jamk.fi

Improving Cyber Security awareness

Health, social services and regional government reform in South Ostrobothnia

Tero Haukilehto

Master’s thesis
April 2019
School of Technology, Communication and Transport
Master’s Degree Programme in Information Technology
Cyber Security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s) Haukilehto, Tero	Type of publication Master’s thesis	Date April 2019
		Language of publication: English
	Number of pages 157	Permission for web publication: x

Title of publication

Improving Cyber Security awareness

Health, social services and regional government reform in South Ostrobothnia

Degree programme

Master’s Degree Programme in Information Technology, Cyber Security

Supervisor(s)

Hautamäki, Jari

Kokkonen, Tero

Assigned by

Hospital District of South Ostrobothnia; Luhtasaari, Seppo

Abstract

As the health, social services and regional government reform set great expectations for the new technology and the savings it brings, the importance of cyber security increases. When training cyber security for the personnel of the South Ostrobothnia Hospital District, the shortcomings in cyber security awareness emerged. Because improving the awareness is the easiest, fastest and cheapest way to improve cyber security level in organizations, the current level of cyber security awareness was seen valuable to measure in organizations under the reform in the region of South Ostrobothnia.

The study investigated the current level of cyber security awareness and the reasons affecting it. The theoretical part discussed the dependencies and challenges of cyber security and critical infrastructure, especially from the health care point of view.

Cyber security awareness was studied with three different surveys. The first two surveys were organized as a part of cyber security lessons for the personnel of the Hospital District of South Ostrobothnia. The third survey was conducted as an internet survey for all organizations involved in the reform in South Ostrobothnia.

A total of over 1,200 responses to the questionnaires were analyzed using material-based content analysis. The results enabled to create an overall view of the current level of cyber security awareness in the organizations, the coverage of the education and the reasons affecting them.

According the results, the cyber security awareness and education are lacking among the personnel and management in the target organization. The overall cyber security awareness should be improved in all target organizations.

Keywords/tags (subjects)

Cyber security, Information security, data protection, awareness, education, Health, social services and regional government reform, Hospital District of South Ostrobothnia

jamk.fi

Kuvailulehti

Tekijä(t) Haukilehto, Tero	Julkaisun laji Opinnäytetyö, ylempi AMK	Päivämäärä Huhtikuu 2019
	Sivumäärä 157	Julkaisun kieli Englanti
		Verkkojulkaisulupa myönnetty: x

Työn nimi

Improving Cyber Security awareness

Health, social services and regional government reform in South Ostrobothnia

Tutkinto-ohjelma

Master's Degree Program in Information Technology, Cyber Security

Työn ohjaaja(t)

Jari Hautamäki
Tero Kokkonen

Toimeksiantaja(t)

Etelä-Pohjanmaan Sairaanhoitopiiri
Seppo Luhtasaari

Tiivistelmä

Sote- ja maakuntauudistuksen asettaessa suuria odotuksia uudelle tekniikalle ja sen tuomille säästöille myös kyberturvallisuuden merkitys korostuu. Kun Etelä-Pohjanmaan sairaanhoitopiirin henkilöstölle pidettiin kyberturvallisuuskoulutuksia, puutteet kyberturvallisuustietoisuudessa nousivat esiin. Koska tietoisuus on helpoin, nopein ja halvin tapa parantaa organisaation kyberturvallisuutta, kyberturvallisuustietoisuuden lähtötaso nähtiin tärkeäksi mitata uudistuksen alaisissa organisaatioissa Etelä-Pohjanmaan maakunnan alueella.

Tutkimuksessa kartoitettiin nykyistä kyberturvallisuustietoisuuden tasoa sekä siihen vaikuttavia syitä. Teoriaosuudessa käsiteltiin kyberturvallisuuden sekä kriittisen infrastruktuurin välisiä riippuvuuksia ja haasteita, etenkin terveydenhuollon näkökulmasta.

Kyberturvallisuustietoisuutta kartoitettiin kolmella eri kyselyllä. Kaksi ensimmäistä kyselyä järjestettiin osana kyberturvallisuuskoulutustilaisuuksia Etelä-Pohjanmaan sairaanhoitopiirin henkilöstölle. Kolmas kysely toteutettiin internetkyselynä kaikille Etelä-Pohjanmaan maakunnan Sote- ja maakuntauudistuksessa mukana oleville organisaatioille.

Vastauksia kyselyihin saatiin yhteensä yli 1200 kappaletta, joita analysoitiin käyttäen aineistolähtöistä sisältöanalyysia. Tuloksilla pystyttiin luomaan kokonaiskäsitys organisaatioissa tällä hetkellä olevasta kyberturvallisuustietoisuuden tasosta, koulutuksen kattavuudesta sekä niihin vaikuttavista syistä.

Tulosten perusteella kohdeorganisaatioiden henkilöstön ja esimiesten kyberturvallisuustietoisuudessa oli puutteita, suurimpana koulutuksen puute. Koulutusastetta tulisikin parantaa kaikissa kohdeorganisaatioissa.

Avainsanat (asiasanat)

Kyberturvallisuus, tietoturva, tietosuoja, tietoisuus, koulutus, Sote ja -maakuntauudistus, Etelä-Pohjanmaan sairaanhoitopiiri

Contents

Figures

Tables

Acronyms

CEO	Chief Executive Officer
CIP	Critical infrastructure protection
CIIP	Critical information infrastructure protection
GCI	Global cybersecurity index
LAN	Local area network
NAO	National Audit Office (United Kindom)
NIS Directive	Directive on security of network and information systems
NHS	National Health Service (United Kindom)
POE	Power over Ethernet
UPS	Uninterruptible power supply
URL	Uniform Resource Locator
VAHTI	The Government Information Security Management Board of Finland

1 Introduction

1.1 Background

The Health, social services and regional government reform and Cyber security awareness are both current topics that concern a great amount of organizations and people in Finland. Whereas the importance of cyber security awareness is becoming clearer, the upcoming reform will even increase the value of the two for the whole society.

Cyber security protects and enables many of the modern services; however, still the terms *cyber*, and *cyber security* are often seen in the news, especially when something bad happens. For example, a big data breach comes to public attention, hackers have caused a distributed denial of service attack, or just a system error causes some trouble in a service that one is so used to think is available all the time in everyday life.

In fact, many of the modern conveniences such as electricity, water supply, transportation and finance depend on cyber environment. Another vital service for everyone is healthcare. No matter if young or old, rich or poor, in case of emergency or just a toothache, everyone recognizes how important it is to get the right treatment and fast.

To get for example an appointment, treatment, prescription and medicine, does not only depend on the availability of nursing staff but a vast amount of systems and services running on many different computers connected to each other on several locations. Systems from air ventilation to lighting and from heating to fire alarm detectors can be dependent on the cyber environment as well, where one single point of failure in this chain can lead into a situation where also the treatment process is disturbed.

To secure these operations and services, the cyber security level must be high in the organizations. The easiest, fastest and cheapest way to improve cyber security level in an organization is to improve the cyber security awareness.

1.2 Organization introduction

This thesis is assigned by the Hospital District of South Ostrobothnia, also known as EPSHP and the organization’s IT department. The Hospital District of South Ostrobothnia is one of the 21 hospital districts in Finland (Finnish Ministry of Social Affairs and Health) and it is owned by 18 surrounding municipals (Figure 1). The EPSHP is a public healthcare organization producing versatile specialist medical care for approximately 200 000 people living the area. The operation of the Hospital District of South Ostrobothnia is based on high quality, respect for people and qualified personnel (EPSHP).

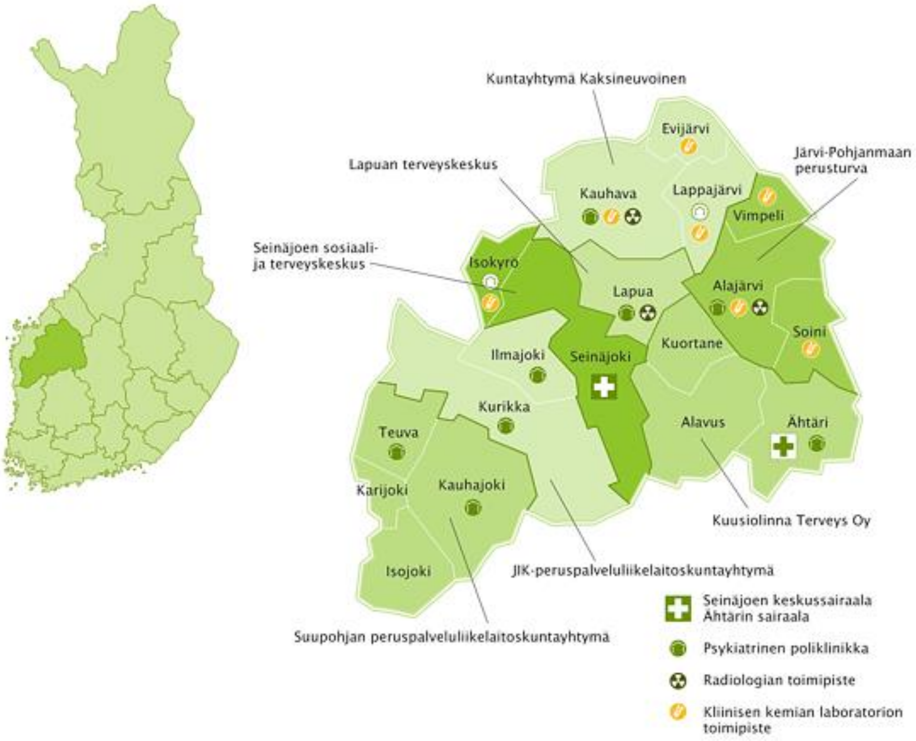

Kuntayhtymä Kaksineuvoinen
Evijärvi
Järvi-Pohjanmaan perusturva
Lapuan terveyskeskus
Kauhava
Lappajärvi
Vimpeli
Seinäjoen sosiaali- ja terveyskeskus
Isokyrö
Lapua
Alajärvi
Soini
Kuortane
Ilmajoki
Seinäjoki
Kurikka
Alavus
Ähtäri
Teuva
Karijoki
Kauhajoki
Kuusiolinna Terveys Oy
Isojoki
JIK-peruspalveluliikelaitoskuntayhtymä
Suupohjan peruspalveluliikelaitoskuntayhtymä
Seinäjoen keskussairaala
Ähtärin sairaala
Psykiatrinen poliklinikka
Radiologian toimipiste
Kliinisen kemian laboratorion toimipiste

Figure 1. The Hospital District of South Ostrobothnia (EPSHP 2016).

The operation of the Hospital District of South Ostrobothnia includes Seinäjoki Central Hospital that offers specialist medical care around the clock and non-emergency services in all special key fields. The Central Hospital operates closely with the surrounding health centers in the Hospital District and offers good collaboration with Vaasa Central Hospital and Tampere University Hospital. (EPSHP).

The Hospital District of South Ostrobothnia has its own IT department producing a variety of ICT services for the Central Hospital and the district's remote locations. In addition, the EPSHP and its IT department provide a virtualized patient information system and other services for the surrounding federations of municipalities via inner network covering the regional area.

1.3 Health, social services and regional government reform

On 1 January 2020, the new Health, social services and regional government reform is to come into force. The reform will establish the new provinces with extended tasks, and the renewal of the structure of social and healthcare including their services and funding. According to the official website of the reform, the biggest change in the reformation will be the division of the public administration into three-tier levels that are central government, autonomous region counties and local government. (Alueuudistus 2017).

The reform will have a major impact on the public healthcare sector in whole Finland and in South Ostrobothnia. The reform has aspiring goals and aims to create a completely new way to organize the social and health services everywhere in the nation, including provision of improved services and more latitude to the end user with lower costs. After the reform, a customer should be able to choose which service provider he or she wants to use. (EP2019).

The reasons behind the reform are, as listed, equal treatment, aging population that need more specialized services, ineffective modes of operation and difficult economic situation as well as the increasing debt of the public sector (Alueuudistus 2017).

2 Research Frame

2.1 Objectives

In an ideal world, the users would know everything related to cyber security and there would be no need to improve cyber security awareness. In the real world, no one knows everything about cyber security; the ever-changing ecosystems, their vulnerabilities and effect on other systems or even the processes behind the systems they are using every day. This produces a fundamental problem, namely, if one cannot know everything about cyber security, what should they at least know, and how could this knowledge be reached? In addition, without knowing the current level of cyber security awareness, the improvement process is difficult.

The main objective for this thesis was to research what the current level of cyber security awareness and education is among employees working in organizations that are to join in the upcoming Health, social services and regional government reform in South Ostrobothnia, and why the awareness is at this level. Secondly, this study aims to study how the cyber security awareness could be improved in the selected organizations and what the elements are that should be taken care of in this process.

This knowledge can be used to form guidelines in improving cyber security awareness inside organizations from strategic to operational planning. The second objective will create an overall picture of the starting level of cyber security awareness for the upcoming organization or organizations and form a base where the organization can continue improving its cyber security.

The hypotheses for this work are following:

- The employees want to know more about cyber security concerning the digital ecosystems they are using.
- The employees are willing to participate in cyber security lectures

- The knowledge is possessed by in employees with good knowledge; on the other hand, there are employees who have a limited or very limited knowledge about the subject.

2.2 Research method

The research subject in this research design is a human subject and the data is gathered via surveys. The data consists of answers from three different surveys. The first two surveys were conducted within cyber security lessons given to the employees of the Hospital District of South Ostrobothnia, and the last survey was conducted as an internet survey to the employees of organizations about to join in the upcoming reform in South Ostrobothnia.

When choosing the best research method for the thesis two research methods quantitative and qualitative were considered. These two research methods have clear difference how they process data; in quantitative research the data is numerical and in qualitative research the data is not numerical. However, these two research methods form a methodological pair that can be used separately or together to complement each other (Koppa 2010).

The quantitative research method is often used when objects are measured and results are described statistically (Koppa 2010). Yet, to find answers to the chosen research questions determining the current level of cyber security awareness, reasons behind the level and how the awareness could be improved, describing the results only statistically was seen insufficient. Statistics and numbers could have shown how many percent of the respondents knew the right answer for example, but the quantitative research method would have not been reliable way to find and describe the information about the level of cybersecurity awareness or reasons behind it.

As opposite to the quantitative research in qualitative research the data is not numerical because it tries to answer to questions that might not be described by statistically such as “how” and “why”. The qualitative research method is ideal to gain deeper information about the topic, -and it is helpful specially to understand the reasons and motivations of people and their answers (Kananen 2015, 70-71).

Based on these descriptions about the two methods the research method chosen for this study is qualitative research that it is align with the chosen research questions and seen to support the objectives better. In addition, quantitative research questions are used in the surveys and the results are described statistically to provide more data for the study to complement the qualitative research method and to improve the reliability of the results.

2.3 Structure

The thesis consists of seven parts. The first chapter introduces the subject and its background. The chapter continues with organization introduction and ends with a brief introduction of the upcoming Health, social services and regional government reform in Finland.

The research frame in the second chapter consists of the chosen objectives for the work, research questions and hypotheses about the results. Additionally, the second Chapter describes the research method and the structure of the thesis.

Chapter three includes the theory about cyber security related to critical infrastructure, especially from healthcare perspective. Subjects such as cyber dependencies, legislation, cyber threats, cyber security human factor as well as opportunities that cyber security offers are described forming a theoretical context for the work.

Chapter four includes a presentation of the surveys and cyber security lectures used to gather the information for the work. The results and analysis are presented in the following chapter five followed by chapter six with conclusions of the results. Finally, chapter seven concentrates on the discussion and critic to the work.

After the last chapter, the references used in the work are listed. The survey forms used with the survey results and other information referred in this work can be found in the Appendices.

3 Cyber security and critical infrastructure

3.1 Healthcare as part of critical infrastructure

The infrastructure providing the most vital functions for a society is called critical infrastructure (European Commission 2017). This kind of infrastructure has several different sectors, for example, the US Department of Homeland security identifies 16 different critical infrastructure sectors, healthcare sector being one of them (DHS 2017). All these sectors have in common that they are essential for the society and if one or more is damaged, it could impact the whole society negatively.

A simplified structure of critical infrastructure is shown below in Figure 2. Although the structure is simple, it shows how strongly today's society depends on the electricity network. Without electricity there are no data networks nor the services using it. If there is electricity but no data network, then again the services built on it do not work. (Lehto et al. 2017, 48).

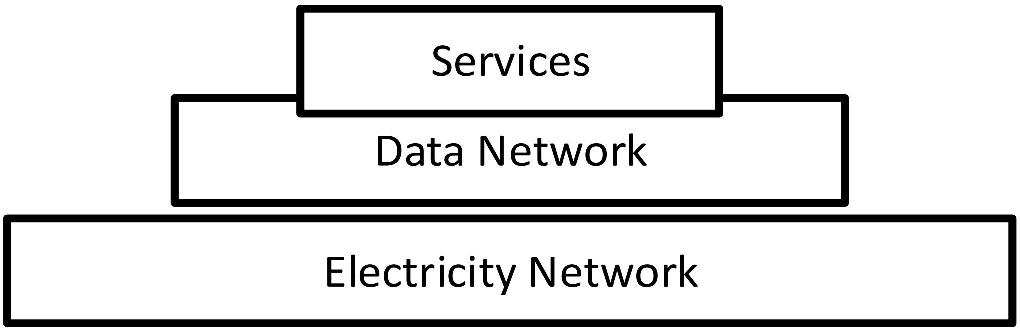


Figure 2. Simplified structure of critical infrastructure (Lehto et al. 2017, 48).

In order to build a data network, first a reliable electricity network providing electricity is needed. Only with these two bottom layers electricity and data network functioning the digital services to help people’s everyday lives can be created and maintained.

Critical infrastructure sectors also depend on each other, and healthcare is no exception. These dependencies are both positive and negative. On the positive side, the sectors support one another; however, on the negative side, they are in need of services the others provide. It is easy to see that without running water or electricity the healthcare sector is in big trouble (Macaulay 2016, 277).

Still, troubles for healthcare can exist without a direct sector correlation. For example, if a healthcare sector is damaged, it will not have a wide effect on transportation systems. However, if the transportation systems are damaged and accidents take place, the healthcare sector is also affected.

In real life, here is an example with a cyber security issue: Patient information system is running improperly due to the cyber security interruption, which causes no effect on transportation systems sector; in comparison, the transportation systems are running improperly due to cyber security issue and healthcare must take care of the possible casualties. The damage will increase more rapidly if it hits both or even more of these sectors at the same time or in the short run.

Clearly, such important infrastructure needs good protection. Securing the nation’s critical infrastructure from threats including national public healthcare in a digitalized world is not a new idea. In the US, the term critical infrastructure protection (CIP) was defined in the 1990s, although the importance of infrastructure had been noted 30 years prior to this, and it has been studied ever since. (Lewis 2014, 3)

Along the digitalization, the terms and definitions evolved during that time also in Finland. According to Kananen (2015, 270-271), the former chief executive officer of Finnish National Emergency Supply Agency, Finland has produced several studies about the resilience of the society’s digital systems for decades. Before these studies were connected to the term cyber security, they were known as ICT security, information system security or data network security, just to name a few. However, that time they did not receive the public attention they are receiving today, and some of those studies were classified as confidential material and were never published. (Kananen 2015, 270-271).

Digitalized infrastructure, the part of infrastructure related to information technology is vital in today’s society because it is used in monitoring, managing and controlling critical technical infrastructure. Infrastructure such as this includes diverse sectors, e.g. energy production and distribution, monetary systems and traffic, water supply, public governance systems, transportation, logistics and healthcare systems, all critical for the society’s stability and safety. (Kananen 2015, 138).

However, it is important to remember that although the critical infrastructure is vital for today’s nations and whole societies, it is often provided by the private sector, not the public sector (Enisa 2014).

Today when it comes to protecting critical infrastructure, critical information infrastructure protection (CIIP) is discussed more and more. The term CIP, with the extra letter “I”, refers to infrastructure sectors and altogether all sectors connected via information infrastructure and therefore, also dependent on it. Consequently, the information infrastructure can be seen as one of the critical information sectors itself. (Personick & Patterson 2003, 9).

As the Global Forum on Cyber Expertise suggests in their paper The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers, the nations should start to determine the set of possible critical information infrastructure. The paper also suggests that the nations should be prepared for critical information infrastructure crises. (GFCE-MERIDIAN 2017, 28-36).

Presently, in the world where sectors dependent on information infrastructure from water supply to healthcare could suffer in a wide scale and produce notable damage for the whole society just because of an IT problem. In addition, the digitalized world and critical information infrastructure have produced another challenge: the dependency on cyber.

3.2 Cyber Dependencies

A cyber dependency (Figure 3) exists if the operation of an infrastructure depends on information transferred through the information infrastructure. Generally, the transfer, processing and use of cyber resources such as data or information are carried out by communications and information technology that both are critical infrastructure sectors. When analyzing the categories of cyber dependencies, the elements such as quality of service (QoS), network performance and internal cyber links should be considered. (Petit et al. 2015, 16).

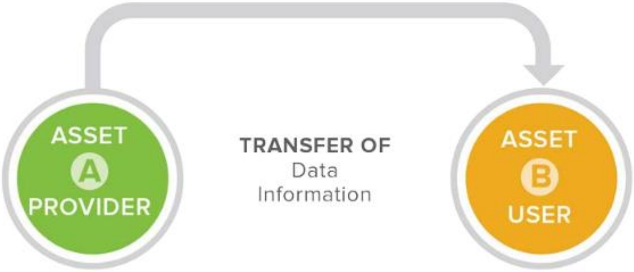


Figure 3. Cyber dependencies (Petit et al. 2015, 16).

3.2.1 Electricity in Finland

Next, electricity is discussed as an example. Electricity is a must for all information technology; no matter if a device is getting its power from a battery or directly from the nearest power plant via a wall socket: if there is no power, there is no ICT, so information technology depends highly on electricity.

The batteries will not run forever, thus, eventually, they need to be charged at some point. If there is no way to produce the electricity locally using a wind power station or solar power for example, users need to rely on the electricity produced in a remote power station and transmitted to users via power grids and possible substations. This is also the usual case, especially in a large scale with high quality and continuity standards such as the ones healthcare has.

The problem with the electricity flowing in the grids is that it needs to be produced as much as it is consumed continuously. This is because there is currently no technology to store the extra power to be consumed during the shortages. (Energiateollisuus 2017).

Because the electric energy consumption varies a great deal, also the electricity production must be controlled to meet the consumption precisely. Electricity production dependent on the current usage is called load following power. A good example of this kind of power plant type are hydropower or water energy plants which use the energy of falling or flowing water to produce electricity. If needed, the hydropower power plant can be started at short notice and the output can also be easily controlled by adjusting the water flow to meet the variation in energy consumption. (Kemijoki 2017).

Unfortunately, unlike its Scandinavian neighbors Sweden or Norway, Finland does not have enough hydropower available in the country to meets its requirements. This is concretized especially in the peak season of energy consumption, during the coldest days of winter when the temperature decreases easily to twenty degrees below zero. During the peak seasons, the shortage is covered by buying power from the neighboring countries. The highest electricity consumption so far in Finland was in the beginning of 2016 with 14 900 Megawatts total where the national production covered only 10 700 MW. The rest was imported from abroad, e.g. Sweden with 2400 MW and Russia 1480 MW, and 320 Megawatts were imported from Estonia. (Fingrid 2016).

Even during the all-time high-energy consumption peak all import grids were at their full capacity and almost every national power plant was running. Finland has also so called power reserve for emergency usage including systems such as gas turbine power plants to cover a short time power shortage and give the nation time to import the needed power from abroad. (Aukia 2015).

Consequently, Finland depends on the import of electricity especially during the coldest days of winter. In November 2016, the National Emergency Supply Agency of Finland estimated that for the winter 2017 peak usage, the national production capacity could be 3 400 MW less than the usage. So far, the import capacity has been enough to cover the lack of national production; however, in a case where the Finnish electricity production or import capacity face notable problems during the peak, the usage might lead to a temporary power deficit and limitations for some of the customers. (Finnish National Emergency Supply Agency 2016).

It is important to note that during the coldest days, the consumption is likely at a high level in the countries exporting power as well. In the future, the risk and dependency on neighboring countries should be decreased with new wind power that has strong funding from the government (Tuulivoimayhdistys 2017) and the upcoming 1600 MW nuclear power plant Olkiluoto 3, the start of operation of which has been delayed for a decade because of several difficulties during the building process (TVO 2017). If something remarkable, besides the fact it was supposed to be the first EPR-type nuclear power plant until the delays, Olkiluoto 3 is the longest lasting building process in Finland (Nikka 2017) and one of the most expensive buildings in the world (Laatikainen 2018).

The second upcoming nuclear power plant Hanhikivi 1 with production capacity of 1 200 Megawatts is estimated to be in operation by 2024 at earliest (Fennovoima 2017). Even though, Hanhikivi's electricity production is still far away, the plans for Finland's sixth nuclear power plant has attracted attention with its funding including shady funding offers from Croatian Migrit Solarna Energijen with connections to Russian business actors (Harala & Blencowe 2015). Currently, the constructor Fennovoima is owned by Finnish Voimaosakeyhtiö SF with holdings of 66 % and the facility supplier RAOS Voima Oy 34 % (Fennovoima 2017). The latter is a subsidiary of Rosatom a Russian state funded nuclear power operator which has been estimated to fund the project with approximately 3 billion euros (Hakala 2015).

There is no short time relief at sight for Finland's electricity production and reliability that is important not only for the whole society but also for powering the national critical information infrastructure. This has been noted as well in the Mid-term adequacy forecast 2017 edition report published by ENTSO-E, the European Network of Transmission System Operators for Electricity. The report predicts that in 2020, the reliability of Finland's electricity delivery has a serious risk of resource deficiency and categorizes the nation's situation to be at the lowest level in the whole Europe with countries such as Albania and Bulgaria (ENTSO-E 2017).

Matti Sohlman, the head of energy delivery from the second largest Finnish energy company Northern Power Company Ltd. states that these forecasts in ENTSO-E paper are alarming and should not be left unnoted because the estimated risks for power outages are serious. Sohlman writes in his blog on the company's web site that generally the acceptable power outage for consumers is three hours, whereas the forecast shows a 24-hour power outage in Finland during the 2020. As the reasons for the current situation, Sohlman lists shutdowns of condensing power plants and the decreasing amount of combined heat and power plants that have been technically at the end of their life cycle and thus financially not feasible to invest in. Sohlman criticizes Finland's national funding for favoring weather dependent energy production with degenerating profitability of delivery reliability production and the way how the nation-wide transmission grid has been built to bank on importing power from the neighboring countries in a case of emergency (Sohlman 2017).

Getting help from neighboring countries even in an emergency case is not clear indeed. Although there is Scandinavian co-operation in the energy-sector, the ENTSO-E paper shows that the production in Sweden and Norway is not enough to cover Finland's power deficiency (ENTSO-E 2017). It should be clear that there can also be situations where the neighbors do what is best for themselves.

During autumn 2017, a secretly prepared offer from Swedish and Norwegian national transmission system operators Svenska Krafnät and Statnett for the Scandinavian power co-operation was revealed. If the previous agreement from a decade ago aimed at balancing the electricity production and consumption together in the Nordic countries in Denmark, Norway Sweden and Finland, the new offer includes parts giving Norway and Sweden in practice the ability to decide how Finland and Denmark could produce their electricity, and in what kind of power plants if a major power plant goes offline or the current consumption exceeds the production during cold winter days for example. (Nikula 2017).

