laptop devices has grown. The share of smart phones has increased yearly and they have become an essential part of the companies' business. If unprotected, these devices, however, pose challenges to the company. The use of personal devices has decreased.

The number of created security policies has grown steadily every year and so has the awareness of the EU legislation. As a phenomenon, this is interesting but it is possible that the participants confused a cybersecurity policy and the general data protection regulation as the terms resemble each other.

Companies' attitudes towards cybersecurity have increased steadily each year. Protecting information and systems is considered important. The companies seem to understand that problems in these areas might cause the business to cease to

operate in the worst case scenario. Companies also think that the cyberthreats are on the increase every year and they would like to react to the threats appropriately but they lack the knowhow on how to do this. The company is at its strongest in their own line of business, not in cybersecurity.

When the companies were asked to evaluate the IT skilss of their personnel, there is a clear decrease in the results every year. However, a questionnaire on cybersecurity may lead the respondents towards assuming that new employyes are already aware of these issues. Unfortunately, very few study programs contain education on these matters or the content of the training may be very varying. IT study programs make an exception to this. Training offered to the personnel has increased every year, especially in the last survey. The cause for this may be issues related to the GDPR. Awareness of the services proviced by the Finnish Communications Regulatory Authority has also increased. Cyberthreats arouse stronger feelings than before and companies are willing to receive help in reacting to these threats.

6 Conclusions

Based on the results of the three-year survey, conclusions can be drawn about the state of cybersecurity in Central Finland. Although the total sampling was small, it was easy to see some guidelines in the results in the timeline of three years. The results resemble the study conducted by Helsinki Region Chamber of Commerce (2016) 'Yrityksiin kohdistyvat kyberuhat 2016', which was dealt with in Chapter 5.1. This reinforces the reliability of the study.

On the basis of the study, it can be stated that companies need advice on how to improve their knowledge on cybersecurity. The hindrance for the development of knowledge is, however, often the lack of time and resources. If the small enterprise focuses on their main expertise and does business in order to stay financially profitable, it is challenging to find the extra time to master cybersecurity. However, the threat is real if the company computers are attacked by a ransomware that locks

all the files. In this case it will be impossible to do business as the documents do not work.

The companies experience cyberthreats stronger than ever and thus, need more help to tackle the threats. Many companies are also worried about not detecting the cyberattacks which target their systems. The problems are visible and they have opinions on what to search help for.

The challenges that arose in this study would be useful to map with a bigger sample in order to draw more statistically reliable conclusions. In further research, it would be beneficial to study the detection of cyberthreats in small enterprises. Also studying the preparedness for cyberthreats on different lines of business would create an interesting topic for further surveys. With the help of additional research, it would be possible to find ways to help small enterprises in cybersecurity issues.

In the digital era, cybersecurity is a challenge to companies because in addition to the hardware and software used, also the knowhow and motivation of the employees affect the cybersecurity of the company. Through technical solutions, it is possible to increase protection and decrease the risk caused by single individuals. On the other hand, taking care of cybersecurity cannot unreasonably affect the work of the employees as this may lead to not following the cybersecurity policies or to poorer work effiency.

Through cybersecurity, also individuals need to focus more on improving their knowhow in order to survive the changes occurring in the work market. This study reinforces the observations made in the previous study (HRCC) and provides the industry with new research information regarding detecting cyberthreats.

References

Edgar, Thomas W., Manz, David O. 2017. Research methods for cyber security. Syngress.

Finnish Standards Association. 2014. SFS-ISO/IEC 27002 - Information technology. Security techniques. Code of practice for information security controls

Gartner. 2017. Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. Accessed 17 October 2018. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

Hayes, Bob E. 2008. Measuring Customer Satisfaction and Loyalty: Survey Design, Use, and Statistical Analysis Methods.. 3rd Edition.Milwaukee, US: ASQ Quality Press.

Helenius, J. 2018. Poliisin tilastopalvelu - Tietotekniikkarikokset 2008-2018 [Police statistical service – Cybercrimes 2008-2018). E-mail message 22 September 2018. Recipient J. Nevala

Helsinki Region Chamber of Commerce. 2016. Yrityksiin kohdistuvat kyberuhat 2016 [Companies cybersecurity review 2016]. Accessed 15 October 2018. Retrieved from https://helsinki.chamber.fi/media/filer_public/ae/a7/aea76c12-c030-4769-ae3e-19c479d222b0/yrityksiin_kohdistuvat_kyberuhat_2016_naytto.pdf

Helsinki Region Chamber of Commerce. 2018. Business community and hybrid threats 2018. Accessed 15 October 2018. Retrieved from http://view.24mags.com/publication/helsinki.chamber/bbc43250c51aa3c0b599cb18066f3c2b

Huizingh, E. 2007. Applied statistics with SPSS. Sage Publications Ltd. California

Hunt, T. 2018. Have I Peen Pwned – Pwned Websites. Accessed 29 April 2018. Retrieved from https://haveibeenpwned.com/PwnedWebsites

Limnell, J., Majewski, K., Salminen, M. 2015. Cyber security for decision makers. Docendo Oy.

Ministry Of Finance. 2016. EU-tietosuojan kokonaisuudistus [EU data protection reform]. Accessed 15 October 2018. Retrieved from https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229

Ministry of Justice. 2015. Translation - The Criminal Code of Finland. Accessed 25 October 2018. Retrieved from https://www.finlex.fi/en/laki/kaannokset/1889/en18890039_20150766.pdf

Nevala, J., Aho, J. 2016. Keskisuomalaisten yritysten kyberturvallisuus [Central Finland cybersecurity review]. Accessed 29 April 2018. Retrieved from https://www.jao.fi/loader.aspx?id=d66a641b-7235-4df0-af5e-8655d81f39ab

Regional Council of Central Finland. 2017. Financial report 2016. Accessed 23 November 2018. Retrieved from https://www.keskisuomi.fi/filebank/25176-KS_liitto_rahoitusraportti2016_valiversio.pdf

Regional Council of Central Finland. 2014. Central Finland Strategy 2040. Accessed 25 October 2018. Retrieved from http://www.keskisuomi2040.fi/lataukset/2014-06-06-Keski-Suomen-liitto-Keski-Suomen-Strategia-2040.pdf

The Ministry of Economic Affairs and Employment. 2012. Innovatiiviset kaupungit (INKA) -ohjelma [Innovative cities program INKA]. Accessed 25 October 2018. Retrieved from https://tem.fi/hankesivu/-/hankesivu/hanke?tunnus=TEM040%3A00%2F2012

The Security Committee. 2013. Finland´s Cyber security Strategy. Accessed 15 October 2018. Retrieved from https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

The Security Committee. 2017. Security Strategy for Society. Accessed 15 October 2018. Retrieved from https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf

The Security Committee. 2017. Implementation Programme for Finland's Cyber Security Strategy for 2017–2020. Accessed 15 October 2018. Retrieved from https://turvallisuuskomitea.fi/wp-content/uploads/2018/10/Implementation-programme-for-Finlands-Cyber-Security-Strategy-for-2017-2020-final.pdf

Appendices

Appendix 1. Finnish Police crime statistics 2008-2017

List of information security crimes. The statistics have been collected by Police University College in autumn 2018. Statistics are separated, notified and solved.

