jamk.fi

The Concept of the Cyber Security in an office

Author Janne Markkanen

Master's thesis
November 2020
Technology, Communication and Transport
Information and Communication Technology
Cyber Security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s)	Type of publication	Date
Markkanen, Janne	Master's Thesis	November 2020
		Language of publication: English
	Number of pages 59	Permission for web publication: Yes

Title of publication

The Concept of the Cyber Security in an office

Degree programme

Master's Degree Programme in Information Technology, Cyber Security

Supervisor(s)

Kotikoski, Sampo

Hautamäki, Jari

Assigned by

Fujitsu Finland, Palomäki, Aki

Abstract

Information security is an important part of everyday life, and its importance has increased considerably recently. During 2020, Covid-19 pandemic has significantly worsened the security situation. Governments restricted free movement. Remote working has increased dramatically. The situation was seen in the press as squashed news coverage related to cyber security. But what cyber security is?

The aim of the study was to find out from employees of Fujitsu's Jyväskylä office what they think cyber security is? With further questions will broaden the awareness of employees' views on issues and asset the need for and level of support measures related to it. Based on the results, more guidance to harmonize staff's knowledge on cyber security and training will be provided.

The study was conducted as a Web online survey. In addition to completing the results of the online survey and providing benchmarks, interviews were conducted remotely for three people.

Employees' perception of cybersecurity was very much in line with the theory, even though they themselves experienced uncertainty about it. There were no differences in evaluations depending on work position or history. The level of training and documentation in cyber security was fairly good, but changes were needed. The perception of the current state of cyber security was better the scale middle.

Employees cyber security views were fairly coherent. Cyber security current state is good. Changes to the trainings and guidelines are needed, but group-specific targeting was not revealed in the study.

Keywords/tags (subjects)

survey, subject view of cyber security, interview, Fujitsu

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Markkanen, Janne	Opinnäytetyö, ylempi AMK	Marraskuu 2020
	Sivumäärä: 59	Julkaisun kieli: Suomi
		Verkkojulkaisulupa myönnetty: Kyllä

Työn nimi
The Concept of the Cyber Security in an office

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

Työn ohjaaja(t)
Sampo Kotikoski, Jari Hautamäki

Toimeksiantaja(t)
Fujitsu Finland, Aki Palomäki

Tiivistelmä

Tietoturva on tärkeä osa nykyistä arkea, sen merkitys on kasvanut viime aikoina huomattavasti. Vuoden 2020 aikana koronanvirus pandemia on omalta osaltaan huonontanut tietoturvan tilannetta merkittävästi. Tilanne näkyy lehdistössä huolestuttavien uutisten lisääntymisenä kyberturvallisuuteen liittyen. Mutta mitä kyberturvallisuus on?

Tutkimuksen tavoitteena oli selvittää Fujitsun Jyväskylän toimiston henkilöstöltä, mitä he ajattelevat kyberturvallisuuden olevan? Jatkokysymyksillä laajennetaan tietoisuutta henkilöstön näkemyksestä asioihin sekä arvioidaan niihin liittyvien tukitoimien tarpeellisuutta ja tasoa. Tutkimustuloksen perusteella pyritään parantamaan ohjeistuksia, kohdentamaan koulutuksia niitä tarvitseville ja sitä kautta yhtenäistämään henkilöstön näkemystä kyberturvallisuudesta.

Tutkimus toteutettiin Web-verkkokyselynä. Verkkokyselyn tuloksia täydentämään ja vertailukohtia antamaan, tehtiin myös haastattelututkimus etänä kolmelle henkilölle.

Työntekijöiden käsitys kyberturvallisuudesta vastasi hyvin teoriaa, vaikka he itse kokivat epävarmuutta sen suhteen. Työnkuvan tai työhistorian vaikutusta vastauksiin, ei pystytty osoittamaan. Kyberturvallisuuden koulutus- ja dokumentaatiotaso oli asiallista, mutta niihin kaivattiin muutoksia. Käsitys kyberturvallisuuden nykytilasta oli asteikon keskiarvoa parempi.

Kyberturvallisuuden näkemys tuntuu yhteneväiseltä ja nykyinen kyberturvallisuuden tila vaikuttaa hyvältä. Muutoksia koulutuksiin ja ohjeistuksiin kaivataan, mutta kaivattua ryhmäkohtaista kohdennusta tarpeille, ei tutkimuksessa saatu esille.

Avainsanat (asiasanat)
kyselytutkimus, haastattelu, subjektinen näkemys, Fujitsu

Muut tiedot

Contents

Figures

Tables

Acronyms

CS	Cyber Security
ECS	Enterprise Cyber Security
HR	Human Resources
ICT	Information and communication technology
CIA	confidentiality, integrity and availability
CIAAN	confidentiality, integrity, availability, authenticity and nonrepudiation

1 Introduction

1.1 Background

Year 2020 has been different than before, because of Covid-19 pandemic. Virus cause lot of sickness. Governments need to do painful decisions to limit opening hours or close public services and companies like restaurant. Free travelling was not possible. Employees need to stay at home.

Those who still have a job, need to do it from home. So remote working growth dramatically. That cause lot challenges and many changes to companies', working culture, security topology and policies. From information technical perspective, working at home is not normally as safe as in office. Threat vector increase and threat realized more often than before. Lot of discussion about cyber security were seen in news and media. But what is cyber security?

There are many books, research, webpage and written document about cyber security. Still is difficult to find written information from employees' thought perspective. This research is opening that perspective view.

Everyone has own idea what is cyber security and what belongs under word. It depends on company, how cyber security and security things are seeing in company. Easily we can understand that cyber security is different in a company working area is industrial manufacturing or other business-like ICT services. If you ask from different employees, even same working job, they are seeing cyber security many ways. This is one main goal, to get knowledge about employee's thoughts, how they feel, and do they think they have enough knowledge about cyber security. That helps to harmonize employee's cyber security view by focusing training and documentation to needed direction and groups.

Web based internet survey and interviews are used in research for gathering answers and information to get knowledge of employees' thoughts. Knowledge helps to focus or tune courses, training and documentation to groups are needing that and that way harmonize employees view of cyber security.

The idea for the thesis came from work and authors own interest of co-workers' thoughts about cyber security. In this case focus is on ICT business company Fujitsu and an office employees.

1.2 Fujitsu

Fujitsu is the leading Japanese information and communication technology (ICT) company, offering a full range of technology products, solutions, and services. over 129,000 Fujitsu people support customers in more than 100 countries. Fujitsu use experience and the power of ICT to shape the future of society with our customers. Fujitsu is the largest IT services provider in Japan and 7th in the world (Gartner Market Share: IT Services, 2019, Dean Blackmore et al., April 2020).

Fujitsu Finland is part of global Fujitsu. Fujitsu Finland Ltd is the 3rd largest information technology service and equipment supplier in Finland. In Finland alone, Fujitsu serves hundreds of companies and organizations, thousands of end-users through them. Cyber security services and products belongs to Fujitsu's offering portfolio (Fujitsu 2020).

Fujitsu has a strong local service capacity in Finland, but at the same time we are an internationally capable and networked company. Fujitsu operate at around 40 locations, so it is possible to support the customer locally. There are 24 employees in Fujitsu Jyväskylä office. Employees roles are nice mixture all kind of expertise, there are directors, managers, ICT architects, specialists, and technical engineers. For mixing things more, most of employees are working in different teams and service lines. That cause challenge for many things, but at same time is give's rich working environment.

Author is working in Enterprise Cyber Security (ECS) organization's firewall team.

2 Research frame

2.1 Objectives

The purpose of the Master's Thesis is to understand what employee think about cyber security.

Research question
"Is it possible to find coherent view of cyber security in the target organization?"

The goal is to get better understanding how employees see or feel cyber security. How different employees are understanding cyber security and how they handle cyber security things in their daily working life? How different working position in same office influent about thought of cyber security? Do employees have enough information about cyber security? How about existing documentation? Is there something to make cyber security things familiar or understandable?

2.2 Research methodology

Choosing research methods for thesis between quantitative and qualitative is not clear. Research might have part of both methods, but mainly from qualitative.

In high level qualitative research tries to explore the subject as comprehensively as possible, whereas the quantitative research method examines the information numerically answering the questions how many, how much and how often.

There have seen many qualitative research marks to confirm that research method is correct. When research emphasis is on understanding the respondent's point of view and proximity of information. Human is data collecting tool (Järvinen S. 2018).

2.3 Information gathering and sources

The research was carried out by investigating the literature such as books of cyber security and thesis. Internet is good source to find information easily, off course is necessary keep in mind those sources reliability. Study course material was useful to remind what has faced earlier. Information from literature to theoretical parts is

easier to find. There is lot of fine books and thesis of cyber security theory, but same time it confuses. Actually, there is so much information, that it is possible to look only small piece of information. These information are used in theorical part of work and at same time is kept in mind using it for research results analyze.

Uncommon research view influent information gathering. There is not found many books or thesis about employees' thoughts of cyber security and how cyber security is seen in different working roles in same company. But there is good thesis where is used survey (Haukilehto T. 2019) and interview (Pellinen A. 2018) to gather information needed to research. That information helps to see what direction research might need to guide and where to focus. Author expertise of current subject helps to see whole picture.

Only way to get research subjective view of employees, is to get information from them. What is way to get that information? Best and almost only way ask questions from them and collect answers for analyze. When thinking of possible ways to get needed information and analyzing different methods, result was clear, main sources for information gathering from employees were web online survey and personal interviews.

2.4 Benefits of Thesis

The results help to get current cyber security knowledge level familiar for Human Resources (HR) and ECS team. They also aim at understanding how different persons in different roles see cyber security. The results might help to understand how to familiarize employees are with cyber security related issues and smooths out information between different role groups. Possibly can help to find out and correct false perceptions or assumptions about cyber security.

How does courses, instruction and documentation help employees and is there need for change? CS training is always needed but research can give more detailed information to focus training to groups are need that. Current state of cyber security help to see level where things are now. With research information is easier to harmonize cyber security knowledge and increase expertise. Good self-confident level gives better opportunities to handle things and that helps to help customers.

3 Cyber Security

”Cyber security is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. It seems that everything relies on computers and the internet now.”
(CISA, 2020)

There is no right or wrong way to define cyber security. CISA’s defining is simple. Defining has change during history and depending on source defining is different.

3.1 Towards cyber security

There is existing two worlds, physical and digital world. Physical world is what see around but digital world is artificial bits world (Limnéll 2014, 29). When bits mean cyber, can say there is cyber world or in different context it is cyber space or cyber domain. “*As cyber security can be considered simply the act of making cyber space safe from damage or threat, it is important to define cyber space before discussing cyber security*” (Edgar 2017, chapter 2).