The offer would also give Sweden and Norway the right to decide the rules for the electricity system of their neighboring countries, their current state and the load following production with the power reserve plants. In Finland, the proposal has been declined because it is against the EU and Finnish legislation; however, this has not stopped the proposers who have even demanded that the current laws should be changed to accept the draft agreement. (Nikula 2017).

Jukka Ruusunen a chief executive officer of Finland's transmission system operator Fingrid has written in the company's press release that the company has received a second updated offer for the agreement from the Svenska Krafnät and Statnett. The new offer was received a month after the first one; however, according to Ruusunen the basic parts of the paper remained the same. Although the Danish national transmission system operator Energinet accepted the first draft agreement Ruusunen writes that Fingrid cannot follow Denmark in a way that negates the equality in the Nordic decision-making in energy cooperation. Ruusunen continues to argue with the draft agreement that the energy system responsibility is a vital element in the national decision-making and the Finnish law does not allow it to be moved to another country as is required in the written offer. (Ruusunen 2017).

Whether it is wanted or not, the energy has and will have a part in politics. In Russia, the politics and national interests are very keen on energy and have been seen even as an element that could enable the nation's great power status (Martikainen, Pynnöniemi & Saari 2016). Still, the situation in Russia differs significantly from the Nordic countries and it should be remembered not to be too gullible to anyone, which also applies to other neighboring countries.

The new Nordic energy draft agreement may affect the relationships between the concerned countries at least in the power sector; however, in order to realize how large consequences these kinds of agreements can have for a country's critical infrastructure and to whole society, it should be noted and brought into public debate. Letting the ability to make the important decisions regarding the energy resilience slip abroad will not improve Finnish cyber security level – this could even lead to a situation where a part of the national cyber secureness is moved with the agreement.

3.2.2 Electricity and Cyber security

As introduced earlier, the energy production needs to meet its consumption, all the time, every minute and every day. To adjust the production in a large scale to meet the persistently changing consumption, the manual adjustment and configuration have been automated. This automation has changed the nature of electricity production where in fact, computers powered with electricity are taking care of the vital processes of the whole energy production. What is more, these computers can be connected to a local network or even directly to the internet making them and the energy production vulnerable to digital flaws such as cyber-attacks.

Cyber-attacks against energy sector have been realized in the past decade as well. Stuxnet, developed by USA and Israel showed the power of cyber operations when their national level malicious software disrupted the nuclear development process in an Iranian nuclear facility in 2009 by reconfiguring frequency adaptors that the Iranians were using manufactured by a Finnish company Vacon. The virus caused physical damage to the centrifuges that were vital for the nuclear process. Later, the malicious software spread from the target facility to the internet revealing its originates; however, unfortunately this was not enough and even assassinations around the cyber operation were suspected. (Järvinen 2014).

Another cyber-attack case against energy sector was from Ukraine in December 2015 when suspected national level hackers caused a total electricity blackout for over

200 000 residents in the country. According to a report from industrial control systems cyber emergency response team of the United States (ICS-Cert), the attack was sophisticated and conducted by multiple attackers including delivery of malware via malicious spear phishing emails and suspected use of remote administration tools with legitimate user credentials. The report states that the attackers corrupted and erased valuable and selected data for the energy operation and even replaced the used firmware of Serial-to-Ethernet devices with having scheduled tasks to disconnect Uninterruptable Power Supplies from the operation. (ICS-CERT 2016).

German authorities have warned that hackers could be able to produce disruption in European electricity production and distribution in wide scale. An attack targeting one or more major power plants in Germany could cause a domino effect leading even to a total electricity blackout in the whole European Union. (Saraste 2018).

Yet, energy sector and cyber security can face other problems than direct and planned cyber-attacks as well. At the end of December 2017, heavy snow load cut trees on power lines causing almost 20 000 households to lose their electricity in North Karelia region in Finland. These power problems started briefly after Christmas and lasted over one week with almost five days when the emergency number was not reachable from the area. Problems in the mobile network were due to the mobile base stations power outage and insufficient backup energy for outage that lasts for hours. In fact, the teleoperators in Finland have to ensure to have on-site backup power to power the mobile base stations only for 2 - 6 hours. (Tekniikka & talous 2018).

Several challenges were noted in the Finnish electricity production and resilience at the national level; however, is this really a cyber security issue? Should it be more the concern of the energy sector to be handled? If the answers to both questions need to be known, there must first be an understanding that the electricity today is highly related to cyber environment, even dependent on it, and the whole energy sector should be aware of the basics of cyber security to provide and design durable and resilient energy for the whole society. Hence, cyber security awareness is important also in the energy sector.

3.2.3 Data Networks

Technology devices used today are often connected to a network in a way or another which means that the devices are part of one or several data networks. As seen in the simplified structure of critical infrastructure figure, data networks are based on electricity and therefore dependent on it. If the power is lost, the data network cannot function. This dependency continues all the way from the machines providing the services to the access level providing the network connection for the end users.

Modern networks are often built using hierarchical network model that includes three layers: Access, distribution and core as in Figure 4. In the model, the core acts as a heart of the environment providing a fast link for the distribution layer and interconnectivity to outer networks such as the internet, whereas the distribution layer works as a policy-based and controlled boundary between the core and access layers. On the bottom, the access layer is where the network connection is provided for the end users and their machines. (Cisco networking academy 2014).

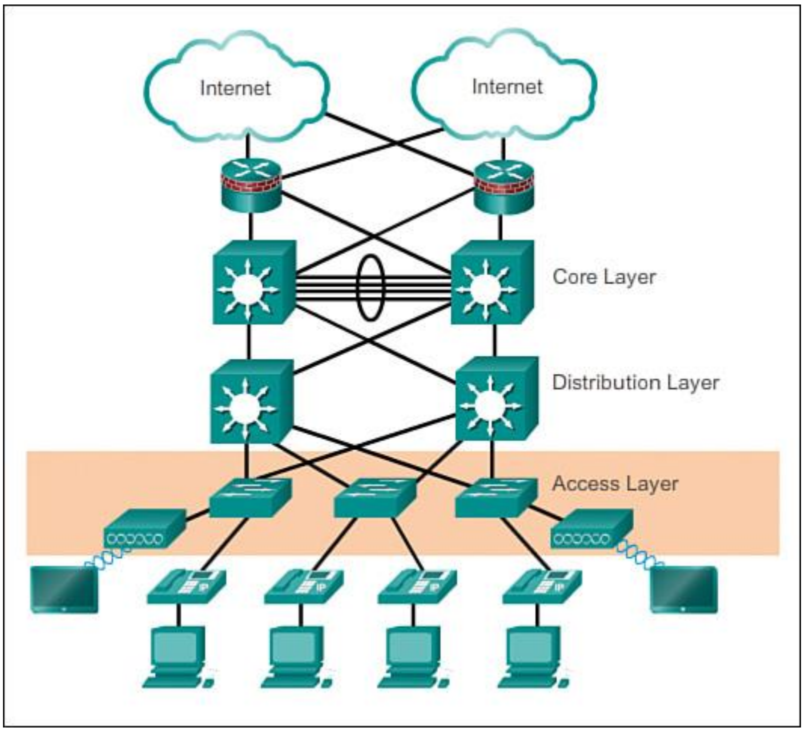


Figure 4. Hierarchical network design (Cisco networking academy 2014).

The network design can vary depending on the current environment. In a small network, the core can be a collapsed version containing the core and distribution layers with just few machines in a closet; however, in a large environment it can contain several different data center rooms all duplicated to ensure the redundancy. Yet, the hierarchical network model is especially used to provide reliable and flexible design that can meet many modern needs with cost-efficiency (Cisco networking academy 2014).

Computers and other digital equipment used at workplaces with network connection are often connected to the access layer switch. Whether the device is connected to the nearest network socket by a data cable, or it is connected to the nearest wireless access point via air. In both cases, the link leads to the access layer switch, because in the end also the access point needs to be connected to the switch by a cable. From the access layer switch the traffic can be transferred to other parts of the local area network (LAN) or into other networks such as internet.

Along with the transferring data, modern LAN switches have power over Ethernet (POE) feature to pass electric power in the Ethernet cabling. The POE feature is typically used to power devices such as wireless access points, VoIP phones and surveillance cameras (Veracityglobal 2018). In addition, modern lighting, tracking devices, locking and access control systems, monitors and especially in healthcare sector nurse call systems used by patients and staff to call help can be powered with POE.

The power over Ethernet offers great benefits such as reducing the need for separate electricity cabling making the installation process more effective, easier and faster. Safety can be also seen as one of the advantages of POE when the power delivered has intelligence included with increased protection against incorrect installation, overloading and under powering. Devices that are using the power over Ethernet can be reset and disabled remotely as well and if the POE switches have been installed with uninterruptible power supplies (UPS) the power redundancy can be increased also with the powered devices. (Veracityglobal 2018).

Still, at the same time all devices powered via POE are dependent on the data network and the switch providing the electricity increasing the importance of the data network. If the data network is not working properly, this can affect to the POE devices as well. Due POE, misconfiguration in network settings can have much wider affects than just traditional computers. What is more, if the data network or part of it is attacked by malicious user or program, the POE devices can be also affected. For example, if an attacker could gain control of POE switch, he or she could turn off the lights, shut down security cameras, cause abnormal operation for doors and other devices powered with POE. This all could be done without even knowing the way to take control of the actual devices and their management because the POE device gets both data and power from the same cable connected to one network switch and from the switch the delivery of POE can be controlled.

Besides connecting the devices to LAN, a common network connection type of a modern mobile device such as laptop or phone is mobile broadband connection.

When mobile connection is used, the traffic is linked to the nearest base station and from there to the wired network. Because a base station can serve only a limited number of users, the amount of base stations must be higher in an area with a high population. Whereas, in less populated areas the number of base stations can be lower and transmission power used can be increased to cover larger areas. In practice, Finland is covered with base stations with one base station for every two kilometers. (STUK 2018).

Regardless of which type of connection is used, wired or wireless, mobile or local area network, in order to transmit data the network must function properly from start to finish. If the connection is unstable or its quality is poor, the transmission can fail and can be seen as poor video quality or unreceived messages, for example.

The network and connection type used should be designed to meet the service level needed. In a case where a single user or device needs only to have access to the internet with normal service level, a mobile broadband connection can be enough, and no additional redundancy is needed. This kind of network connection can be secured with encryption to access different services or used to connect the device to workplace environment securely via the internet.

When higher service level is needed, the network should have strengthened implementation. In critical environment, this means redundancy with all vital network devices. Redundancy network connection is often configured to be used automatically if the primary connection fails (Shimonski 2010). Connections can also be dedicated and therefore separated for specific use or for certain organization and this can be achieved on both virtual and physical layers.

Physically separated networks are using different cables and wires, whereas virtually separated networks can use same wires and cables, but the traffic is virtually divided into different logical virtual networks instead. When virtual network segmentation is used, different networks using same cabling can be separated with access lists or firewall and security level increased. (Koivunen 2010).

An example of virtually segmented network is seen in Figure 5. In the example network, the segmentation is implemented using Virtual Local Area Networks (VLANs) to separate the network into two VLANs 1 and 2. Although the traffic can be transferred in the same cables, the traffic of Human Resources department on VLAN 1 cannot see the traffic of Accounting Department on VLAN 2. If the two departments want to share data, the traffic must be routed and accepted between the VLANs. (Olzak 2010).

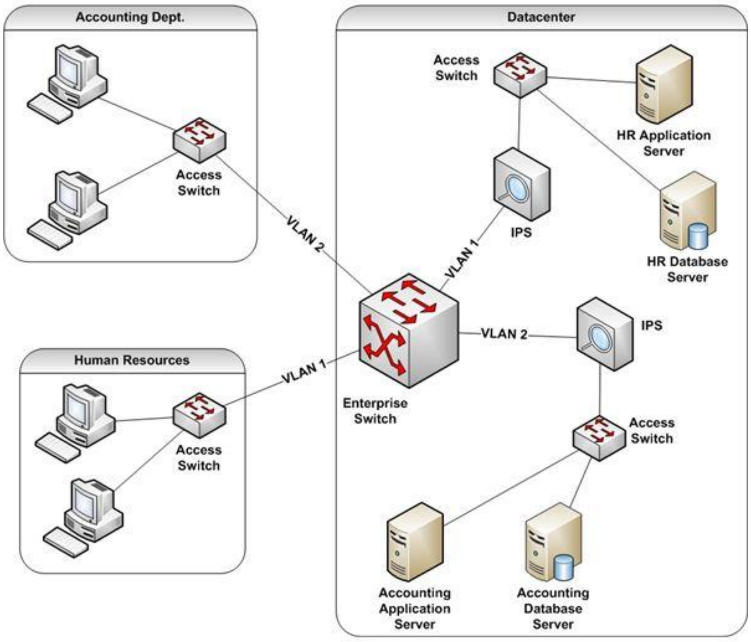


Figure 5. Virtually segmented network (Olzak & Scudder 2010).

Although network segmentation is used in local area networks, and the traffic between network segments is monitored and controlled with security devices such as firewalls, the traffic inside a certain segment may not be controlled by these security features. Therefore, if the devices themselves do not have limitations or restrictions to the incoming or outgoing traffic, the network traffic is not secured inside the segment.

In practice, if a computer is connected to a free wireless network at a cafeteria for example, a malicious user inside the same network could be able to see all unencrypted traffic coming in and out of the computer. This means that the attacker could be able to perform a man-in-the-middle attack where he or she captures or intercepts the traffic such as login credentials, emails or financial information or injects a malicious software into the computer (Globalsign 2017).

If the computer with malicious software is then connected to another segmented network such as work network, the malicious software could now spread inside the network segment into other devices with the same vulnerability or be used to scan other vulnerabilities without even being detected by network firewall located between the segments, because if the traffic stays in the segment, it does not pass the firewall. Fortunately, the devices themselves can be equipped with firewall, antivirus and other security tools to protect the attacks coming also from inside the same network.

Yet, the network segmentation reduces the attack surface and infections from spreading from segment to another and allows isolation of certain segments without affecting the whole network. The segmentation also introduces one security measure against malicious users from moving from segment to another and gaining deeper control and view of the network (Olzak & Scudder 2010).

In the healthcare sector, there can be numerous different critical devices with limited ability for security settings and abilities. Installing an antivirus or host-based firewall on them might not even be possible or allowed by the manufacturer. Medical devices might not even be designed to be attached into data networks securely. Therefore, these kinds of vulnerable and critical devices should be carefully segmented and separated from other devices and segments to reduce the attack surface and the risk that these devices are infected by other types of devices or used for malicious purposes.

As described in Chapter 1.4, the ongoing Health, social services and regional government reform aims at a situation where organizations are joined together, and their operations are integrated. In the reform, data networks might be integrated as well to simplify the environment and reduce the costs. If healthcare networks are connected to the social service networks and other organization networks, the importance of network segmentation will eventually increase, when the same company could be managing a network for medical devices located in hospitals as well as machines controlling operation of dams or laptops used by Environmental Health Manager.

When several different types of networks and devices are used inside one organization, the risk of connecting a device into a wrong segment by a human error can increase. Therefore, it is vital for these kinds of organizations to understand the importance of cyber security awareness because if users are not aware of basic structure of networking such as the segmentation and meaning of it, it can be difficult for them to understand the risks as well.

In Finland, data networks and their vitality for multiple infrastructure sectors have been actualized and noted, especially when the networks are not working. An example of this kind of scenario occurred on 15 May 2018 when Finland's largest teleoperator Elisa (Elisa 2018) executed fiber cable configuration changes in the city of Helsinki, which led to several public services to be out of order. Due to the incident, the patient information system used in the area was failing and non-emergency patients were advised to postpone their appointments. In addition, the capital suffered other problems as well including nonfunctioning email and phone call services in public sector, having most of the ticket machines of public transportation and even some of the safety systems for metros and trains to be offline. (Helsingin Sanomat 2018).

Because the problem occurred in the operator network, the systems failed even in the city of Helsinki, and its public sector had backup connections in their inner network. Shortly after the case Jukka-Pekka Juutinen, the Head of Security Supervision from the Finnish Communications Regulatory Authority Ficora asked if having the local public transportation ticket machines and hospitals behind the same network connection is reasonable and suggested that organizations should test and ensure the functioning of the backup connections in practice against these kinds of incidents. Furthermore, Juutinen noted that organizations should consider using separate network connections for different services and keeping some of the smaller services running via the backup connections to help monitoring the state of these connections. (Tekniikka&talous 2018).

3.2.4 Services

After electricity and data networks are functioning, the data can be transferred on the network enabling devices to be connected to each other and to machines and networks providing different services. In other words, digital services are built on electricity and data networks as seen in the simplified structure of critical infrastructure (Figure 2) showing the dependencies between these levels.

Digital services used today can be divided into three categories: telecommunications, broadcasting and electronically supplied services as regulated by the Council of the European Union (EUR-Lex 2013). The telecommunication services are telephone services including mobile data, voice and video calls as well as access to the internet, for example. Broadcasting services include radio and television programs except for programs distributed via IP protocol or via internet. Services categorized to be electronically supplied services or e-services, are services delivered over the internet or other similar network. A list of examples of e-services contains services from use of search engines to downloading music and viewing weather reports online. (Office of the Revenue Commissioners 2015).

These three categories of services, also known as TBE services are all dependent on electricity and data networks; however, the e-services using internet are highly dependent on the internet as well. As seen in the Hierarchical network design (Figure 6) in the previous chapter, the computers and devices below the access layer have the connection to the internet through the example network. In practice, the internet is considerably larger and more complex than a cloud that is often used to describe it.

The internet is so vast, complex and changing all the time that it would be impossible to draw the internet in practice, which is why the cloud is a more useful way to describe it. The internet consists of numerous machines connected to each other forming numerous networks connected to each other located all over the world, which means that the internet is a network of networks. However, the internet itself needs a great amount of infrastructure and functions to work and to provide many of the e-services that are used today. If these functions are not working properly, the whole internet and all services depending on it will be affected. (Shuler 2002).

When digital services such as e-services are used over a data network such as the internet, the actual services are located on one or several computers. If the computer providing the service is located in the same local area network, or even in the same room, the infrastructure between the service and the machine where it is used from should be determinable. In this case, the used electricity, data network as well as the service and the secureness of these actors might be checked and risks estimated.

However, these actors are more difficult to determine and to be followed in a case where a service is used from the other side of the world. For example, end-user machine locating in Finland and the service used over the internet is running on a machine in China. The secureness of the used infrastructure can be difficult to estimate if there are numerous of different computers running on numerous different networks powered by numerous different electricity companies between the user and the service. This kind of calculation is probably impossible in practice, due the complexity and ever-changing nature of the internet; however, it shows that when the distance and the number of points-of-failure increases between the two, the risks may increase as well.

3.2.5 Cloud computing

In contrast to the case where the service used is running on a local machine or in a local datacenter, many of the modern services are provided remotely from cloud. The definition for cloud services is that they are actually running on cloud service providers' datacenters and made available for customers via the internet. As seen in Figure 4, cloud services can be divided into three major categories: SaaS (Software-as-a-service), IaaS (Infrastructure-as-a-service) and PaaS (Platform-as-a-service). (Violino 2017).

In Computerworld's Tech Forecast 2017 survey 79% of IT managers and leaders answered that they have a planned or ongoing cloud project (Computerworld 2017). Cloud computing is a big business where services are provided from large datacenters owned by IT-giants such as Microsoft or Amazon. The cloud enterprise has also a great financial value where seven biggest enterprise-cloud vendors had total revenue of over 76 billion dollars in 2017 (Evans 2018).

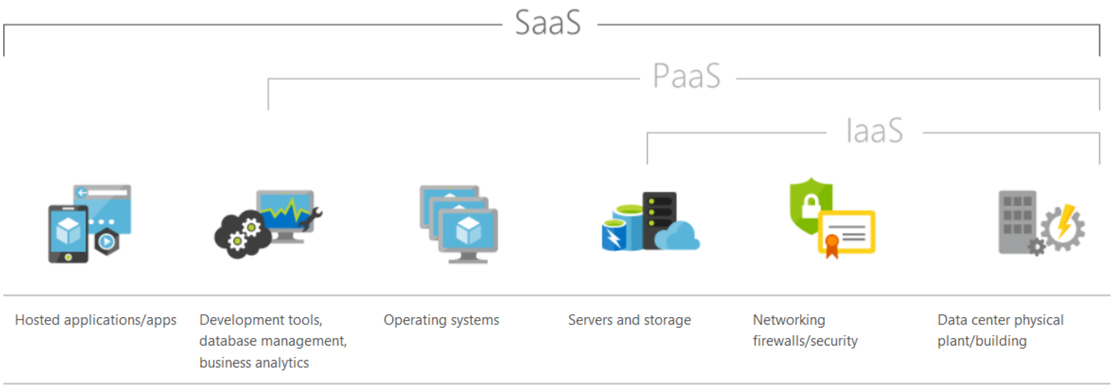

SaaS
PaaS
IaaS
Hosted applications/apps
Development tools, database management, business analytics
Operating systems
Servers and storage
Networking firewalls/security
Data center physical plant/building

Figure 6. Cloud services (Microsoft Azure 2018)

The term SAAS is often mentioned when modern services and technologies are discussed. SAAS means that the application software is provided from the service provider's datacenter via the internet and used as if it was installed on the end user's computer. Typical SaaS services are business related services such as email, document editing, human resources management as well as enterprise resource planning, all typically used via web browser. Whereas the traditional way to provide software and applications is to provide them from organization’s own datacenter servers, the SAAS model makes them available everywhere. The nature of cloud computing makes the services more flexible than the traditional versions enabling easy scalability for the needed resources at the needed time. Cloud services such as SaaS can often also be used with many types of devices and platforms. If the SaaS service and its provider takes care of security and updates it, this can as well reduce the needed resources from the user organization. (Violino 2017).

For the budget, scalability of the used IT is important as well in the healthcare sector. A recent IT budget report from the world’s leading research and advisory company Gartner shows that in almost 75% of the healthcare companies IT budgets are spent on the upkeep and maintenance of the internal systems (Gartner 2017). Sometimes the total costs of the software ownership can be difficult to estimate or even calculate, and this is where the cloud computing and its so called pay-as-you-go pricing based on the usage can be helpful for calculating the budget.

Yet, cloud services include also risks and challenges that the user organization should be aware. Richard Mosher writes in his article Cloud computing risks (ISSA Journal 2011), that even if cloud computing is used, all relevant security provider operations and the controls for them should be determined and complied with the provider in the same manner as if they were internally operated (Mosher 2011).

Sandy Shrum and Paul Murray from the US-CERT (United States Computer Emergency Readiness Team) lists common risks for cloud computing in their paper Common Risks of Using Business Apps in the Cloud. The list begins with losing the control over the vital computing resources for the business to the provider and its pricing. The lack of standardization is as well a problem among cloud providers where services used from one cloud does not mean that they will work on another cloud. If the services are not properly designed, the dependency on the chosen provider can be increased and changing between suppliers is made difficult. (Shrum & Murray 2012).

3.2.6 Encrypt vs. decrypt

Many modern web services are provided over encrypted HTTPS protocol today. Whereas HTTP traffic is unencrypted plaintext and vulnerable to interception, impersonation and manipulation, HTTPS aims to overcome these vulnerabilities by creating an end-to-end protection between the user and the service. With HTTPS, almost all information between the user and the service is encrypted making reading or changing the information difficult when transferred. (U.S CIO 2018).

A recent study from Scott Helme, a Security Researcher shows that the use of encrypted HTTPS traffic had grown to over 38% total with the most-visited sites. What is more, the number had grown over 30% from the study conducted six months earlier and the trend seems to continue in the future. (Helme 2018).

The numbers can be even higher regarding the point of view. According to Mozilla, nearly 70 % of all web pages loaded by Mozilla Firefox used encrypted HTTPS protocol in the beginning of 2018 (Let's Encrypt 2018). Google's corresponding statistics show that the use of HTTPS varies depending on the selected country from 59 % in Japan to 80 % in the United States of all web pages loaded with Google Chrome web browser with HTTPS in March 2018 (Google 2018).

At the same time as the use of encryption increases, the secureness of the web traffic making eavesdropping difficult, for example, it introduces a new problem for protecting the digital environment by decreasing the visibility into network traffic. When HTTPS is used, and the web traffic is encrypted, security tools such as firewall products are not able to see inside the encrypted network traffic. If these products fail to inspect the traffic, whether it is malicious or not, the security features are also bypassed. (Martin 2015).

In order to meet the challenge of decreased security level and to gain visibility to the encrypted HTTPS traffic, a technical procedure called HTTPS interception (also known as SSL inspection) is introduced. The main idea for HTTPS interception method is to place a man-in-the-middle proxy between the client and the server to intercept and decrypt the traffic for the inspection procedure. For a complete interception, the proxy machine should then rebuild the encrypted connection again. In an ideal scenario, the traffic is encrypted all the way between the client and server except in the interception machine or software as seen in the Figure 7.

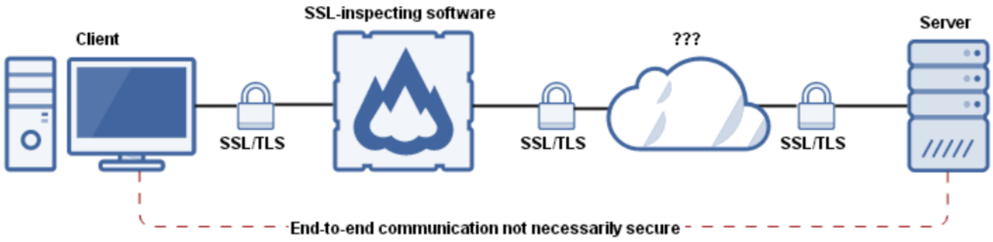


Figure 7. HTTPS interception (Cimpanu 2017)

However, as illustrated in Figure 7, if not configured properly, the interception process can be the weakest link and weaken the overall security allowing the traffic to be intercepted also by a malicious user, for example. A study published in 2017, The Security Impact of HTTPS Interception, shows that popular devices and software used to intercept the encrypted HTTPS traffic in fact “*have a dramatically negative impact on connection security* “. According to the study, in many cases the negative security impact occurs due to neglected security configurations, use of unsecure default settings and variance in how and where the HTTPS interception should or should not be done. In addition, the study suggests the security community to reassess the need of HTTPS interception and to find alternative ways for the issue. (Durumeric et al. 2017).

The United States Computer Emergency Readiness Team (US-CERT) have as well warned organizations using HTTPS interception products after the paper published by Durumeric et al. to take care that the used product is properly verifying the certificate chains and to ensure that the client receives warning and error messages regarding to it. Yet, the US-CERT suggests that if an organization is going to use the HTTPS interception, both benefits and reasons against the procedure should be considered. (US-CERT 2017).