		2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Ilmoitettu Kpl	SALASSAPITORIKOS	26	30	29	57	45	48	40	48	41	53
Ilmoitettu Kpl	TIETOMURTO	183	140	292	410	503	580	339	347	409	411
Ilmoitettu Kpl	TÖRKEÄ TIETOMURTO	0	0	1	8	14	5	6	3	8	19
Ilmoitettu Kpl	VIESTINTÄSALAISUUDEN LOUKKAUS	214	258	295	297	268	279	297	298	414	364
Ilmoitettu Kpl	VIESTINTÄSALAISUUDEN LOUKKAUKSEN YRITYS	0	3	1	0	1	0	0	1	3	1
Ilmoitettu Kpl	LIEVÄ TIETOLIIKENTEEN HÄIRINTÄ	4	1	8	3	5	9	5	6	9	7
Ilmoitettu Kpl	TIETOLIIKENTEEN HÄIRINNÄN YRITYS	0	0	0	1	1	0	0	1	0	0
Ilmoitettu Kpl	TIETOLIIKENTEEN LIEVÄN HÄIRINNÄN YRITYS	0	0	0	1	0	0	0	0	0	1
Ilmoitettu Kpl	TÖRKEÄ TIETOLIIKENTEEN HÄIRINTÄ	4	6	2	4	7	13	6	3	9	15
Ilmoitettu Kpl	TIETOJÄRJESTELMÄN HÄIRINNÄN YRITYS	0	0	0	0	0	0	1	4	0	0
Ilmoitettu Kpl	TIETOJÄRJESTELMÄN HÄIRINTÄ	3	8	3	3	9	11	11	30	38	24
Ilmoitettu Kpl	TÖRKEÄ TIETOJÄRJESTELMÄN HÄIRINTÄ	0	0	0	0	0	0	3	7	16	14
Ilmoitettu Kpl	SUOJAUKSEN PURKUJÄRJESTELMÄRIKOS	0	0	0	0	0	0	2	0	0	0
Ilmoitettu Kpl	HENKILÖREKISTERIRIKOS	20	38	36	91	148	119	488	122	105	96
Ilmoitettu Kpl	IDENTITEETTIVARKAUS	0	0	0	0	0	0	0	534	3354	3945
Ilmoitettu Kpl	TÖRKEÄ VIESTINTÄSALAISUUDEN LOUKKAUS	4	1	1	1	6	3	4	0	3	1
Ilmoitettu Kpl	TIETOLIIKENTEEN HÄIRINTÄ	36	33	25	79	50	93	57	85	67	62
Ilmoitettu Kpl	**RL 38**	**494**	**518**	**693**	**955**	**1057**	**1160**	**1259**	**1489**	**4476**	**5013**
Ilmoitettu Kpl	DATAVAHINGONTEKO	0	0	0	0	0	0	0	2	14	7
Ilmoitettu Kpl	DATAVAHINGONTEON YRITYS	0	0	0	0	0	0	0	0	1	0
Ilmoitettu Kpl	LIEVÄ DATAVAHINGONTEKO	0	0	0	0	0	0	0	1	0	2
Ilmoitettu Kpl	LIEVÄ VAHINGONTEKO	12 169	11 318	10 015	10 371	9628	9207	8418	8055	7598	7 382
Ilmoitettu Kpl	TÖRKEÄ DATAVAHINGONTEKO	0	0	0	0	0	0	0	0	3	1
Ilmoitettu Kpl	TÖRKEÄ VAHINGONTEKO	240	196	227	221	227	250	235	249	286	250
Ilmoitettu Kpl	TÖRKEÄN VAHINGONTEON YRITYS	15	16	16	8	12	17	18	5	14	15
Ilmoitettu Kpl	VAHINGONTEKO	44 178	39 206	38 948	44 464	34 712	33 946	33 857	29 530	27 451	25 904
Ilmoitettu Kpl	VAHINGONTEON YRITYS	43	36	47	50	44	50	60	29	0	0
Ilmoitettu Kpl	VAARAN AIHEUTTAMINEN TIETOJENKÄSITTELYLLE	7	4	2	7	1	6	36	4	4	8
Ilmoitettu Kpl	LIEVÄ LUVATON KÄYTTÖ	1858	1460	1320	1214	1036	876	667	622	432	304
Ilmoitettu Kpl	LUVATON KÄYTTÖ	2979	2562	2171	2169	2755	1799	1444	1222	1065	1009

Ilmoitettu Kpl	TÖRKEÄ LUVATON KÄYTTÖ	4	10	6	11	12	4	4	5	4	2
Ilmoitettu Kpl	LUVATTOMAN KÄYTÖN YRITYS	66	57	38	52	40	40	33	35	23	21
Ilmoitettu Kpl	TÖRKEÄN LUVATTOMAN KÄYTÖN YRITYS	0	0	0	1	0	0	0	0	0	0
Ilmoitettu Kpl	**Muut yhteensä**	**61 559**	**54 865**	**52 790**	**58 568**	**48 467**	**46 195**	**44 772**	**39 759**	**36 895**	**34 905**
Lähde: Poliisin tilastopalvelu 08/2018		2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Selvitetty Kpl	SALASSAPITORIKOS	16	13	14	16	18	20	15	19	17	20
Selvitetty Kpl	TIETOMURTO	72	63	50	108	145	146	142	42	64	49
Selvitetty Kpl	TÖRKEÄ TIETOMURTO	0	0	0	0	14	2	3	0	7	5
Selvitetty Kpl	VIESTINTÄSALAISUUDEN LOUKKAUS	127	130	189	154	91	201	151	174	143	164
Selvitetty Kpl	VIESTINTÄSALAISUUDEN LOUKKAUKSEN YRITYS	0	2	0	0	0	0	0	0	1	0
Selvitetty Kpl	LIEVÄ TIETOLIIKENTEEN HÄIRINTÄ	2	0	2	1	4	7	1	6	4	1
Selvitetty Kpl	TIETOLIIKENTEEN HÄIRINNÄN YRITYS	0	0	0	0	0	0	0	0	0	0
Selvitetty Kpl	TIETOLIIKENTEEN LIEVÄN HÄIRINNÄN YRITYS	0	0	0	0	0	0	0	0	0	1
Selvitetty Kpl	TÖRKEÄ TIETOLIIKENTEEN HÄIRINTÄ	0	5	1	2	4	10	9	1	5	13
Selvitetty Kpl	TIETOJÄRJESTELMÄN HÄIRINNÄN YRITYS	0	0	0	0	0	0	0	0	0	0
Selvitetty Kpl	TIETOJÄRJESTELMÄN HÄIRINTÄ	0	2	1	1	0	1	3	3	7	13
Selvitetty Kpl	TÖRKEÄ TIETOJÄRJESTELMÄN HÄIRINTÄ	0	0	1	0	0	0	0	1	0	3
Selvitetty Kpl	SUOJAUKSEN PURKUJÄRJESTELMÄRIKOS	0	0	0	0	0	0	0	0	0	0
Selvitetty Kpl	HENKILÖREKISTERIRIKOS	10	30	23	42	99	146	41	1065	566	80
Selvitetty Kpl	IDENTITEETTIVARKAUS	0	0	0	0	0	0	0	28	937	1851
Selvitetty Kpl	TÖRKEÄ VIESTINTÄSALAISUUDEN LOUKKAUS	1	1	5	1	1	2	8	1	1	0
Selvitetty Kpl	TIETOLIIKENTEEN HÄIRINTÄ	9	18	8	37	17	28	15	33	9	31
Selvitetty Kpl	**RL 38**	**237**	**264**	**294**	**362**	**393**	**563**	**388**	**1373**	**1761**	**7228**
Selvitetty Kpl	DATAVAHINGONTEKO	0	0	0	0	0	0	0	0	2	3
Selvitetty Kpl	DATAVAHINGONTEON YRITYS	0	0	0	0	0	0	0	0	0	0
Selvitetty Kpl	LIEVÄ DATAVAHINGONTEKO	0	0	0	0	0	0	0	0	0	1
Selvitetty Kpl	LIEVÄ VAHINGONTEKO	4542	4111	3897	3900	3508	3283	3011	2926	2754	2544
Selvitetty Kpl	TÖRKEÄ DATAVAHINGONTEKO	0	0	0	0	0	0	0	0	0	0
Selvitetty Kpl	TÖRKEÄ VAHINGONTEKO	95	96	121	104	127	100	108	121	163	92
Selvitetty Kpl	TÖRKEÄN VAHINGONTEON YRITYS	6	4	9	6	7	5	8	2	5	4
Selvitetty Kpl	VAHINGONTEKO	8806	7916	7720	7741	6595	6255	5777	5464	4866	4917
Selvitetty Kpl	VAHINGONTEON YRITYS	12	11	10	11	7	14	12	9	1	1
Selvitetty Kpl	VAARAN AIHEUTTAMINEN TIETOJENKÄSITTELYLLE	3	3	1	3	4	1	5	18	9	6
Selvitetty Kpl	LIEVÄ LUVATON KÄYTTÖ	264	236	233	224	192	168	137	147	81	74
Selvitetty Kpl	LUVATON KÄYTTÖ	857	774	748	767	767	638	530	495	459	417
Selvitetty Kpl	TÖRKEÄ LUVATON KÄYTTÖ	0	4	5	7	2	6	2	3	0	1
Selvitetty Kpl	LUVATTOMAN KÄYTÖN YRITYS	16	13	5	12	6	5	4	3	5	4
Selvitetty Kpl	TÖRKEÄN LUVATTOMAN KÄYTÖN YRITYS	0	0	0	0	0	0	0	0	0	0
Selvitetty Kpl	**Muut yhteensä**	**14 601**	**13 168**	**12 749**	**12 775**	**11 215**	**10 475**	**9 594**	**9 188**	**8 345**	**8 064**