The data perspective (data) initially focused on digitalizing and coding data. The focus is largely on how information can be produced in cyberspace and provide it with safeguards or access control. Later, a broad information assurance topic emerged, partly addressing some limitations on computer and network security only. It would be more important to identify the information itself, appreciate it and protect it during transport and at rest.

The technological perspective (system) is that data and the technology needed to transmit it are encapsuled into cyberspace. This includes hardware, as well as software, operating systems, and network protocols. Most definitions basically use cyberspace and the Internet among themselves. Some of these definitions include all data transfer.

The most recent cybernetic perspective (human) is that cyber space includes not only data and technology, but also human beings. Because cyber space is a metaphysical structure created from the confluence of digital hardware, the data it creates and

manages, and people who interact with the hardware and produce and consume the data contained in the data. Man is as much responsible for the dynamics of the system as data and technology. Cyber systems would have no action without human intervention. It is recognized that users are the weakest link in security. This is because users are often directly targeted by attacks on their psychological behavior, such as clicking on bad links or running malware (Edgar 2017, chapter 2).

Cyber space is defined to data, system and human perspective (Figure 1).

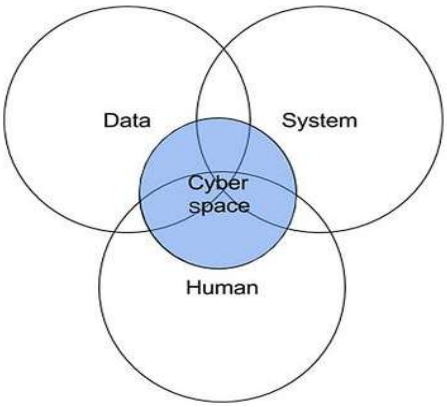

Figure 1. Cyber space at the overlap of data, system, and human (Edgar 2007)

3.2 Cyber security

Wikipedia says that cyber security equals computer security equals information technology security all is merging together. According Finnish cyber security strategy it is desired end state where cyber space is ensured and reliable. (Defmin 2013)

In cyber space there are many things involving each other. Those involving things need to trust each other, see correct things, right time, right place and so on. Everything based on trust.

3.2.1 CIA to CIAAN

Over time, a number of basic cybersecurity features have been defined. The original core set of the discussion is confidentiality, integrity and availability (CIA). That is well

known triad model as information security basics. However, the CIA is too crude, so additional features have been added to differentiate the finer aspects of cyber security. Those features are authenticity and nonrepudiation (CIAAN). (Edgar 2017)

Confidentiality is a key feature of the cyber security, which only allows those parties who should be aware of it to keep their data private in cyber space. Data should not be accessed or read without authorization. It ensures that only authorized parties have access. Cryptography is used storing and transmitting confidential data. (Cisecurity 2020)

Integrity allows only authorized users to edit data in cyberspace. When data is exchanged between cyberspace actors, it often passes through shared areas, where other actors have the ability to edit the data before they reach their recipients. Therefore, it is important that some critical data or information remains unchanged between the sender and the recipient. Digital Signatures and hash algorithms are mechanisms used to provide data integrity. (Smart Eye Technology 2020)

The resources and information of cyberspace are available on timely and reliable manner. The availability helps to balance the limitations of the system with the usefulness of the system. High availability protocols, fully redundant networks, and system hardware without any single points of failure ensure system reliability and robustness. (Forcepoint 2020)

Authenticity is the assurance that the data, transactions, communications, or documents are genuine. It is also important for authenticity to confirm that both parties involved are who they claim they are. This is usually done via an approved third-party digital signature, which are widely used to confirm the parties involved are genuine. (Edgar 2017)

Non-repudiation is achieved through cryptographic methods which prevents a person or entity from denying having performed a particular action related to data for proof of obligation, intent, or commitment, or for proof of ownership.

Signing off a document is a case of non-repudiation showing that the signer is responsible for approval of the document being signed. (Securopia 2011)

Inside cyber security attributes or features there are those smaller parts which helps to make more things secure. Limnéll said (2014, 47) that cyber security includes 2/3 part other than technology. But information technology parts are often seen discussions and those are easier to think belongs to cyber security. This includes all technology that stores, manipulates, or moves data, such as computers, data networks, and all devices connected to or included in networks, such as routers and switches firewalls, and antivirus software.

4 Research

This section presents the analysis part.

4.1 Gathering data

The material of this thesis was gathered online survey and persons interviewed. The interviews were carried out in November 2020, during office hours. Interviews were done through Teams-meeting because company policy was not allowing visiting at office during Covid-19 pandemic. Teams application was chosen because it is company's working tool and everyone has that application.

Interviews questionary material was same than in survey, all respondents were already replied to that, therefore was not needed to go through reason and goals of the thesis. The interviewee had the possibility to make questions and interrupt the interview at any point.
During the interview, the findings were written down simultaneously. Interview was recorded for case that all answers were not able to write down. The researcher's own personality is a research and data gathering tool, which are used to get most out of the interviewed person. The importance of observation is to gain interviewees trust and the ability to remain neutral. It was easily arranged neutral behavior because interview was done remotely. It is possible that the interviewer's own knowledge and experiences on the subject influent the interview and the way the conversation proceeds. It is important to remember to focus on the interview

questions and make sure that the conversation does not end up in the wrong direction or out of the topic.

4.2 Planning the survey

Survey is possible do many ways. First thought how to do survey was by sending questions to each respondent by email. In small number of respondents, it works fairly well but collecting reply's and put those to reports were not effective. After short analyse of other different way to make survey, was clear to make survey with online software with automatic reply collection. Webropol seemed good platform and tool for making survey and got answers to report nice way. When realized that JAMK has co-operation deal with Webropol, that was chosen for survey platform.

Fujitsu used English in normal work language. Because of author knowledge, survey questions were done in responders native language Finnish for getting respondents to feel familiar with questions and for preventing questions misunderstanding.

There was not survey base for questions in Webropol. Even cyber security is parts of many thesis and survey, the research view of survey was different. Research gather personnel subject feeling about cyber security. From beginning idea was clear there is no survey questions to choose from somewhere, questions need create self to survey, but it was additional and time-consuming work to do those questions. One important plan was kept survey quite simple and not too long.

Knowledge of subject and working environment help author a lot of made questions. Questions were going through with representative person. During process questions seems divide to five sections. First section was to get background info for respondent. Second section was the most interesting to gather respondent knowledge about cyber security. Third section was about cyber security documentation. Section four was gathering information about cyber security courses. Last section was to get reviews of the current state of cyber security.

Many questions were asking numerical value to get replies measured level. Measured level gives estimation of current question or subject importance. If level was poor, need to found reason for that. In survey, poor level answer, gave additional question to find out reason for poor answer.

4.3 Publish the survey

The survey must be accompanied by a covering letter that approaches the respondent and aims to motivate the answer (Kananen 2011, 46). Before sending current survey email, author sent prewarning and motivation email about survey. Survey email itself was short and the escort words were kept short so that they could read it quickly.

Questions were unnumbered that responders do not get bad feelings from so many questions. But survey include progress bar for length of survey.

4.4 Survey questionary

This chapter presents the personnel survey questions and explained purpose of them. Questions are translated from Finnish to English, but original questions are found in appendix 1.

Survey questions were unnumbered to the respondents. In this chapter question numbers are added to use for clarifying relations between questions and answers.

4.4.1 Employee backgrounds

1. *Working role in Fujitsu?*
    - *Chief, Director*
    - *Specialist, consultant*
    - *Technical specialist*

The purpose of the question: Because all almost every employees play a different role, therefore answers are limited to only three groupings, so that the answer provider cannot be identified from the results. Grouping is used for finding individual group thoughts about cyber security and therefore focus education needs. Groups are used for comparing or analysing question results.

2. *Employment history in Fujitsu?*
    - *less than 2 years*
    - *2 - 5 Years*
    - *over 5 years*

The purpose of the question: Trying to explain whether there was a difference in cyber security views, when worked in Fujitsu short or long time.

3. *Employment history in IT-* industry*?*
    - *less than 2 years*
    - *2 -10 years*
    - *over 10 years*
4. *Total employment history?*
    - *Years*

The purpose of the question: Does working in the IT industry have any impact on the answer results comparing to working in Fujitsu. Whether work experience is reflected in the answers.

4.4.2 Cyber security

5. *What is cyber security based on your experience or vision?*
    - *list five things or sub-areas*

The purpose of the question: The main question was trying to find out, how employees were seen cyber security and what they thought belong to cyber security. Was their view coherent?

6. *What two things do you feel is important/most important in cyber security?*
    - *list two things*

The purpose of the question: What were the most important cyber security issues, mirrored to cyber security theory and between different groups.

7. *Self-assessment of your own cyber security competence level?*
    1. *I really don't know much.*
    2. *I know some things, but I feel insecure about things.*
    3. *I can't say or I don't have an opinion*
    4. *I think I know quite a lot about things.*
    5. *I think I know things very well*

The purpose of the question: Subjective assessment of the state of itself. How employee were seen own knowledge about CS. The goal of obtaining a numerical value from competence. If level was below middle of scale, it might indicate some problems.

8. *Have you experienced cyber security threats in the past year?*

    Yes / No

The purpose of the question: To get information and experiences how many has facing cyber security threats.

Yes answer gives additional questions

9. *What kind of cyber security threat have you experienced?*
10. *How have you acted since facing the cyber security threat?*

The purpose of the question: What kinds of threats are faced and how those are handled? Are those threats handled correct way or can it cause security problems? Also this might give extra knowledge is there something going on.

11. *Do you know to where you will contact if you receive cyber security threats or issues?*

Yes / No

The purpose of the question: Everyone should know where to contact. If there was no answers, education, and documentation is needed to update right away.

4.4.3 Questions about cyber security documentation in Fujitsu

12. *Do you know where Fujitsu's cyber security documentation can be found?*

Yes / No

The purpose of the question: Everyone should know where documentation is found. If there was no answers, education, and documentation is needed to update .

13. *Have you read Fujitsu's cyber security guidelines?*

Yes / No

The purpose of the question: If documentation is read, then can give estimate state of documentation level

14. *The current state of cyber security guidelines?*

Poor 1 2 3 4 5 Excellent

The purpose of the question: The goal of obtaining a numerical value from subjective guideline level. If level is below three, there is something wrong and need to fix.

15. *Suggestions for improvements to the documentation?*

The purpose of the question: To get assistance how to improve documentation.

4.4.4 Questions about Cyber security courses in Fujitsu.

16. *Do you think mandatory cyber security courses are necessary?*

Yes / No

No, answer gives additional question.