Marnix Dekker, the former cyber security expert of the European Commission’s IT Security Strategy and Policy, discusses the pros and cons of the HTTPS interception in his article The HTTPS interception dilemma: Pros and cons. Dekker’s pros include the increased ability to detect malware, exfiltration and malicious command and control traffic as well as a possibility for an easy implementation to existing internet proxies. The interception process could also be potentially about bypassing some of the weaknesses and problems with the use of HTTPS. However, according to Dekker there are much more cons than pros with this method from whitewashing the original certificates and disrupting the personal use to endanger the users and their browser to accept untrusted connections. Dekker notes that the benefits from HTTPS interception are short-term and diminishing and suggest that at a time of cloud services and mobility, instead of investing network monitoring and detections the organizations should consider putting their security resources to the endpoint protection (Dekker 2017).

3.2.7 Logs

When digital services and systems are used, logs are generated based on the events occurring on the devices and applications. From the security point of view, the logs are essential as they can tell who, what, when, where and why an event took place on the recording system. With this information, monitoring the environment or a part of it and its normal and abnormal operation can be enabled. (SANS 2001)

When referring to logs, there are usually more than just one single file located on a machine. Actually, there can be many types of different logs from event logs to error logs and change logs to audit logs all for a special purpose and use. (Ficora 2016).

Unfortunately, not all logs are in the same format or equally informative. Even if the logs are in common ASCII format, a log output of one system can vary considerably compared to another system’s log output, making them hard to read and understand. (SANS 2001)

As the amount of digital and network attached machines is rapidly increasing, the number of logs created is increasing as well. More is not always better, and logging everything can eventually lead to a situation where finding valuable information is not effective. Therefore, The National Cyber Security Centre of Finland (NCSC-FI) suggests creating a log policy to determine what is logged, how and why. Because legislation sets requirements for the logs and their contents, use, storing and integrity, the log policy helps the organization to ensure these requirements are taken into account as well. (Ficora 2016).

As the NCSC-FI notes, every organization’s IT environment is unique setting challenges, not only for the log gathering but for the analyzation and turning the massive amount of data into a more informative form. For these purposes, log gathering tools and especially their centralized versions with multiple data sources have been gaining popularity among cyber security personnel to help creating the cyber situation awareness and status of communication networks and services. Yet, because of the unique nature of every IT environment and despite the marketing promises of commercial products, the log gathering and analyzation systems such as Security information and event management systems (SIEM) require a notable effort and knowledge about the current cyber ecosystem to define the normal and abnormal behavior before benefits and secureness can be reached. (Ficora 2016).

3.3 Cyber security in hospital district of South Ostrobothia

In the heart of digitalized healthcare operation is one program: patient information system. Patient information systems handle the data needed before and during the patient’s treatment process from appointments to the administrative data processing. Diagnoses, treatments, reports, statistics and billing are just brief examples of the data that is stored, processed and transferred via these systems.

Today, there are multiple different patient information systems, -and several versions of the same software are used in healthcare sector in Finland (Jormanainen 2015). This would not be a problem if these systems and versions could communicate and transfer data with each other. Unfortunately, this is not the case.

Especially, if the systems are located in different sectors, such as specialist medical care, primary healthcare or private sector, the information does not move between them (Jormanainen 2015). What is more, this has led to a situation where information is stored and processed individually in each system, at the same time increasing the dispersion of data, where the same data can locate in many different systems but none of these has the whole of it.

The area of the Hospital District of South Ostrobothnia is no exception, where until the beginning of 2018 one single municipality used a different and unconsolidated version of the same patient information system to take care of the same matters as the rest of the surrounding Hospital District. Luckily, the situation has been improved, and now the Hospital District can provide the same centralized patient information system for the whole area.

The advantages of this kind of operation are significant. If instead of several different systems a single patient information system is used, the need to transfer and process the data between different systems is decreased; however, also the needed time to start the actual healthcare is lowered, which can even improve the treatment process and patient safety (Tieto 2013).

In terms related to the cyber security, one patient information system can offer better confidentiality, integrity and availability compared to many diverse systems. With a single system, the same level of control and secureness of the data can be offered to all users in the area, which can increase confidentiality as the integrity of the data increases when the dispersion is decreased by storing and processing the data in one system, and the same coherent data can be made available for all users. In addition, the availability can be improved when the same patient information system with high service level agreements and robust technical implementation with good security can be provided for all users in the area.

By moving into one integrated patient information system, also the maintenance can be simplified when there is need for only one test platform to be used and maintained as well as the system in the operation to be updated, secured and monitored. In addition, multiple systems can include more cyber security weaknesses compared to one system.

A notable factor in the patient information system that the Hospital District of South Ostrobothnia provides for its users as a service is the way it is provided in: the same patient information system that was used in district's central hospital for years is provided for the rest of the district as a virtualized remote application.

Compared to traditional Windows applications, virtualized remote applications work as they were installed to the computer as the traditional applications. Instead of installing the application to every single computer that need to access the application and resources it offers, the remote application is only started from the end user computer such as a traditional local installed app. Even though the remote application can look and feel like the traditional Windows application such as document editing software, the virtualized remote application is actually running on a remote machine located in an on premise datacenter or at service provider datacenter. From the user's perspective, remote application does not differ from the locally installed application; however, from the technical perspective the difference is great, and many advantages can be achieved. (Madden 2016).

By offering the virtualized application, the need for resources on both the end users' computer and the transportation layer between the Hospital District's data center and the end user has been lowered. Resilience for response times as well as secureness are also improved when the actual virtualized program is running on the same physical location as the patient information system, and only the remote view and control data are moved between the user's device and the remote machine. By providing virtualized remote application the scalability can be as well improved when resources needed can be optimized in datacenters. The service implementation of this virtualized and centralized patient information system was also noted by the system developers, and earned the Hospital District of South Ostrobothnia an annual prize from the Tieto Oy, the developer of the current system. (Tieto 2013).

3.4 Legislation

In Finland, the public healthcare is highly controlled with legislation. This can be seen starting from the national constitution. Finland’s constitution chapter 2 basic rights and its article 19§ define that the right of healthcare must be guaranteed for everyone (Finlex 1999). Even though the constitution may seem slightly far away when talking about today’s digitalized world and cyber threats, the whole healthcare sector nowadays runs on a digitalized environment, and in order to guarantee the healthcare for everyone, also the function of digitalized environment must be guaranteed. How is that kind of environment secured? With cyber security.

The strict requirements for the public health care system can be seen as one key element of Finland’s high-level public health care sector and its services and functions. As the country provides a great deal of good health care for every citizen, it also has plenty of legislation defining how the health and social services must be organized. The fulfillment of these laws and sets is strictly monitored by regional administrators, and coordinated as well as instructed by National Supervisory Authority for Welfare and Health, both subordinated to the national Ministry of Social Affairs and Health (STM 2017)

Regarding to the health care legislation and cyber security two terms needs to be clarified: Data protection and Information Security. Both are very important and valuable particular to the healthcare. They are important as well for the patients and employees as for the service provider itself.

Before the digitalization invaded every room in the hospital, the two were used with the information on paper for transmission, processing and storage as the digital information is used today. Nowadays, just the amount of the information handled in the in digital format has expanded rapidly and could not even fit in the archives in printed format.

Of course, not every bit needs to be secured. To create a good securing process, data that really needs protection needs to be focused on. Therefore, it is essential to know what the files and the data under a specific legislation are.

Just as the data has value and hierarchy, the same applies to legislation. The norm hierarchy of legislation defines that the Finnish data protection and information security are based first on the international convention of human rights; secondly, on regulation and directives of the European community; thirdly, on the Finnish constitution and then on other laws and regulations (Ylipartanen 2004, 35).

Still, also the legislation changes and for a reason. If a law set before the internet fit in a pocket, it probably did not take into account what would happen if one’s advanced reality social media app started leaking one’s personal information, for example. One major change in legislation regarding to cyber security, data protection and information security is the EU’s new General Data Protection Regulation GDPR.

The GDPR replaces the former Directive 95/46/EY on the protection of individuals regarding the processing of personal data and on the free movement of such data from 1995. The new regulation applies to the whole EU and its member states from 25 May 2018. Yet, some leeway is granted for the national legislator to define and complement the regulation at national level (Finnish Government 2017).

The new regulation aims to make stronger rules on data protection in the whole EU by giving the citizens more control over their personal data and to balance the business playing field. The GDPR widens the concept of personal data to any information that can be used to identify a person including pieces of data that together can lead to identification. If personal data is anonymized, the anonymization must be irreversible to not to be considered as personal data. In addition, if personal data is processed manually or automated, the GDPR regulation applies to all technologies from paper to video surveillance. (European Commission 2018).

If one thing has aroused a great attention in GDPR, it is the possible sanctions. Breaking the regulation can lead to penalties up to 20 000 000 euros or 4 percent annual global turnover, whichever is higher (itGovernance 2018).

The GDPR itself is a large regulation that has consumed a great amount of resources from the organizations trying to prepare for it (Latvanen 2018). At the same time, it has opened markets for consultants to sell services and equipment to take actions that would help organizations to meet the new requirements and to avoid the possible sanctions. The situation has been noted as well by Reijo Aarnio, the Finnish data protection ombudsman, who has criticized consulting firms frightening customers with the possible sanctions. (Helsingin Sanomat 2018).

The GDPR is in force now and plenty of resources have been used to meet the EUs new regulation by companies and nations, only the time will show what its real consequences are. The first public sanctions from breaking the GDPR will have a great influence to show how organizations interpret the new regulation in practice.

Besides the GDPR, the EU's new Directive on security of network and information systems (NIS Directive) came into force on 9 May 2018. The NIS directive adopted on 6 July 2016 by the European Parliament aims to improve the common cyber security on networks and information systems on the EU countries. NIS directive creates a must for EU countries to have national cyber capabilities to ensure their cooperation among cyber security authorities for operational and information sharing levels. In addition, the directive sets security and notification requirements especially for the critical infrastructure and critical information infrastructure sectors in the EU member states. (Eur-lex 2016).

Managing risks that are related to personnel is called personnel security. Personnel security is a vital part of an organization’s cyber and information safety and it can be improved and maintained with systematic education, proper management, risk analyzation, defining responsibilities and creating safety culture, for example (Finnish Ministry of Finance 2008). Legislation concerning personnel security have been included in several different laws and injunctions (Finnish Ministry of Finance 2009).

3.5 Cyber threats

The healthcare sector is an attractive target for cyber criminals worldwide. There are several reasons for this, including important and high-value data, a wide level of different systems and devices creating a large attack surface and utilize capability but also its critical nature that can be used against the organization, patient or the whole society. In short, the healthcare sector can be seen as a target that offers more with less effort.

The situation of healthcare regarding cyber threats has been noted in the statistics and reports for the past few years, and the numbers are not good. In 2015, the healthcare industry was ranked first in attacks by IBM X-Force Research in their annual Cyber Security Intelligence Index leaving behind sectors such as manufacturing, financial services and government. If an average client organization utilizing IBM security services faced nearly 53 million events in 2015, the average healthcare organization experienced 36 percent more with 73 million security events during the same time period. According to the report, the leading cause of security incidents for all industries was 45 % as well as for healthcare 42 % was unauthorized access. (IBM 2016).

A study Medical Device Security: An Industry Under Attack and Unprepared to Defend produced by Ponemon Institute finds that both users and device makers believe that the used medical devices do not provide protection for the clinicians and patients. According to the study, 67 percent of device makers and 56 percent of healthcare delivery organizations believed their equipment will be attacked over the next year; however, only 17 percent of device makers and 15 percent of healthcare delivery organizations are going to improve their ability to prevent cyber attacks. The study reveals many fundamental problems with medical devices starting from the lack of testing and responsibilities to the difficulty of securing the medical devices and lack of interest to invest in cyber security. Why so? Over half of the respondents said the rush to release is a reason for low-level cyber security and vulnerabilities. What is more, the organizations seem to increase the cyber security budget only after a serious hacking incident. (Ponemon 2017).

Ransomware is one type of attack that has been in the headlines with healthcare sector recently. There have been cases where specific hospitals or healthcare organizations have been infected with ransomware that encrypts the valuable data or even entire computers and devices and then tries to get money from the users by blackmailing cryptocurrency such as bitcoins to get a decryption key to restore the files.

In a situation where the whole operation of a hospital is down because of an attack such as the one described above, paying the ransom can be a tempting way to solve the problem. This was the case in 2016 when Hollywood Prebyterian Medical Center, a hospital located in California in the United States paid a ransom worth of 17 000 dollars in bitcoins in order to get the systems back up and running and to continue its original operation. Allan Stefanek, the Hospital’s CEO even said that it was the quickest and most efficient way to restore their systems and administrative functions. (Ragan 2016).

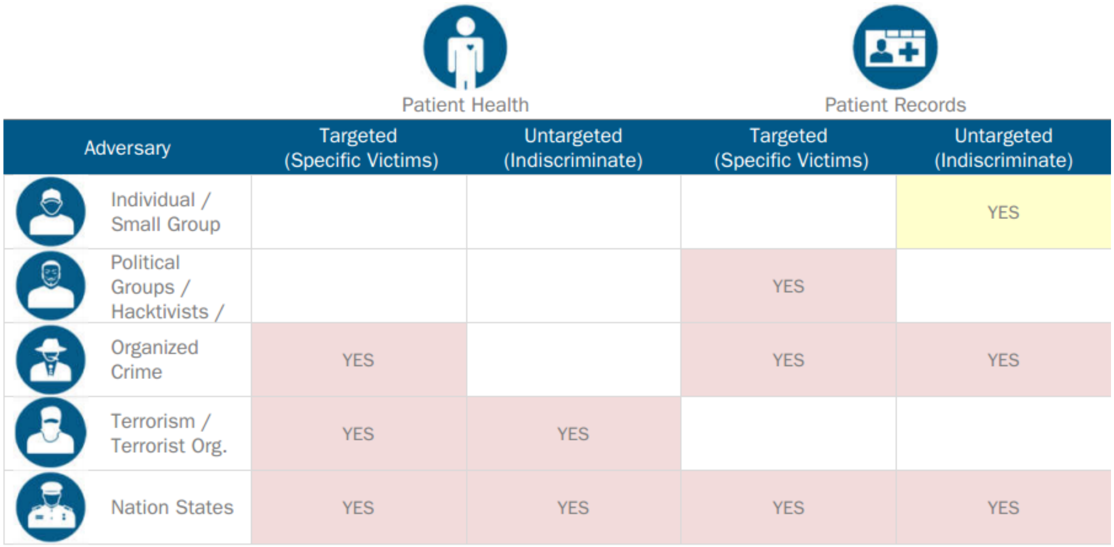
Still, in a case of ransomware authorities and cyber security experts instruct the users and organizations not to pay the ransom because this is what the cybercriminals want and what keeps them to continue this profitable but illegal business. In addition, when acting with criminals there is no guarantee that after the payment the victim will get the encrypted files back. Keeping regular backups of important files in a safe place is the best way to secure the digital information from cyber threats such as ransomware. (Ficora 2016).

A cyberattack with a complete different scale was experienced in May 2017, when so-called WannaCrypt (also known as Wannacry or Wcry) ransomware software quickly spread globally infecting hundreds of thousands of computers and devices all over the world. The WannaCrypt and its several variants used the exploits stolen or leaked from the NSA the National Security Agency of the United States (Smith 2017).

Such a powerful cyber weapon turned out to be also dramatically powerful in the hands of its new users and according to a report from the National Audit Office (NAO) of the United Kingdom, it had serious impact on the health services especially in the UK disrupting at least 34 percent of trusts in England. The report investigated the National Health Service's (NHS) (a health care system standing more than 64 million people in the UK (NHS 2016)) response to the Wannacry attack, and the report was published April 2018. The report states that although the NHS was warned several times about cyber attacks and asked to take steps to improve their preparedness for being attacked and despite the fact that the NHS had been infected by ransomware before leading cancellation of thousands of appointments, the NHS had not taken proper actions to meet the recommendations. (NAO 2018).

If healthcare organizations are interesting targets to attack who are the attackers and what do they want? A security firm, Independent Security Evaluators have summarized the common profiles of attackers and their targets in a table below (Table 1) from their report Securing Hospitals from 2016. A notable finding in the research was that the health organizations mostly focused on cyber security perspective and on protecting the patient health records letting securing of the patient health aside (ISE 2016, 3).

Table 1. Healthcare sector adversaries and targets (ISE 2016, 3)



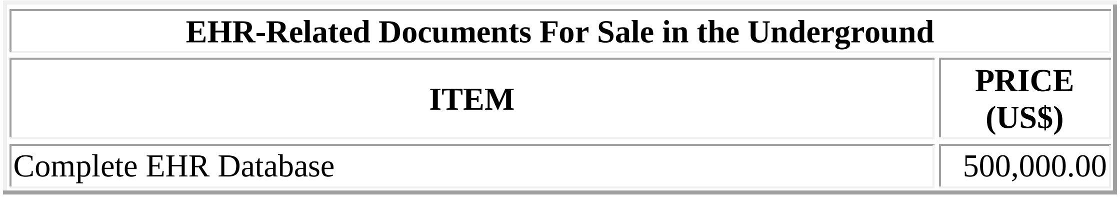
	Patient Health		Patient Records	
Adversary	Targeted (Specific Victims)	Untargeted (Indiscriminate)	Targeted (Specific Victims)	Untargeted (Indiscriminate)
Individual / Small Group				YES
Political Groups / Hacktivists /			YES	
Organized Crime	YES		YES	YES
Terrorism / Terrorist Org.	YES	YES		
Nation States	YES	YES	YES	YES

Table 1 introduces five different adversaries from individual to nation level actors describing what the main goal their malicious activities could try to achieve. Are they interested of e.g. the patients or their records?

As seen in Table 1, small and non-organized groups are more likely targeting the patient records than the patient’s health directly. The reasons for this can be found in the high value of patient health records in black markets. Compared to other valuables sold in black markets such as social security numbers or credit card numbers worth less than a dollar per each, patient health records including detailed and even unchangeable information of person’s personal data, history, relatives plus the two social security numbers and credit cards numbers can vary from a dollar to thousand US dollars per each (Yao 2017).

A cyber security firm TrendMicro has gathered some of the prices of electronic health record related documents sold in the underground markets in the following table (Table 2).

Table 2. Electronic health record related documents sold in underground markets (Trendmicro 2017)



EHR-Related Documents For Sale in the Underground	
ITEM	PRICE (US$)
Complete EHR Database	500,000.00

Medical Insurance ID	1.00
Personal profile (with medical and insurance data)	0.99
Comprehensive personal profile (with PII, Social Security number, appointment schedule, date of birth, insurance ID number, etc.)	5.00
Driver’s license	170.00
Farmed Identity	1,000.000

When the attacker is interested in getting money by selling these kinds of documents, they choose a target easy to breach by making their targets untargeted, in other words, they are interested in money and not the targets. Instead of making money with stolen medical records, terrorists and nation state actors can be interested in affecting the patient’s health directly. Whereas terrorists would want to affect public health or safety, the nation state actor can be interested in all information and possibilities that they could benefit from and that could give their leaders time to make decisions. In this kind of case, the target can be chosen depending on the attacker motivation making the target type targeted. (ISE 2016, 16–24).

An example of well-planned cyber-attack in health care sector was seen In July 2018, when hackers stole the health records of approximately 1.5 million citizens from Singapore’s Ministry of Health. The main target in this operation is believed to be the Prime Minister’s personal health information. (Cimpanu 2018).

If the prices for stolen records are high so are the costs of the cyber security breaches for the victims. The costs of data breach are estimated to be the highest in the healthcare sector among industries, as revealed in a study made by Ponemon institute in partnership with IBM. If the average global cost of a stolen record was 141 USD, the average cost for a record stolen from healthcare industry was over twice as much being 380 USD. (Ponemon 2017).

Even though the healthcare sector poses an interesting target for different adversaries from criminals to terrorists and state funded actors, not all cyber threats originate from actors trying to break into systems and/or steal valuable data or cause trouble. The threats to cyber security have a much wider scale, which should not be forgotten when focusing exclusively on preventing different types of attacks and attackers who often get the public attention and are seen in the headlines. An everyday cyber threat can be the users and used policies themselves as well. These factors are discussed in more detail in the following chapter.

3.6 Cyber Security human factor

When talking about cyber security, one still often tends to think of it as a technical challenge. Yet, humans are the creators of the digital environment and the only ones responsible for it. Humans are also the only users of these digital systems who make mistakes, errors, faulty design, and users also are in charge of coding as well as poor management. In addition, if focusing on cyber-attacks, there is always a human (one or more) behind them.

Thus, the human factor is inseparable in cyber security and can be seen as one of the three security measures linked with information states and critical information characteristics. An illustrative way to visualize these factors and the interconnections between them is the three-dimensional McCumber cube. The McCumber cube, created by John McCumber in the beginning of 1990s is a security model that defines the relationship between different security disciplines. The main idea of the McCumber model is that in order to develop proper information assurance systems, all dimensions and attributes with their interconnectedness must be considered. As seen in the McCumber cube (Figure 8), this also applies to the human factors: education, training and awareness. (McCumber 2005, 99 - 110).

Altough McCumber cube is over a quarter of a century old, it is still a good and versatile tool to use in various situations from analyzing to developing and designing secure information systems. It can be used from gaining high-level information located on the sides to a very detailed level located on every single piece of the cube. What is more, when using the model as a result, there should be a system where all security disciplines are taken into account.

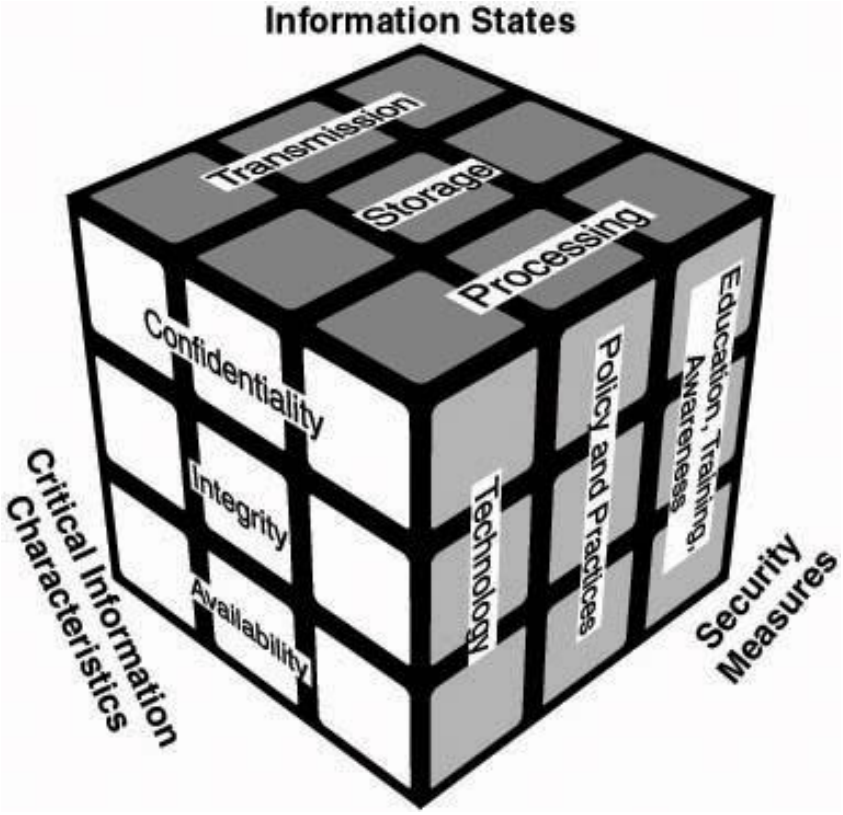
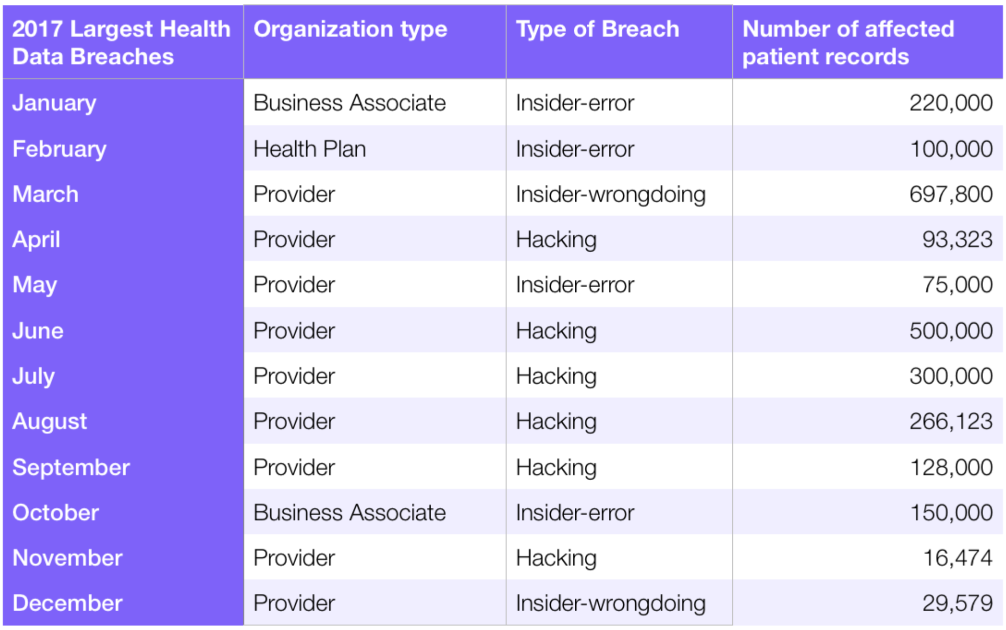


Figure 8. The McCumber Cube (McCumber 2005, 99)

The human factor and its significance in cyber security incidents can be seen in the statistics as well. A cyber security intelligence index report conducted by IBM Security Services in 2014 showed that more than 95 percent of all security incidents investigated were due to a human error, including misconfiguration, easy-to-guess passwords or even default user names and passwords. In addition, poor patch management, lost devices and sending sensitive information to incorrect email address were mentioned. Moreover, or should it be said, unfortunately, the most common human error in the study was a user clicking on an infected attachment or URL. (IBM 2014).

An annual breach barometer report 2017 from Protenus examining data breaches in healthcare sector in the US states that many of the cases are due to an insider actor and can be continued undetected for several years. The insider threat, whether malicious or not, can be as harmful as the outsider threat as seen in the figure from the report showing health care data breaches by type (Figure 9). (Portenus 2018).



2017 Largest Health Data Breaches	Organization type	Type of Breach	Number of affected patient records
January	Business Associate	Insider-error	220,000
February	Health Plan	Insider-error	100,000
March	Provider	Insider-wrongdoing	697,800
April	Provider	Hacking	93,323
May	Provider	Insider-error	75,000
June	Provider	Hacking	500,000
July	Provider	Hacking	300,000
August	Provider	Hacking	266,123
September	Provider	Hacking	128,000
October	Business Associate	Insider-error	150,000
November	Provider	Hacking	16,474
December	Provider	Insider-wrongdoing	29,579

Figure 9. Figure showing the scale of data breaches by type. (Protenus 2018, 4)

Although a malicious insider can be hard to detect due his or her legitimate access to the systems and might continue his or her operation for long periods undetected, according to the Protenus report, the human error or wrongdoing is more common in health data breaches (Protenus 2018). This kind of case occurred in Finland in 2016 when an unknown external hard drive was found connected in Kanta-Häme Hospital District’s network. The device was then located and found to be a private device belonging to a hospital employee. Even though the employee was not working directly with patients and might not have wanted to cause harm, he or she should have known the risks and was fired, said Iisakki Kiemunki, the Hospital District’s head of communications (Leinonen 2016).