Appendix 2. Research question 2016,2017,2018

Updated 10.10.2018, Author: Jarmo Nevala

1. Details of the responder (optional)	2016	2017	2018	Question type
Name	Yes	Yes	Yes	Textfield
Company	Yes	Yes	Yes	Textfield
E-mail	Yes	Yes	Yes	Textfield
2. Location of the Company (optional)	**2016**	**2017**	**2018**	
Hankasalmi	Yes	Yes	Yes	Multiple Choice (one option)
Joutsa	Yes	Yes	Yes	Multiple Choice (one option)
Jyväskylä	Yes	Yes	Yes	Multiple Choice (one option)
Jämsä	Yes	Yes	Yes	Multiple Choice (one option)
Kannonkoski	Yes	Yes	Yes	Multiple Choice (one option)
Karstula	Yes	Yes	Yes	Multiple Choice (one option)
Keuruu	Yes	Yes	Yes	Multiple Choice (one option)
Kinnula	Yes	Yes	Yes	Multiple Choice (one option)
Kivijärvi	Yes	Yes	Yes	Multiple Choice (one option)
Konnevesi	Yes	Yes	Yes	Multiple Choice (one option)
Kuhmoinen	Yes	Yes	Yes	Multiple Choice (one option)
Kyyjärvi	Yes	Yes	Yes	Multiple Choice (one option)
Laukaa	Yes	Yes	Yes	Multiple Choice (one option)
Luhanka	Yes	Yes	Yes	Multiple Choice (one option)
Multia	Yes	Yes	Yes	Multiple Choice (one option)
Muurame	Yes	Yes	Yes	Multiple Choice (one option)
Petäjävesi	Yes	Yes	Yes	Multiple Choice (one option)
Pihtipudas	Yes	Yes	Yes	Multiple Choice (one option)
Saarijärvi	Yes	Yes	Yes	Multiple Choice (one option)
Toivakka	Yes	Yes	Yes	Multiple Choice (one option)
Uurainen	Yes	Yes	Yes	Multiple Choice (one option)
Viitasaari	Yes	Yes	Yes	Multiple Choice (one option)

Äänekoski	Yes	Yes	Yes	Multiple Choice (one option)
3. I am a member of the following organization (optional)?	**2016**	**2017**	**2018**	**Question type**
Suomen yrittäjät (Finnish entrepreneurs)	Yes	Yes	Yes	Check box (multiple options)
Kauppakamari (Chamber of commerce)	Yes	Yes	Yes	Check box (multiple options)
4. What is your position in the company?	**2016**	**2017**	**2018**	**Question type**
Chief executive officer	Yes	Yes	Yes	Multiple Choice (one option)
Entrepreneur / the owner or shareholder of the Company	Yes	Yes	Yes	Multiple Choice (one option)
Other director	Yes	Yes	Yes	Multiple Choice (one option)
Other employee	Yes	Yes	Yes	Multiple Choice (one option)
Person responsible for security matters	Yes	Yes	Yes	Multiple Choice (one option)
IT manager	Yes	Yes	Yes	Multiple Choice (one option)
Some other position, which?	Yes	Yes	Yes	Multiple Choice (one option)
5. Number of employees?	**2016**	**2017**	**2018**	**Question type**
1-4	Yes	Yes	Yes	Multiple Choice (one option)
5-9	Yes	Yes	Yes	Multiple Choice (one option)
10-19	Yes	Yes	Yes	Multiple Choice (one option)
20-49	Yes	Yes	Yes	Multiple Choice (one option)
50-99	Yes	Yes	Yes	Multiple Choice (one option)
100-	Yes	Yes	Yes	Multiple Choice (one option)
6. Where do you do business?	**2016**	**2017**	**2018**	**Question type**
In Finland	Yes	Yes	Yes	Check box (multiple options)
In other EU countries	Yes	Yes	Yes	Check box (multiple options)
Outside the EU	Yes	Yes	Yes	Check box (multiple options)
7. What kind business does your company do?	**2016**	**2017**	**2018**	**Question type**
Business-to-business (B2B)	Yes	Yes	Yes	Check box (multiple options)
Business-to-consumer (B2C)	Yes	Yes	Yes	Check box (multiple options)
Business-to-government (B2G)	Yes	Yes	Yes	Check box (multiple options)

8. The company's main business?	**2016**	**2017**	**2018**	**Question type**
Industry	Yes	Yes	Yes	Multiple Choice (one option)
Construction	Yes	Yes	Yes	Multiple Choice (one option)
Business and trade	Yes	Yes	Yes	Multiple Choice (one option)
Services	Yes	Yes	Yes	Multiple Choice (one option)
Logistics	Yes	Yes	Yes	Multiple Choice (one option)
Technology	Yes	Yes	Yes	Multiple Choice (one option)
Any other, which?	Yes	Yes	Yes	Multiple Choice (one option)
9. With / through / on which devices does your company have access to the Internet?	**2016**	**2017**	**2018**	**Question type**
Desktop computers	Yes	Yes	Yes	Check box (multiple options)
Laptop computers	Yes	Yes	Yes	Check box (multiple options)
Tablet computers	Yes	Yes	Yes	Check box (multiple options)
Smartphones	Yes	Yes	Yes	Check box (multiple options)
Equipment related to company production (IoT)	Yes	Yes	Yes	Check box (multiple options)
Any other, which?	Yes	Yes	Yes	Check box (multiple options)
10.Do you use non-enterprise equipment to manage your business?	**2016**	**2017**	**2018**	**Question type**
Yes	Yes	Yes	Yes	Multiple Choice (one option)
No	Yes	Yes	Yes	Multiple Choice (one option)
11. Is there a security policy for your company?	**2016**	**2017**	**2018**	**Question type**
Yes	Yes	Yes	Yes	Multiple Choice (one option)
No	Yes	Yes	Yes	Multiple Choice (one option)
12. Are you aware of the EU legislation regarding cybersecuroty?	**2016**	**2017**	**2018**	**Question type**
Yes	Yes	Yes	Yes	Multiple Choice (one option)
No	Yes	Yes	Yes	Multiple Choice (one option)
13. Are employees controlled to follow the security policy?	**2016**	**2017**	**2018**	**Question type**
Yes	Yes	Yes	Yes	Multiple Choice (one option)

No	Yes	Yes	Yes	Multiple Choice (one option)
I don't know	Yes	Yes	Yes	Multiple Choice (one option)
I don't want to answer this question	No	No	Yes	Multiple Choice (one option)
14. Which of the following things are covered in your company's security policy?	**2016**	**2017**	**2018**	**Question type**
Use of terminals and tools	Yes	Yes	Yes	Check box (multiple options)
Access rights, login ID, passwords	Yes	Yes	Yes	Check box (multiple options)
Use of the Internet and e-mail	Yes	Yes	Yes	Check box (multiple options)
Security of premises	Yes	Yes	Yes	Check box (multiple options)
Use of social media	Yes	Yes	Yes	Check box (multiple options)
Confidentiality (silence)	Yes	Yes	Yes	Check box (multiple options)
Remote Work and Remote Access	Yes	Yes	Yes	Check box (multiple options)
Responsibilities and organization	Yes	Yes	Yes	Check box (multiple options)
Problems and consequences	Yes	Yes	Yes	Check box (multiple options)
Something else, What?	Yes	Yes	Yes	Check box (multiple options)
The company has no security policy in use	No	No	Yes	Check box (multiple options)
15. Is the staff familiarized with the identification of confidential business information?	**2016**	**2017**	**2018**	**Question type**
Yes	Yes	Yes	Yes	Multiple Choice (one option)
No	Yes	Yes	Yes	Multiple Choice (one option)
I don't know	Yes	Yes	Yes	Multiple Choice (one option)
I don't want to answer this question	No	No	Yes	Multiple Choice (one option)
16. How are company security issues resourced?	**2016**	**2017**	**2018**	**Question type**
Things are handled alongside their own work	Yes	Yes	Yes	Multiple Choice (one option)
There is a hired person to this job	Yes	Yes	Yes	Multiple Choice (one option)
The task has been outsourced	Yes	Yes	Yes	Multiple Choice (one option)
This is not a single person's responsibility	Yes	Yes	Yes	Multiple Choice (one option)
Something else, What?	Yes	Yes	Yes	Multiple Choice (one option)
I don't want to answer this question	No	No	Yes	Multiple Choice (one option)