16.1 Why don't you think courses are necessary?

The purpose of the question: Fujitsu is keeping trainings and courses to all employees. Other courses are mandatory and other are volunteer. The objective of gaining an idea of whether mandatory courses are necessary and if mandatory courses are not needed, try to find reason for that.

17. *Should more training be organized on cyber security?*
    - *There should be more trainings*
    - *There should be fewer trainings*
    - *There are enough trainings*

The purpose of the question: To understand need of volume for mandatory courses.

18. *What you have learned from the trainings?*

The purpose of the question: To get knowledge what is learned from mandatory courses, is there is something special.

19. *The main language of training for web online courses is English, how it influences your learning?*
    - *improve my learning*
    - *language does not matter/no opinion*
    - *impair my learning*

The purpose of the question: Mandatory course language is English is that causing learning problems. If there are problems, need to find out is used wording too complex or is there possibilities to arrange courses with own native language.

20. *Should more training be organised on cyber security?*

Yes / No

Yes, answer give additional question.

21. *What type of training would you need?*
    - *Web - online training*
    - *onsite training*

- *something else*

The purpose of the question: Try to find out, is optional cyber security training needed or wanted.

22. *What kind of training you would like?*

The purpose of the question: What kind of optional cyber security training would be interesting.

23. *Fujitsu has developed the safety of workers' equipment and connections, enabling more secure workstations, multilevel authentications, and VPN connections. Do you have any technical equipment or products, that you think could be deployed to use or that could help with cyber security?*

The purpose of the question: Sometimes there is some software or devices used at home (or somewhere else), what can be useful or helpful for working. Those new ideas are welcome.

4.4.5 Reviews of the current state of cyber security

24. *The current state of cyber security at the office?*

Poor 1 2 3 4 5 Excellent

Poor state answer (1) gives new question.

The purpose of the question: Subjective measurement level at current state of office cyber security. If answer is poor, keep management or HR need to do something or locally one needs to do something to improve situation.

25. *The current state of cyber security at home/working remotely?*

Poor 1 2 3 4 5 Excellent

The purpose of the question: Subjective measurement level at current state of home office cyber security. If level is poor, try to find out reason for correcting that situation.

26. *How do you feel cyber security has changed during the Covid-19 pandemic?*
    - *Degraded*
    - *No change detected*

- *Improved*

The purpose of the question: Covid-19 pandemic is caused lot of extra activity in threat sector, is that seen for employees.

27. *How do you think Fujitsu has succeeded cyber security guidelines during Covid-19 pandemic?*

Poorly 1 2 3 4 5 Very well

The purpose of the question: The objective of obtaining a numerical value about guidelines during Covid-19 pandemic.

28. *Give a general rating on Fujitsu cyber security as a whole?*

Poor 1 2 3 4 5 Excellent

The purpose of the question: The objective of obtaining a numerical value from the level of the enterprise.

29. *How do you think of Fujitsu's level of cyber security compared to other enterprises?*

Poor 1 2 3 4 5 Excellent

Poor state answer (1) gives new question

30. *Why do you think the cyber security level is like that compared to others?*

The purpose of the question: The objective of obtaining a numerical value from the level of the enterprise compared to other enterprises. If answer is poor, keep management or HR need to do something or locally one needs to do something to improve situation.

31. *Do you want to say something to human resources or another group (e.g. ECS) cyber security? Hope for improvements to cyber security issues that were not ignored in the survey? Maybe comment on the questions of the investigation? The word is free...*

The purpose of the question: Always there is many things cannot handle in survey. All information which help to understand employees mind is good get… probably better survey in future.

5 Survey results

Survey was send to 23 employees at beginnig of November 2020. Reply period was two weeks. After 10 days, remainding survey link was sent persons not answered yet. Total 18 answers were get during two week survey period. Allways there is many things prevent answering, on going holidays, other out of work situations and busy at work, then 100% answer rate is almost imposible. Survey answer rate was good in this period.

Interview was done to three persons during November 2020. There was one respondent from each group management, specialists and technical engineers chosen without any special plan by quessing who has time answer interview. Respondents were familiar to author therefore was easy to corfirm interview times. Covid-19 prevent posibilities to do face-to-face interview, so interviews were done by calls. Annoinly “bodylanguage” was not possible to see or read during interviews. Interview questions were same than in web-online survey.

During next chapters answers and informations are cathered from Webropol-survey reports and interviews. Answers are divided to five sections: backgrounds, cyber security, courses, documentation and analyzing current state. Answers are composed to famialiar mode, but text answers are not sanitized and those are in respondents raw mode, only translated to English. Grouping is seen in answers. In answer section groups are named Management (Chiefs, managers), Specialist (specialists, consultants) and Technical engineer.

5.1 Employee backgrounds

On question 1 was asked employee to choose group belongs to. All group get at least four partisipants. This information was used in further answer analysing. In Figure 2 is seen precents of respondents per group slices, 22% management, 39% specialists and 39% technical engineers.

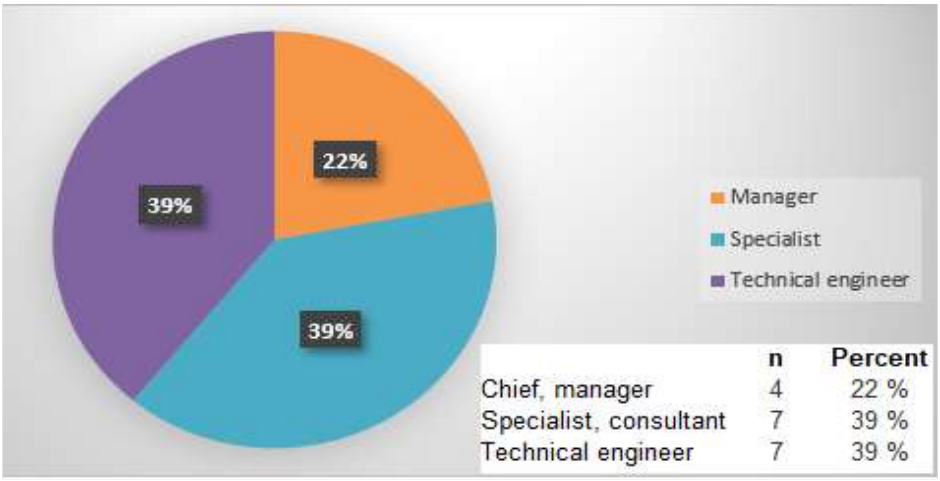

Figure 2. Respondents per groups

Employees' has lot of working experience. Most of employees has been in Fujitsu at least five years (Figure 3).

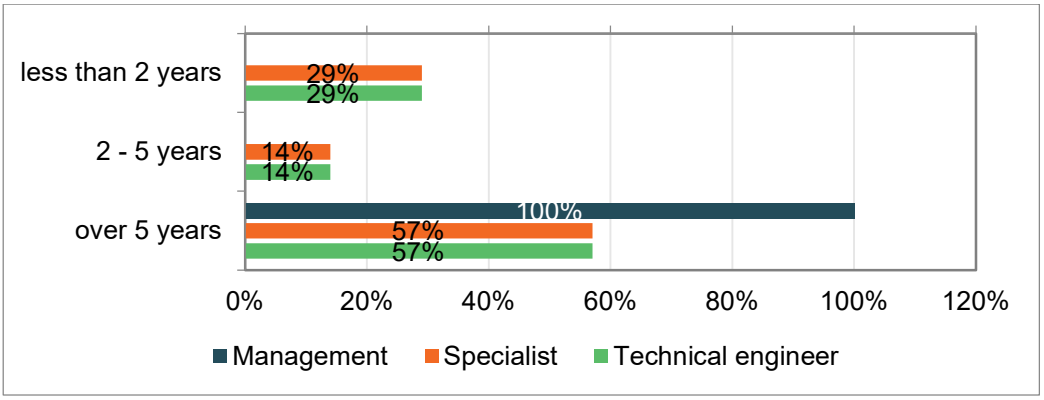

Figure 3. Working history in Fujitsu.

Working history in IT business is longer than history in Fujitsu (Figure 4). Most of have over 10 years history in IT business.

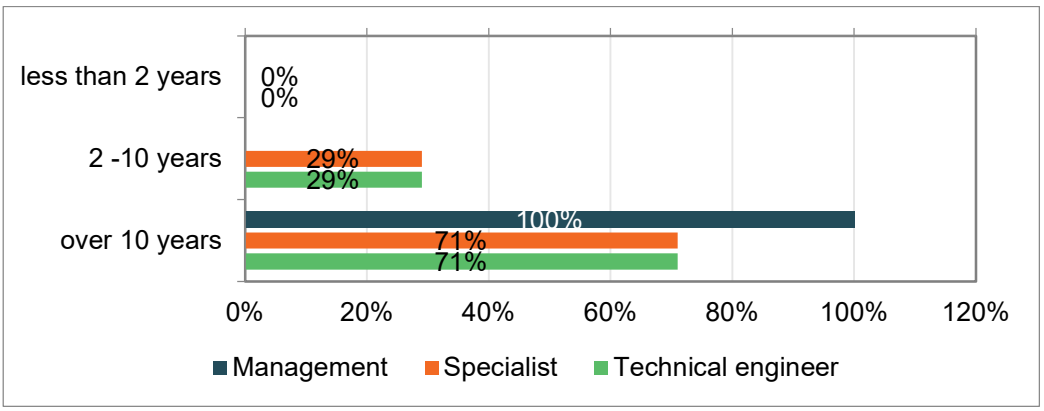

Figure 4. Working history in IT business.

Average working history per groups are at least twenty years (Figure 4) and overall average working history is about 23 years.

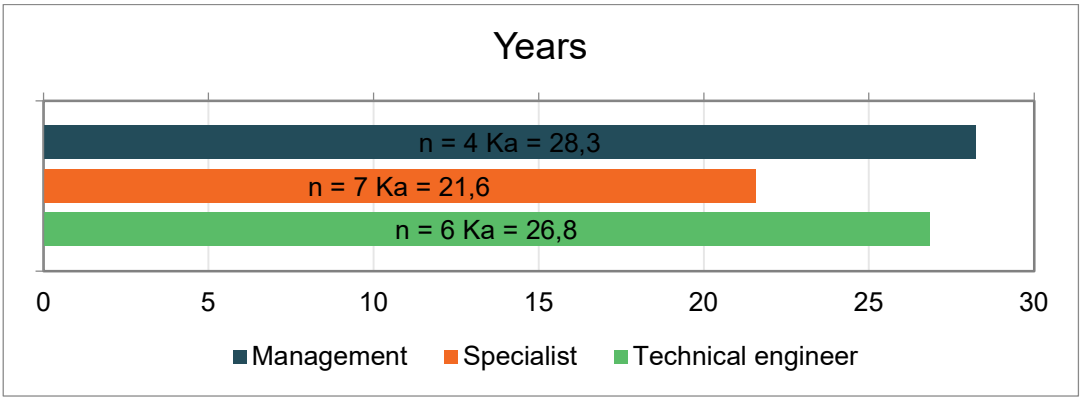

Figure 5. Average working history years per groups.