As these kind of statistics and real-life cases show, the cyber security level could be increased by decreasing the human errors. A survey of hundreds of IT experts from various countries and organizations revealed that only 35 percent of organizations had a dedicated department or person that is responsible for cyber security. Answers stated as well that lack of budget and time as well as insufficient staff training were the three most common reasons for organizations' problems with cyber security. (Brooks 2017).

3.6.1 Legal cyber security business

Cyber security is a trendy subject with plenty of money involved in it as well, and now the discussion is not about data breaches, hackers or state funded espionage groups stealing digital information, selling it or blackmailing owners, for example. This time the discussion is about joint-stock companies doing their completely legal business, and the business is good.

A report from Cybersecurity Ventures lists 500 companies with definition "world's hottest and most innovative companies in the cybersecurity industry". The report for second quarter in 2017 includes companies from small firms to big corporations that are all working on industry the spending of which is predicted to exceed one trillion dollars in the next five years. (Morgan 2017).

With a market that is as big as the legal cyber security industry is now and will be in the future, the firms, whether small or large, are benefitting from selling products and services to users and companies to protect against cyber security threats. The media, keeping the cyber security and especially the threats in the headlines can be boosting this business as well. When a person or a company takes actions to improve their cyber security level it should be planned and for a purpose, not because of frightening news or a marketing person from a cyber security firm selling products that are said to make you secure.

3.6.2 Authentication

An authentication ensures that the access will be granted only for users with the access right to the resource. If the user does not have the access right to the resource he or she has asked for, the authentication should reject the permission. (Järvinen & Rousku 2017, 57).

There are many ways to authenticate people; however, they all are based on three following approaches: Something you know, something you are and something you have (Schneider 2005).

“Something you know” such as passwords and usernames are vital elements in cybersecurity to authenticate users to get access to services and processes. For over a decade, the password recommendations have included the following: special characters, numbers, and capitals. In addition, a recommendation for changing the passwords regularly is familiar in many systems used today. Unfortunately, many of these recommendations still in practice have been proven to be unnecessary or unsecure and modern knowledge about a secure password has changed also the recommendations.

In a review of The Wall Street Journal, Bill Burr, the former manager of National Institute of Standards and Technology (NIST) who wrote many of these recommendations in 2003, now regrets much of what he did (The Wall Street Journal 2017). If Mr. Burr has changed his mind during the past fifteen years, it should be time to change the practice as well.

According to the NIST Special Publication 800-63B from 2017, the updated guidelines for secure passwords no longer contain a mixture of special characters, numbers or letters because the analysis of the breached password databases have shown that they are not effective to create a secure password as have been thought. In fact, there are signs that the old recommendations have been weakening the passwords. Humans that all have limited ability to memorize random and complex phrases are proven to create passwords that are easier to guess. Composition rules including special characters and numbers does not take the effect if they are used with very predictable ways such as transforming a password “Password” to “Password1!”. Complex passwords are also harder to remember which can lead into situation where they are written down or stored electronically insecurely. (NIST 2017).

To avoid the frustration with passwords that are complex and hard to remember, the new recommendations take into account both usability and security to find best practices for creating passwords with a more simple approach. The recommendations from the NIST now focus on length which is seen as a primary element for the password strength. Whereas the minimum password length should be dependent on the addressed threat model, NIST recommends encouraging the users to use as lengthy passwords as they are willing to. (NIST 2017).

Another modern password recommendation comes from Microsoft Identity Protection Team, which have been using data from their systems including over ten million authentication attacks per day. The paper Microsoft Password Guidance from 2016 shares the same frustration from the user perspective to create a new password that meets the composition rules. According to the paper, understanding the human nature is essential for the administrators to admit the fact that almost every implemented composition rule decreases the password quality. (Hicock 2016).

The Password guidance from Microsoft recommends eliminating character composition requirements, banning common passwords and maintaining the minimum password length with 8-characters. Educating users is seen as important also in the paper that insist to educate the users not to use same passwords for work and non-work purposes. (Hicock 2016).

Ficora has published similar recommendations for creating passwords. Short passwords and using the same passwords in different services are the biggest weaknesses in Finland among cyber security states Arttu Lehmuskallio, the head of Coordination Centre at National Cyber Security Centre Finland. In their consumer research from 2018, Ficora revealed that only one third are using a different password on every service. The authority strongly suggests and reminds that the most effective way to improve one’s personal cyber security is to use longer passwords. (Ficora 2018).

Even if using longer passwords can improve one’s cyber security, it is important to remember that there are still common attacks such as social engineering, keystroke logging and phishing that do not take into account how the password is formed. Even the best recommendations to create passwords do not help if the attacker has other ways to get the password.

To help against the weaknesses in the use of one password per service, many passwords or factors per service can be used instead. This kind of authentication is called depending on the factors from two-way authentication to multi-factor authentication. For example, Google has provided its users a two-step authentication for years in their email service Gmail where two authentication factors “something you know” (username and password) and “something you have” (cell phone) are used combined. In practice, when a user logs in with his / her username and password combination, the service provider such as Google then sends an SMS message containing a single use code to user’s phone which is asked by the email login screen. Only if both username and password combination and the SMS code are correct, the access is granted. (Google 2018).

It is even more secure to use a software based token application installed in the user’s phone. This is because there has been criticism about using SMS messages in authentication, and it has been proven to be vulnerable to attacks where the victim’s mobile provider has been tricked to swap the SIM card or change the victim’s phone number to name an example. Google has announced that they have had even better results with giving their employees physical USB security keys to be attached to the machines that user wants to log into and that no user has yet been successfully phished. (Krebs 2018).

In healthcare sector, the population register centre of Finland is offering a certificated personal chip cards that the healthcare workers can use in authentication process (Eevertti 2018). In this authentication process, a card reader and proper software are required. Still, when adding a physical element to the authentication process such as a chip card, the physical safety of these items should be taken care of.

If used properly, personal authentication methods can offer enough cyber security, however, unfortunately not all organizations have implemented and ensured that the best authentication practices are in use. This is the case especially within the critical infrastructure where according to assessments conducted by the United States Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) one of the biggest issues in cyber security was the use of shared and group accounts and that the problem is going to get even worse. (ICS-CERT 2017).

When shared accounts are used, the real user can be as well one of the group members as a malicious outsider making the actual identifying and monitoring process problematic. Shared accounts can offer anonymity for personnel where it should not and make the account management process more difficult. According to ICS-CERT, these kinds of accounts usually have easy-to-guess and poor passwords that are not changed as the members leave. (ICS-CERT 2017).

3.6.3 Cyber security awareness

Cyber security level can be improved in many ways, for example by updating machines, purchasing new security features and components, tightening policies and setting limitations. However, as seen in the McCumber cube in Figure 8, training, education and awareness are equally important security measures compared to technology, policy and practices. In other words, instead of concentrating on one security measure, all of them should be taken proper care of.

The best way to prepare against cyber threats is to take care of the basics. In their book Kyberturvallisuus, Limnéll et al. (2014, 107) remind that the only way to defend against both known and unknown cyber threats is by keeping the cyber security updated, improving the overall cyber security awareness and resilience with reactive practices.

The Federal Bureau of Investigation of the United States, also known as FBI, calls in their internet crime report 2017 for increased public awareness to learn to recognize the dangers online and then simply avoid them. For organizations and employees, the report states the awareness and training are critically important when defending against cyber threats such as ransomware. (FBI 2017).

Insufficiency and lack in staff training and getting dedicated information security staff are mentioned in many reports and papers worldwide when talking about the biggest problems regarding the organization's cybersecurity level and preparedness in combating against cyber threats (ISE 2016, 41-44, Trendmicro 2017, 8, Gartner 2018, Sheridan 2018, NAO 2018, 10, KPMG 2017, 8). In addition, many of these documents are subject directly to healthcare sector.

Still, even today, not all employees have attended cyber security lessons or training. In fact, organizations may have not even organized training for their employees to improve the overall cyber security awareness and create a cybersecurity culture. A study from a cyber security company ESET from 2017 reveals that one third of participants did not have cyber security training at their organization at all and 16 percent did not know if they had. What is more, according to the survey nearly half of the respondents would attend if offered, even if it were optional. (ESET 2017).

There are many ways to improve cyber security awareness. The National Cyber Security Centre of UK have listed 10 steps to Cyber Security listing user education and awareness as one that targets to keep the organization secure and working. With a security-conscious culture, the organization is actively offering tools and awareness to the employees to achieve this goal. These steps include clearly defined policies with limited jargon, for example using devices (personal and organization owned), informing users about legal and regulatory sanctions and their responsibilities, improved dialogue between users and a designated security team where incident reporting is encouraged and misunderstandings are clarified in a friendly manner to make sure that the users realize that they can be targets of cyber-attacks such as phishing and social engineering in order to gain an attacker the access to the organization’s systems. (NCSC 2016).

An improved dialogue between users and the security personnel is especially important for the cyber security. In an organization where the distance between the two is great, the adverse cyber events can be left unreported or the users may even hide their mistakes while feeling ashamed (Dunn 2018).

However, cyber security should be an enabler of the work, not a disabler. If security is seen to block one’s job, the ignorance of these controls can increase. Therefore, the right balance in security controls should be carefully prepared and monitored to ensure that the users have efficient working conditions and avoid frustration. There are signs that malicious activity can be increased among dissatisfied personnel. For the insider threat, sanctions and disciplinary actions of abusing any of the security policies in action should be made clear at practical level to all employees including contractors and third party users. (NCSC 2016).

Improving the overall awareness is not only one of the key security measures in cyber security. Yet, it has been stated to be the fastest, easiest and the most cost-effective way to improve the overall cyber security level in Finland (Lehto et al. 2017). This should be taken into account when seeking ways to improve the cyber security from personal to organization level and especially when planning the upcoming health, social services and regional government reform.

3.7 Cyber Opportunities

When discussing cybersecurity, one important fact is often forgotten, the opportunities it offers. Cybersecurity can be seen as a compulsory and unpleasant subject that sets restrictions and limits the usage of technology without even producing any direct profit.

People’s lives have changed faster than ever during the last few decades and almost all of it because of technologies without any slowing down in sight. Technologies have boosted work, made it easier and safer and at the same time, according to the World Bank (2016), nearly 1.1 billion people have been lifted out of extreme poverty since 1990. Technology has and will change lives irreversibly, whether people like it or not. Still, it is good to remember that the underlying reason for using a technology is to help people with their daily lives, and this is where cyber comes in to the picture.

Unlike the world inhabited by humans, the digitalized world, also known as cyber world has been made by humans, which sets a fundamental difference between the two. Whereas the real world and people in it can only operate under the laws of physics, the cyber world operates on somewhat unlimited level where the only limit is the imagination.

In the real world, one would not be able to transfer information to the opposite side of the globe under a blink of an eye; however, by using technology one carries in one's pocket today that is no problem. This can be done even without additional costs, at least in Finland where the usage of mobile data per capita is one of the highest in the world. (OECD 2017, 143.)

The digitalization has enabled incredible things and ways to carry out tasks also in the healthcare. Tasks such as X-ray images have been fully digitalized and can be taken, processed and stored via a computer; or, a patient's personal medical records can be opened from the doctor's laptop at the same moment when the patient steps in, or there is no need to pre-order the records from the physical archives or even from another hospital. Even the first transatlantic surgeries have been conducted since the beginning of 2000s, which even today sounds more like the future (Ircad 2001).

These tremendous achievements are just a prelude from the digitalized era, however, in order to get the full benefit from the digitalized environment, cyber security must be taken seriously. If security and reliability of the current and upcoming digital processes and services are not taken care of in the healthcare sector, the X-rays could fail; a patient could get an unsuitable or even lethal medicine prescription or even become the first victim of denial of service attack in a remote surgery operation.

Also in the upcoming national Health, social services and regional government reform, digitalization plays a big role. This can be seen only by taking a look at the financial targets where the Finnish government aims to save 3 billion Euro with the reform, which; however, has been estimated overly optimistic by the National Audit Office of Finland (2017).

In order to achieve these numbers, Annika Saarikko, the current Minister of Family Affairs and Social Services, responsible for the reform has estimated that a major part of the savings the reform could produce are achieved from the digitalization and that this has also been included in the government's plans. Saarikko has also noted that the digitalization plus other developing technologies and electronic services that can earn savings, need a strong national control. (Mäkelä 2017.)

The cyber security will not and should not stop or prevent this kind of great development; hence, cyber should be seen as the enabler of these things and not the opposite. If the cybersecurity is neglected, new technological innovations or resources spent on it may come across as worthless.

3.8 Future

The amount of information produced and flowing on the internet is dramatically increasing in every continent; if in 2016 the internet traffic was 10 GB per capita in Cisco's forecast, it will reach 30 GB per capita by 2021 (Cisco 2017). Today the amount of information is not the problem, actually, there is so much information available that the biggest problem is how it can be processed, or in automated way, how the systems are built to process it into usable form.

If the amount of information is increasing rapidly on the global level, today much more data is produced on a personal level. This does not only mean the web traffic including Netflix or Facebook but also information and history from a person's health status, exercises and time and quality of sleep, to name a few examples. This kind of data is valuable for the web companies of course; however, it is and will be used more and more also in the healthcare for maintaining people's health and getting the best and most effective treatment if a person's status decreases.

According a recent study from Terveystalo, the largest private healthcare service company in Finland (Terveystalo 2018), over one-third of all Finns are using electronic devices or applications such as wearable activity trackers to monitor their health status (Terveystalo 2018). Unfortunately, these devices and applications may not have good security controls and may risk both the user's data and health in the worst case (Kotz et al. 2016). At least this equipment and software should be designed with built-in privacy and security.

In a short run, remote healthcare has a great deal of potential in Finland, a country with long distances. Currently, there are nursing services available which can use hand held devices when nurses e.g. visit the elderly; however, in the future, the technology will replace more and more the need of personal visiting.

During the past decade, many countries over the world set their national cyber strategies and in 2011, the president of Finland and Finnish Cabinet Committee on Foreign and Security Policy decided to start to form the first Finnish cyber strategy. The strategy was published after two years in 2013 accompanied with an enforcement program published a year later. These were set and compiled in collaboration with authorities and business actors. The main goals for the strategy were to create a joint comprehension of cyber security and to strengthen the overall safety in the whole society. (Turvallisuuskomitea 2015).

The original strategy from 2013 had the following vision: "By 2016 Finland should be a global forerunner in cyber threat preparedness and in managing the incidents caused by these threats" (Turvallisuuskomitea 2015). Unfortunately, this goal was too optimistic, and allocating only one million Euro for this kind of task indicates that something was not understood or cybersecurity was not taken seriously. However, one of the most significant achievements for this strategy was forming the National Cyber Security Centre Finland (NSCS-FI) in 2014 (Ficora 2013).

In 2017 the Government's analysis, assessment and research activities published a report with title "Finland's cyber security: the present state, vision and the actions needed to achieve the vision". The report about the current state of Finland's cyber security no longer contained the goal of being the forerunner in cyber threat preparedness by 2016 and that Finland is actually behind all peer countries such as Estonia, Israel and Sweden in global cybersecurity index. The new goal was that by 2020 cybersecurity is built-in feature in society enabling its security and operation instead. According to the study, the healthcare sector in Finland is one of the top sectors facing cybersecurity threats now and in the future this should be noticed (Lehto et al. 2017, 50-69)

To implement the strategies and visions, the Security Committee of Finland has published an implementation program for Finland's cyber strategy for 2017 – 2020 where cybersecurity in healthcare is seen as one key sector for society's operation. Still, the upcoming reform entrusts the cybersecurity to ministries and regions for keeping the whole healthcare ecosystem safe including public and private organizations and service providers. (The Security Committee of Finland 2018, 4 - 15).

Since the beginning of the internet, its neutrality has been considered self-evident. This fundamental idea has created the base for the whole internet enabling the change for it in becoming a globally used network for communication and services that it is today. The neutrally treated internet offers major advantages for the whole society by supporting freedom of speech, innovations and consumer rights. In other words, the equal internet is open, independent and uncorrupted (Kassinen 2014).

The definition of the net neutrality or sometimes-called Internet Freedom varies; however, the main idea is that internet service providers (ISP) must treat all data transferred in their networks equally. In Finland and in the whole European Union, the net neutrality is regulated by the EU regulation 2015/2120 (EUR-Lex 2015), which ensures that the ISPs treat the internet traffic equally, and the consumer's right to the open internet is realized. In Finland, the actualization of the law is monitored by Ficora.

Yet, in the United States, the net neutrality has been questioned during the 21st century and during November 2017, President Donald Trump's administration set in motion its plan for the country's telecom agency Federal Communication Commission (FCC) to repeal the existing rules for the net neutrality (Romm 2017).

The net neutrality is not only important for the freedom of speech and equality but it can open completely different scenarios where rich can pay for the faster services whereas poor cannot. When this kind of scenario takes place with healthcare services, the issue is not only about surfing on the internet or watching movies via internet connection. There has been criticism about ending net neutrality and its consequences to future and future healthcare services and even granting special rights for critical healthcare data has been introduced (Pham 2017).

Besides net neutrality, many nations have set rules for data localization to ensure that the data is stored in the nation, not abroad. These plans are often explained by national safety that indeed is a valuable argument when remembering the issues regarding cyber security. However, some nations have taken further steps to ensure their own agenda resulting narrowing the neutrality of the internet in their countries. Countries may have national firewall blocking sites and traffic that are against the current administration or some have even stated to create an internet of their own. (Hallamaa 2018).

Instead of one, there can be actually many internets formed by national interests in the future. The former Google Chief executive officer Eric Schmidt has predicted the internet will bifurcate into two distinct internets in the next decade. In Schmidt's prediction, these internets might contain a strong influence and control from their leaders when one internet is led by China including tens of countries affected by the China's Belt and Road Initiative as the other internet would be led by the United States. (Kolodny 2018).

3.9 Similar studies

The Government Information Security Management Board of Finland (VAHTI) has conducted two information security barometers for personnel and management in 2016 and 2017. These barometers were targeted to public administration organizations and personnel in Finland focusing on the importance and challenges in taking cybersecurity into practice. (Rousku & Mellin 2018)

The first barometer included only few respondents from the healthcare sector; however, the second barometer had answers from 791 respondents working in three hospital districts. The key observations from both barometers included positive findings such as: Cyber security is seen as an important and necessary enabler to the work, the cybersecurity level in the organizations is seen high and the respondents feel safe when using digital systems. As a result, both barometers suggest that the personnel should be educated and trained regularly about cyber security and topical threats related. (Rousku & Mellin 2018).

In addition, the results showed that the level of knowledge is higher in government ministries, public agencies and institutes than in municipalities and hospital districts. Yet, the main the suggestion from these barometers was that the level of knowledge should be improved in all organizations. (Rousku & Mellin 2018).

Helja Kurunmäki (2013) conducted a survey of privacy protection and information security for a Finnish public healthcare organization in her thesis Privacy Protection and Information Security in the Health Care Sector, Case Organization published in 2013. The primary conclusion of her study was that the education regarding both privacy protection and information security should be increased for the personnel working in the case organization. Kurunmäki also suggested to increase the amount of personnel with good knowledge about these areas to help to improve the overall awareness in the case organization. (Kurunmäki 2013).

4 Gathering data via cyber security lectures and surveys

4.1 Cyber security lectures

Before the first survey an idea of giving cyber security lessons for the employees of the Hospital District of South Ostrobothnia were thought about. Because no lessons had been given previously by the employees of the Hospital District's IT department or third-party consultants, a proposal to the chief information officer was made about giving the employees free cyber security lessons besides their own personal job in the organization to improve the overall cyber security level and awareness as well as the image of the information technology department in the Hospital District.

The permission was granted with a note that an invitation of this kind lecture must be made by the department willing to have one. Therefore, a few brief info sessions about topical cyber security issues with duration of approximately ten minutes were given within IT department's semiannual briefings for nurse managers about the current topics concerning the department's operation and IT services. In the cyber security sections, a possibility to invite a lecturer to give a lecture about cyber security directly in the department was introduced and contact information was given.

After the info sessions, many invitations were received via email and phone and soon most of the workweeks in 2017 included two one-hour cyber security lessons in different departments of the hospital district. For a few weeks only one lesson per week and one time was included; there were two lessons in a row in different departments. Most of the lessons were given in the break rooms of the departments in Tuesday and Thursday evenings suitable for departments and to the personnel's work timetable. However, some of the departments had the only suitable hour early in the morning because e.g. of the reception and surgery times.

As mentioned, the lectures lasted approximately one hour and the discussion that had aroused about the topic. The material contained a brief introduction to information and cyber security in theory; however, the major part consisted of examples of cyber security in a simple and practical form. A simplified and down-to-earth presentation at a practical level was thought to be a profitable form to describe cyber security to persons who are not necessarily keen on technology but are using it in their work every day.

4.2 First survey

The first survey was conducted during the first half of 2017 with cyber security awareness lectures for the employees of Hospital District of South Ostrobothnia. The attendees consisted mostly of nursing staff and their supervisors at the Seinäjoki central hospital. In addition, lectures were held for supervisors training attendees, hospital supporters, mental health personnel and executive groups working in the Hospital District in Seinäjoki City area. After an approximately one-hour lesson the attendees were given the survey forms to be filled in and returned directly back to the lecturer (Appendix 1).

The questions of the first survey form consisted of grading the lecture, its importance and usefulness in work and off work as well as giving a grade for the lecturer and for the presentation material. This survey was to give data to show if these kinds of lectures are needed and wanted by the participants and to point out what the weakest links are in the lecture. What is more, these results could be used to prove the importance and effectiveness of the lectures.

4.3 Second survey

The second survey was a continuum for the first survey and was conducted during the second half of 2017 during the cyber security awareness lectures for the employees of the Hospital District of South Ostrobothnia. After a successful first survey with over hundred respondents, the results were analyzed. As seen in the average numeric results of the first survey in Appendix 2, the average grades were similar to each other varying only by 0.5 points from 4.4 to 4.9 on scale 1 to 5 with median value of all grades being excellent 5. Therefore, after the 153 answers were tabulated, continuing with the same survey form was thought not to produce any new information.

Because of the results, a change of approach seemed necessarily in order to gather deeper knowledge about the feelings and thoughts of the users about the subject. A new survey form was created with open questions and grading the personal and organizational level of information security. This survey form was then given to the participants after the lectures (Appendix 3).

4.4 Third survey conducted online

4.4.1 Preparation

The third survey had a more ambitious plan than the two previous surveys; to gather data of cyber security knowledge from employees and their supervisors of all organizations that are to join in the upcoming health, social services and regional government reform in South Ostrobothnia.

Gathering data via lectures for the focus group could have taken considerably long time from one person and conducting this kind of survey with paper was estimated not to be feasible, which is why an online survey was created to be sent to the participant organizations. A great opportunity to reach all organizations in the area with improved value and profile arose when the CIO (chief information officer) from the Hospital District of South Ostrobothnia was able to contribute to The Head of Change from Regional Council of South Ostrobothnia to forward the survey to the target organizations.

The first version of the survey was designed with Google Forms, a free online survey tool, which was then dismissed because of the difficultness of seeing where the data gathered via the survey would have ended and under what terms and conditions. This kind of survey was to produce a great amount of data that could contain nonpublic and sensitive information such as weaknesses about the organization’s operation.

Therefore, the survey was remade with Webropol that the Hospital District was using for surveys and for which it had an appropriate license. Webropol is a Scandinavian survey tool that does not transfer personal data outside the EU or ETA (Webropol 2018). Later when the problems with the Webropol survey occurred, it was notified that the company uses the services of a Finnish data center service provider Nebula to provide the surveys in Finland (Appendix 7).

The survey consisted of eight pages total. The first page was a welcoming page with a welcoming text, the current regional logo for the reform and personal contact information and reminder that the data gathered via the survey will be anonymized and no personalized information will be shown in the final data. The first page included a selection of organizations to be chosen by the respondent. An approximation duration for answering the survey was mentioned as well, based on the average duration of ten separate test users’ answers.

The second page consisted of demographic questions such as age, gender, qualification, and job description with a question if the respondent has participated in a cyber or information security training or not. If information management was selected as job description, the respondent was then redirected to page three containing open questions for information management professionals about how he or she would act in various situations concerning cyber security. If another job description was selected, the redirection was made to page four.

Page four included questions and answer options to be chosen for all respondents about everyday information security practices and use cases. The following page five consisted of questions and answers to characterize the respondent’s knowledge about cyber security using Likert scaling. After page five, the respondent was then to be asked if he or she is working as supervisor or not on page six. If the answer was yes, the respondent was redirected to page seven containing a Likert scale questionnaire how he or she felt about the cyber security knowledge level of his or her subordinates and his or her own knowledge level to instruct subordinates about cyber security in their work.

The final page eight included questions for all respondents to rate their own knowledge level about cyber security using Likert scaling with a question if they have read the information security policy of their current organization and how they would like to get information concerning cyber security. The last two questions were about how the respondents felt about their own confidential information is secured in the current working organization and how it could be secured in the future organization after the reform. Above the send-button at the bottom of the page, a blank text-box was shown to the respondents with a possibility to give feedback about the survey before submitting the answers.

As mentioned, before the survey was published, a test group of ten persons tested the survey to gather feedback. This feedback was essential to ensure the proper operation of the survey and was used to improve the survey's functions, instructions, questions and to find out the average duration the survey will take.

4.4.2 Publication and problems with Webropol

On 15 January 2018 when the proper operation of the survey was verified, an email with a welcoming text and short introduction to the questions including a link to the survey was sent to the Chief information officer of the Hospital District of South Ostrobothnia to be forwarded towards the target organizations. The welcoming text in the email included a notice about the importance of participating to help gathering data to be used to improve the digital security in the participating organizations.

However, shortly after the email was sent, problems in the survey's operation were noted and forwarding the email to the target organizations was delayed. During this time an enquiry about the problems was sent to the Webrobol support and only after a confirmation of the problems being fixed was received and proper operation of the survey was practically tested, a permission to forward the email was granted. The problems were an unwanted side effect of security update against Meltdown security vulnerability installed on the systems by the service provider Nebula (Appendix 7).

The second attempt to publish the survey was conducted almost one week after the first one on 22 Januaryv2018. Unfortunately, soon after the survey was published, the problems with Webropol started again and this time they were worse. A great amount of contacts were received from participating organizations about the survey's website to be unreachable, and the survey stopped working losing all answers. A reply with apologies was sent to these users and they were asked to try again later. In addition, an email to the Webropol support was sent again asking about the problems and for a possible timetable needed to fix them.

An answer from the Webropol support was received a day after. Before this information about the problems was searched from the Webropol's social media and webpages. The only place with information about the current situation concerning the problems was found from the Webropol page that could be reached only after a successful login. Unpleasantly, during the problems the login page was working extremely slow often failing the login process and making reaching the page very difficult.

The first information about the problems was seen after a successful login later that day informing that the problems from the security update for Meltdown vulnerability are continuing and the problems should be fixed by the next morning 23 January 2018. The email from the Webropol support contained this same information as well (Appendix 7).