17. What disruption situations has your company prepared for?	**2016**	**2017**	**2018**	**Question type**
Abuse	Yes	Yes	Yes	Check box (multiple options)
System malfunction	Yes	Yes	Yes	Check box (multiple options)
Power outages	Yes	Yes	Yes	Check box (multiple options)
Information leaks	Yes	Yes	Yes	Check box (multiple options)
The company is not prepared for disturbances	Yes	Yes	Yes	Check box (multiple options)
Something else, What?	Yes	Yes	Yes	Check box (multiple options)
18. How important do you consider securing the following things?	**2016**	**2017**	**2018**	**Question type**
Customer register	Yes	Yes	Yes	Not important (Value: 1) - Very important (Value: 5)
Products / Product details	Yes	Yes	Yes	Not important (Value: 1) - Very important (Value: 5)
Financial management	Yes	Yes	Yes	Not important (Value: 1) - Very important (Value: 5)
Own skills, know-how	Yes	Yes	Yes	Not important (Value: 1) - Very important (Value: 5)
Research & development information	Yes	Yes	Yes	Not important (Value: 1) - Very important (Value: 5)
Banking details	Yes	Yes	Yes	Not important (Value: 1) - Very important (Value: 5)
Securing / updating computer hardware	No	Yes	Yes	Not important (Value: 1) - Very important (Value: 5)
19. Which of the following issues do you consider a major cyber security threat in your business?	**2016**	**2017**	**2018**	**Question type**
Internal threat of the company (own employees)	Yes	Yes	Yes	Not high (Value: 1) - Very large (Value: 5)
Phishing and malware attacks	Yes	Yes	Yes	Not high (Value: 1) - Very large (Value: 5)
Intrusion to information systems	Yes	Yes	Yes	Not high (Value: 1) - Very large (Value: 5)
DDoS (to prevent the operation of the web service)	Yes	Yes	Yes	Not high (Value: 1) - Very large (Value: 5)
Attacks targeting to company's production process (e.g. network-connected production equipment or device (IoT))	Yes	Yes	Yes	Not high (Value: 1) - Very large (Value: 5)

Ransom malmware (encrypters which asks for ransom)	No	Yes	Yes	Not high (Value: 1) - Very large (Value: 5)
Computers that have not been upgraded	No	Yes	Yes	Not high (Value: 1) - Very large (Value: 5)
20. How big an obstacle do you consider the following issues to be to make effective cyber safety (more) effective in your company?	**2016**	**2017**	**2018**	**Question type**
The difficulty of finding skilled professionals	Yes	Yes	Yes	Not high (Value: 1) - Very large (Value: 5)
Maintaining the knowledge of current staff regarding cyberthreats	Yes	Yes	Yes	Not high (Value: 1) - Very large (Value: 5)
Personnel's disregard for information security and cyberthreats	Yes	Yes	Yes	Not high (Value: 1) - Very large (Value: 5)
Insufficiency of information related to cyber security	Yes	Yes	Yes	Not high (Value: 1) - Very large (Value: 5)
Insufficiency of information related to security measures and methods	Yes	Yes	Yes	Not high (Value: 1) - Very large (Value: 5)
Inappropriate / obsolete tools (software and devices with network connection)	Yes	Yes	Yes	Not high (Value: 1) - Very large (Value: 5)
The lack of cyber security services in the area of Central Finland	No	Yes	Yes	Not high (Value: 1) - Very large (Value: 5)
21. How significant do you consider the consequences of the following cyberattacks?	**2016**	**2017**	**2018**	**Question type**
Loss of immovable property	Yes	Yes	Yes	Not high (Value: 1) - Very large (Value: 5)
Negative publicity	Yes	Yes	Yes	Not high (Value: 1) - Very large (Value: 5)
Loss of market share	Yes	Yes	Yes	Not high (Value: 1) - Very large (Value: 5)
Infringement of Privacy (staff or customer)	Yes	Yes	Yes	Not high (Value: 1) - Very large (Value: 5)
Loss of income - Direct or indirect	Yes	Yes	Yes	Not high (Value: 1) - Very large (Value: 5)
Business interruption	No	Yes	Yes	Not high (Value: 1) - Very large (Value: 5)
Criminal liability	No	Yes	Yes	Not high (Value: 1) - Very large (Value: 5)
Damage payment to the customer	No	Yes	Yes	Not high (Value: 1) - Very large (Value: 5)
22. Main development targets for your company's cybersecurity?	**2016**	**2017**	**2018**	**Question type**
Own / entrepreneur's knowledge of information security	Yes	Yes	Yes	Check box (multiple options)

Competence of staff / users	Yes	Yes	Yes	Check box (multiple options)
Backup / backups	Yes	Yes	Yes	Check box (multiple options)
Increasing education / knowledge	Yes	Yes	Yes	Check box (multiple options)
Equipment / hardware / machines	Yes	Yes	Yes	Check box (multiple options)
Backup systems	Yes	Yes	Yes	Check box (multiple options)
Upgrading software	Yes	Yes	Yes	Check box (multiple options)
Access control	Yes	Yes	Yes	Check box (multiple options)
Something else, What?	Yes	Yes	Yes	Check box (multiple options)
I don't want to answer this question	No	No	Yes	Check box (multiple options)
23. Do you believe you are aware of the cyberthreats to your organization?	**2016**	**2017**	**2018**	**Question type**
Yes	No	Yes	Yes	Multiple Choice (one option)
No	No	Yes	Yes	Multiple Choice (one option)
I don't know	No	Yes	Yes	Multiple Choice (one option)
24. Do you believe that your organization will be able to detect cyberattacks?	**2016**	**2017**	**2018**	**Question type**
Yes	No	Yes	Yes	Multiple Choice (one option)
No	No	Yes	Yes	Multiple Choice (one option)
I don't know	No	Yes	Yes	Multiple Choice (one option)
I don't want to answer this question	No	No	Yes	Multiple Choice (one option)
25. Do you think that the risk of a cyberattack has increased during the past year?	**2016**	**2017**	**2018**	**Question type**
Yes	No	Yes	Yes	Multiple Choice (one option)
No	No	Yes	Yes	Multiple Choice (one option)
I don't know	No	Yes	Yes	Multiple Choice (one option)
26. Do you think that the need to prepare for cyberattacks has changed in your organization during the past year?	**2016**	**2017**	**2018**	**Question type**
Yes	No	Yes	Yes	Multiple Choice (one option)
No	No	Yes	Yes	Multiple Choice (one option)

I don't know	No	Yes	Yes	Multiple Choice (one option)
I don't want to answer this question	No	No	Yes	Multiple Choice (one option)
27. How likely do you think that	**2016**	**2017**	**2018**	**Question type**
Your organization has been targetted cyber/information leak by anyone not knowing it?	No	Yes	Yes	I totally agree (Value: 5) - I totally disagree (Value: 1)
Your organization will be subjected to a cyberattack in the next year?	No	Yes	Yes	I totally agree (Value: 5) - I totally disagree (Value: 1)
28. Which of the following security threats have occurred in your company?	**2016**	**2017**	**2018**	**Question type**
User IDs and passwords have been stolen and have been misused	23.Yes	Yes	Yes	Check box (multiple options)
Ransomware has locked a computer	No	Yes	Yes	Check box (multiple options)
There have been attempts to spy on work related information	23.Yes	Yes	Yes	Check box (multiple options)
Identity has been stolen and has been misused	23.Yes	Yes	Yes	Check box (multiple options)
The organization has lost money because of online scams	23.Yes	Yes	Yes	Check box (multiple options)
Company data has leaked	23.Yes	Yes	Yes	Check box (multiple options)
The company has lost important information due to hardware failure	23.Yes	Yes	Yes	Check box (multiple options)
A terminal (phone, computer, etc..) has been stolen or lost	23.Yes	Yes	Yes	Check box (multiple options)
An employee has been exposed or has become aware of the confidential information he or she has not been entitled to	23.Yes	Yes	Yes	Check box (multiple options)
The workplace credit card has been misused	23.Yes	Yes	Yes	Check box (multiple options)
A security breach / denial of service has been targeted to the company	23.Yes	Yes	Yes	Check box (multiple options)
The company has not been exposed to a security breach	23.Yes	Yes	Yes	Check box (multiple options)
Something else, What?	23.Yes	Yes	Yes	Check box (multiple options)
I don't want to answer this question	23.No	No	Yes	Check box (multiple options)
29. How did you find out about the security threat referred to in the previous question?	**2016**	**2017**	**2018**	**Question type**
We detected it ourselves using our own prevention and intrusion detection systems	24.Yes	Yes	Yes	Check box (multiple options)
Our users recognized it and reported it	24.Yes	Yes	Yes	Check box (multiple options)
We recognized it by ourselves because we checked and analyzed our logs	24.Yes	Yes	Yes	Check box (multiple options)