5.2 Cyber security

Answers about cyber security include lot of different areas. According answers could see that everyone has own kind of view about cyber security. One respondent was thinking that everything belongs to cyber security. Other respondent has more narrowly view and think devices and encryption are in centre of cyber security. Answers were so different that was hard to see is there differences per groups. One goal was found that group difference from cyber security thoughts, that it could use in future focus needed education per group, but that was not able find. Survey answers are seen in Table 1.

Table 1. Things belongs to cyber security, answers random order per groups

Management				
Smartphones	PCs and tablets	secure login and use	Work and home LAN / WAN	All online transactions
Information security for internet use	Security of personal IDs	Protection of one's personal identity	My activity in internet, which sites to use and what you click on	Finland's IT policies, solutions, and services
Technical architecture	People's activities and their education	Adequate up-to-date products and their updates	Data verification	Recovery and recovery
Physical data security	Security of systems and communications	Security and secure use of data	Manage access and access rights	Identify people and organizations
Specialist				
Safe use of equipment	Identifying and preventing security threats	Good password policies and MFA	Cybersecurity trainings	Correct processing of confidential information
Work instructions	Protocols	Encryption, encryption, encryption of information and equipment	VPN, encrypting connections	there won't be a fifth.
Data security and, above all, data protection and plan em. implementation	Manage cloud services	Architectural choices	Up-to-date platform and software updates	Politics and practices within the organization
Communications	End-user terminals	Data centre entity	Information services on the Internet	Other networks such as electricity networks, voice-over networks, government communication channels, television and radio networks
Networked electronic systems	Societal impact	Information Security	Crisis management/blocking	Linking and interfaces between the previous ones to the 'physical' world
Online security	Identity security	Continuity	Traceability	Track
Technical engineer				
Technical security	Physical security	Privacy	Security threats	Hedging methods
Security threat detection	Preparing for security threats	Preparing for fluffy communications	Strong identification	Continuity management and crisis management
Secure website	Reliable sign-in to different services	Antivirus & Anti-Malware	User awareness	Operating system updates
Security	Message secrecy	Device protection	Firewalls	Internet security
information networks	Terminals	Users	Services	Software
protecting data from third parties	preventing cyberattacks	secure communications	network management and monitoring	anticipation of related matters

Interviews confirm survey answers. Interviews give mainly deeper information to answers they give in survey. But few new things need to mention. One respondent thought that everything belongs to cyber security. Other thought that cyber security is necessary even internet connected televisions. In Finnish media seen news about realized cyber security threat case Vastaamo, give horrible reminding that everyone can be victim or participant of cyber security theft. One discussed thing was survey subject, still they think they don't know what cyber security is.

In question six was asked two main cyber security subjects Table 2 is presenting all respondents answers random order about most important things belongs to cyber security.

Table 2. Most important cyber security areas per group.

Management	
Safe operation	Identity management
Attitude to cybersecurity issues and its continued implementation.	A comprehensive understanding of the technical environment and its risk locations.
Data security	Identify people
Internet security	My activity on the Internet
Specialist	
Threat identification and prevention	Safe use of devices (passwords, security, etc.)
Work instructions	Protocols and regulations
Practices user training	Modern technology that supports practices taking security challenges into account
Accuracy of information	The confidentiality of the information, i.e. the information remains only there and for the purpose for which it is intended.
Timelyness (above) in an ever-changing environment	Legislation
persons, etc. protecting important information	threat response/vulnerability fix
identity security	continuity of services
Technical engineer	
Strong authentication	Trust in the level of encryption of different parties.
Reliability of data	Combating intruders
Security threat detection	Minimizing security threats
Technical security	Physical security
protecting data	countering and anticipating cyber attacks
Functionality of computer networks	Securing electricity supply
strong identification	encrypted data storage

When answers are harmonized at group level, seems that management sees identity control or protection and safe internet use important. Specialists thought that education/training/legislation and updates or up-to-date are important. Technical engineers thought that technical and physical security are most important. These answers gave a little perpective about group difference.

Interview participants has difficulties to choose two most important cyber security things, there are so many important things. One important is, use your common sense to keep you out of cyber security trouble.

Self-assessment of your own cyber security competence level seems to were rather good (Figure 6 and Figure 7), only one thoughts own poor knowledge. 1/3 part of respondents think they did not have enough knowledge about cyber security. Half of respondents think they knew at least lot of cyber security. Even answers were from subjective view, it indicates that some kind training is needed to improve own confident to know cyber security.

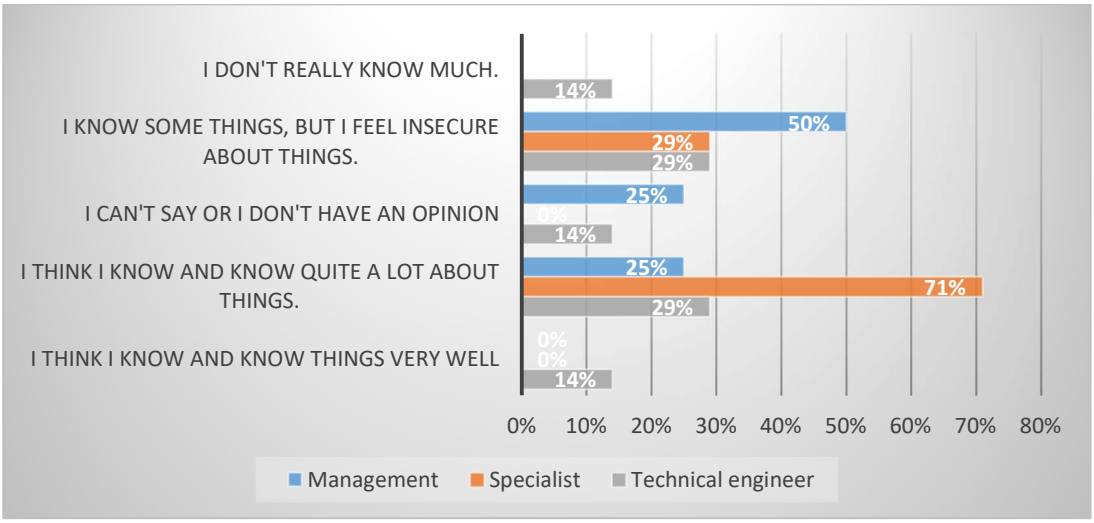

Figure 6. Self-assessment of own cyber security competence level per group.

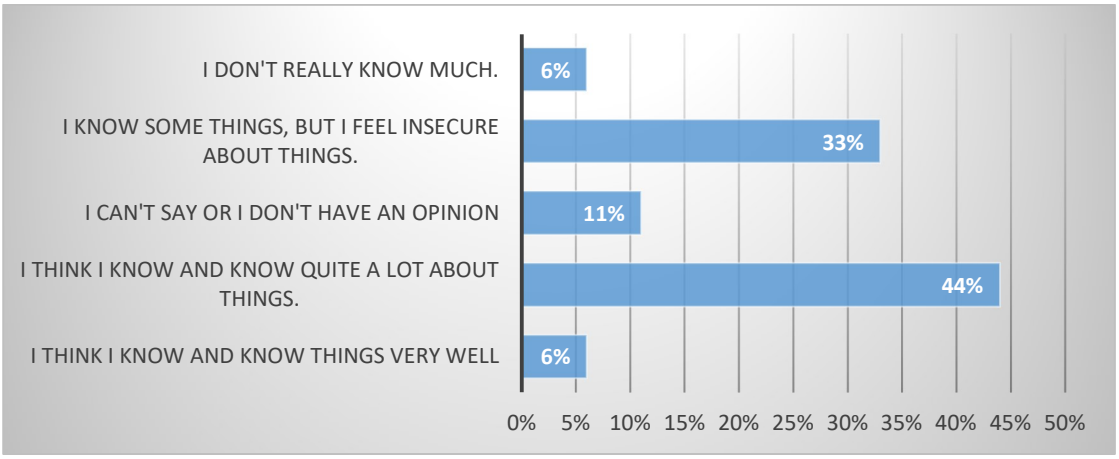

Figure 7. Self-assessment of own overall cyber security competence level.

How employees have experienced cybersecurity threats in the last year (question eight)? Half of management and 57% of specialists were experienced threats. Most of technical engineer (71%) respondents has not face threat according answers (Figure 8). There is little suspicion that everyone did not answer truth, or they do not though that those fake or phishing emails coming through spam-filter are not threats. Because answer was subject view, it might be possible that employees did not recognize threats or thought those are not threats and that was not good situation. Again, important place to increase employees knowledge and harmonize their view.

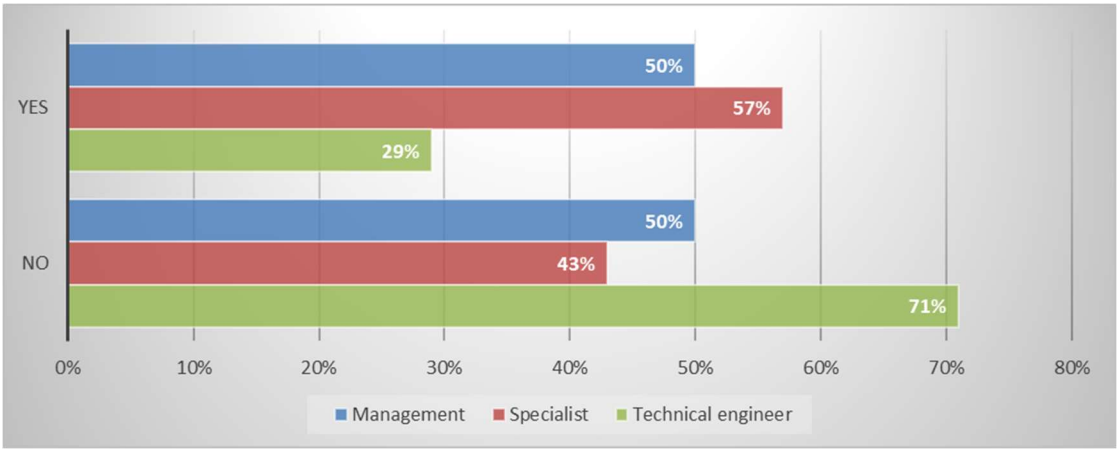

Figure 8. Experience of cyber security threats per group.