Yet, the problems with Webropol continued through the whole time the survey was active. The information published on the Webropol website accessible only after login from the first days after the survey was published was captured for this study and has been included in Appendix 7. However, not all messages were captured and when searching for them from the news archive of Webropol, it was found out that for some reason all information concerning the major problems in the survey system and continuing for weeks in January 2018 was removed. Only one piece of news about problems in the survey system was found insisting that the survey system had problems due to the service provider’s updates; nevertheless, the problems lasted only one morning of tenth of January 2018 (Appendix 8).

Despite the problems and uncertainty about the current operational status of the Webropol system, many respondents finished the survey successfully. Still, due to the problems, the availability time for the survey was extended from two to three weeks and closed only after the amount of finished answers was dropped to one per day.

5 Results

5.1 Numerical information

Thirty-nine cyber security lectures were given in 2017 with over 900 participants. The first survey form (Appendix 1) was answered by 153 participants producing average results that can be seen in Appendix 2 and written feedback in Appendix 3. The second survey form Appendix 4 received answers from 195 participants, and the average grades for the cyber security levels are seen in Appendix 5 and written feedback in Appendix 6. The third survey form (Appendix 7) was answered by 881 respondents total, and the results to the questions are listed in Appendix 8. Besides the large number of answers, a great result was that respondents from all target organizations participated in the online survey.

The results were analyzed by using data-driven content analysis. Data-driven content analysis can be used to form interpretations from the content and to increase the value of the gathered information. (Kamk 2018). The results are discussed and analyzed in the following three chapters. In the first chapter, the key observations and recommendations are made. The results and analysis of the first two surveys are discussed in more depth in the second chapter, and the third survey’s results in more depth in the last chapter.

5.2 Key observations and recommendations

It is often said that the user is the weakest link in the cyber security. Yet, according to the results, the weakest link in cyber security awareness is actually the organization, not the user. When combining the analysis from the first two surveys and the online survey, the results show that most of the users are aware of cyber security, its importance and issues related to it. They have knowledge about the use of digital systems securely in theory and they are able to make observations and improvement suggestions from the used infrastructure as well as their own and others’ behavior regarding cyber security. The users know that their knowledge about the cyber security should be improved and they want it as well.

Still, the organization has not taken care of improving the cyber security awareness; neither do their employees have enough knowledge for their jobs. What is more, the management does not have enough knowledge to instruct their subordinates in cyber security. It can be questioned if the current level of cyber security awareness and education comply with laws and regulations for personnel security.

There is a contradiction between the feel of personal cyber security level and the answers concerning the actual cyber security awareness. According to the results, the respondent’s own cyber security level is felt to be high even as most of the respondents have not participated in any cyber security lecture or training. In addition, many of the respondents answered that they have not read their organization’s information security instructions, and most of the respondents are not sure where they could even find them, signaling lack of active cyber security culture in the organizations.

The reasons behind the low amount of people that have participated in cyber security training or lectures are found in the overall level of knowledge. The results signal that the organizations are not committed to improve their cyber security awareness. This is because the importance and meaning of the cyber security awareness to the overall cybersecurity level and to the organization’s operation have not been realized. Yet, the results do not include signs about keeping the employee's cyber security awareness level low intentionally.

Based on the results, the prediction for the future is that if the cyber security awareness stays on the current level and will not be improved the lack of the awareness will be causing problems in the target organization’s operation sooner or later. In critical infrastructure sector these kind of events can have devastating consequences affecting large amount of valuable information, people and services.

These scenarios include losing control of large amount valuable information or losing confidence to an organization operation or public sector. In the worst case scenario the patient safety is affected and the lack of cyber security awareness will be risking someone’s health indirectly or directly.

What is more, the importance of cyber security awareness is likely to be increased than decreases in the future. An organization or an individual with high cyber security awareness is likely to be more secure against the cyber threats of tomorrow as well.

The lower the level of cyber security awareness is the higher the risks are. Currently, the cyber security awareness is not on acceptable level and the risks are too high. Unfortunately, until the lack of cyber security training and education have proven to have serious consequences such as to be blamed on dangerous situations the resources are not likely to be spent on improving cyber security awareness.

As recommendations, the lacks in cyber security awareness should be taken seriously and the organizations should take immediate actions to improve the cyber security awareness and cyber security related personnel security. Improving the overall cyber security awareness requires that the heads of the organizations have understood the meaning and importance of cyber security awareness to the whole operation of the organizations and they are committed to improve it; i.e., the level of cyber security awareness is improved first among the heads of the organizations and the management level.

After the organization is committed to improve the cyber security awareness, the road map to educate the employees should be created. This road map should include a plan for continuous education and testing the skills and knowledge of all current and future employees in the organization. Participating in the education and testing should be mandatory with no exceptions. Employees from trainees to managers should provide a proof of a basic understanding about cyber security before any access to the organization's digital ecosystem is granted. Advanced education and training should be organized related to the employees' work and tasks. Participating in education and training should be documented and revisable.

Educating employees with lectures about cyber security is one considerable way to improve cyber security awareness in the organizations. The participants experienced the cyber security lectures given as important, educative and instructive as well as useful in work and off-work.

5.3 Results from the lectures and first two surveys

The direct feedback from the lectures was positive only; especially the lecturer's way of presentation and expression were mentioned. Yet, people may avoid giving negative feedback directly face-to-face giving an illusion about positive only experiences. However, the written feedback from the first two surveys supports the spoken feedback being positive. In addition, notes such as a clear and understandable way of presentation appeared in the written feedback.

The first survey form (Appendix 1) was answered by 153 participants producing an average results that can be seen in Appendix 2. The themes that arose from the written feedback were the subject being felt as important and the lecture being felt as important and educational. The importance of the subject was also graded with the highest average score along with the lecturer's expertise. Some of the feedback hinted that even the subject or parts of it were familiar to the participant, and the lecture was felt to be interesting and necessary. Discussion and reminding participants about the cyber security was written to be necessary and thought-provoking. The numeric results seem to support these thoughts as well.

When asked if the participant had learned something about the subject during the lecture, the answers produced the lowest average grade including four of all five nearly poor grades that decreased the average grade. This can signal few individuals with a good knowledge about the basics of the subject. However, the average instructiveness of the lecture was still graded nearly excellent. These results show that the participants did not feel the lecture was a waste of their working time and that there is an actual need as well as a benefit from educating users with this kind of lectures instead. (Appendix 2).

Both the participants' and organization's level of knowledge was rated good, in fact better than the feedback from the lectures could reveal. If participants had had a good knowledge about the subject, the basics should have been familiar to them and not rated as educative. Still, participating in a cyber security lecture for the first time can have an effect where the participant realizes that he or she in fact has knowledge about the subject but has not used it. A similar analysis can be made from the written feedback that bringing up the subject among the participants was seen as important.

According to the average grade, the participants' own information security knowledge was graded somewhat lower than the organization's level. Whether this is reality or not, the organization's higher lever can be due to the lecture and the information lecturer shared recently. However, rating the organization's cyber security level higher than one's own personal level signs that the actions towards digital security are valued and trusted by the participants.

Whereas the open question for the feedback about the lecture was the last question in the first survey, the open question "What did you think about the lecture?" was the first question in the second survey form. This was hoped to produce more and deeper thoughts about the lecture and the subject instead of plain numbers.

As a result, the answers for the first question about feedback were longer than in the first survey. Yet, some of the answers were replied to with just one or two words. When examining words that appear frequently in the answers to question one, words such as: Very, good, plenty, interesting, essential and clear stood out, for example. All in all, the feedback was positive, thankful and supported the results from the first survey.

Besides grateful and supportive feedback, one individual comment from a person working at management level caught attention "Those who needed the lecture most did not come and participate". As mentioned, these lectures were held as voluntary, invited and not as compulsory. Still, the head of the department may have asked for all employees available to take part in the lecture to ensure that as many as possible would participate; however, many departments remained non-visited. The comment; however, refers that there are employees whose cyber security awareness should be improved more than that of some others. This can mean that their level of awareness is known to be low or that their behavior is known to be against best practices discussed during the lecture or it could even be wrong.

The reasons behind not participating in cyber security lecture can be many. One can simply be overworked and feel that he or she does not have time to participate or that the subject is not seen by the person in question as important enough to participate, or his or her superior demands the participation from his or her subordinate. The employee can as well feel that he or she already has enough knowledge and there is no need to participate or that there is simply no reason at all.

Yet, as the comment suggests, these persons did not participate intentionally. In an organization where participating in cyber security lectures is not compulsory, it is possible that the employees can intentionally avoid participation in the lecture. This is because there is no actual need to participate if no regulation or a supervisor is expecting it.

The reasons behind this kind of behavior can be the same than described above. However, the person can have acknowledged his or her non-secure behavior and does not want to hear that it is not acceptable and could be sanctioned, and that his or her behavior should be changed. In this case, the change resistance or fear of facing the reality to understand the connection between the organization’s cyber security level and one’s own personal behavior can be too high, and therefore the participation is avoided.

A person who has increased risk behavior increases the risk to the whole organization and its operation. The non-participation can be used against the organization as well, for example in a situation where an individual has been a part of an adverse cyber event and then uses his or her lack of education or instructions as an excuse. Hence, it is the organization’s responsibility to take care that all employees know the rules, instructions and consequences for their behavior.

The amount of answers was smaller when asked what kind of security risks one confronts in one’s work regarding cyber security. Because these answers contained information that could be used against the organizations, the answers are discussed on a general level. These answers included receiving spam emails and leaving computers unlocked. Some of the users were concerned about physical issues such as unlocked doors, USB drives and too easy physical access to the organization’s digital equipment. When finding commonality among the answers, they were often related to a user’s irresponsibility. Even indifference was mentioned as a faced security risk at workplace; however, the majority of the answers pointed more to things been done unintended rather than intentionally.

The last question in the survey two was “How you would improve cyber security in the Hospital District of South Ostrobothnia”. Many improvement proposals received included topics discussed during the lecture such as using privacy filters that can be installed on the screens restricting the viewing angle, so only the user located directly behind the screen can see the screen’s content. Physical safety issues and improvement to the physical environment were proposed. Other proposals mentioned varied from proper use of confidential papers to secure use of digital credentials and identity cards. Yet, the most common improvement proposals were related to training and educating and that users should be educated with similar lectures. (Appendix 2).

The notes and proposals from the survey one and two show that users have made observations about their physical and digital environment related to the cyber security. According to the answers, there are people who are able to scrutinize the behavior of their own and colleagues as well as physical and digital infrastructure. Therefore, it can be said they are at least somewhat aware of cyber security and issues related to it. Next, the results from the online survey are examined to get better confirmation for this analyzation.

5.4 Online survey results

When profiling an average respondent based on the most common answers to the demographic questions, the average respondent was a 50 – 64 year-old female with a Bachelor’s degree and working as a nurse in the Hospital District of South Ostrobothnia. The average respondent supports the statistics with the healthcare as being a field with more women working in it than men (Tilastokeskus 2008). The nurses in Finland have to have the Bachelor’s degree, which explains the common education and the Hospital District was the largest organization that participated on the survey. The second most common education was a former post-secondary education that supports the middle-aged employees with a completed post-secondary nursing education. The average age was higher than expected; however, in line with the age structure in Finland (Tilastokeskus 2018).

The first question after the demographic questions in the third survey was “Have you participated on cybersecurity training or lecture?” According to the results, most of the respondents have not participated in any training or lectures related to the subject. The amount of people that have been participated in training or lecture on-site versus participated online was alike. These numbers signal that cybersecurity awareness is not trained in the organizations or the training is not compulsory. When analyzing people who have not participated in any cyber security training, the answers to the demographic questions are similar to all respondents, which can mean that the participation is not directly dependent on the demographic measures.

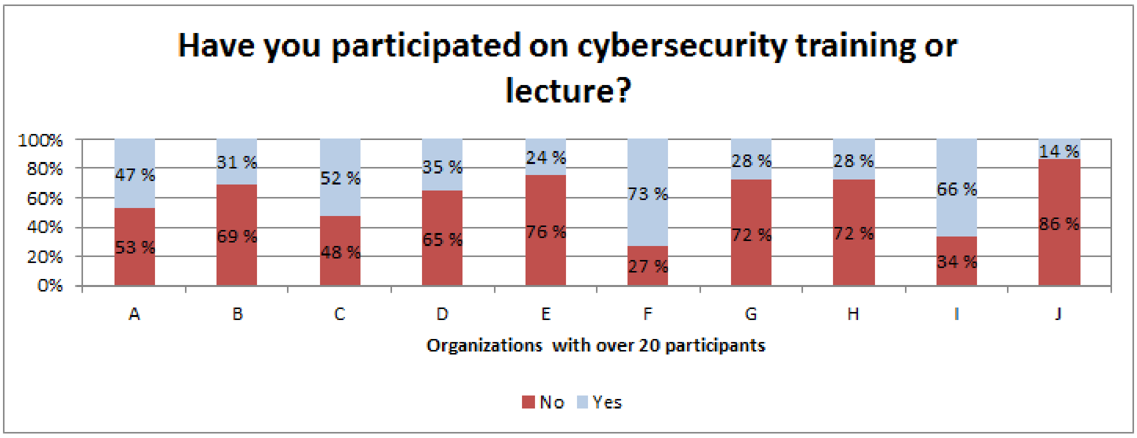


Figure 10. Participation activity between organizations.

In Figure 10 above, the answers are compared between organizations with over twenty respondents. For the confidentiality reasons, the organizations are in a random order and named with letters from A to J. The results vary between organizations, most of the respondents having not participated in any cyber security training or lecture in many organizations. Although, few exceptions existed in organizations F and I, where clearly over half of the respondents had participated in cybersecurity training or lecture. In other organizations the percentages were half or below.

When compared to the results of the two information security barometers conducted by VAHTI, the respondents of survey three have had less cyber security training and education. There can be regional differences; however, the difference is highest when comparing the results to the VAHTI barometer’s governmental sector and it is notable compared to the municipal sector as well. These differences include a signal from a lower cyber security culture in the target organizations. The Cyber security awareness may not have been included in the organization’s risk management at all, or it has been measured as a low-level risk. One reason for this can be the usage of VAHTI instructions especially targeted and used by the governmental sector. Stronger use of national instructions for information security in organizations participated in the survey three as well as in the whole public health care sector in Finland should be considered. There is room for improvement in cyber security awareness in all target organizations.

Even though most of the respondents have not participated in any education regarding cybersecurity, only few answered that they do not need more information about the topic. This supports the results from previous surveys showing that respondents have acknowledged that they need more information about cyber security. According to the answers, the best way to get more information about cybersecurity was by participating onsite in a lecture or training. Participating in online training was the least desired option for getting more information and by advertisement such as email a quarter of the respondents answered.

The popularity of onsite training was higher than expected. It would have been less surprising to find that people want to participate in online education about things related to the internet and digital ecosystems; however, it is understandable when considering the excellent feedback given from the lectures.

Onsite lectures and training can pose a better change for the participants to ask questions about cyber security and to discuss the subject especially about things that the participant is feeling difficult to understand or is even frightened about than during online training. Improved understanding can also relieve these negative feelings and lead to a better security level where feelings always play a big role. On the other hand, online training can be more interactive and produce data that can be used in measuring for example the educational objectives. Nevertheless, because individuals have different ways to learn, multiple learning methods should be used.

Respondents who did not want more information about the subject were a clear minority. If compared to the majority who wanted more information about cyber security they were often younger with lower education and working elsewhere than at IT-department nor management sector. Similarly to the others, most of these participants did not have participated on any cyber security lectures or training. In fact, the participation percentage were even lower than with those who wanted more information.

According to this group, the answered cyber security awareness were at the same level or higher compared to the other respondents and they estimated that they have more knowledge about cyber security for their jobs. Still, the respondents who did not want more information about cyber security felt the subject less important and the need of education about it less valuable. Surprisingly, they have not read the organization’s information security instructions more than others.

Motives for not wanting more information about cyber security can be the same as the mentioned earlier when discussing about why people might not want to participate on cyber security lecture or training. The online survey results support mostly the motive to be a feeling that respondent thinks he or she has enough knowledge about the subject already. This could be a good thing if the knowledge would be good also in reality.

When comparing answers from respondents who did not want more information about cyber security to respondents who had participated to cyber security lessons or training, the results are signaling that the first group can be thinking that they have enough knowledge about the subject but in reality they do not. What should be noted is that these respondents should be more familiar with their organization’s security instruction, now only half of the respondents not wanting more information about cyber security have actually read the instructions. Another supported motive is that they have not found the subject as important and that there is no reason to know more about it.

When considering the young age and lower education of these respondents their knowledge could still be improved in the future. They may have a better overall knowledge about the subject but there are no signs that they do not need participation on cyber security lessons or training like others. Especially an organization and their job related cyber security awareness could be improved if participated and the meaning and importance of the subject could be increased.

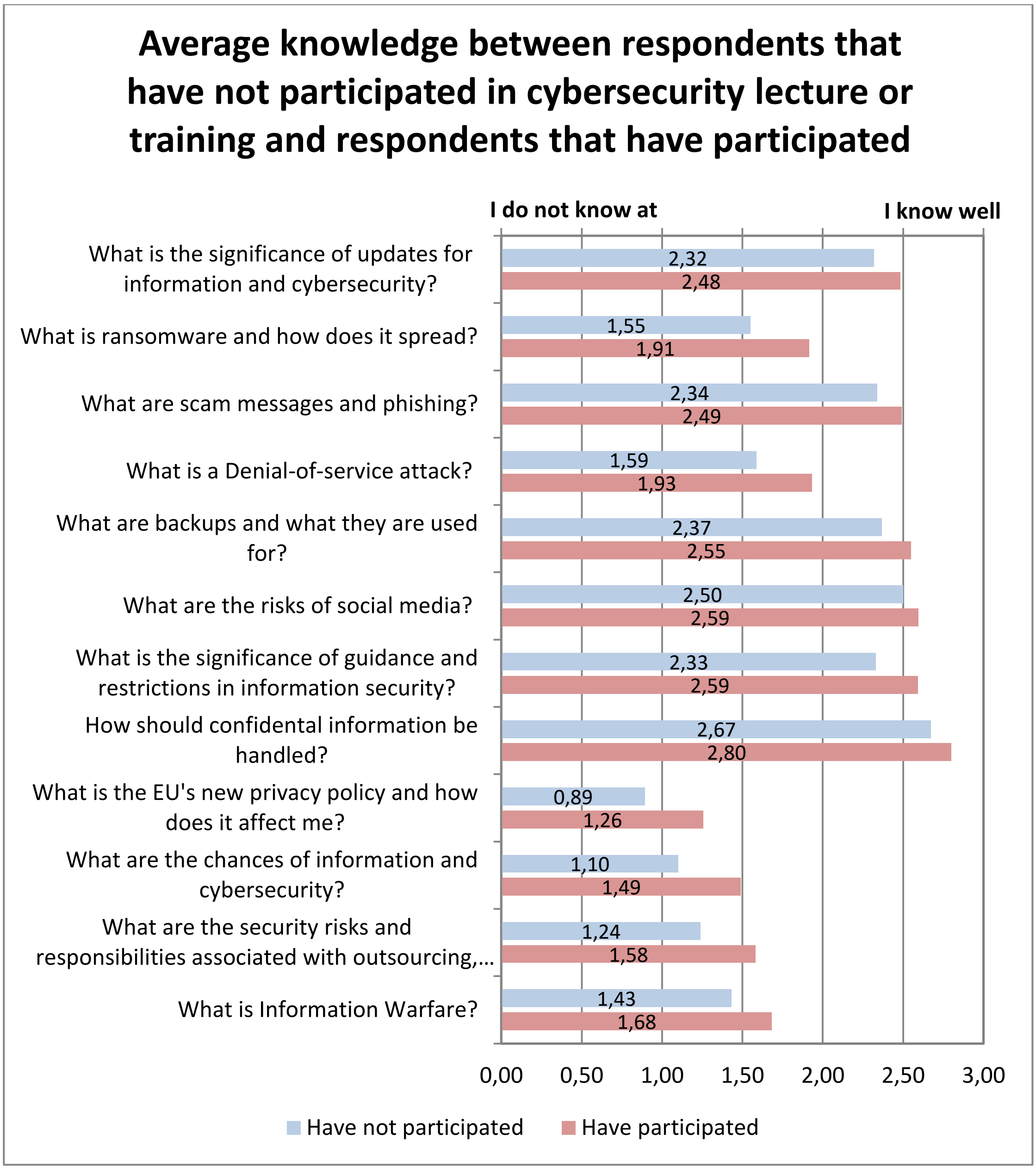


Figure 11. Level of knowledge about cybersecurity related topics estimated by all participants

If the overall knowledge is compared between the participants (Figure 11) that have participated in cybersecurity training or lecture to participants that have not participated in one, the results from the latter group are better. The difference is not wide but visible and repeated in every question through the survey (Figure 12) and seen as well in the answers from the management on Figure 13.

The difference could be due to the better overall knowledge about the topic among respondents who have participated and who would be more likely to answer to survey about topic they are interest in already. Still, because the difference is repeated through the survey with high amount of respondents it is assumable that respondents could learn and improve their cyber security by participating as well, even if they are not keen on the topic. The lecturer's way of presentation and making the topic interesting and easy to understand can have had effect to the positive results.

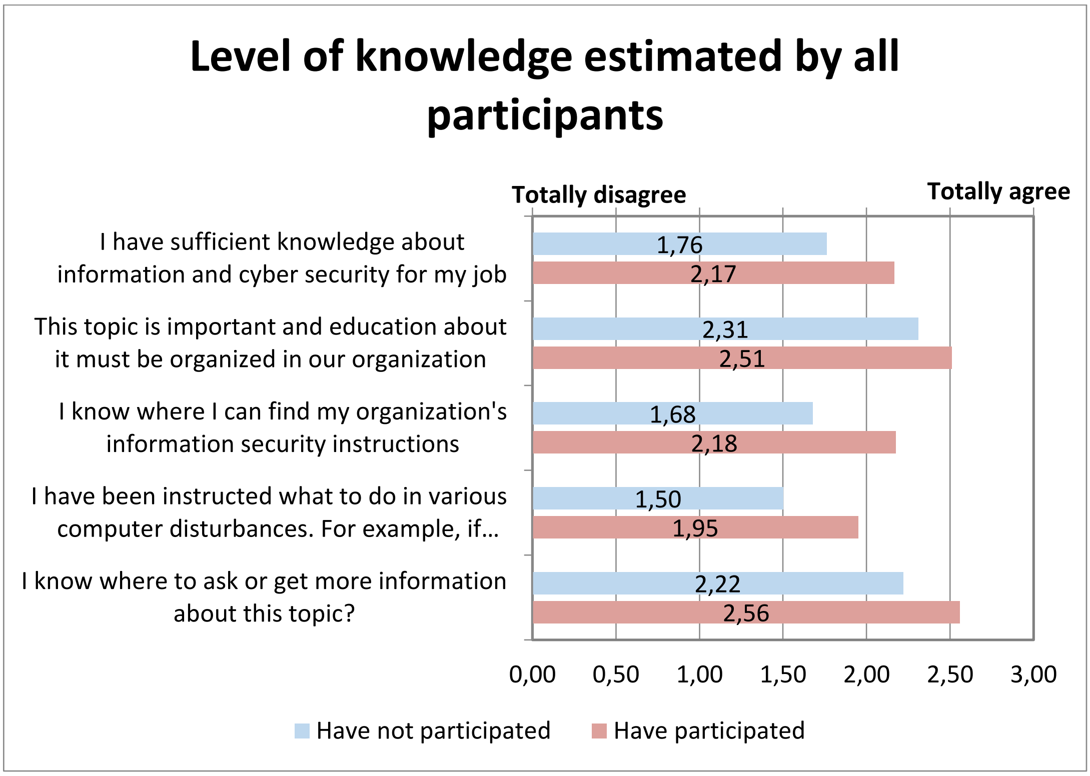


Figure 12. Level of knowledge estimated by all participants

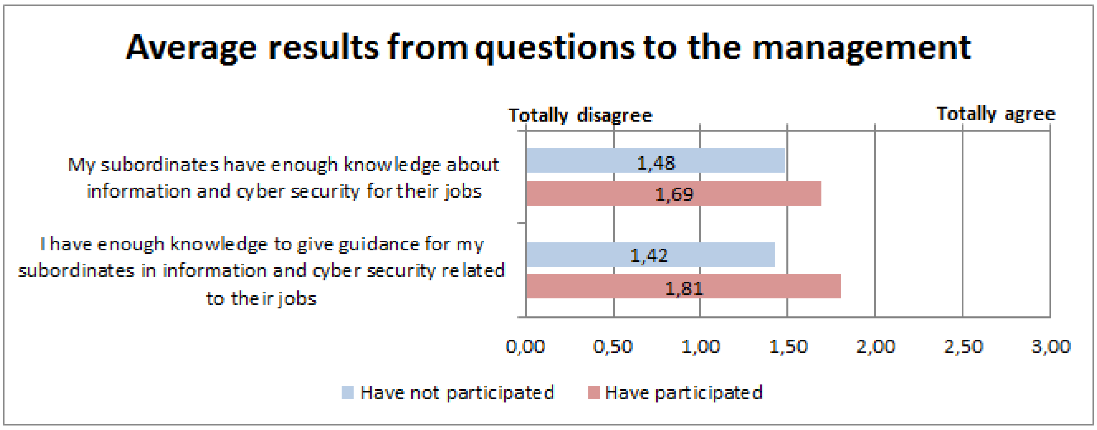


Figure 13. Level of knowledge estimated by the management

One of the most surprising findings from the results was the low rate of Cyber Resilience, “the ability to continuously deliver the intended outcome despite adverse cyber events” as defined by Björck et al. (2015, 311). According to the answers, it is not clear for the respondents what to do if something unexpected happens in cyber environment. Most of the respondents have not been instructed what to do in various computer disturbances, for example, if their computer has been infected with a malicious software or a critical system for their work is not available.

In such a case, most of the respondents know where to ask or get more information about cyber security. Yet, the management might not help because most of them have answered that they do not have enough knowledge to give guidance to their subordinates in information and cyber security issues related to their jobs. What is more, persons with subordinates have answered that they do not think their subordinates have enough knowledge about information and cyber security for their jobs.

If the employee does not know what to do in a case of adverse cyber event that can be intentional or unintentional and happen at any time, the operational risks can be high. In a case of an adverse cyber security event, an uninstructed person may stagnate or cause more trouble by wrong actions. Especially in critical infrastructure, the consequences from this kind of risk can be serious and should be therefore carefully analyzed by the risk management to ensure the continuity and vital operations such as patient safety.

However, these answers included the largest difference when comparing the participated and non-participated respondents. This means that by participating in cyber security lecture or training the knowledge and confidence are improved. This analysis is supported by the answers to the question “I have sufficient knowledge about information and cyber security for my job” where respondents who had participated also had better felt knowledge.

When the results are compared between two questions: “If requested by an authority, I can tell my password on phone” and “If requested by IT management, I can tell my password on phone” the total results for not telling passwords on phone were high and should prevent users from being victims to phishing campaigns and social engineering, which is a common way for hackers to gain access to systems (Thycotic 2018). Yet, when the questioner changes from authority to IT management, telling passwords on phone is not completely denied anymore.

Despite the varying answers, there is no reason for employees to give their passwords to IT management in case of cyber security threat or other contact because real IT management can solve problems without knowing them. Passwords should be not shared with anyone, especially not over phone with an unknown person. Personal passwords are private for a purpose and therefore banks, police or other authorities never ask them, not via phone or email. This should be educated to all employees.