Law enforcement/intelligence organizations warned us	24.Yes	Yes	Yes	Check box (multiple options)
Third party, such as an internet operator or service provider, informed us	24.Yes	Yes	Yes	Check box (multiple options)
Something else, What?	24.Yes	Yes	Yes	Check box (multiple options)
I don't want to answer this question	No	No	Yes	Check box (multiple options)
30. What kind of information do you think intruders are looking for?	**2016**	**2017**	**2018**	**Question type**
Personal information of senior management	25.Yes	Yes	Yes	Check box (multiple options)
Personnel information such as names, responsibilities and units	25.Yes	Yes	Yes	Check box (multiple options)
Information of subcontractors, partners, suppliers, or customers	25.Yes	Yes	Yes	Check box (multiple options)
Confidential information about our products or services	25.Yes	Yes	Yes	Check box (multiple options)
Network related information, such as network structure and other devices on your company network	25.Yes	Yes	Yes	Check box (multiple options)
I don't know	25.Yes	Yes	Yes	Check box (multiple options)
Something else, What?	25.Yes	Yes	Yes	Check box (multiple options)
I don't want to answer this question	No	No	Yes	Check box (multiple options)
31. Was the police notified for a breach of information or cyberattack?	**2016**	**2017**	**2018**	**Question type**
Yes	No	Yes	Yes	Multiple Choice (one option)
No	No	Yes	Yes	Multiple Choice (one option)
I don't know	No	Yes	Yes	Multiple Choice (one option)
I don't want to answer this question	No	No	Yes	Multiple Choice (one option)
32. Did the information breach or cyberattack become public or come to customers´ knowledge?	**2016**	**2017**	**2018**	**Question type**
Yes	No	Yes	Yes	Multiple Choice (one option)
No	No	Yes	Yes	Multiple Choice (one option)
I don't know	No	Yes	Yes	Multiple Choice (one option)
I don't want to answer this question	No	No	Yes	Multiple Choice (one option)
33. Have your company's employees attended an information security training during the past year?	**2016**	**2017**	**2018**	**Question type**

No	26. Yes	Yes	Yes	Multiple Choice (one option)
Yes, Where?	26. Yes	Yes	Yes	Multiple Choice (one option)
34. Are you familiar with FICORA's instructions and warnings (cyber security)	**2016**	**2017**	**2018**	**Question type**
No	No	Yes	Yes	Multiple Choice (one option)
Yes	No	Yes	Yes	Multiple Choice (one option)
35. In which information security areas would you like to receive more training?	**2016**	**2017**	**2018**	**Question type**
Administrative Security - Information security leading and control	27.Yes	Yes	Yes	Check box (multiple options)
Physical security - Physical protection of premises and equipment	27.Yes	Yes	Yes	Check box (multiple options)
Hardware security - For example, general protection of the computer	27.Yes	Yes	Yes	Check box (multiple options)
Software Security - Software security issues	27.Yes	Yes	Yes	Check box (multiple options)
Security of data files - Handling and protecting electronic and paper documents	27.Yes	Yes	Yes	Check box (multiple options)
Telecommunications security - For example, data transfer security mechanisms	27.Yes	Yes	Yes	Check box (multiple options)
Personnel Safety - Issues related to roles, responsibilities, and information security	27.Yes	Yes	Yes	Check box (multiple options)
Operational security - For example, passwords	27.Yes	Yes	Yes	Check box (multiple options)
Something else, What?	27.Yes	Yes	Yes	Check box (multiple options)
36. Once you have hired a new person, they have	**2016**	**2017**	**2018**	**Question type**
Vocational qualification	30.Yes	Yes	Yes	Check box (multiple options)
Bachelor's Degree	30.Yes	Yes	Yes	Check box (multiple options)
Master's Degree	30.Yes	Yes	Yes	Check box (multiple options)
We have not hired new employees	No	Yes	Yes	Check box (multiple options)
Something else, What?	30.Yes	Yes	Yes	Check box (multiple options)
37. Evaluate the IT skills level of new employees	**2016**	**2017**	**2018**	**Question type**
Weak	31.Yes	Yes	Yes	Multiple Choice (one option)
Average	31.Yes	Yes	Yes	Multiple Choice (one option)
Good	31.Yes	Yes	Yes	Multiple Choice (one option)

We have not hired new employees	No	Yes	Yes	Multiple Choice (one option)
38. Comments	**2016**	**2017**	**2018**	**Question type**
	36.Yes	Yes	Yes	Textfield

Appendix 3. Example on 2018 survey form

Keski-Suomen kyberturvallisuuden tilanne

Keskisuomalaisten yritysten kyberturvallisuuskysely on toteutettu aikaisemmin 2016 ja 2017. Nyt on kyselyn viimeinen kerta, jonka jälkeen tuloksista tullaan muodostamaan kolmen vuoden kooste YAMK opinnäytetyönä.

Kyberuhat koskettavat meistä jokaista, joten on tärkeää, että yrityksissä ja koulutussektorilla osaaminen on ajan tasalla. Kyberturvallisuus on noussut myös Keski-Suomen strategian painopistealueeksi. Jotta voisimme kehittää tulevaisuudessa osaamista tietoturvan eri osa-alueista, tarvitsemme yritysmaailman tilannetietoutta.

Vastaamalla kyselyyn annat tärkeää tietoa siitä, miten tietoturvallisuus on huomioitu tällä hetkellä yrityksissä ja osallistut Keski-Suomen elinkeinoelämän kyberturvallisuuden sekä koulutuksen kehittämiseen. Annat myös omalta osaltasi tietoa siitä, miten tietoturvallisuus on huomioitu yrityksessänne tällä hetkellä.

Kysely pitää sisällään 38 kysymystä, jotka ovat pääasiassa monivalinta ja mielipidekysymyksiä. Aikaa vastaamiseen menee noin 15 minuuttia. Edellisestä kyselystä tuli myös palautetta, joten osaan kysymyksistä on laitettu myös vastaus vaihtoehdoksi "En halua vastata kysymykseen".

Kysely on avoinna 08.06.2018 saakka. Vastaajan henkilötietoja ei luovuteta eteenpäin.

Kiitos vastaamisesta!