When asking what kind of cyber security threat, you have experienced (Table 3), answers were quite similar. There were two main type of threats experienced, emails and little surprising, scam calls. One respondent has even experienced network attack.

Table 3. Experienced cyber security threats per groups.

Management
The vulnerabilities revealed in the systems are a threat every time. In addition, on the civilian side, there is a threat of breaches of various public services that have been used by themselves.
Various letters of Nigerian, scam, extortion attempt, etc. general matters.
Specialist
Password phishing
Scam calls
Email phishing
I've received scam calls in Microsoft's name.
scam messages have been sent to email
Technical engineer
Network attack
Phishing for personal and banking information via e-mail.

It was interesting to get knowledge what kind of security threats respondents are experienced, but information how they were reacting when facing that threat was more needful. Wrong kind of reacting might cause lot of problems in company level, so it is not indifferent how threat handle is proceeded.

Question 10, How have you acted since facing the cyber security threat? Many research results prove that biggest cyber security problem is user itself. Question answers were giving relief that there are hope with user behaviour (Table 4). Reacting seemed to be correct direction by cyber security perspective. Messages and

emails are unread or deleted. Scam calls are ignored in many cases. Information in company level and news has improved knowledge of scam calls behalf of Microsoft helpdesk. Respondents seems to recognize those calls.

In interview came up information that scam calls are difficult, because one respondent has got scam calls from Finnish phone numbers.

Table 4. Cyber security threats reacting.

Management
We have a defined process according to which things are classified and it guides operations.
Deleted messages.
Specialist
Notification to the data security officer
Ignored suspicious messages
Since there had already been some news, it was quite easy to react to the call and identify it as a scam attempt. What I did was that the impostor got tired of seeing me as a potential target and stopped calling.
I have deleted messages without opening links, etc.
Technical engineer
Notification to antivirus team
Ignoring/deleting messages.

Facing threats gave additional question for respondents. Getting help to those problems is good to know where to contact when facing security problem. According answer, 83% know contact, so there is work to do for share correct contact information (Figure 9 and Figure 10). But that is not whole truth, because helpdesk helps always also with this kind of problems and everyone knows helpdesk.

Figure 9. Knowledge of security contact.

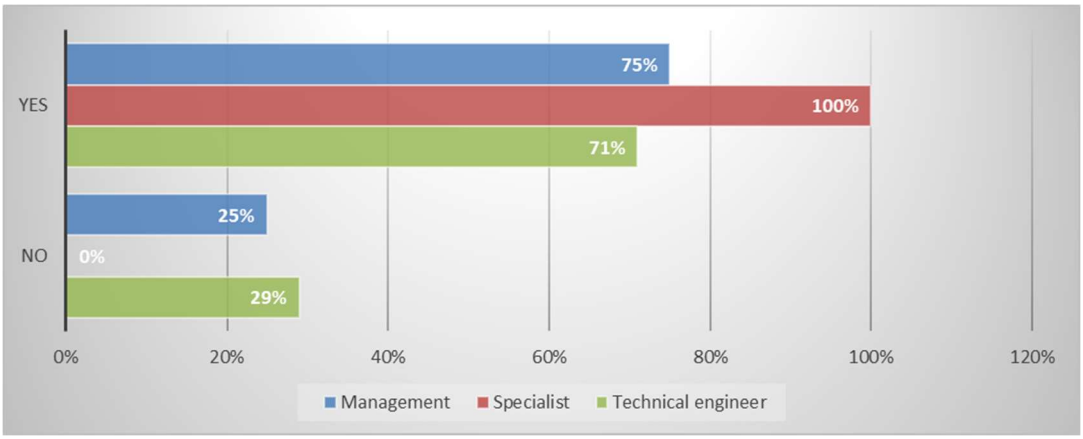

Figure 10. Security contact knowledge level per group.

5.3 Cyber security documentation in Fujitsu

Most of respondents (83 %) knows where Fujitsu's cyber security documentation is (Figure 11). But there are some respondents how are not known documentation therefore education and training are needed to fix that level to 100%.

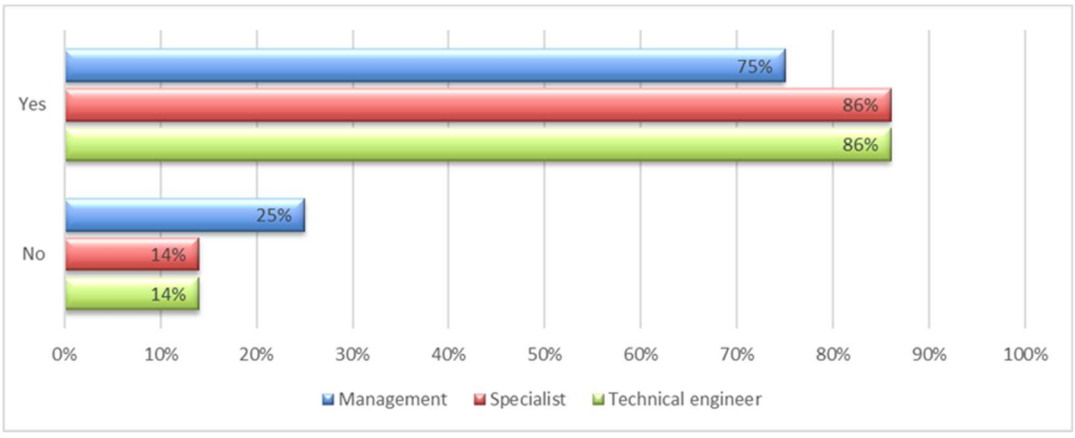

Figure 11. Knows Fujitsu's cyber security documentation location per group.

Overall, 78% on respondents has read Fujitsu's cyber security documentations or guidelines. In Figure 12 is seen reading level per grouping.

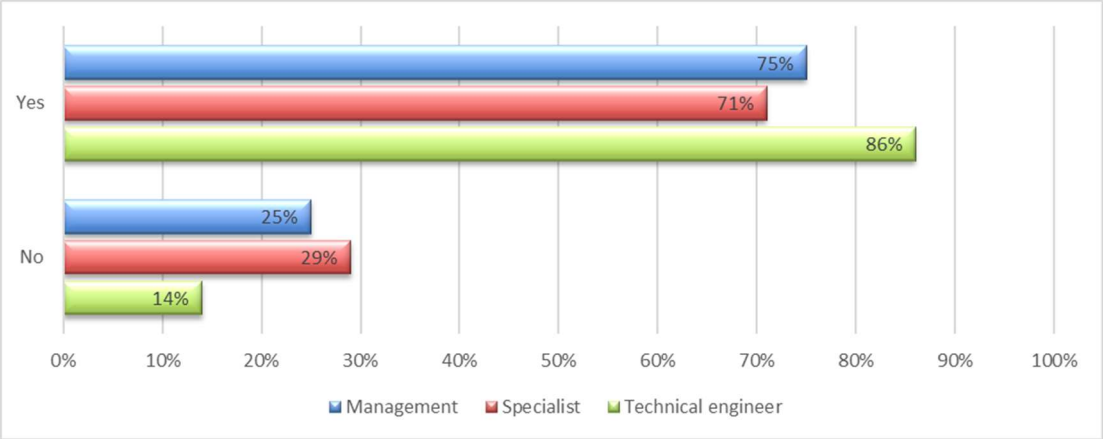

Figure 12. Guideline reading level percent per group.

Those respondents who has read documentation, are grading documentation to better level that average (Figure 13). Per grouping grading are management 4,00, specialist 3,60 and technical engineer 3,83. Overall grade level was 3,79.

	1	2	3	4	5	Average
Management	0	0	0	3	0	4,00
Specialist	0	0	2	3	0	3,60
Technical engineer	0	0	1	5	0	3,83

Figure 13. Grade level of guideline.

Next question was asking improvements to documentation. There were only few suggestions in surveys answers. According answers and interviews, there is need to use native language to understand guidelines and documentation better. Documentations should be easier to find. Language should be simpler. Survey answers are seen in Table 5.

Table 5. Guideline improvement

Answers
The documentation is really extensive and has different layers (global, regional...) Often it is those top-level policies that are really comprehensively written and described. Retrieving certain information is not very simple. When you start applying the matter to your own needs, you often need to meet the needs of the customer organization, and then the policies no longer work.
There is always a need to develop
Link to material for the front page to be more visible

5.4 Cyber security courses and training in Fujitsu

Most of respondents were seeing mandatory courses necessary (Figure 14), which is good because often there is possibilities that doing things mandatory reverse against learning. All together 89% of respondents answered yes.

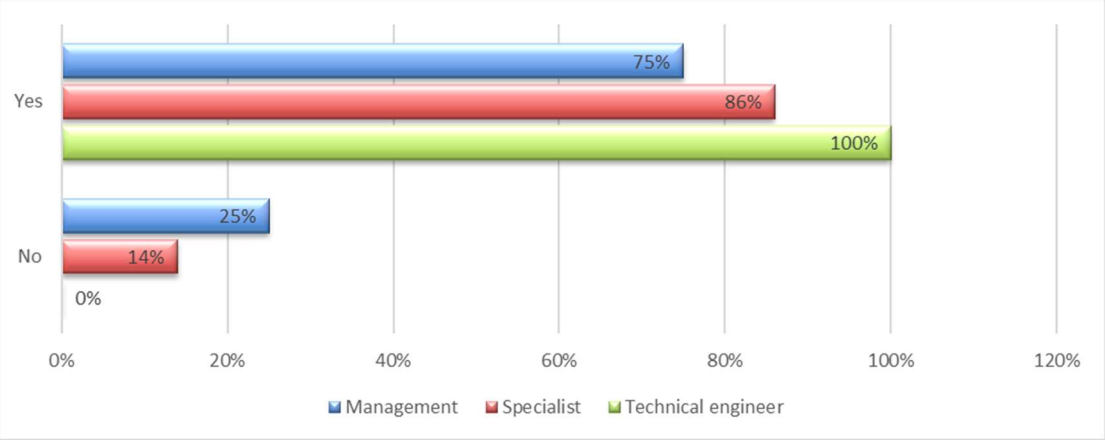

Figure 14. Need of mandatory courses per group.

No answer gives new question in survey to find reason why not need mandatory courses. There were two answers "*I don't think it makes sense to be generic, to force everyone*." and "*I think they are such a basic thing that there is no need to visit them*

again and again." . Both answers are reasonable. When making new mandatory courses findings are good to keep in mind.