According to the results, most of the respondents use their personal account when logging into computers. However, there are still employees using shared accounts regularly. These answers do not tell whether there is really an identified and documented need for the use; however, a shared account should not be the preferred account to be used when logging into a work computer. Yet, this has not been clear among the people participating to the cyber security lectures

Locking the computer was the second most common action when not using a computer and logging out the most common. In survey number three, no-one answered that he or she usually used someone else’s account; however, according to the feedback and discussions on the cyber security lectures given, there is occasionally use of work computer logged in someone else’s account. There can be a connection between locking or logging out and using someone else’s account because some of the participants answered that they leave the computer unlocked when not using it anymore.

Choosing the most secure password turned out to be strongly linked with the old password recommendations. Instead of choosing the longest password option “hiirikauppahaaste” consisting of words mouse, store and challenge in Finnish and according to tools estimating the secureness of given password the most secure password of the four password examples, most of the respondents chose the option “*5Qx7lxv"yg*” as the most secure password. The latter password is an example fulfilling many of the old recommendations with uppercase and lowercase letters, numbers and special characters making it complex and hard to remember as well as lacking on length. Even the Finnish equivalent for the “password1!” was chosen as the most secure password twice the number than the longest example “hiirikauppahaaste”.

As a positive finding the password example shows that the respondents have adopted security instructions such as the password recommendations albeit they are allowed to choose another type of password. In real life the users might not be able to follow other than the set password policy.

As a negative finding the knowledge concerning passwords is outdated and should be updated. If an organization operating in critical sector is using services following old password recommendations users may think these recommendations are still secure and use this kind of passwords in other services or even all services they are using as well. This can lead to lowering both the organization’s and user’s personal cyber security levels. That is why the knowledge and services should be updated regularly to meet the known secure recommendations and best practices. This also applies to third party services that should be required to meet these recommendations.

Most of the respondents answered they do not use the same passwords at work and off work. The results denying the use of the same password are high compared to study of OpenVPN in 2018, where 25 percent of respondents admitted they use the same password for everything (Madsen 2018).

Using other than organization's own USB sticks should be minimized as they can pose a serious risk to digital environment from leakage of confidential material to modern version of classic Troy Horse, where an infected USB stick is left on employees' parking lot, and an employee carries it and connects to a work device with his or her own credentials. Still, the answers show that using one's own USB stick with work computers or even taking workplace's USB sticks home and connecting them to a personal home computer is real and happening. Whether the rules of using USB sticks are not clear or they are not respected.

During cyber security lectures given several participants told that especially third-party consultants often connect their USB stick to the organization's computers and that the organizations employee have not known should they allow it or not. The results from the survey three support this, as some of the respondents do not know how they should use the USB sticks and they might be using same device on and off work. It is said that email is as secure as a postcard because a basic email does not include any security features at all and if intercepted, the content is visible. In addition, email is known to be source of frauds, phishing and malicious software as well. Nonetheless, the respondents consider email a safe way to communicate.

However, most of the respondents think they are able to identify suspicious and spam emails and know what to do with them; however, they recognized that it is difficult to identify spam emails or that they are not able to do it. This result does not indicate if the skills are high or not because if created carefully, identifying spam can be difficult even for an experienced person. The level of awareness can be actually low among the respondents who answered that they are able to identify spam emails if they are too trustful towards emails.

Fake invoices can earn the sender a great amount of money if paid. According to the results, most of the respondents do not pay or accept an unexpected invoice even if the due date is today and they do not have time to find out what it is all about. Yet, some respondents are not sure what they should do, and a quarter would send the invoice to someone else. Resending the invoice may be a good idea if in a hurry; however, it can lower the threshold of the receiver to accept or pay the invoice if it came from a trusted source.

Overall, the knowledge about topical threats and issues regarding cyber security varied depending on the subject. Significance of updates, guidance and restrictions for information and cybersecurity were well known to the respondents as well as fraud messages, phishing, risks of social media and backups.

Explicitly the highest rated knowledge level according to the answers were about how confidential information should be handled. Confidentiality and data protection are subjects that have been taken care of for years in the healthcare sector before modern digital systems have formed a point of reference for a somewhat newer cyber security awareness. If similar resources and attention would be spent on cyber security awareness, an improved level of awareness would be presumably achieved.

Less-known topics included ransomware, denial-of-service attack, the GDPR and its effect on personal level, security risks and responsibilities associated with outsourcing and purchases and information warfare. What is more, most of the respondents were not familiar with the changes of information and cybersecurity.

Some of the less-known topics can be hard to understand or totally unknown for persons who are not interested in technology or cyber security. Still, respondents who had participated in cyber security lecture or training had a better average knowledge and awareness about these subjects. The respondents who had participated in cyber security lecture or training can be more technically oriented or interested in the cyber security related subjects and therefore be more likely to participate or have better knowledge already.

Even the average respondent, as profiled earlier, could be less oriented in technology than others, according to the results, most of the respondents are willing to participate in cyber security lectures and training to get more information and to improve their cyber security awareness. If a person is willing to participate this kind of event, it is likely that he or she is able to learn as well.

It is said that security is all about trust. It is hard to earn but easy to lose. When asked if the respondent trust their confidential information be secured in the current organization versus in the future organization after the reform, the uncertainty clearly increases regarding the future organization. The overall results show that the respondents trust, but not totally in the current organization’s ability to secure the confidential information and that the participation in cyber security lectures or training is increasing; however, the trust not significantly.

The number of respondents answering that they do not trust at all or that they are not sure trust is increased when asked about the future organization. The participation in cyber security lecture or training did not change the results drastically; however, it decreased the uncertainty as well as the amount of totally trusting respondents resulting in the option trust; yet, not totally being the highest.

If compared to a similar survey conducted by Taloustutkimus to Lännen Media in 2017, the results were slightly different. In the results of the online survey conducted for this thesis, the number of respondents that answered that they trust totally were higher and the number answered they are not trusting at all lower, than in the survey conducted by Taloustutkimus. The results of the latter survey were commented to be alarming by Finnish Ministers. (Puukka & Kuikka 2017).

Reasons for not trusting in the future organization’s ability to secure the confidential information can be related to the change resistance and general uncertainty regarding one’s own personal workplace after the future reform that contains several changes and political debates. All in all, the results give a signal that many of the respondents trust the organization’s ability to secure their confidential information now and in the future. Nevertheless, the trust is important to be monitored and should be improved in all organizations.

6 Conclusions

This thesis studied improving cyber security awareness in the selected organizations. The target organizations were located in the region of South Ostrobothia in Finland; and they were to join in the upcoming Health, social services and regional government reform.

The main objective was to study what the level of cybersecurity awareness and education is in the target organizations and to find reasons affecting them. The results included positive and negative findings.

As positive results, cyber security is seen as important, and the respondents trust their organizations’ cyber security and think that the organizations’ cyber security is at a high level. In addition, the respondent’s own cyber security level is perceived to be high. Most of the respondents have information about the basics of cyber security and they know how to use digital systems and devices securely and avoid common issues in theory.

Yet, according to the results, the overall knowledge is not at a sufficient level in the organizations. The knowledge lacks among the personnel as well as among the management. This analysis is supported by the data gathered; most of the personnel or management have not participated in any training or lectures related to cyber security, many subordinates have answered that they do not have the sufficient knowledge about cyber security for their work, and most of the superiors replied they do not have the sufficient knowledge about cyber security to give guidance to their subordinates in cyber security for their jobs.

Cyber resilience in the target organizations is low and instructions for working in case of computer malfunction or when a critical service for the work is not available are unknown for many. Most of the employees have not read the organization's information security instructions and a significant number of respondents does not know where to find them.

The second objective for this thesis was to study how the cyber security awareness could be improved in the selected organizations. According to the results, the employees are most willing to participate in cyber security training or lectures onsite.

The onsite lectures given were seen as important and educational by the participants. The results show that persons who had participated in cyber security lectures had better know-how and confidence in cyber security compared to persons who had not participated in any cyber security lectures or training.

The amount of education received is low and lacks behind the level in municipal and governmental sectors in Finland. As a conclusion, cyber security awareness has not been taken care of and should be improved in all target organizations.

7 Discussion

This study started by gathering theory about cyber security and its dependencies on critical infrastructure. The theory was plentiful and gathered from multiple sources and formed a good base for the research. After the research questions and methods were chosen, the theory focused more on the research questions. Gathering the theory increased the personal knowledge about the subject and especially about the dependencies such as the dependency between national energy production and cyber ecosystems. The state and condition of the Finnish energy production seems to face major challenges now and in the future to overcome, and these challenges affect the cyber environment on wide level.

Improving cyber security awareness seem to be a quite new topic, especially in the healthcare. Similar studies and theory about the subject is needed. Fortunately, the few studies mentioned provided a viewpoint for this study and gave a reference for the results.

The lectures and the three surveys conducted were a success, producing a great amount of data to be analyzed. In fact, the amount of data gathered was greater than expected and produced a positive dilemma; how to ensure that the analysis increases the value of the data. Still, with careful analysis of the data with data-driven content analysis the proper answers to the research questions were found.

The surveys concentrated on giving the respondents an occasion to rate their personal knowledge about subjects related to cyber security. The questions included topics from work and free time, which both should be seen as important for the organization’s cyber secureness. If one knows how he or she should act in a secure way in the digital world during his or her free time, he or she is probably able to do it at work as well and vice versa.

In addition, real-life examples from off-work can be easier to understand and awaken the interest in the cyber security. Therefore, the organization as well as the whole nation could benefit from increasing the overall cyber security awareness including the off-work cyber security more than just concentrating on the organization’s systems and use cases.

However, surveys did not concentrate on testing the respondents’ cyber security abilities or knowhow in practice. This kind of cyber security testing that was also wanted in the feedback of the surveys could be a good next step to improve the overall cyber security awareness. With digital interactive tests, the employees could take the test when available by using computers or mobile devices. Gamification, for example, could make the tests easier to approach and more profitable as well. Test results from digital tests could provide interesting data that could be analyzed and used for improvement process and statistics of cyber security.

Webropol and the problems in its services during the survey three were a great example of the importance of communication during an adverse cyber event. In such case, the customers should be kept updated about the situation using methods and tools that are working and available. If the organization’s website is having problems, the information on it might not reach everyone. Still, the organization’s social media channels or email-traffic between the organization and customers could be working and usable instead.

The need for situation information increases the longer the event lasts, and with Webropol, the problems lasted for several weeks. Hiding or removing the publications about these kinds of incidents or modifying them afterwards is not an acceptable or trusting way to take care of cyber events. Hopefully, Webropol has objectively analyzed what happened and has made changes to their processes.

The long time period that was spent on this study seemed to increase the maturity of the whole work as well as the reliability of the results. If the time period had been shorter, the quality of the work could have been considerably lower.

The upcoming reform is a great challenge, not only for a region but also for the whole country. However, as always, a reform includes opportunities. The reform sets great expectations for the use of technology to optimize the operations and to gain savings in the future. In order to achieve these goals, along the technology, the cybersecurity should be seen as an enabler - not as disruptor and there is no reason why the reform would not be a chance to improve cybersecurity as well.

If there are hopes to gain savings from centralized ecosystems, the risks and dependencies should be carefully managed. Providing data and services from one point for increased amount of users and systems, the dependency from this point will also be increased. Services such as suomi.fi and Kanta have great potential to improve the digital services for Finnish citizens now and in the future; however, only if they are secured enough. If working, the services can be provided for all users but if not, no one is reached. Lacks in cyber security design with these systems will not only slow down the deployment but also decrease the trust in these systems and organizations.

As the results showed, there are differences even between regional organizations in cybersecurity awareness. When joined, all of these organizations should be taken onto the same improved level of cybersecurity awareness, which could be done by educating all employees. According to the results, people with higher knowledge about the subject have increased feel of trust in the organization’s and their own cyber security level. Therefore, the Finnish saying “knowledge increases pain” does not take place in this context.

Yet, one fundamental question is: who is responsible for taking care that the workers have enough cyber security in the organization? Is it the head of the organization, head of security, IT management, the immediate manager, the employee him- or herself or someone else? There could be reasons to select each of the mentioned but before the responsible one is really determined and accredited in practice, the responsible is no one.

Besides the responsible(s) for taking care of the cyber security awareness in the organization another question is: whose duty is it to improve the awareness among the employees in practice? For this task, an organization could use its own resources or outsourced resources.

Whereas an outsourced consultant, for example, might be more skilled and specialized in cyber security education, the organization’s own resources can have better knowledge of the organization’s digital ecosystem, practices and culture including strengths and weaknesses. Depending on the human and financial resources available, an organization could choose to use one type of resource to educate the employees or to use both types to ensure that the awareness is improved properly. In both cases, testing and information gathering from the progress should be considered.

This study has potential for further usage. The results produced a great amount of information that can be used in the target organizations as well as in other organizations trying to improve their cyber security awareness. Some of the results have already been implemented in the Hospital District of South Ostrobothnia, and there is potential to distribute the knowledge to other target organization after the reform at the latest. For the wider usage, the results of this study have been introduced in a workshop concentrating on improving cyber security awareness in the health care sector in Finland organized by the Finnish National Emergency Supply Agency.

Especially the online survey results could be used in further studies and analyzed in more detail with a quantitative analysis, for example. In addition, the survey results could be used as a baseline when renewing the survey or parts of it in the target organizations to estimate and calculate the progress. The results can also be used when comparing them against other similar studies about cyber security awareness in other organizations such as hospital districts.

Still, even the World Health Organization’s constitution enshrines the right to health for every human being (WHO 1946, 1), healthcare must not be considered as a self-evident worldwide service. It is important to note that there are hundreds of millions of people on this planet missing it every day (WHO 2015). Finns are so used to thinking that if there is time to wait in a line, there is always the public healthcare sector to support the people. To ensure that this kind of luxury service will be within reach also in the future, people must be well aware of how it is built in the digitalized environment and what its risks, threats and dependencies are as well as what the positive potentiality of the cyber is.

References

Alueuudistus 2017. *Maakunta- ja sote-uudistuksen yleisesittely* [General description of the reform package]. Accessed on 9 November 2017. Retrieved from http://alueuudistus.fi/uudistuksen-yleisesittely

Aukia, J-P. 2015. *Miten sähköjärjestelmä toimii?* [How electricity system works?]. Helsinki: National Emergency Supply Agency. Accessed on 21 November 2017. Retrieved from https://www.varmuudenvuoksi.fi/aihe/toimintaymparisto/158/miten_sahkojarjestelma_toimii

Björck F., Henkel M., Stirna J., Zdravkovic J. (2015) Cyber Resilience – Fundamentals for a Definition. In: Rocha A., Correia A., Costanzo S., Reis L. (eds) New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing, vol 353. Springer, Cham.

Brooks, R. 2017. [Infographics] Top Cybersecurity Risks 2017. Accessed on 20 July 2018. Retrieved from https://blog.netwrix.com/2017/06/09/infographics-top-cybersecurity-risks-2017/

Cisco Networking Academy 2014. Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design. Accessed on 7 February 2018. Retrieved from http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4

Cisco 2017. The Zettabyte Era: Trends and Analysis. Accessed on 7 November 2017. Retrieved from https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html

Cimpanu, C. 2017. US-CERT: Security Products That Perform HTTPS Interception Weaken Security. Accessed on 19 March 2018. Retrieved from https://www.bleepingcomputer.com/news/security/us-cert-security-products-that-perform-https-interception-weaken-security/

Cimpanu, C. 2018. Hackers Stole a Third of Singapore's Healthcare Data, Including Prime Minister's. Accessed on 23 July 2018. Retrieved from https://www.bleepingcomputer.com/news/security/hackers-stole-a-third-of-singapores-healthcare-data-including-prime-ministers/

Computerworld 2017. Tech Forecast 2017. Accessed on 12 March 2018. Retrieved from https://www.computerworld.com/resources/122905/tech-forecast-2017-complete-survey-results

Dekker, M. 2017. The HTTPS interception dilemma: Pros and cons. Accessed on 25 March 2018. Retrieved from https://www.helpnetsecurity.com/2017/03/08/https-interception-dilemma/

Dunn, J. 2018. Feel the shame: Email-scammed staffers aren't telling bosses about it. Accessed 19 November 2018. Retrieved from https://www.theregister.co.uk/2018/09/07/scam_business_emails_on_the_rise/

Durumeric, Z., Ma, Z., Springall, D., Barnes, R., Sullivan, N., Bursztein, E., Bailey, M., Halderman, J., Paxson, V. 2017. The Security Impact of HTTPS Interception. PDF-document. Accessed on 19 March 2018. Retrieved from https://jhalderm.com/pub/papers/interception-ndss17.pdf

Eevertti 2018. Healthcare CA services. Accessed on 25.7.2018. Retrieved from https://eevertti.vrk.fi/terveydenhuollolle

Elisa 2018. *Tietoa Elisasta* [Information about Elisa]. Accessed on 25 May 2018. Retrieved from http://corporate.elisa.fi/tietoa-elisasta/

Energiateollisuus 2017. *Säätövoima - säädettävää sähköntuotantoa* [Regulated power and its production]. Accessed on 13 November 2017. Retrieved from https://energia.fi/perustietoa_energia-alasta/energiantuotanto/sahkontuotanto/saatovoima

EP2019. *Etelä-Pohjanmaan SOTE* [The Health, social services and regional government reform in South Ostrobothnia]. Accessed on 9 November 2017. Retrieved from https://sote.ep2019.fi/

ESET 2017. Cybersecurity training in the workplace. PDF-document. Accessed on 23 July 2017. Retrieved from https://cdn1.esetstatic.com/ESET/US/docs/business/ESET-Cybersecurity-Training-Survey-Data.pdf

European Commission 2017. Critical infrastructure. Accessed on 15 October 2017. Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en

European Commission 2018. What is personal data? Accessed on 7 July 2018. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

European Union Agency for Network and Information Security 2015. Methodologies for the identification of Critical Information Infrastructure assets and services. Accessed on 23 October 2017. Retrieved from https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis

EUR-Lex 2015. Regulation (EU) 2015/2120 of the European Parliament and of the council. Accessed on 16 December 2017. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R2120&from=FI

EUR-Lex 2016. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Accessed on 7 July 2018. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

European Network of Transmission System Operators for Electricity 2017. Mid-term adequacy forecast 2017 edition. PDF-document. Accessed on 9 December 2017. Retrieved from https://www.entsoe.eu/Documents/SDC documents/MAF/MAF_2017_report_for_consultation.pdf

Evans, B. 2018. Why Microsoft Is Ruling The Cloud, IBM Is Matching Amazon, And Google Is $15 Billion Behind. Accessed on 12 March 2018. Retrieved from https://www.forbes.com/sites/bobevans1/2018/02/05/why-microsoft-is-ruling-the-cloud-ibm-is-matching-amazon-and-google-is-15-billion-behind/#5535b87d1dc1

FBI 2017. 2017 Internet crime report. PDF-document. Accessed on 1 June 2018. Retrieved from https://pdf.ic3.gov/2017_IC3Report.pdf

Fennovoima 2017. Hanhikivi 1 Timeline. Accessed on 7 December 2017. Retrieved from https://www.fennovoima.fi/en/hanhikivi-1-project/timeline

Fennovoima 2017. *Fennovoimalla on kaksi omistajaa* [Fennovoima has two owners]. Accessed on 8 December 2017. Retrieved from https://www.fennovoima.fi/fennovoima/omistajat

Ficora 2013. *Kyberturvallisuuskeskus vahvistaa Viestintäviraston nykyisiä tietoturvatehtäviä* [The Cyber Security Center will strengthen current FICORA's security duties]. Accessed on 27 July 2018. Retrieved from https://www.viestintavirasto.fi/viestintavirasto/ajankohtaista/2013/kyberturvallisuuskeskusvahvistaaviestintavirastonnykyisiatietoturvatehtavia.html

Ficora. Open internet or net neutrality. Accessed on 16 December 2017. Retrieved from https://www.viestintavirasto.fi/en/internettelephone/openinternet.html

Ficora 2016. *Lokien keräys ja käyttö* [Collecting and using logs]. PDF-document. Accessed on 5 May 2018. Retrieved from https://www.viestintavirasto.fi/attachments/tietoturva/Lokitusohje.pdf

Ficora 2016. *Selviytymisopas kiristyshaittaohjelmia vastaan* [Survival guide against ransomware]. Accessed on 18 July 2018. PDF-document. Retrieved from https://www.viestintavirasto.fi/attachments/tietoturva/Kiristyshaittaohjelmat__teemakooste_07_2016.pdf

Ficora 2018. Consumer survey on communications services. Accessed on 24 July 2018. Retrieved from https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/06/ttn201806201436.html

Fingrid 2017. *Sähkönkulutus kaikkien aikojen ennätystasolla 7.1.2016* [Energy consumption at all time high 7.1.2016]. Accessed on 20 November 2017. Retrieved from http://www.fingrid.fi/fi/ajankohtaista/tiedotteet/Sivut%2FS%C3%A4hk%C3%B6nkulutus-kaikkien-aikojen-enn%C3%A4tystasolla-7.1.2016.aspx

Finlex 1999. *Suomen perustuslaki* [The Constitution of Finland]. Accessed on 16 October 2017. Retrieved from http://www.finlex.fi/fi/laki/ajantasa/1999/19990731#a731-1999

Finnish Government 2017. *EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö* [Memorial of EU's General Data Protection Regulation executive work group (TATTI)]. Helsinki: Author. Accessed on 27.10.2017. Retrieved from https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80098/OMML_35_2017_EUn_yleinen_tietosuoja.pdf?sequence=1

Finnish Ministry of Finance. 2008. *Tärkein tekijä on ihminen* [The most important factor is human]. PDF-document. Accessed 2 February 2019. Retrieved from https://www.vahtiohje.fi/c/document_library/get_file?uuid=af5614a4-fa44-482c-9886-0af9e6a13929&groupId=10128&groupId=10229

Finnish Ministry of Finance. 2009. *5 Henkilöstöturvallisuus* [5 Personnel security]. Accessed 2 February 2019. Retrieved from https://www.vahtiohje.fi/web/guest/henkilostoturvallisuus

Finnish Ministry of Social Affairs and Health. 2017. *Sairaanhoitopiirit ja erityisvastuualueet* [Hospital districts and Expert Responsibility areas]. Helsinki: Author. Accessed on 19 November 2017. Retrieved from http://stm.fi/sairaanhoitopiirit-erityisvastuualueet

Finnish Ministry of Social Affairs and Health. 2017. *Lainsäädäntö* [Legislation]. Helsinki: Author. Accessed on 16 October 2017. Retrieved from http://stm.fi/sotepalvelut/lainsaadanto

Finnish National Emergency Supply Agency 2016. *Huoltovarmuusneuvoston kannanotto sähkötehon riittävyydestä Suomessa* [Statement of power sufficiency in Finland from counsil of National Emergency Suplly Agency of Finland]. Accessed on 25 November 2017. Retrieved from https://www.varmuudenvuoksi.fi/aihe/huoltovarmuuden_toteutuksia/345/huoltovarmuusneuvoston_kannanotto_sahkotehon_riittavyydesta_suomessa

Gartner 2017. Healthcare Providers vertical industry comparison. Accessed on 16 July 2018. Retrieved from http://www.gartner.com/downloads/public/explore/metricsAndTools/ITBudget_Sample_2012.pdf

GFCE-MERIDIAN 2017. The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers. PDF-document. Accessed on 11 March 2018. Retrieved from https://www.thegfce.com/initiatives/c/critical-information-infrastructure-protection-initiative/documents/reports/2017/10/22/the-gfce-meridian-good-practice-guide-on-critical-information-infrastructure-protection-for-governmental-policy-makers

GlobalSign 2017. What is a Man-in-the-Middle Attack and How Can You Prevent It? Accessed on 23 February 2018. Retrieved from https://www.globalsign.com/en/blog/what-is-a-man-in-the-middle-attack/

Google transparencyreport 2018. *HTTPS-Salaus verkossa* [HTTPS encryption online] Accessed on 20 March 2018. Retrieved from https://transparencyreport.google.com/https/overview

Google 2018. Google 2-Step Verification. Accessed on 24 July 2018. Retrieved from https://www.google.com/landing/2step/

Hakala, P. 2015. *Rosatom-johtaja HS:lle: Totta kai Hanhikiven voimala rakennetaan venäläisellä rahalla* [The head of Rosatom to HS: Of course the Hanhikivi power plant will be funded with russian money]. Accessed on 8 December 2017. Retrieved from https://www.hs.fi/talous/art-2000002838694.html

Hallamaa, T. 2018. *Kiina estää tehokkaasti tiedonkulun, Venäjä uhoaa perustavansa oman internetin: Hajoaako internet osiin?* [China prevents effective communication, Russia has set up its own Internet: Does the Internet disintegrate?]. Accessed on 9 August 2018. Retrieved from https://yle.fi/uutiset/3-10226579

Harala, S. Blencowe A 2015. *Tällainen on uuden ydinvoimalan kroatialainen omistaja* [This is the new Croatian owner of the new nuclear power plant]. Yle 2015. Accessed on 8 December 2015. Retrieved from https://yle.fi/uutiset/3-8116193

Helme, R. 2018. Alexa Top 1 Million Analysis - February 2018. Accessed on 17 March 2018. Retrieved from https://scotthelme.co.uk/alexa-top-1-million-analysis-february-2018/

Helsingin Sanomat 2018. *Kaapelityö Hakaniemessä pani Helsingin tietojärjestelmän täysin sekaisin* [Cable work in Hakaniemi made the information system of Helsinki completely messy]. Accessed on 18 May 2018. Retrieved from https://www.hs.fi/kaupunki/art-2000005681696.html

Helsingin Sanomat 2018. *Konsultit ratsastivat EU:n tietosuoja-asetuksen uhkakuvilla – Tietosuojavaltuutetun mukaan jättimäisillä viranomaissanktioilla uhkailu oli täysin väärin* [The consultants ridden with threats of the EU's privacy policy - The Data Protection Ombudsman said threatening with the possible charges was completely wrong]. Accessed on 18 July 2018. Retrieved from https://www.hs.fi/kotimaa/art-2000005730671.html

Hicock, R. 2016. Microsoft Password Guidance. PDF-document. Accessed on 19 February 2018. Retrieved from https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf

Hospital District of South Ostrobothnia. *Toiminta* [The operation]. Accessed on 16 September 2017. Retrieved from http://www.epshp.fi/1/toiminta

IBM Security Services 2014. Cyber Security Intelligence Index: Analysis of cyber attack and incident data from IBM’s worldwide security operations. PDF-document. Accessed on 27 November 2017. Retrieved from https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf

IBM X-Force Research 2016. 2016 Cyber Security Intelligence Index: A survey of the cyber security landscape for healthcare. PDF-document Accessed on 3 January 2018. Retrieved from https://public.dhe.ibm.com/common/ssi/ecm/se/en/se912352usen/SE912352USEN.PDF

ICS-CERT 2017. ICS-CERT Monitor. PDF-document. Accessed on 26 July 2018. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2017_S508C.pdf

Independent security evaluators 2016. Securing hospitals. PDF-document. Accessed on 12 November 2017. Retrieved from https://securityevaluators.com/hospitalhack/

IRCAD France - Research Institute against Digestive Cancer 2001. “OPERATION LINDBERGH” A World First in TeleSurgery: The Surgical Act Crosses the Atlantic! PDF-document. Accessed on 7 November 2017. Retrieved from https://www.ircad.fr/wp-content/uploads/2014/06/lindbergh_presse_en.pdf

ItGovernance 2018. GDPR enforcement and penalties. Accessed on 18 July 2018. Retrieved from https://www.itgovernance.co.uk/dpa-and-gdpr-penalties

Jormanainen, V. 2015. *Terveydenhuollon tietojärjestelmät Suomessa nyt ja tulevaisuudessa* [Patient information systems in Finland now and in future]. PDF-document. Accessed on 15 December 2017. Retrieved from http://elec.aalto.fi/fi/midcom-serveattachmentguid-1e57d7f5ac168b07d7f11e589b0f5ad480af4e8f4e8/s1_jormanainen.pdf

Järvinen, P. 2014. *NSA - Näin meitä seurataan* [NSA - this is how we are monitored]. Jyväskylä: Docendo.