Lisätietoja: Jarmo Nevala, jarmo.nevala@gradia.fi, 0403415715

1. Vastaajan tiedot (vapaaehtoinen)

Nimi	
Yritys	
Sähköpostiosoite	

2. Yrityksen toimipaikka (vapaaehtoinen)

Valitse

3. Olen alla olevan järjestön jäsen (vapaaehtoinen)?

- ☐ Suomen yrittäjät
- ☐ Kauppakamari

4. Asemanne yrityksessä? *

- ○ Toimitusjohtaja
- ○ Yrittäjä/omistaja
- ○ Muu johtaja
- ○ Muu työntekijä
- ○ Tietoturva-asioista vastaava henkilö
- ○ Tietohallintopäällikkö
- ○ Jokin muu, mikä

5. Henkilöstön määrä? *

- ○ 1-4
- ○ 5-9
- ○ 10-19
- ○ 20-49

Appendix 4. Correlation table on question 18. from 2018

2018 - Question 18. How important do you consider securing the following things?		Customer register	Products / Product details	Financial management	Own skills, know-how	Research & development information	Banking details	Securing / updating computer hardware
Customer register	Pearson Correlation	1	0.152	.305**	0.107	0.038	.304**	0.171
	Sig. (2-tailed)		0.185	0.007	0.351	0.738	0.007	0.134
	N	78	78	78	78	78	78	78
Products / Product details	Pearson Correlation	0.152	1	0.222	.357**	.469**	0.131	.259*
	Sig. (2-tailed)	0.185		0.051	0.001	0.000	0.252	0.022
	N	78	78	78	78	78	78	78
Financial management	Pearson Correlation	.305**	0.222	1	.353**	.429**	.308**	0.125
	Sig. (2-tailed)	0.007	0.051		0.002	0.000	0.006	0.275
	N	78	78	78	78	78	78	78
Own skills. know-how	Pearson Correlation	0.107	.357**	.353**	1	.451**	0.147	.319**
	Sig. (2-tailed)	0.351	0.001	0.002		0.000	0.198	0.004
	N	78	78	78	78	78	78	78
Research & development information	Pearson Correlation	0.038	.469**	.429**	.451**	1	0.000	.232*
	Sig. (2-tailed)	0.738	0.000	0.000	0.000		1.000	0.041
	N	78	78	78	78	78	78	78
Banking details	Pearson Correlation	.304**	0.131	.308**	0.147	0.000	1	0.222
	Sig. (2-tailed)	0.007	0.252	0.006	0.198	1.000		0.051
	N	78	78	78	78	78	78	78
Securing / updating computer hardware	Pearson Correlation	0.171	.259*	0.125	.319**	.232*	0.222	1
	Sig. (2-tailed)	0.134	0.022	0.275	0.004	0.041	0.051	
	N	78	78	78	78	78	78	78
**. Correlation is significant at the 0.01 level (2-tailed).								
*. Correlation is significant at the 0.05 level (2-tailed).								

Appendix 5. Correlation table on question 18. from 2017

2017 - Question 18. How important do you consider securing the following things?		Customer register	Products / Product details	Financial management	Own skills, know-how	Research & development information	Banking details	Securing / updating computer hardware
Customer register	Pearson Correlation	1	,340**	,343**	0,120	,290**	,397**	,582**
	Sig. (2-tailed)		0,001	0,001	0,236	0,004	0,000	0,000
	N	100	98	99	100	99	97	100
Products / Product details	Pearson Correlation	,340**	1	0,167	,405**	,555**	,247*	,260**
	Sig. (2-tailed)	0,001		0,101	0,000	0,000	0,016	0,010
	N	98	98	97	98	97	95	98
Financial management	Pearson Correlation	,343**	0,167	1	,357**	,219*	,471**	,380**
	Sig. (2-tailed)	0,001	0,101		0,000	0,030	0,000	0,000
	N	99	97	99	99	98	96	99
Own skills, know-how	Pearson Correlation	0,120	,405**	,357**	1	,445**	,278**	,201*
	Sig. (2-tailed)	0,236	0,000	0,000		0,000	0,006	0,045
	N	100	98	99	100	99	97	100
Research & development information	Pearson Correlation	,290**	,555**	,219*	,445**	1	0,122	,231*
	Sig. (2-tailed)	0,004	0,000	0,030	0,000		0,238	0,021
	N	99	97	98	99	99	96	99
Banking details	Pearson Correlation	,397**	,247*	,471**	,278**	0,122	1	,451**
	Sig. (2-tailed)	0,000	0,016	0,000	0,006	0,238		0,000
	N	97	95	96	97	96	97	97
Securing / updating computer hardware	Pearson Correlation	,582**	,260**	,380**	,201*	,231*	,451**	1
	Sig. (2-tailed)	0,000	0,010	0,000	0,045	0,021	0,000	
	N	100	98	99	100	99	97	100

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Appendix 6. Correlation table on question 18. from 2016

2016 - Question 18. How important do you consider securing the following things?		Customer register	Products / Product details	Financial management	Own skills, know-how	Research & development information	Banking details
Customer register	Pearson Correlation	1	.387**	.406**	.286**	.322**	.285**
	Sig. (2-tailed)		0.000	0.000	0.000	0.000	0.000
	N	194	191	185	191	189	192
Products / Product details	Pearson Correlation	.387**	1	.274**	.543**	.532**	0.077
	Sig. (2-tailed)	0.000		0.000	0.000	0.000	0.292
	N	191	191	182	189	187	189
Financial management	Pearson Correlation	.406**	.274**	1	.221**	.310**	.381**
	Sig. (2-tailed)	0.000	0.000		0.003	0.000	0.000
	N	185	182	185	182	180	183
Own skills, know-how	Pearson Correlation	.286**	.543**	.221**	1	.395**	0.032
	Sig. (2-tailed)	0.000	0.000	0.003		0.000	0.659
	N	191	189	182	191	187	189
Research & development information	Pearson Correlation	.322**	.532**	.310**	.395**	1	0.033
	Sig. (2-tailed)	0.000	0.000	0.000	0.000		0.656
	N	189	187	180	187	189	187
Banking details	Pearson Correlation	.285**	0.077	.381**	0.032	0.033	1
	Sig. (2-tailed)	0.000	0.292	0.000	0.659	0.656	
	N	192	189	183	189	187	192

**. Correlation is significant at the 0.01 level (2-tailed).

Appendix 7. Correlation table on question 19. from 2018

2018 - Question 19. Which of the following issues do you consider a major cyber security threat in your business?		Internal threat of the company (own employees)	Phishing and malware attacks	Intrusion to information systems	DDoS (to prevent the operation of the web service)	Attacks targeting to company's production process (e.g. network...)	Ransom malmware (encrypters which asks for ransom)	Computers that have not been upgraded
Internal threat of the company (own employees)	Pearson Correlation	1	0.087	0.052	0.086	0.045	.262*	0.157
	Sig. (2-tailed)		0.447	0.654	0.455	0.693	0.021	0.170
	N	78	78	78	78	78	78	78
Phishing and malware attacks	Pearson Correlation	0.087	1	.750**	.532**	.238*	.475**	.315**
	Sig. (2-tailed)	0.447		0.000	0.000	0.036	0.000	0.005
	N	78	78	78	78	78	78	78
Intrusion to information systems	Pearson Correlation	0.052	.750**	1	.787**	.417**	.455**	.377**
	Sig. (2-tailed)	0.654	0.000		0.000	0.000	0.000	0.001
	N	78	78	78	78	78	78	78
DDoS (to prevent the operation of the web service)	Pearson Correlation	0.086	.532**	.787**	1	.444**	.440**	.392**
	Sig. (2-tailed)	0.455	0.000	0.000		0.000	0.000	0.000
	N	78	78	78	78	78	78	78
Attacks targeting to company's production process (e.g. network-connected production equipment or device (IoT))	Pearson Correlation	0.045	.238*	.417**	.444**	1	.263*	0.214
	Sig. (2-tailed)	0.693	0.036	0.000	0.000		0.020	0.060
	N	78	78	78	78	78	78	78
Ransom malmware (encrypters which asks for ransom)	Pearson Correlation	.262*	.475**	.455**	.440**	.263*	1	.374**
	Sig. (2-tailed)	0.021	0.000	0.000	0.000	0.020		0.001
	N	78	78	78	78	78	78	78
Computers that have not been upgraded	Pearson Correlation	0.157	.315**	.377**	.392**	0.214	.374**	1
	Sig. (2-tailed)	0.170	0.005	0.001	0.000	0.060	0.001	
	N	78	78	78	78	78	78	78