There will be mandatory courses in future. Everyone were thinking that there are at least enough courses, half of respondents thought there should be more training than at the moment. Positive news is that no one is not thinking reducing training (Figure 15).

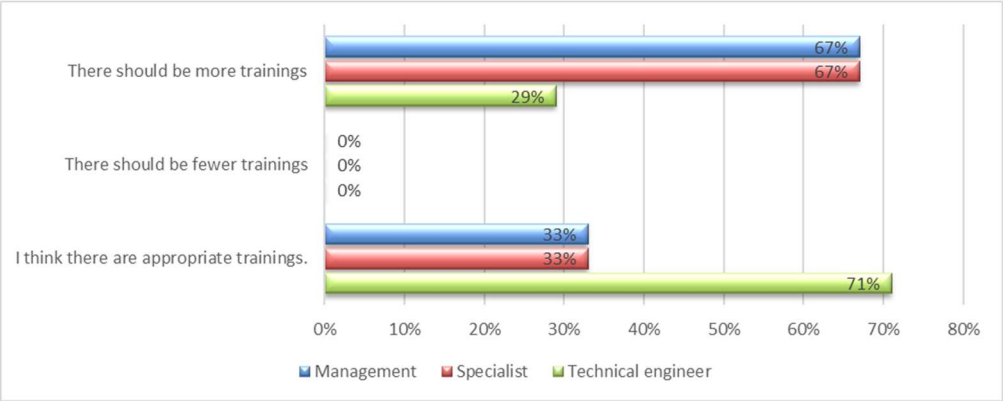

Figure 15. Need for change number of training per group

When courses and training are mandatory, it was good to see is there learned anything from courses. There were seen in answers many kind of things, but company policies and company related information are important, because those are for which they are intended. Rest respondents' answers learned things from courses are seen in Table 6.

Table 6. Things learned from mandatory courses

Answers
I use things to work with, such as password policies, multi-step authentication, and tailgating
The basics are reminded and emphasized on everyday practices.
Caution and the use of common sense.
Opened eyes to understand how easy penetration is to an unprotected environment
To detect potential data-killing threats
It's pretty general. It should be more technical and deeper.
Fujitsu's policies on how to act when faced with various security exceptions/situations.
As far as I know, I have not participated in the actual cyber security course, but I have participated in more than one security course. Most of the content of these courses is taken for granted and understood in common sense. But it is always good to remind you of them, especially how much and in many different ways the snooping of information takes place.
The trainings are very basic, I would also like to see more advanced training
Basic things
caution and perhaps some instructions have been received
how to act securely at work
How to prepare against threats

Because course language is English, it was useful to know what language is meaning for learning. In Figure 16 is seen that language reduce learning in many cases. Almost 1/3 of all are thing it is reducing and that is annoying thing.

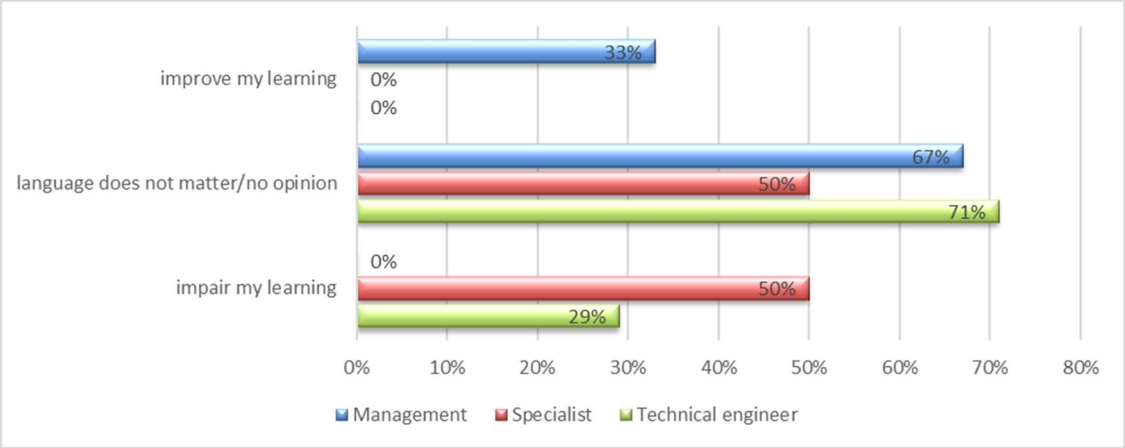

Figure 16. Language meaning for learning per group.

Answer for question should there be more training on cyber security is seen in Figure 17. Overall, 89% of employees wants more training about cyber security.

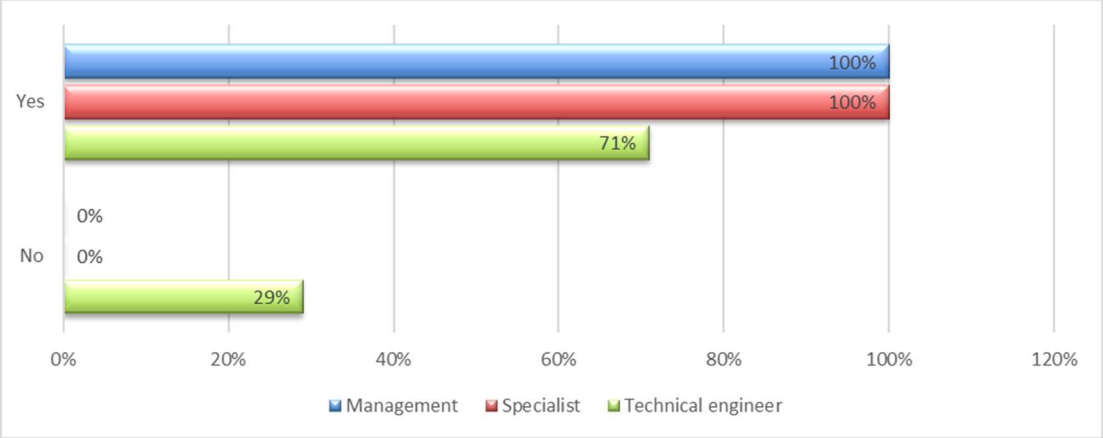

Figure 17. Is more cyber security training needed, answer per group.

When asking what kind of training is needed, management and technical engineers thoughts that web-online training is only needed type. Specialist wants many types of training (Figure 18). In interview came up that some kind of short info notes by Teams will be useful. Also need for interactive training, can ask questions during training, came up from interviews.

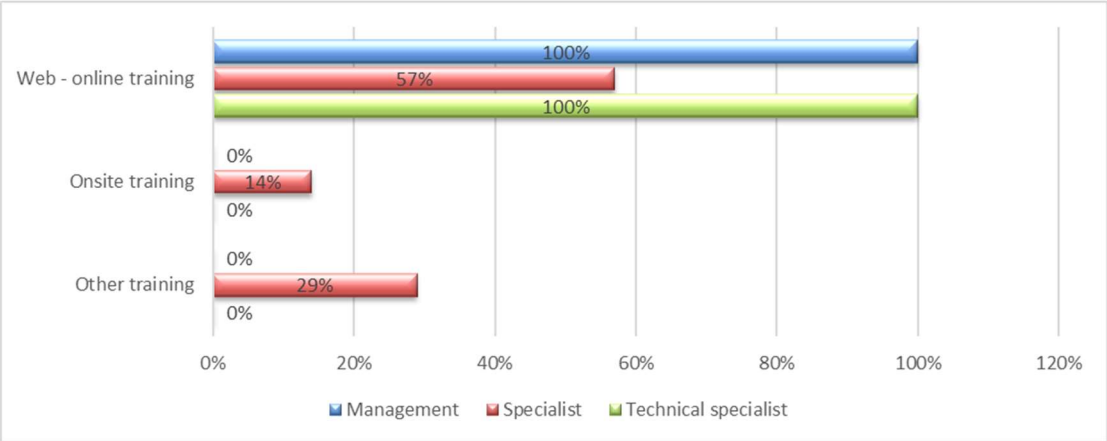

Figure 18. Different type of training wanted per group.

5.5 The current state of cyber security

It was difficult to compare or rate cyber security current state. Table 7 shows current state per groups at office (Management 3,5; Specialist 3,29; Technical engineer 3,86) and at home/remotely (Management 3,25; Specialist 3,86; Technical engineer 3,71). Current state was over average and good in office, but suddenly state was better at home than in office. It feels strange that cyber security was in better level at home, because office network security should be better than at home. In office there is electronic access control, area monitoring and many more advantage for physical safe.

Table 7. Cyber security current state at office and home/remotely

The current state of cyber security at office

	1	**2**	**3**	**4**	**5**	**Average**
Management	0	0	2	2	0	**3,5**
Specialist	0	1	4	1	1	**3,29**
Technical engineer	0	0	2	4	1	**3,86**

Cyber security state at home/working remotely

Management	0	0	3	1	0	**3,25**
Specialist	0	0	3	2	2	**3,86**
Technical engineer	0	1	2	2	2	**3,71**

Covid-19 pandemic has influent to living hard way. In cyber security sector there has been more news in TV and newspaper about cyber security problems. Was that activity seen in daily work and current state? Respondents estimate state to little degraded during pandemic (Figure 19). Someone thoughts even improvements to state. According Interviews there was no change to state seen. But in news and media information about threats were seen more often than before pandemic. Knowledge about threats has grown.

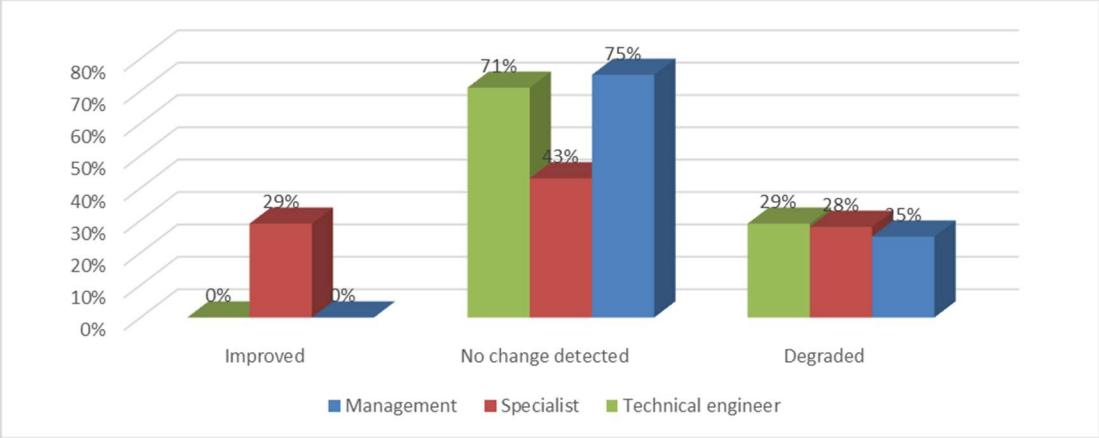

Figure 19. Cyber security state change during Covid-19 per group.