Järvinen, P., Rousku, K. 2017. *Työpaikan tietoturvaopas* [Information security guide for workplaces]. Helsinki: Alma Talent.

Kamk 2018. *Laadullisen aineiston analyysi ja tulkinta* [Analysis and interpretation of qualitative data]. Accessed on 21 August 2018. Retrieved from https://www.kamk.fi/fi/opari/Opinnaytetyopakki/Teoreettinen-materiaali/Tukimateriaali/Laadullisen-analyysi-ja-tulkinta

Kananen, I. 2015. *Suomen huoltovarmuus* [Finland’s Emergency supply]. Jyväskylä: Docendo.

Kananen, J. 2015. *Opinnäytetyön kirjoittajan opas – Näin kirjoitan opinnäytetyön tai pro gradun alusta loppuun.* [Thesis Writer's Guide - This is how I write the thesis or pro gradu from the beginning to the end]. Jyväskylä: Jyväskylän Ammattikorkeakoulu.

Kassinen, O. 2014. *Verkkoneutraliteetti (nettineutraliteetti) - mitä se on ja miksi se on tärkeää?* [Neutrality of the internet (net neutrality) – what is it and why it is important?]. Accessed on 16 December 2017. Retrieved from https://effi.org/nettineutraliteetti

Kemijoki 2017. *Säätövoima* [Load following energy production]. Accessed on 20 November 2017. Retrieved from https://www.kemijoki.fi/vesivoima/saatovoima.html

Koivunen, E. 2010. *Verkon aktiivilaitteet* [Network devices]. Ministry of Finance of Finland. Accessed on 21 February 2018. Retrieved from https://www.vahtiohje.fi/web/guest/verkon-aktiivilaitteet

Kolodny, L. 2018. Former Google CEO predicts the internet will split in two — and one part will be led by China. Accessed on 11 August 2018. Retrieved from https://www.cnbc.com/2018/09/20/eric-schmidt-ex-google-ceo-predicts-internet-split-china.html

Koppa 2019. Quantitative Research. Accessed 10 January 2019. Retrieved from https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/en/methodmap/strategies/quantitative-research

Kotz, D., Gunter, C. A., Kumar, S., W, J. P. 2016. Privacy and Security in Mobile Health: A Research Agenda. Accessed on 27 July 2018. Retrieved from Privacy and Security in Mobile Health: A Research Agenda

KPMG 2017. The healthy approach to cyber security. Accessed on 20 July 2018. PDF-document. Retrieved from https://www.kpmg-institutes.com/content/dam/kpmg/healthcarelifesciencesinstitute/pdf/2017/cyber-report-healthcare.pdf

Krebs, B. 2018. Google: Security Keys Neutralized Employee Phishing. Accessed on 25 July 2018. Retrieved from https://krebsonsecurity.com/2018/07/google-security-keys-neutered-employee-phishing/

Kurunmäki, H. 2013. *Tietosuoja ja tietoturva terveydenhuollon alalla, Case Organisaatio A* [Privacy Protection and Information Security in the Health Care Sector, Case Organization A]. *Vaasan Ammattikorkeakoulu* [Vaasa University of Applied Sciences]. Accessed on 5 August 2018. Retrieved from https://www.theseus.fi/bitstream/handle/10024/54166/Kurunmaki_Helja.pdf?sequence=1&isAllowed=y

Laatikainen, T. 2018. *Olkiluoto 3 on maailman 2. kallein rakennus – Svenska Yle: Kheopsin pyramidin rakentaminen kesti muutaman vuoden enemmän* [Olkiluoto 3 is the 2nd most expensive building in the world - Svenska Yle: The construction of the Kheops pyramid took a few more years]. Accessed 7 December 2018. Retrieved from https://www.tekniikkatalous.fi/tekniikka/rakennus/olkiluoto-3-on-maailman-2-kallein-rakennus-svenska-yle-kheopsin-pyramidin-rakentaminen-kesti-muutaman-vuoden-enemman-6706672

Latvanen, K. 2018. *Gdpr on täällä kohta, rikkoja voi saada jopa 20 miljoonan sakot – näin organisaatiot valmistautuvat asetukseen* [Gdpr is here, the offender can get up to 20 million fines - this is how the organizations are preparing for the regulation]. Accessed on 18 July 2018. Retrieved from https://www.tivi.fi/Kaikki_uutiset/gdpr-on-taalla-kohta-rikkoja-voi-saada-jopa-20-miljoonan-sakot-nain-organisaatiot-valmistautuvat-asetukseen-6701121

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T. & Salminen, M. 2017. *Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi* [Finland's cyber security: the present state, vision and the actions needed to achieve the vision]. PDF-document. Accessed on 9 January 2018. Retrieved from http://tietokayttoon.fi/documents/10616/3866814/30_Suomen+kyberturvallisuuden+nykytila%2C+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf/372d2fd4-5d11-4991-862c-c9ebfc2b3213?version=1.0

Leinonen, L. 2016. *Vakava sairaalan tietoturvapoikkeama johti työntekijän potkuihin – Potilastietojen ei uskota vaarantuneen* [Serious hospital security breach led to employee to be fired - Patient information is not believed to be compromised]. Accessed on 19 July 2018. Retrieved from https://yle.fi/uutiset/3-9361946

Let's Encrypt 2018. Let's Encrypt Stats. Accessed on 20 March 2018. Retrieved from https://letsencrypt.org/stats/

Lewis, T. G. 2015. Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation 2nd ed. Hoboken: John Wiley & Sons.

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

Macaulay, T. 2016. Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies. Boca Raton: CRC Press.

Madden, B. 2016. What is app virtualization? Part 1: Remote Apps. Accessed on 3 March 2018. Retrieved from http://www.brianmadden.com/opinion/What-is-app-virtualization-Part-1-Remote-Apps

Madsen, N. 2018. OpenVPN Study Reveals Employee Behaviors Have a Direct Impact on Corporate Cybersecurity Effectiveness. Accessed on 16 September 2018. Retrieved from https://www.privatetunnel.com/news/cyber-hygiene-openvpn-study/

Martikainen, T., Pynnöniemi, K., Saari, S., & the Finnish Institute of International Affairs team 2016. *Venäjän muuttuva rooli Suomen lähialueilla* [Russia's changing role in Finland's neighbourhood]. Prime Minister's Office Finland 30.8.2016. PDF-document. Accessed on 13 January 2018. Retrieved from https://storage.googleapis.com/upi-live/2017/01/loppuraportti_venajan_muuttuva_rooli.pdf

Martin, V. 2015. Why you should use SSL inspection. Accessed on 20 March 2018. Retrieved from http://cookbook.fortinet.com/why-you-should-use-ssl-inspection/

McCumber, J. 2005. Assessing and Managing Security Risk in IT Systems: A Structured Methodology. Auerbach Publications.

Microsoft azure 2018. What is SaaS? Accessed on 13 March 2018. Retrieved from https://azure.microsoft.com/en-us/overview/what-is-saas/

Morgan, S. 2017. 2018 Cybersecurity Market Report. Accessed on 4 July 2018. Retrieved from https://cybersecurityventures.com/cybersecurity-market-report/

Mosher, R. 2011. Cloud computing risks. ISSA Journal July 2011. Accessed on 16 March 2018. Retrieved from http://www.experis.us/Website-File-Pile/Articles/Experis/FIN_Cloud-Computing-Risks_071111.pdf

Mäkelä, J. 2017. Saarikko: *Teknologia tuo sote-säästöt* [Saarikko: the savings of the reform comes from technology]. Ilkka, 4 November 2017, 5.

National Audit Office Of Finland 2017. *Finanssipolitiikan valvonnan arvio julkisen talouden hoidosta* [Estimation of public economy by the National Audit Office Of Finland]. PDF-document. Helsinki: Author. Accessed on 6 November 2017. Retrieved from https://www.vtv.fi/files/5908/Finanssipolitiikan_valvonnan_arvio_julkisen_talouden_hoidosta_03112017.pdf

National Audit Office of the United Kindom 2018. Investigation: WannaCry cyber attack and the NHS. Accessed on 18 July 2018. PDF-document. Retrieved from https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

National Cyber Security Centre. Guidance: 10 Steps: User Educationand Awareness. Accessed on 26 July 2018. Retrieved from https://www.ncsc.gov.uk/guidance/10-steps-user-education-and-awareness

National Health Service of the United Kindom 2016. About the National Health Service (NHS). Accessed on 7 January 2018. Retrieved from https://www.nhs.uk/NHSEngland/thenhs/about/Pages/overview.aspx

National Institute of Standards and Technology 2017. NIST Special Publication 800-63B: Digital Identity Guidelines – Authentication and Lifecycle Management. Accessed on 14 February 2018. Retrieved from https://pages.nist.gov/800-63-3/sp800-63b.html#appA

Nikka, A. 2017. *Olkiluoto 3 pitää hallussaan rakentamisen Suomen ennätystä – valmistuminen yhdeksän vuotta myöhässä* [Olkiluoto 3 has the Finnish national record in building – ready with 9 years of delay]. Accessed on 8 December 2017. Retrieved from https://www.satakunnankansa.fi/satakunta/olkiluoto-3-pitaa-hallussaan-rakentamisen-suomen-ennatysta-valmistuminen-yhdeksan-vuotta-myohassa-200284400/

Nikula, P. 2017. *Kaappausyritys Suomen kantaverkossa* [Hijack attempt in the Finland's national power grid]. Accessed on 12 January 2018. Retrieved from https://m.kauppalehti.fi/uutiset/kaappausyritys-suomen-kantaverkossa/QG2sVeDP

Office of the Revenue Commissioners 2015. Telecommunications, broadcasting and electronic (TBE) services - new rules (2015). Accessed on 9 March 2018. Retrieved from https://www.revenue.ie/en/vat/vat-moss/telecommunications-broadcasting-and-electronic/index.aspx

Olzak, T., Scudder, R. 2010. Network segmentation tips. Accessed on 6 March 2018. Retrieved from http://www.brighthub.com/computing/enterprise-security/articles/67023.aspx

Pham, S. 2017. What does the end of U.S. net neutrality mean for the world? Accessed on 27 July 2018. Retrieved from https://money.cnn.com/2017/12/15/technology/net-neutrality-global-implications/index.html

Personick, S. D., Patterson, C. A. 2003. Critical Information Infrastructure Protection and the Law : An Overview of Key Issues. National Academies Press, 2003. ProQuest Ebook Central. Retrieved from https://ebookcentral-proquest-com.ezproxy.jamk.fi:2443/lib/jypoly-ebooks/detail.action?docID=3375827.

Petit, F., Verner, D., Brannegan, D., Buehring, W., Dickinson, D., Guziel, K., Haffenden, R., Phillips, J. & Peerenboom, J. 2015. Analysis of Critical Infrastructure Dependencies and Interdependencies. Argonne, Ill.; Argonne National Laboratory, Global Security Sciences Division. PDF-document. Accessed on 25 November 2017. Retrieved from http://www.ipd.anl.gov/anlpubs/2015/06/111906.pdf

Ponemon 2017. 2017 Ponemon Cost of Data Breach Study. Accessed on 12 November 2017. Retrieved from https://www.ibm.com/security/data-breach/

Ponemon 2017. Medical Device Security: An Industry Under Attack and Unprepared to Defend. PDF-document. Accessed on 19 July 2018. Retrieved from https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/medical-device-security-ponemon-synopsys.pdf

Puukka, J., Kuikka, J. 2017. *LM-kysely paljasti epäilyksen varjon: Viranomaisten kykyyn suojata arkoja henkilötietoja ei luoteta* [The LM survey revealed a shadow of doubt: The ability of the authorities to protect sensitive personal data is not trusted]. Accessed 15 January 2019. Retrieved from https://www.kainuunsanomat.fi/kainuun-sanomat/kotimaa/lm-kysely-paljasti-epailyksen-varjon-viranomaisten-kykyyn-suojata-arkoja-henkilotietoja-ei-luoteta/?_ga=2.11165620.1497555680.1548679518-854348170.1548679518

Ragan, S. 2016. Ransomware takes Hollywood hospital offline, $3.6M demanded by attackers. Accessed on 7 January 2018. Retrieved from https://www.csoonline.com/article/3033160/security/ransomware-takes-hollywood-hospital-offline-36m-demanded-by-attackers.html

Romm, T. 2017. Trump's FCC has revealed plans to wipe out net neutrality. Accessed on 17 December 2017. Retrieved from https://www.recode.net/2017/11/21/16679114/fcc-ajit-pai-net-neutrality-rules-donald-trump

Rousku, K., Mellin, L. 2018. Data security barometer for personnel and management 2017. Accessed on 3 August 2018. Retrieved from http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160944/19_18_Henkiloston%20ja%20johdon%20tietoturvabarometri%202017.pdf?sequence=1&isAllowed=y

Ruusunen, J. 2017. *Ruotsin ja Norjan kantaverkkoyhtiöiden uusi ehdotus ei poista epäkohtia - Kahden maan erityisasema päätöksenteossa ei ole mahdollista* [The new draft agreement of Swedish and Norwegian transmission system operators does not remove the grievances – The special status of the two countries is not possible in decision making]. Accessed on 13 January 2018, Retrieved from https://www.fingrid.fi/sivut/ajankohtaista/tiedotteet/2017/ruotsin-ja-norjan-kantaverkkoyhtioiden-uusi-ehdotus-ei-poista-epakohtia---kahden-maan-erityisasema-paatoksenteossa-ei-ole-mahdollista/

SANS 2001. Importance of Understanding Logs from an Information Security Standpoint. Accessed on 5 May 2018. Retrieved from https://www.sans.org/reading-room/whitepapers/logging/importance-understanding-logs-information-security-standpoint-200

Saraste, A. 2018. *Uusi kyberraportti Saksasta varoittaa: hakkerit voisivat pimentää koko Euroopan sähköverkon* [A new cyber report from Germany warns: hackers could cause a total blackout in the entire European electricity grid]. Accessed on 30 August 2018. Retrieved from https://yle.fi/uutiset/3-10369841

Schneider, P. 2005. Something You Know, Have, or Are. Accessed on 24 July 2017. Retrieved form https://www.cs.cornell.edu/courses/cs513/2005fa/NNLauthPeople.html

Shimonski, R. 2015. The importance of Network Redundancy. Accessed on 4 March 2018. Retrieved from http://techgenix.com/importance-network-redundancy/

Shrum, S., Murray, P. 2012. Common Risks of Using Business Apps in the Cloud. Accessed on 3 April 2018. PDF-Document. Retrieved from https://www.us-cert.gov/sites/default/files/publications/using-cloud-apps-for-business.pdf

Shuler, R. 2002. How Does the Internet Work. Accessed on 10 March 2018. Retrieved from https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm

Smith, B. 2017. The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack. Accessed on 7 January 2018. Retrieved from https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/

Sohlman, M. 2017. *Suomi sai tehovajeesta hälyttävän analyysin – mitä pitäisi tehdä?* [Finland got alarming analysis of its power deficit – what should we do?]. Accessed on 9 December 2017. Retrieved from https://www.pohjolanvoima.fi/uutishuone/blogit/kirjoitukset/50/suomi_sai_tehovajeesta_halyttavan_analyysin_-_mita_pitaisi_tehda

STUK 2018. *Matkapuhelinverkon toiminta ja tukiasemat* [Operation of mobile broadband and base stations]. Accessed on 20 February 2018. Retrieved from http://www.stuk.fi/aiheet/matkapuhelimet-ja-tukiasemat/matkapuhelinverkko/matkapuhelinverkon-toiminta-ja-tukiasemat

The Organisation for Economic Co-Operation and Development 2017. OECD Digital Economy Outlook 2017. Retrieved from http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/oecd-digital-economy-outlook-2017_9789264276284-en#.Wd3ppFu0PKk#page1

The Security Committee of Finland 2018. *Suomen kyberturvallisuusstrategian toimeenpano-ohjelma vuosille 2017 -2020* [Implementation program for Finland's cyber strategy for 2017 – 2020]. PDF-document. Accessed on 27 July 2018. Retrieved from https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Toimeenpano-ohjelma-2017-2020-final.pdf

The Wall street journal 2017. The man who wrote those password rules has a new tip: N3v$r M1^d!. Accessed on 14 February 2018. Retrieved from https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118

Thycotic. Black Hat 2018 Hacker Survey Report. PDF-document. Accessed on 19 September 2018. Retrieved from https://thycotic.com/resources/black-hat-2018-survey/black-hat-2018-survey-thank-you/

Tekniikka & Talous 2018. *Hätäkeskuslaitos 112:n pimentymisestä: "Emme voi velvoittaa operaattoreita parempaan, yhteydet katkeavat, kun varavoima ehtyy"* [Emergency Center's response about blackout of emergency number 112: "We can not force operators to improve their backup systems, connections break when the reserve power runs out"]. Accessed 15 November 2018. Retrieved from https://www.tekniikkatalous.fi/talous_uutiset/yritykset/hatakeskuslaitos-112-n-pimentymisesta-emme-voi-velvoittaa-operaattoreita-parempaan-yhteydet-katkeavat-kun-varavoima-ehtyy-6694849

Tekniikka & Talous 2018. *Viestintävirasto Elisa-häiriöstä: Varayhteydet tulisi testata etukäteen – kaikkea ei pitäisi laittaa yhden yhteyden päähän* [FICORA on the Elisa disturbance: Backup connections should be tested in advance - not all should be behind same connection]. Accessed on 18 May 2018. Retrieved from https://www.tekniikkatalous.fi/tekniikka/ict/viestintavirasto-elisa-hairiosta-varayhteydet-tulisi-testata-etukateen-kaikkea-ei-pitaisi-laittaa-yhden-yhteyden-paahan-6725297

Terveystalo 2018. Terveystalo in brief. Accessed on 9 April 2018. Retrieved from https://www.terveystalo.com/en/Company/Terveystalo-in-brief/

Tieto 2013. *Tietoteko 2013 -palkinto Etelä-Pohjanmaan sairaanhoitopiirille* [2013 Tietoteko award to the Hospital District of South Ostrobothnia]. Accessed on 7 July 2018. Retrieved from https://www.tieto.fi/uutiset/tietoteko-2013-palkinto-etela-pohjanmaan-sairaanhoitopiirille

Tilastokeskus 2008. Liitetaulukko 1. *Suurimmat naisten ammattiryhmät (naisia 90–100 % ammattiryhmästä) vuonna 2008* [Appendix table 1. The largest professional women-dominated groups (90-100% women of the group) in 2008. Accessed on 16 Septemeber 2018. Retrieved from https://www.stat.fi/til/tyokay/2008/04/tyokay_2008_04_2010-12-03_tau_001_fi.html

Tilastokeskus 2018. *Väestö* [Population structure]. Accessed on 16 September 2018. Retrieved form https://www.tilastokeskus.fi/tup/suoluk/suoluk_vaesto.html

Turvallisuuskomitea 2015. *Suomen kyberturvallisuusstrategia* [Finnish cyber strategy]. Accessed on 11 December 2017. Retrieved from https://www.turvallisuuskomitea.fi/index.php/fi/component/k2/14-suomen-kyberturvallisuusstrategia

Tuulivoimayhdistys 2017. *Miksi tuulivoima tarvitsee tukea?* [Why wind power needs (financial) support?]. Accessed on 8 December 2017. Retrieved from http://www.tuulivoimayhdistys.fi/tietoa-tuulivoimasta/tietopankki-tiiviisti-tarkeista-kysymyksista/miksi-tuulivoima-tarvitsee-tukea

TVO 2017. Plant supplier informs that regular electricity production of Olkiluoto 3 EPR starts in May 2019. Accessed on 8 December 2017. Retrieved from http://tvo.fi/news/1918

US-CERT 2017. HTTPS Interception Weakens TLS Security. Accessed on 24 March 2018. Retrieved from https://www.us-cert.gov/ncas/alerts/TA17-075A

U.S. CIO 2018. The HTTPS-Only Standard. Accessed on 20 March 2018. Retrieved from https://https.cio.gov/

Veracityglobal 2018. Power over Ethernet (POE) Explained. Accessed on 12 February 2018. Retrieved from http://www.veracityglobal.com/resources/articles-and-white-papers/poe-explained-part-1.aspx

Violino, .B 2017. What is SaaS? The modern way to run software. Accessed on 13 March 2018. Retrieved from https://www.infoworld.com/article/3226386/saas/what-is-saas-the-modern-way-to-run-software.html

Webropol 2018. *Webropol Oy:n asiakas-ja käyttäjärekisterin tietosuojaseloste* [Webropol Customer and User Register Privacy Statement]. PDF-document. Accessed on 18 August 2018. Retrieved from http://webropol.fi/gdpr/Tietosuojaseloste%20k%C3%A4ytt%C3%A4j%C3%A4-%20ja%20asiakasrekisterist%C3%A4.pdf

Worldbank 2016. Infographic: Poverty and Shared Prosperity 2016 - Taking on Inequality. Accessed on 5 November 2017. Retrieved from http://www.worldbank.org/en/news/infographic/2016/10/02/infographic-poverty-and-shared-prosperity-2016-taking-on-inequality

World Health Organization 1946. Constitution of the World Health Organization. PDF-document. Accessed on 28 October 2017. Retrieved from http://apps.who.int/gb/bd/PDF/bd47/EN/constitution-en.pdf

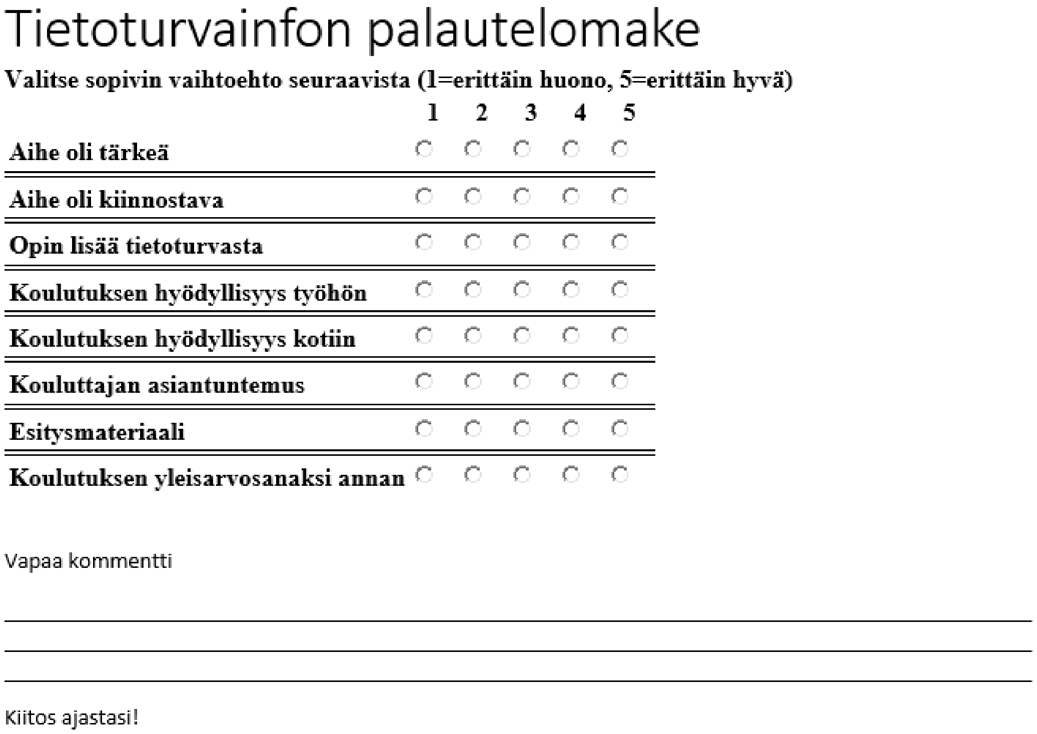
World Health Organization 2015. New report shows that 400 million do not have access to essential health services. Accessed on 28 October 2017. Retrieved from http://www.who.int/mediacentre/news/releases/2015/uhc-report/en/

Yao, M. 2017. Your Electronic Medical Records Could Be Worth $1000 To Hackers. Accessed on 19 July 2018. Retrieved from https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#243eca2e50cf

Ylipartanen, A. 2004. *Tietosuoja terveydenhuollossa* [Data protection in healthcare] 2nd ed. Helsinki: Tietosanoma

Appendices

Appendix 1. Survey 1 Form



Tietoturvainfon palautelomake

Valitse sopivin vaihtoehto seuraavista (1=erittäin huono, 5=erittäin hyvä)

	1	2	3	4	5
Aihe oli tärkeä	○	○	○	○	○
Aihe oli kiinnostava	○	○	○	○	○
Opin lisää tietoturvasta	○	○	○	○	○
Koulutuksen hyödyllisyys työhön	○	○	○	○	○
Koulutuksen hyödyllisyys kotiin	○	○	○	○	○
Kouluttajan asiantuntemus	○	○	○	○	○
Esitysmateriaali	○	○	○	○	○
Koulutuksen yleisarvosanaksi annan	○	○	○	○	○

Vapaa kommentti

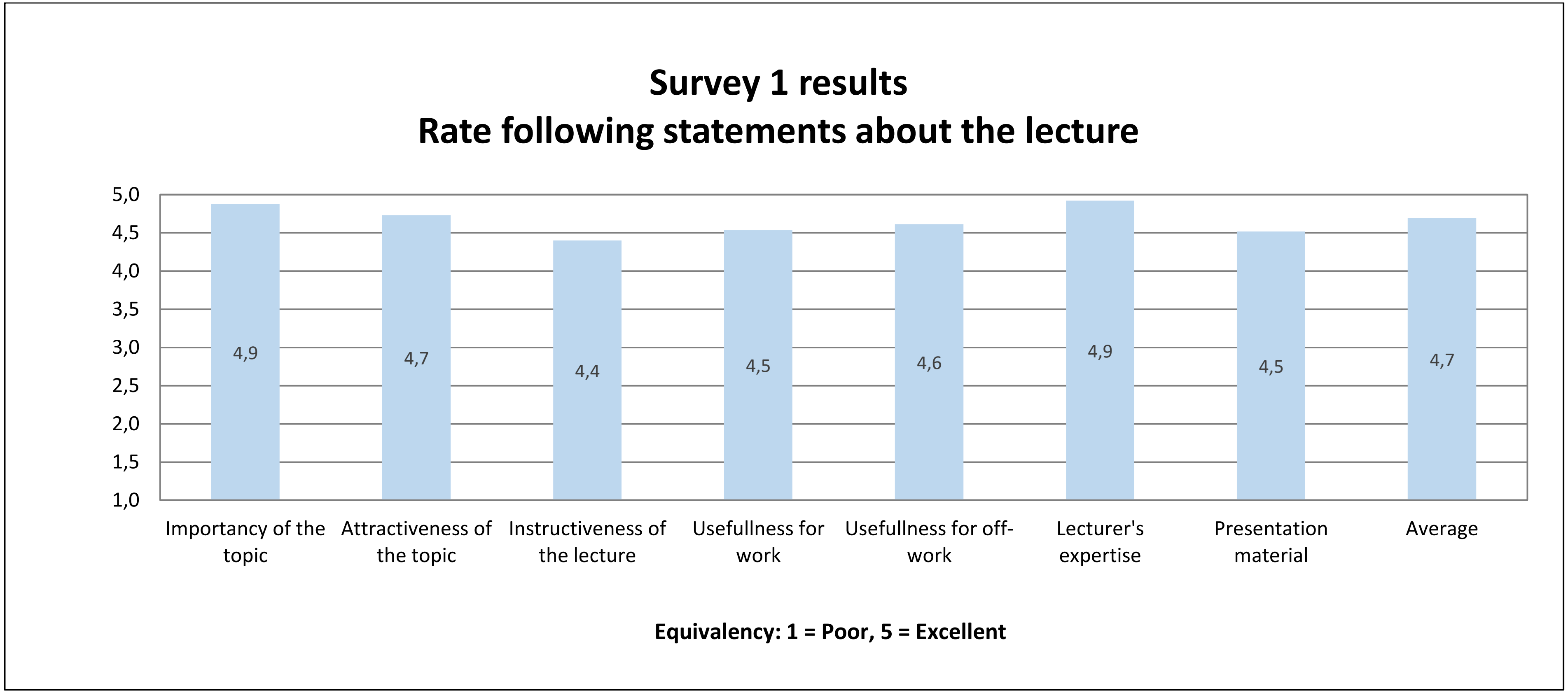
____

____

____

Kiitos ajastasi!