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

Appendix 8. Correlation table on question 19. from 2017

2017 - Question 19. Which of the following issues do you consider a major cyber security threat in your business?		Internal threat of the company (own employees)	Phishing and malware attacks	Intrusion to information systems	DDoS (to prevent the operation of the web service)	Attacks targeting to company's production process (e.g. network-connected production equipment or device (IoT))	Ransom malmware (encrypters which asks for ransom)	Computers that have not been upgraded
Internal threat of the company (own employees)	Pearson Correlation	1	.395**	.322**	.290**	.393**	.313**	0.096
	Sig. (2-tailed)		0.000	0.001	0.004	0.000	0.002	0.348
	N	97	94	97	95	97	95	97
Phishing and malware attacks	Pearson Correlation	.395**	1	.750**	.537**	.515**	.495**	.293**
	Sig. (2-tailed)	0.000		0.000	0.000	0.000	0.000	0.004
	N	94	94	94	92	94	92	94
Intrusion to information systems	Pearson Correlation	.322**	.750**	1	.668**	.464**	.476**	.293**
	Sig. (2-tailed)	0.001	0.000		0.000	0.000	0.000	0.004
	N	97	94	97	95	97	95	97
DDoS (to prevent the operation of the web service)	Pearson Correlation	.290**	.537**	.668**	1	.608**	.495**	.327**
	Sig. (2-tailed)	0.004	0.000	0.000		0.000	0.000	0.001
	N	95	92	95	95	95	93	95
Attacks targeting to company's production process (e.g. network-connected production equipment or device (IoT))	Pearson Correlation	.393**	.515**	.464**	.608**	1	.499**	.381**
	Sig. (2-tailed)	0.000	0.000	0.000	0.000		0.000	0.000
	N	97	94	97	95	97	95	97
Ransom malmware (encrypters which asks for ransom)	Pearson Correlation	.313**	.495**	.476**	.495**	.499**	1	.368**
	Sig. (2-tailed)	0.002	0.000	0.000	0.000	0.000		0.000
	N	95	92	95	93	95	95	95
Computers that have not been upgraded	Pearson Correlation	0.096	.293**	.293**	.327**	.381**	.368**	1

	Sig. (2-tailed)	0.348	0.004	0.004	0.001	0.000	0.000	
	N	97	94	97	95	97	95	97
**. Correlation is significant at the 0.01 level (2-tailed).								

Appendix 9. Correlation table on question 19. from 2016

2016 - Question 19. Which of the following issues do you consider a major cyber security threat in your business?		Internal threat of the company (own employees)	Phishing and malware attacks	Intrusion to information systems	DDoS (to prevent the operation of the web service)	Attacks targeting to company's production process (e.g. network-connected production equipment or device (IoT))
Internal threat of the company (own employees)	Pearson Correlation	1	.250**	.184*	.216**	.416**
	Sig. (2-tailed)		0.001	0.012	0.003	0.000
	N	191	189	187	191	188
Phishing and malware attacks	Pearson Correlation	.250**	1	.709**	.573**	.425**
	Sig. (2-tailed)	0.001		0.000	0.000	0.000
	N	189	190	186	190	187
Intrusion to information systems	Pearson Correlation	.184*	.709**	1	.582**	.437**
	Sig. (2-tailed)	0.012	0.000		0.000	0.000
	N	187	186	188	188	186
DDoS (to prevent the operation of the web service)	Pearson Correlation	.216**	.573**	.582**	1	.535**
	Sig. (2-tailed)	0.003	0.000	0.000		0.000
	N	191	190	188	192	189
Attacks targeting to company's production process (e.g. network-connected production equipment or device (IoT))	Pearson Correlation	.416**	.425**	.437**	.535**	1
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	
	N	188	187	186	189	189
**. Correlation is significant at the 0.01 level (2-tailed).						
*. Correlation is significant at the 0.05 level (2-tailed).						

Appendix 10. Correlation table on question 20. from 2018

2018 - Question 20. How big an obstacle do you consider the following issues to be to make effective cyber safety (more) effective in your company?		The difficulty of finding skilled professionals	Maintaining the knowledge of current staff regarding cyberthreats	Personnel's disregard for information security and cyberthreats	Insufficiency of information related to cyber security	Insufficiency of information related to security measures and methods	Inappropriate / obsolete tools (software and devices with network connection)	The lack of cyber security services in the area of Central Finland
The difficulty of finding skilled professionals	Pearson Correlation	1	,379**	,419**	,431**	,484**	,343**	,487**
	Sig. (2-tailed)		0,001	0,000	0,000	0,000	0,002	0,000
	N	78	78	78	78	78	78	78
Maintaining the knowledge of current staff regarding cyberthreats	Pearson Correlation	.379**	1	,486**	,637**	,656**	,522**	,336**
	Sig. (2-tailed)	0.001		0,000	0,000	0,000	0,000	0,003
	N	78	78	78	78	78	78	78
Personnel's disregard for information security and cyberthreats	Pearson Correlation	.419**	,486**	1	,432**	,449**	,415**	,267*
	Sig. (2-tailed)	0.000	0,000		0,000	0,000	0,000	0,018
	N	78	78	78	78	78	78	78
Insufficiency of information related to cyber security	Pearson Correlation	.431**	,637**	,432**	1	,739**	,637**	,415**
	Sig. (2-tailed)	0.000	0,000	0,000		0,000	0,000	0,000
	N	78	78	78	78	78	78	78
Insufficiency of information related to security measures and methods	Pearson Correlation	.484**	,656**	,449**	,739**	1	,619**	,433**
	Sig. (2-tailed)	0.000	0,000	0,000	0,000		0,000	0,000
	N	78	78	78	78	78	78	78
Inappropriate / obsolete tools (software and devices with network connection)	Pearson Correlation	.343**	,522**	,415**	,637**	,619**	1	,498**
	Sig. (2-tailed)	0.002	0,000	0,000	0,000	0,000		0,000
	N	78	78	78	78	78	78	78
The lack of cyber security services in the area of Central Finland	Pearson Correlation	.487**	,336**	,267*	,415**	,433**	,498**	1
	Sig. (2-tailed)	0.000	0,003	0,018	0,000	0,000	0,000	
	N	78	78	78	78	78	78	78
**. Correlation is significant at the 0.01 level (2-tailed).								
*. Correlation is significant at the 0.05 level (2-tailed).								

Appendix 11. Correlation table on question 20. from 2017

2017 - Question 20. How big an obstacle do you consider the following issues to be to make effective cyber safety (more) effective in your company?		The difficulty of finding skilled professionals	Maintaining the knowledge of current staff regarding cyberthreats	Personnel's disregard for information security and cyberthreats	Insufficiency of information related to cyber security	Insufficiency of information related to security measures and methods	Inappropriate / obsolete tools (software and devices with network connection)	The lack of cyber security services in the area of Central Finland
The difficulty of finding skilled professionals	Pearson Correlation	1	.597**	.550**	.442**	.515**	.514**	.598**
	Sig. (2-tailed)		0.000	0.000	0.000	0.000	0.000	0.000
	N	95	92	95	95	92	95	94
Maintaining the knowledge of current staff regarding cyberthreats	Pearson Correlation	.597**	1	.713**	.596**	.714**	.619**	.441**
	Sig. (2-tailed)	0.000		0.000	0.000	0.000	0.000	0.000
	N	92	92	92	92	90	92	91
Personnel's disregard for information security and cyberthreats	Pearson Correlation	.550**	.713**	1	.577**	.651**	.578**	.419**
	Sig. (2-tailed)	0.000	0.000		0.000	0.000	0.000	0.000
	N	95	92	95	95	92	95	94
Insufficiency of information related to cyber security	Pearson Correlation	.442**	.596**	.577**	1	.831**	.545**	.508**
	Sig. (2-tailed)	0.000	0.000	0.000		0.000	0.000	0.000
	N	95	92	95	95	92	95	94
Insufficiency of information related to security measures and methods	Pearson Correlation	.515**	.714**	.651**	.831**	1	.625**	.542**
	Sig. (2-tailed)	0.000	0.000	0.000	0.000		0.000	0.000
	N	92	90	92	92	92	92	91
Inappropriate / obsolete tools (software and devices with network connection)	Pearson Correlation	.514**	.619**	.578**	.545**	.625**	1	.524**
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000		0.000
	N	95	92	95	95	92	95	94
The lack of cyber security services in the area of Central Finland	Pearson Correlation	.598**	.441**	.419**	.508**	.542**	.524**	1
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000	0.000	
	N	94	91	94	94	91	94	94