Respondents asked give reason what is causing feeling that the situation has deteriorated during Covid-19. Actually, answers seemed not be only Covid-19 reason. These answers were reflecting problems of remote working, when in discussion was for example VPN problems and home network risks. Respondents answers are in Table 8.

Table 8. Things causing the feeling to situation deteriorated during Covid-19

Answers
Working remotely increases security risks, a VPN may sometimes be forgotten, or you may have to do more than just work on your work computer that increases the risks. There may also be a lack of control in places.
The generic situation around the world is weaker and it occurs to me that this may direct criminal activity to try to wound e.g. health care issues. In addition, it is recent issues related to The Answer Room that materialize the threat and what indifference to cyber security can mean for people.
A lot of people working remotely and the instructions are easily forgotten
I believe that attempts to pry into information and phishing have increased during the coronavirus epidemic.
A quick transition to using your home network/connection, not everyone is fully aware of the security(insecurity) of the home network.

Opposite way, what was causing improvements to situation. Respondent thought that "*there's no one else at home to hear the contents of my meetings*" and *"moving from an open-plan office to an isolated home has improved security".* Couple of respondents thought that home office is better place for working than open-plate office.

It was seen that Fujitsu Covid-19 guidance and informing has been succeeded; current state was 4,17. In Table 9 we see how states were per groups (Management 4,25 ; Specialist 4,00 ; Technical engineer 4,29). Fujitsu should use this kind procedure of guidance in future because employees seems to like that.

Table 9. Fujitsu Covid-19 guidance state per group

	1	2	3	4	5	average
Management	0	0	0	3	1	4,25
Specialist	0	0	1	5	1	4,00
Technical engineer	0	0	0	5	2	4,29

It was hard to give current cyber security state (Table 10) to Fujitsu (Management 3,5; Specialist 4,29 ; Technical engineer 4,00) or to other enterprises (Management 3,33; Specialist 3,83 ; Technical engineer 3,57). In comments was seen that employees are working for different customers and they see situation in those customer companies. Comparing to that, could say that Fujitsu has better cyber security level than other organizations or enterprises. But same time, they saw that comparing level to enterprises are in same business than Fujitsu, level is much harder to thought and it was fairly equal to Fujitsu. Interviews confirmed that measurement or state giving problem.

Table 10. Current state of Fujitsu and state comparing to other enterprises

Fujitsu current state of cyber security

	1	2	3	4	5	Average
Management	0	0	2	2	0	**3,50**
Specialist	0	0	0	5	2	**4,29**
Technical engineer	0	0	0	7	0	**4,00**

Cyber security state comparing to other organizations

Management	0	0	2	1	0	**3,33**
Specialist	0	0	3	1	2	**3,83**
Technical engineer	0	0	3	4	0	**3,57**

Free word section was couple of comments seen. More Training and information are useful. Language caused problems, so native language should use in trainings.

"*More technical information and guidance on cyber security issues would be welcome. The best thing would be to be able to organise internal courses for those interested in these, which would start with (technically) the basics and move forward from the course. So there is nothing 'don't fuss about things on the train in public', but an increase in technical know-how, for example. encryption techniques, etc.*"

"Even though we are an international company, and the official language of the company is English, if we feel that our message is important, then it is worth communicating in everyone's mother tongue. When communicating in English, there are two places where a message can go wrong.

> *1st communicator (in Finnish) translates his timing into English - something might go wrong.*
>
> *2. The recipient of the message (in Finnish) interprets and translates the message in Finnish in their own head - in which case the message may continue to be distorted.*

The more important it is, the more reason to eliminate those two points where a message can go wrong."

"The questions in the study were quite tricky, and we should start by explaining more about what cyber security means."

5.6 Summary of answers

Grouping (management, specialist, and technical engineer) itself was quite successful, group sizes were near each and correspond estimation. Groups meaning to different question results was disappointment. Expect value was to see difference between group answers and that way focus training or education to group is needing that.

Questions about working history was other disappointment. There was not seen mentioned difference of cyber security view between different length of working

history in Fujitsu or ICT sector. Reason for that could be employees' expertise and overall long working experiences, which might harmonized difference.

Respondents view about cyber security were variable. But in big picture was possible see lot of common things at cyber security thoughts and that perspective survey answers seemed good.

Employees were facing cyber security threats. Threats seemed to stay mainly phishing or that kind of emails, and scam calls. Subjective view of answers were not finding one big problem, how to answer question about facing cyber security threats, if you do not know what those are and you already have faced that threat without noticed it. That is the place where technical things like antivirus software helps.

According answers, behaviours when facing cyber security problems seemed reasonable. Suspicious emails were not read and those were deleted. Respondents were thinking and seemed avoiding hitting unknown web links. Avoiding scam calls were challenging. Worrying think was that there were seen scam calls from Finnish phone numbers. Foreign phone numbers were causing problems too. Fujitsu is international company and there were many international customers and projects ongoing. Phone call could come from almost any country touching to those customers. Therefore, was challenging to made decision, was it possible to answer that call. Answering to phone was not probably causing anything, but needed to be carefully and understood with whom was discussing and what information could give.

Courses about cyber security was needed more. Mandatory courses were not so wanted, but still those were seen needful. Other kind of web training from cyber security what was expecting more. Cyber security documentation and guidance were in good level, but native language documentation helps to motivate to red documents and got better understanding of subject.

When Covid-19 pandemic started at Spring and employees needed to start working remotely. Advance wait was that cyber security threats will be the big problem. Luckily for employees, pandemic was not caused bigger problems in office or home working environment.

Cyber security state was good at office, home and when comparing to other enterprises, according answers. Problem was that there was no value where to compare, but many employees were working in customer environment and that way they had reference point.

Interviews were nice extra for answers. Answers deepened view and thoughts of respondent. Couple of new thoughts came up which was not seen survey answers. In questions, where needed to give numerical value, was possible to ask reason for that value. Unfortunately, many questions were not getting any additional information to result, that might be because of question type.

6 Conclusions

Research survey worked fairly well, one respondent said that survey was jammed during answering. Survey respondent count was smaller than expected even answer rate was good. Interviews through Teams succeeded well, respondents were well oriented, and survey based structured interview was easily approachable.

“Is it possible to find coherent vision of cyber security in the target organization?”

Answer to research were not get. Employees subjective view about cyber security is now known. But there were variations with answers, which shows that view was not coherent. From answers was seen lot of similar things, therefore coherent view is possible reach in future. One purpose was trying to find view difference between groups and then focus training specific group. That goal was not reach, but there was seen some common subjects or same view per groups. It follows that, grouping information can partially use for training and education and then things are going towards coherent view of cyber security.

After result analysing can say that research saturation was not reached. Answer group were too small to get all goals what tried reach with this research. Specially to focus training to specific group was not giving information that were straight useful, but there was seen good things.

When discussion survey reliability, survey view was subjective therefore survey reliability cannot be confirmed. But doing survey again, consumption is that, results are near the same or at least include lot of same topics.

6.1 Development

During analyzing process was seen that questionary need some improvements. Some questions need to add to get more dedicate information. Some questions are possible merge together. But when looking other surveys (Haukilehto 2019) came to my mind that it could be useful to add measured or realistic view to research. Reason for thought about realistic view is because of these situations: Almost every person's own subjective view about things are normally little over average, comparing this cyber security view to well-known situation that almost every car driver thinks trey are better than average. Even researches subjective view was main idea, realistic view might give extra knowledge of employees and that information helps to compare which level subjective view is compared to real or measured knowledge of cyber security.

Survey is easy to multiple. Same questions are usable to other offices. Increasing count of respondents might give saturation to some answers and therefore result is more usable and for example some courses and education can focus to some group.

Same way, survey is possible to do other section type enterprises. Questions might need fine tuning, but base can be same. Collecting together many different enterprises survey results, is possibly make larger database and that way build view to find each enterprise sections cyber security main problems. That information might help management to focus straight to right cyber security things.

There is lot of small things what can find text answers. Those things can use for fine tuning guidance and documentation. Those are giving small information to courses and that improve employees knowledge and working welfare. When cyber security knowledge is in good level, it makes employees self-confident. Assurance helps at work for helping customers. Helping customers with cyber security things improve possibilities to make more business.

7 Discussion

Studying process has been long, but same time too short. Mandatory courses of studied were ended at summer 2018. Thesis subject was missing long time.

7.1 Challenges of the thesis process schedule

New thesis subject about firewalls was waiting at beginning of 2019. Thesis topic proposal got negative feedback, thesis idea was not master's level. Motivation to do thesis disappeared. Studying time was ending and need plead more time. Thoughts do thesis was visiting in head time after time. But new idea started spinning in head beginning of 2020. Thesis idea and material gathering seemed to be clear. Discussion about thesis topic proposal started, light green light about idea was seen. Covid-19 pandemic was spreading. Full time remotely working started. Seemed that the moment to do thesis was going far away. Summer was coming and studying time was ending again and need plead more. Summer came and gone; pandemic was still running but panic was not so high than at spring. Again, idea to finish study spun in head. End of October decided to do thesis topic proposal and it was accepted. Little later came email information that right to study ends to 31st December 2020. Two months to made thesis ready sounds quite tight but it was doable. First steps agreed with supervisor and started to arrange research survey. Some ideas about questions was write down earlier, so that was base when thought survey questions. Survey published last Friday of October. Same time was little thinking what things try to put to research. 10th of November at evening came information that thesis and all related documents need to be ready 23rd of November. Survey was still open and hardly anything else was done. After that started thesis writing and information gathering. Survey closed 13th of November after. Completing thesis was going. Few days overtime off work helped with schedule.

7.2 Process and learnings

Thesis process helped to realize researches and that process itself. It opened to think and find other possibilities to see and do things.

Research scope was fairly clear at beginning and that was helping to finish work. But scope was not ideal to results.

Information gathering from literature and thesis before hands was minimal. Afterwards could say that theoretical part should be wider and more deeply. Problem was that there is some much material that it is time consuming walk through even little part of information. Then it was difficult choose what material and references to use. During writing process information gathering was too time consuming and therefore minimized. Of course, many research had information gathering and material problem.

Survey itself was nice to do. Even Webropol survey software was not familiar, it was pretty easy to use to build up that survey. It helped with schedule, that questions were ready (in some level) from last spring thoughts. Actually, this survey part was mostly ready before focusing theoretical part.

Interviews was easy to do. Time to interviews were get easily. Respondents were known so was possible to do additional targeting with some questions. Interview was made through Teams, but probably there was not missing information comparing to face-to-face interview or body language does not give extra info.

Survey answers handling and analyzing were straight part. But analyze was done quite high level and with only few nuances. So deeper analyze and different perspectives might give more dedicated information.

Two things were most difficult in research, one was that theoretical part and information gathering that and second was writing. Writing was probably most difficult part. There were ideas and thoughts, but often those did not go to documentation. Also writing simple thing with long sentence was not familiar and language give extra challenge.

References

CISA 2020 retrieved from https://us-cert.cisa.gov/ncas/tips/ST04-001 accessed 11 November 2020

Edgar T., Manz D. 2017 Research Methods for Cyber Security

Syngress Publishing © 2017 accessed 11 November 2020 retrieved from books24x7.com through Janet, https://library-books24x7-com.ezproxy.jamk.fi:2443/toc.aspx?bookid=128019

Ciseurity 2020, Center for Internet Security, retrieved https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-cia-triad/ accessed 21 November 2020

Defmin, Ministry of Defence Finland, Finland's Cyber Security Strategy 2013 accessed 18 November 2020 retrieved PDF https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf page 13

Forcepoint 2020, retrieved https://www.forcepoint.com/cyber-edu/cia-triad accessed 19 November 2020

Fujitsu 2020, retrieved https://www.fujitsu.com/fi/about/ https://www.fujitsu.com/global/about/index.html accessed 18 November 2020

Haukilehto T. 2019. Improving Cyber Security awareness accessed 12 November 2020 retrieved PDF https://www.theseus.fi/bitstream/handle/10024/166501/Thesis_final.pdf?sequence=2&isAllowed=y

Hirsijärvi, S. Remes P. & Paula Sajavaara 2012. Tutki ja kirjoita. [Reasearch and write] Hämeenlinna: Kariston Kirjapaino Oy.

Järvinen S., 2018. Study cource material: Laadullinen tutkimus [Qualitative Reaseach]

Katakri accessed 3 November 2020 retrieved PDF
https://www.defmin.fi/files/3417/Katakri_2015_Information_security_audit_tool_for_authorities_Finland.pdf

Kananen, J. 2011. Kvantti: Kvantitatiivisen opinnäytetyön kirjoittamisen käytännön opas. [Practical guide to writing a quantitative thesis]
Tampere: Tampereen Yliopistopaino Oy.

Limnéll, J., Majewski, K., & Salminen, M. 2014. Kyberturvallisuus [Cyber security].
Jyväskylä: Docendo.

Pellinen A. 2018. Thesis Pk-yritysten varautuminen kyberturvallisuusuhkien varalle [Cyber security preredness is SMEs] accessed 16 November 2020 retrieved PDF
https://www.theseus.fi/bitstream/handle/10024/151491/Pellinen_Aimo.pdf?

Securopia 2011, retrieved https://securopia.wordpress.com/2011/08/25/security-models-cia-and-ciaan/#more-7 accessed 22 November 2020

Smart Eye Technology 2020, retrieved
https://smarteyetechnology.com/confidentiality-integrity-availability-basics-of-information-security/ accessed 23 November 2020

Appendices

Appendix 1. Survey question in Finnish.

FUJITSU

Kyberturvallisuuskysely

Tervetuloa vastaamaan tutkimuskysymyksiin kyberturvallisuudesta. Kysely liittyy JAMKin YAMK opinnäytetyöhöni. Tutkimuksen tavoitteena on saada käsitys, mitä kyberturvallisuus on teidän mielestä, mitä siihen liittyy, miten se näkyy työssä sekä teidän kokemasta kyberturvallisuuden nykytilanteesta.

Kyselyn tuloksia pyritään hyödyntämään kyberturvallisuuteen liittyvien toimenpiteiden ja ohjeistusten kehittämiseen sekä koulutusten tarkempaan kohdentamiseen sitä tarvitseville henkilöille tai ryhmille.

Kysely on luottamuksellinen, eikä kyselyn perusteella annettavia vastauksia pystytä kohdentamaan kehenkään henkilöön. Kohderyhmänä on oman toimistomme henkilöstö. Kysymyksissä ja vastauksissa keskitytään lähinnä Fujitsuun, Jyväskylän toimipisteen sekä kotitoimiston asioihin. Kyselyyn vastaaminen kestää 10 - 30 minuuttia

Toivon saavani teiltä kaikilta vastauksen, jotta tutkimuksen materiaali saadaan mahdollisimman laajaksi ja monipuoliseksi.

Kiittäen
Janne Markkanen

Aluksi hieman taustaa työhistoriastasi

Työroolisi Fujitsussa

Valitse jokin ryhmä, johon koet kuuluvasi, vaikka se ei olisikaan juuri toimenkuvaasi vastaava.

- ◯ Päällikkö, johtaja
- ◯ Asiantuntija, konsultti
- ◯ Tekninen asiantuntija

Työhistoria Fujitsussa?

- ◯ alle 2 vuotta
- ◯ 2 - 5 Vuotta
- ◯ yli 5 vuotta

Työhistoria IT-alalla?

- ◯ alle 2 vuotta
- ◯ 2 -10 vuotta
- ◯ yli 10 vuotta

Työhistoria yhteensä?

Vuosina

Sitten itse asiaan...

Mitä sinun kokemuksesi tai näkemyksesi perusteella kuuluu kyberturvallisuuteen?

luettele viisi asiaa tai osa-aluetta

1
2
3
4
5

Mitkä kaksi asiaa koet tärkeänä/tärkeimpänä kyberturvallisuudessa?

1
2

Itsearvio omasta kyberturvallisuuden osaamistasostasi?

- ◯ en osaa oikeastaan tiedä juuri mitään
- ◯ tiedän jotain asioita, mutta koen epävarmuutta asioiden suhteen
- ◯ en osaa sanoa tai ei ole mielipidettä
- ◯ mielestäni osaan ja tiedän asioista melko paljon
- ◯ mielestäni osaan ja tunnen asiat erittäin hyvin

Oletko kokenut kyberturvallisuusuhkia viimeisen vuoden aikana?

- ◯ Kyllä
- ◯ En

Minkälaista kyberturvallisuusuhkaa olet kokenut?

Kuinka olet toiminut kohdattuasi kyberturvallisuusuhan?

Tiedätkö mihin otat yhteyttä, jos vastaan tulee kyberturvallisuusuhkia tai -ongelmia?

- ◯ Kyllä
- ◯ En

Kyberturvallisuus dokumentaatio Fujitsussa

Tiedätkö mistä Fujitsun kyberturvallisuusdokumentaatiota löytyy?

- ◯ Kyllä
- ◯ En

Oletko lukenut Fujitsun kyberturvallisuusohjeistuksia?

- ◯ Kyllä
- ◯ En

Dokumentaation taso mielestäsi

	1	2	3	4	5	
Huono	◯	◯	◯	◯	◯	Erittäin hyvä

Parannusehdotuksia dokumentaatioon?

Fujitsu on monin tavoin panostanut kyberturvallisuuteen liittyviin asioihin. Yhtenä esimerkkinä ovat pakolliset kyberturvallisuuden web-verkkokurssit.

Pidätkö pakollisia kyberturvallisuudenkursseja tarpeellisina?

- ◯ Kyllä
- ◯ En

Pitäisikö koulutuksien määrää muuttaa?

- ◯ Koulutuksia saisi olla enemmän
- ◯ Koulutuksia saisi olla vähemmän
- ◯ Koulutuksia on mielestäni sopivasti

Mitä olet koulutuksista oppinut?

Pääasiallinen web-verkkokurssien koulutuskieli on englanti, miten se vaikuttaa sinun oppimiseesi?

- ◯ parantaa oppimistani
- ◯ kielellä ei ole väliä / ei mielipidettä
- ◯ heikentää oppimistani

Miksi et koe kursseja tarpeellisina?

Pitäisikö kyberturvallisuudesta järjestää lisää koulutusta?

- ◯ Kyllä
- ◯ Ei

Minkä tyyppistä koulutusta kaipaisit?

- ◯ Web - verkkokoulutusta
- ◯ Lähikoulutusta
- ◯ jotain muuta koulutusta

Minkälaista koulutusta kaipaisit?

Fujitsu on kehittänyt työntekijöiden laitteiden ja yhteyksien turvallisuutta, ottamalla käyttöön tietoturvallisempia työasemia, monitasoisia autentikointeja ja VPN yhteyksiä. Onko jotain teknisiä laitteita tai tuotteita, jotka sinun mielestä voitaisiin ottaa käyttöön tai joista voisi olla apua kyberturvallisuudessa?

Seuraavaksi arvioita kyberturvallisuuden nykytilasta

Kyberturvallisuuden nykytila toimistolla?

	1	2	3	4	5	
Huono	○	○	○	○	○	Erittäin hyvä

Kyberturvallisuuden nykytila kotona / etätöissä?

	1	2	3	4	5	
Huono	○	○	○	○	○	Erittäin hyvä

Miksi koet tilanteen olevan niin huonon?

Miksi koet tilanteen olevan kotona/etätöissä niin huonon?

Miten koet kyberturvallisuuden muuttuneen koronan aikana?

- ◯ Huonontunut
- ◯ Ei havaittua muutosta
- ◯ Parantunut

Miksi koet tilanteen huonontuneen koronan aikana, onko tapahtunut jotain?

Miksi koet tilanteen parantuneen koronan aikana?

Miten Fujitsu on mielestäsi onnistunut korona-ajan ohjeistuksessa?

	1	2	3	4	5	
Huonosti	◯	◯	◯	◯	◯	Erittäin hyvin

Anna yleisarvo arvosana Fujitsun kyberturvallisuudesta kokonaisuutena?

	1	2	3	4	5	
Huono	◯	◯	◯	◯	◯	Erittäin hyvä

Miksi koet tason olevan huonon?

Anna parannusehdotuksia?

Mitä mieltä olet Fujitsun kyberturvallisuuden tasosta verrattuna muihin toimijoihin?

	1	2	3	4	5	
Huono	◯	◯	◯	◯	◯	Erittäin hyvä

Miksi arvioit kyberturvallisuudentason olevan tuollainen toisiin verrattuna?

Haluatko sanoa jotain henkilöstöhallinnolle tai jollekin toiselle ryhmälle (esim. ECS) kyberturvallisuudesta? Toivoa parannuksia kyberturvallisuusasioihin, joita ei kyselyssä sivuttu? Ehkä kommentoida tutkimuksen kysymyksiä? Sana on vapaa...