**. Correlation is significant at the 0.01 level (2-tailed).

Appendix 12. Correlation table on question 20. from 2016

2016 - Question 20. How big an obstacle do you consider the following issues to be to make effective cyber safety (more) effective in your company?		The difficulty of finding skilled professionals	Maintaining the knowledge of current staff regarding cyberthreats	Personnel's disregard for information security and cyberthreats	Insufficiency of information related to cyber security	Insufficiency of information related to security measures and methods	Inappropriate / obsolete tools (software and devices with network connection)
The difficulty of finding skilled professionals	Pearson Correlation	1	.631**	.345**	.510**	.585**	.276**
	Sig. (2-tailed)		0.000	0.000	0.000	0.000	0.000
	N	185	182	183	183	182	182
Maintaining the knowledge of current staff regarding cyberthreats	Pearson Correlation	.631**	1	.569**	.600**	.661**	.339**
	Sig. (2-tailed)	0.000		0.000	0.000	0.000	0.000
	N	182	185	183	183	182	182
Personnel's disregard for information security and cyberthreats	Pearson Correlation	.345**	.569**	1	.517**	.532**	.432**
	Sig. (2-tailed)	0.000	0.000		0.000	0.000	0.000
	N	183	183	186	184	183	183
Insufficiency of information related to cyber security	Pearson Correlation	.510**	.600**	.517**	1	.835**	.516**
	Sig. (2-tailed)	0.000	0.000	0.000		0.000	0.000
	N	183	183	184	186	184	184
Insufficiency of information related to security measures and methods	Pearson Correlation	.585**	.661**	.532**	.835**	1	.507**
	Sig. (2-tailed)	0.000	0.000	0.000	0.000		0.000
	N	182	182	183	184	185	183
Inappropriate / obsolete tools (software and devices with network connection)	Pearson Correlation	.276**	.339**	.432**	.516**	.507**	1
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000	
	N	182	182	183	184	183	185

**. Correlation is significant at the 0.01 level (2-tailed).

Appendix 13. Correlation table on question 21. from 2018

2018 - Question 21. How significant do you consider the consequences of the following cyberattacks?		Loss of immovable property	Negative publicity	Loss of market share	Infringement of Privacy (staff or cust.)	Loss of income - Direct or indir.	Business interruption	Criminal liability	Damage payment to the customer
Loss of immovable property	Pearson Correlation	1	.389**	.565**	.513**	.602**	.422**	.410**	.512**
	Sig. (2-tailed)		0.000	0.000	0.000	0.000	0.000	0.000	0.000
	N	78	78	78	78	78	78	78	78
Negative publicity	Pearson Correlation	.389**	1	.533**	.611**	.441**	.325**	.527**	.499**
	Sig. (2-tailed)	0.000		0.000	0.000	0.000	0.004	0.000	0.000
	N	78	78	78	78	78	78	78	78
Loss of market share	Pearson Correlation	.565**	.533**	1	.469**	.674**	.565**	.492**	.575**
	Sig. (2-tailed)	0.000	0.000		0.000	0.000	0.000	0.000	0.000
	N	78	78	78	78	78	78	78	78
Infringement of Privacy (staff or customer)	Pearson Correlation	.513**	.611**	.469**	1	.611**	.467**	.715**	.667**
	Sig. (2-tailed)	0.000	0.000	0.000		0.000	0.000	0.000	0.000
	N	78	78	78	78	78	78	78	78
Loss of income - Direct or indirect	Pearson Correlation	.602**	.441**	.674**	.611**	1	.738**	.673**	.636**
	Sig. (2-tailed)	0.000	0.000	0.000	0.000		0.000	0.000	0.000
	N	78	78	78	78	78	78	78	78
Business interruption	Pearson Correlation	.422**	.325**	.565**	.467**	.738**	1	.709**	.578**
	Sig. (2-tailed)	0.000	0.004	0.000	0.000	0.000		0.000	0.000
	N	78	78	78	78	78	78	78	78
Criminal liability	Pearson Correlation	.410**	.527**	.492**	.715**	.673**	.709**	1	.796**
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000	0.000		0.000
	N	78	78	78	78	78	78	78	78
Damage payment to the customer	Pearson Correlation	.512**	.499**	.575**	.667**	.636**	.578**	.796**	1
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000	0.000	0.000	
	N	78	78	78	78	78	78	78	78

**. Correlation is significant at the 0.01 level (2-tailed).

Appendix 14. Correlation table on question 21. from 2017

2017 - Question 21. How significant do you consider the consequences of the following cyberattacks?		Loss of immovable property	Negative publicity	Loss of market share	Infringement of Privacy (staff or cust.)	Loss of income - Direct or indir.	Business interruption	Criminal liability	Damage payment to the customer
Loss of immovable property	Pearson Correlation	1	.427**	.579**	.587**	.624**	.476**	.441**	.480**
	Sig. (2-tailed)		0.000	0.000	0.000	0.000	0.000	0.000	0.000
	N	96	95	93	94	96	96	94	92
Negative publicity	Pearson Correlation	.427**	1	.688**	.593**	.530**	.461**	.540**	.619**
	Sig. (2-tailed)	0.000		0.000	0.000	0.000	0.000	0.000	0.000
	N	95	95	92	93	95	95	93	91
Loss of market share	Pearson Correlation	.579**	.688**	1	.640**	.746**	.543**	.572**	.560**
	Sig. (2-tailed)	0.000	0.000		0.000	0.000	0.000	0.000	0.000
	N	93	92	93	91	93	93	91	89
Infringement of Privacy (staff or customer)	Pearson Correlation	.587**	.593**	.640**	1	.750**	.613**	.580**	.639**
	Sig. (2-tailed)	0.000	0.000	0.000		0.000	0.000	0.000	0.000
	N	94	93	91	94	94	94	92	90
Loss of income - Direct or indirect	Pearson Correlation	.624**	.530**	.746**	.750**	1	.715**	.602**	.578**
	Sig. (2-tailed)	0.000	0.000	0.000	0.000		0.000	0.000	0.000
	N	96	95	93	94	96	96	94	92
Business interruption	Pearson Correlation	.476**	.461**	.543**	.613**	.715**	1	.698**	.641**
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000		0.000	0.000
	N	96	95	93	94	96	96	94	92
Criminal liability	Pearson Correlation	.441**	.540**	.572**	.580**	.602**	.698**	1	.852**
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000	0.000		0.000
	N	94	93	91	92	94	94	94	90
Damage payment to the customer	Pearson Correlation	.480**	.619**	.560**	.639**	.578**	.641**	.852**	1
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000	0.000	0.000	
	N	92	91	89	90	92	92	90	92

**. Correlation is significant at the 0.01 level (2-tailed).

Appendix 15. Correlation table on question 21. from 2016

2016 - Question 21. How significant do you consider the consequences of the following cyberattacks?		Loss of immovable property	Negative publicity	Loss of market share	Infringement of Privacy (staff or customer)	Loss of income - Direct or indirect
Loss of immovable property	Pearson Correlation	1	.409**	.526**	.347**	.462**
	Sig. (2-tailed)		0.000	0.000	0.000	0.000
	N	187	186	184	186	181
Negative publicity	Pearson Correlation	.409**	1	.616**	.509**	.449**
	Sig. (2-tailed)	0.000		0.000	0.000	0.000
	N	186	186	184	185	181
Loss of market share	Pearson Correlation	.526**	.616**	1	.507**	.668**
	Sig. (2-tailed)	0.000	0.000		0.000	0.000
	N	184	184	184	183	179
Infringement of Privacy (staff or customer)	Pearson Correlation	.347**	.509**	.507**	1	.558**
	Sig. (2-tailed)	0.000	0.000	0.000		0.000
	N	186	185	183	187	181
Loss of income - Direct or indirect	Pearson Correlation	.462**	.449**	.668**	.558**	1
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	
	N	181	181	179	181	182

**. Correlation is significant at the 0.01 level (2-tailed).

Appendix 16. Correlation table on question 27. from 2018 and 2017

2018 - Question 27. How likely do you think that		Your organization has been targetted cyber/information leak by anyone not knowing it?	Your organization will be subjected to a cyberattack in the next year?
Your organization has been targetted cyber/information leak by anyone not knowing it?	Pearson Correlation	1	.629**
	Sig. (2-tailed)		0.000
	N	78	78
Your organization will be subjected to a cyberattack in the next year?	Pearson Correlation	.629**	1
	Sig. (2-tailed)	0.000	
	N	78	78
**. Correlation is significant at the 0.01 level (2-tailed).			

2017 - Question 27. How likely do you think that		Your organization has been targetted cyber/information leak by anyone not knowing it?	Your organization will be subjected to a cyberattack in the next year?
Your organization has been targetted cyber/information leak by anyone not knowing it?	Pearson Correlation	1	.552**
	Sig. (2-tailed)		0.000
	N	97	96
Your organization will be subjected to a cyberattack in the next year?	Pearson Correlation	.552**	1
	Sig. (2-tailed)	0.000	
	N	96	96
**. Correlation is significant at the 0.01 level (2-tailed).			