Appendix 2. Survey 1 Results



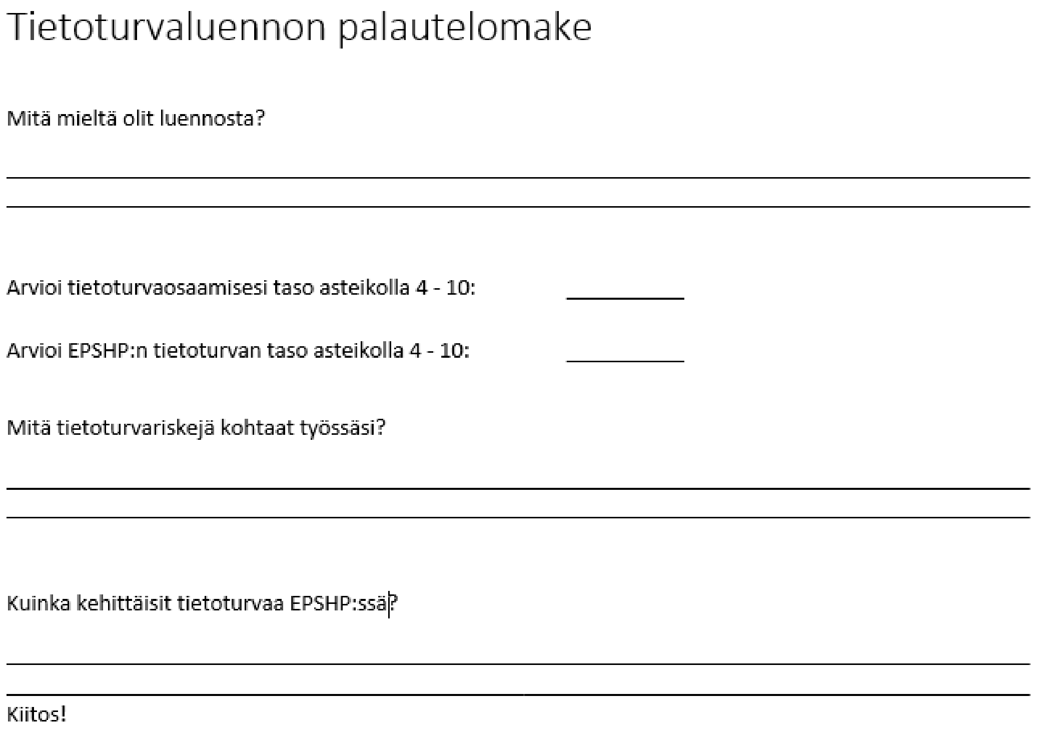
Survey 1 results
Rate following statements about the lecture

Equivalency: 1 = Poor, 5 = Excellent

Appendix 3. Survey 1 Feedback

ERITTÄIN HYVÄ!
Mielenkiintoisesti ja ymmärrettävästi kerrottu. Sai vastauksia
Selkeä ilmaisu. Kiitos! :)
Herätti ajatuksia, liikaa tuudittunut turvallisuuden tunteeseen
Hyvää perustietoa, voisi olla pidempikin luento
Tietoturvaesimerkit olivat parhainta antia
Hyvä asiantunteva esittäjä :)
Olisi paljon opittavaa, lähinnä uhat!
Opin lisää tietoturvasta todellakin!
Kiitos!
Hyvät esimerkit eri tilanteista. Uutisartikkelit oli hyviä!
Miellyttävän rauhallinen esittäjä ja esitystapa!
Hyvää muistutusta vaikka asiasta jotain tietääkin. Hyvä tyyli luennoitsijalla. Hyvä huumori!
Oli hyvä palauttaa asia mieleen ja miettiä muutoksia
Hyvä muistuttaa välillä tärkeistä asioista!!
Iso Kiitos! Tärkeä asia
Tosi mielenkiintoinen luento
Mielenkiintoinen luento vaikka aiheen olisi voinut luulla olevan tylsempi :)
:)
OK!
Kiitos!
Monipuolinen ja kattava esitys. Tuli hyviä muistutuksia
Kiitos, hyvää tietoa käytäntöön!
Hyvä ja kattava infopläjäys
Kiitos!
Tämä on erittäin tärkeää ja tätä koulutusta voisi päivittää säännöllisesti
Todella ajankohtainen ja tärkeä aihe
Hyvä ja kiinnostava esitys

Appendix 4. Survey 2 Form



Tietoturvaluennon palautelomake

Mitä mieltä olit luennosta?

Arvioi tietoturvaosaamisesi taso asteikolla 4 - 10: __________

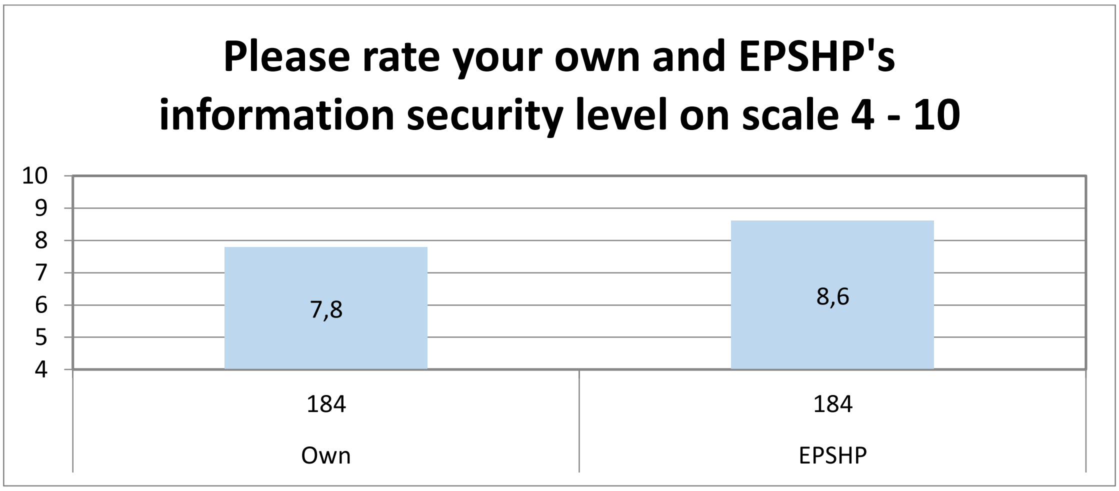
Arvioi EPSHP:n tietoturvan taso asteikolla 4 - 10: __________

Mitä tietoturvariskejä kohtaat työssäsi?

Kuinka kehittäisit tietoturvaa EPSHP:ssä?

Kiitos!

Appendix 5. Survey 2 Results



Appendix 6. Survey 2 Feedback

Mitä mieltä olit luennosta?
Hyvää ja ajankohtaista asiaa selkeästi esitettynä
Hyvä luento. Kattava ja ymmärrettävä
OK
Ne jotka eniten luentoa tarvitsivat eivät tulleet paikalle
Ihan jees
Asiallinen ja selkeä, tosin uutta tietoa ei paljoa tullut
Hyvä kokonaisuus
Hyvä tietoisku
Ok
Luento oli hyvä. Sain myös hieman uutta tietoa
Hyvä luento. Paljon oleellista tietoa
Ihan mielenkiintoinen luento
OK
Hyvä
Hyvä
Hyvä
Kattava kooste, sopivan konkreettisella tasolla
Erittäin hyvä, huomioiden ettei aihe ole sydämmellä päivittäin
Asiallinen ja tarpeellinen luento
Hyvä muistutus perusasioista
Tarkemmin olisi voinut potilasasiakirjojen käsittelyä ja oikeuksia käydä effican eri osa-alueilla. Arkistokatselu, C-reseptit
Ihan ok
Yleissivistävä
En tiedä tuliko siinä ainakaan minulle kauheasti uutta asiaa
Hyvä, mielenkiintoista asiaa. Tärkeä
Hyvä
Oikein hyvä!
Hyvää yleistietoa ATK-asioista
Hyvä kokonaisuus. Tärkeää asiaa
Mielenkiintoinen
Hyvä muistutus järjen käytöstä
Monipuolinen ja kattava. Herätti ajatuksia siviilielämän nettikäyttäytymisestä
Hyvä luento, helpolla kielellä viritetty asiat
Mielenkiintoisia ja herättäviä esimerkkejä
Tarpeellinen ja kiinnostava

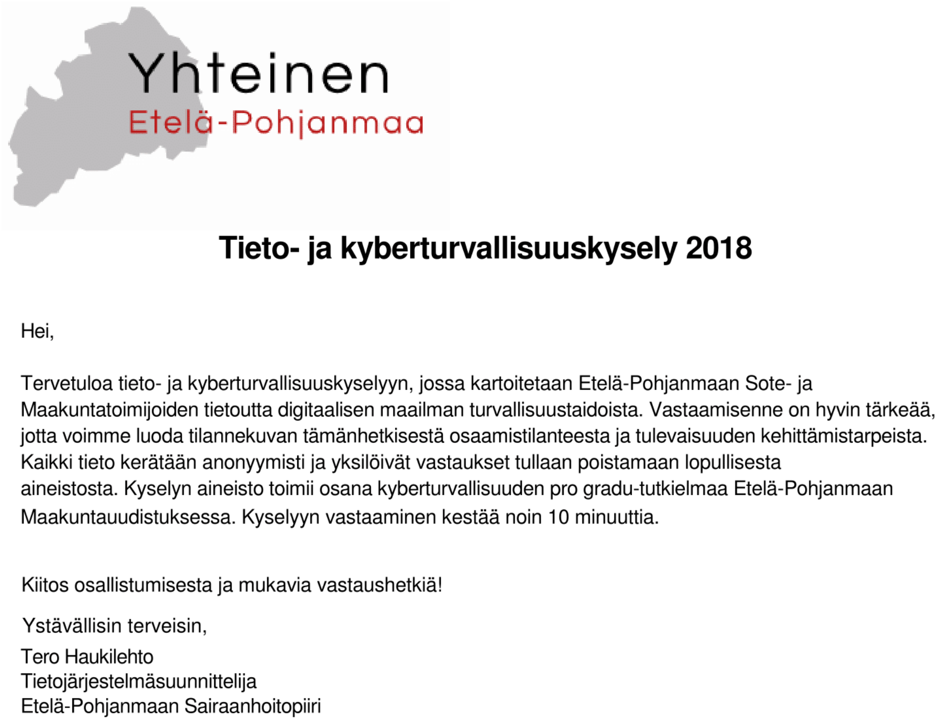
Hyödyllinen
Hyvää ja ajankohtaista asiaa
Hyvä!
Hyvä oli
Oli hyvä ja monipuolinen. Paljon kiinnostavaa ja uutta
Hyvä, asiallinen
Hyvää asiaa tuli
Paljon hyödyllistä asiaa, selkeästi esitettynä
OK!
Tuli paljon tarpeellista tietoa HYVÄ!!!
Todella hyvä. Näitä "muistutus" luentoja saisi olla ainakin kerran vuodessa
Hyvä ja tarpeellinen luento. Näitä saisi olla vähintään kerran vuodessa
Luento oli kattava ja pisti miettimään
Erittäin hyvä
Erittäin hyvä, sujuva, luonteva, selkeä, paljon hyvää tietoa helposti lähestyttävä luennoitsija
Todella valaiseva! Hyödyllistä tietoa ja hyvä muistutus tietoturvan haavoittuvuudesta. -Kiitos-
Hyvä luento ja asia eritätin ajankohtaisia. Antoi ajattelemisen aihetta, vaikka asioista osa oli jo tuttujakin.
Asiallinen, monipuolinen
Paras luento aikoihin, tykkäsin
Erittäin hyvää tietoa, selkeästi esitetty
Loistava, luetettava, asiallinen
Hyödyllinen, esimerkit hyviä
Erittäin hyvää tietoa
Todella hyvä luento, herättelevä!
Hyvää tietoa
Hyvää tietoa,asiantuntevaa.
Erittäin hyvä ja hyödyllinen
Aivan hyvä, itselle ei oikeastaan mitään uutta. Hyvää kertausta
Tarpeellinen, napakka
Todella hyvä, tärkeää kerrata asioita, vaikka olisivat tuttujakin
Hyvä käydä vuosittain läpi tämä tietoturvaluento kaikkine pelotteineen
Hyvä, kattava
Kiinnostava ja todella tarpeellinen
Asiaa!
Älyttömän hyvä :) kiitos
Paljon hyvää asiaa. Luento syytä toistaa aika ajoin. Selkeä esitys
Hyvä ja hyödyllinen
Aiheellinen
Monipuolinen

Paljon hyvää tietoa
Todella hyvä ja asiantunteva luento. Hyvä muistutella mieliin asioita turvallisuudesta
Hyvä ja mielenkiintoinen
Tarpeellinen , avasi silmiä!!
Hyvä ja monipuolinen, selkeä luento
Herätti oman tietosuojan huonoa osaamista
Hyvä että asiaa oli myös yksityiselämän puolelta huomioitavista asioista
Hyvä ja tärkeä luento
Asiallista tietoa ja herättää ajatuksia. Muutama asia itselläkin parannettavana
Tieto lisää tuskaa
Hyvä luento
Hyvä
Tärkeää asiaa
Paljon hyödyllistä tietoa
Sopivasti tärkeää asiaa
Selkeää ohjeistusta, hyvä diaesitys, hyviä esimerkkitapauksia
Hyvä luento edelleen
Selkeää ja paljon hyvää tietoa tuli
Selkeä ja informatiivinen luento
Hyvää asiaa ja kertausta tietoturva-asioista
Hyvä luento ja luennoitsija
Erittäin hyvä ja selkeä, herätti paljon ajatuksia ja muutan toimintatapoja työpaikalla
Hyvä luento! Herätti paljon ajatuksia. Hyvä muistutus tietoturvaan
Ihan hyvältä vaikutti, mitä kerkesin olla. Näki nyt mustaa valkosella
Hyvä! Ytimekäs, johdonmukainen, oleellisiin asioihin keskitytty ja ymmärrettävästi esitetty
Ihan OK, asia jota pitää ajoittain muistuttaa
Lyhyt, Ytimekäs, ajankohtainen
Paljon oli hyvää asiaa
Sopivan monipuolinen
Hyvä, tosin ei enää tee mieli tehdä mitään netissä
Mielenkiintoinen, ajankohtaista asiaa
Erittäin hyvä ja kattava
OK! Hyvä oli
Erittäin hyvä ja tarpeellinen. Selkeä esitys
Erittäin hyvä ja "silmiä avaava" luento
Luennolla tuli ilmi monta sellaista asiaa mitä ei ole tullut ennen ajatelleeksi. Tylsästä asiasta sait mielenkiintoisen!
Hyvä luento, hyvää tietoa työhön ja siviiliin
Selvä ja hyvä luento

Hyvä luento, mielenkiintoinen
Oli hyvä luento, Aina hyvä kerrata
Hyvä
Kattava ja selkeä luento
Avartava ja laittaa miettimään asioita mitä netti tarjoaa / ottaa
Hyvä! Aiheellinen! Tärkeää!
Hyvä ja tarpeellinen luento
Hyvä ottaa asioita esille
Tarpeellinen esitys
OK
Asiallista, Tärkeää asiaa
Hyvä ulosanti
Hyvää asiaa, Sai ajatuksia aikaan
Hyvää asiaa
Hyvää kertausta asiasta, Herätti ajateltavaa, Selkeä esitys
JES!
Todella hyvä ja tarpeellinen
Hyvä, Aina aihetta muistutella asiasta
Ok
Hyvä, Selkeä, Asiallinen, Tiivis paketti
Hyvä
Hyvä, Selkeä
Hyvä, Ajatuksia herättävä
Mielenkiintoinen, Herättelevä luento
Tarpeellinen, Käytännönläheinen
Monipuolinen ja Valaiseva
Todella mielenkiintoinen ja Sain paljon uutta tietoa
Tosi Mielenkiintoinen. Puhuttiin asioista selkeästi
Selkeä, Hyvä luento. Paljon uutta tietoa
Asiallinen ja Hyvä, Kiitos!
Hyvä ja Selkeä luento
Oikein hyvä
Tarpeellinen luento
Hyvä luento, Selkeä luennoitsija
Hyvä, Vanhaa ja uutta tietoa. Hyvää muistutusta
Hyvä luento. On aina tärkeää muistuttaa salasanoista ja olemasta liian sinisilmäinen netissä! Vaikka asiat "tietää", niin silti hyvä muistuttaa!
Hyvä ja selkeä. Paljon tarpeellista tietoa myös kotiin
Tärkeät asiat tuli hyvin esille

Ihan hyvä, Tarpeellinen, Hyvä muistuttaa
Hyvä luento. Kiitos
Hauska ja Selkeäsanainen
Hyvä ja Tarpeellinen, Yllättäviäkin asioita tuli mietittäväksi
Sopivan pituinen ja Selkeä, Ymmärrettävä. Hyvää tietoa tuli. Sai muistutuksen miten tulee toimia
Mielenkiintoinen
Hyvä luento, Paljon asiaa johon sai varmistusta
Monipuolinen, Hyvä sisältö
Hyvää perustietoa tietoturvasta
Erittäin hyvä ja Tarpeellinen
Hyvä luento, Ajatuksia herättävä
Hyvä, Ytimekäs
Hyvää yleistajuista tietoa, Ei menty liian syvälle teknisiin yksityiskohtiin, mutta tuli uusiakin asioita esiin
Hyvää tietoa tärkeistä asioista! Näistä asioista on hyvä saada tietyin väliajoin muistutusta
Hyvä, Ajankohtainen, Ei liian simppeli muttei liian tekninenkään
Mielenkiintoinen
Hyvä ja Informaatiorikas
Hyvä luento! Sai varmuutta asioihin
Hyödyllinen kertaus ja jotain uuttakin
Valaiseva luento, Laittoi miettimään
Yksinkertaisesti ja ymmärrettävästi kerrottu tärkeästä asiasta
Hyvä, Luennoitsija puhui selvästi
Hyvä luento
Asiasisältö hyvä ja Tarpeellinen, Hyvää keskustelua ja vastauksia sai kysymyksiin
Monipuolinen, Ei pelkästään työhön liittyvää
Ihan ok
Asiallinen, Selittävä, Tehokas tietoisku
Mielenkiintoinen, Ajatuksia herättävä
Hyvä, Tärkeää Asiaa
Hyvä, Sisälsi Tärkeää Tietoa
Hyvä, Tarpeellinen
Hyvä luento, Opettavainen
Erittäin Hyvä
Erinomaisen Mielenkiintoinen, Hyvä Esitys

Appendix 7. Survey 3 Form



Yhteinen
Etelä-Pohjanmaa

Tieto- ja kyberturvallisuuskysely 2018

Hei,

Tervetuloa tieto- ja kyberturvallisuuskyselyyn, jossa kartoitetaan Etelä-Pohjanmaan Sote- ja Maakuntatoimijoiden tietoutta digitaalisen maailman turvallisuustaidoista. Vastaamisenne on hyvin tärkeää, jotta voimme luoda tilannekuvan tämänhetkisestä osaamistilanteesta ja tulevaisuuden kehittämistarpeista. Kaikki tieto kerätään anonyymisti ja yksilöivät vastaukset tullaan poistamaan lopullisesta aineistosta. Kyselyn aineisto toimii osana kyberturvallisuuden pro gradu-tutkielmaa Etelä-Pohjanmaan Maakuntauudistuksessa. Kyselyyn vastaaminen kestää noin 10 minuuttia.

Kiitos osallistumisesta ja mukavia vastaushetkiä!

Ystävällisin terveisin,

Tero Haukilehto
Tietojärjestelmäsuunnittelija
Etelä-Pohjanmaan Sairaanhoitopiiri

Valitse nykyinen organisaatiosi *

○ Aluehallintovirasto

○ Eskoon sosiaalipalvelujen kuntayhtymä

○ Etelä-Pohjanmaan ELY-keskus

○ Etelä-Pohjanmaan Liitto

○ Etelä-Pohjanmaan Sairaanhoitopiiri

○ JIK-peruspalveluliikelaitoskuntayhtymä

○ Järvipohjanmaan perusturva

○ Kuntayhtymä Kaksineuvoinen

○ Kuusiolinna Terveys Oy

○ Lapuan kaupunki

○ Pelastuslaitos

○ Seinäjoen kaupunki

○ Suupohjan peruspalveluliikelaitoskuntayhtymä

○ TE-toimisto

○ Muu, Mikä? ____________________________

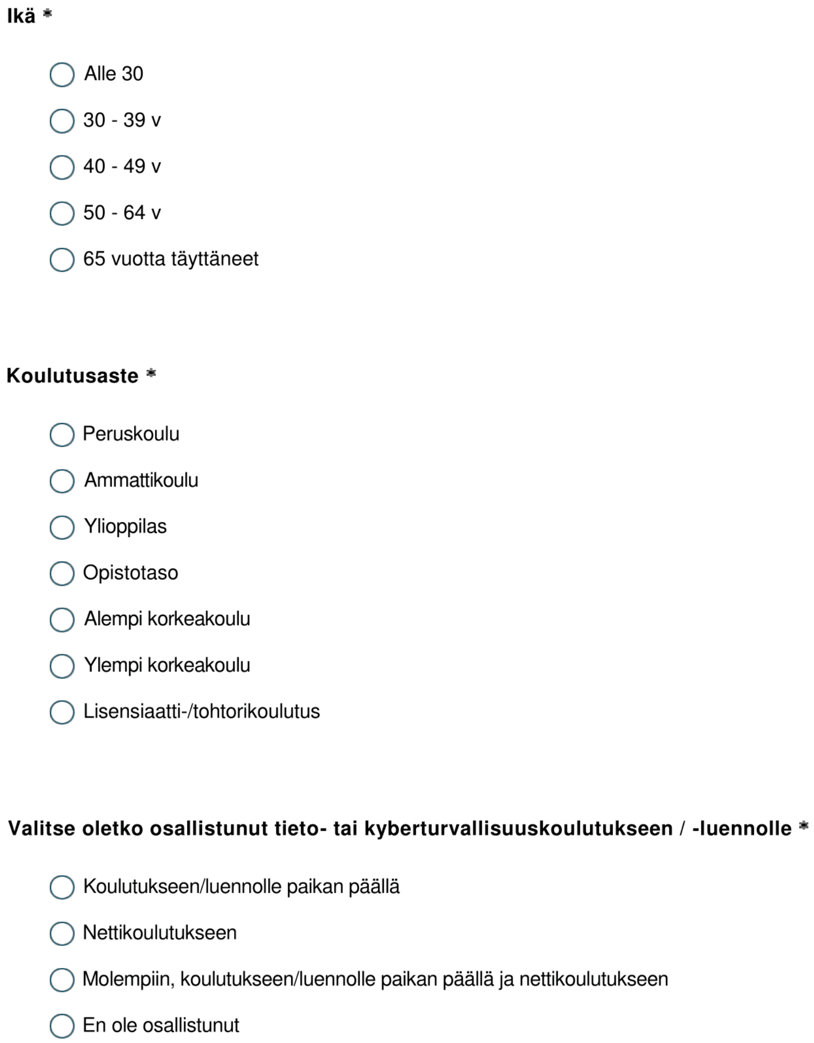
Esitiedot

Sukupuoli *

○ Nainen

○ Mies

○ Muu



Ikä *

○ Alle 30

○ 30 - 39 v

○ 40 - 49 v

○ 50 - 64 v

○ 65 vuotta täyttäneet

Koulutusaste *

○ Peruskoulu

○ Ammattikoulu

○ Ylioppilas

○ Opistotaso

○ Alempi korkeakoulu

○ Ylempi korkeakoulu

○ Lisensiaatti-/tohtorikoulutus

Valitse oletko osallistunut tieto- tai kyberturvallisuuskoulutukseen / -luennolle *

○ Koulutukseen/luennolle paikan päällä

○ Nettikoulutukseen

○ Molempiin, koulutukseen/luennolle paikan päällä ja nettikoulutukseen

○ En ole osallistunut

Työnkuva *

○ Lääkärit

○ Sairaanhoitajat ja muut vastaavat henkilöt

○ Tutkimus- ja hoitohenkilöt

○ Tutkimusta ja hoitoa avustavat henkilöt

○ Muut hoitohenkilöt

○ Sosiaalitoimen henkilöt

○ Huoltohenkilöt

○ Tietohallinnon tehtävissä toimivat henkilöt

○ Hallinto- ja taloushenkilöt, muut kuin tietohallinnon henkilöt

○ Pelastushenkilöt

○ Aluekehityspalveluhenkilöstö

○ Muu, mikä?

Tietohallinnon henkilöille suunnattuja kysymyksiä siitä kuinka toimisit eri tilanteissa.
Mikäli et kuulu tietohallinnon henkilöstöön, ole hyvä ja valitse sivun alareunasta edellinen.

Käyttäjä ilmoittaa avanneensa epämääräisen sähköpostiviestin liitetiedoston ja hänen koneensa käyttäytyy oudosti, kerro lyhyesti kuinka toimisit. *

Käyttäjän koneella on kiristyshaittaohjelma, kerro lyhyesti kuinka toimisit. *

Sinulle entuudestaan tuntematon henkilö esim. remontoija, pyytää pääsyä konesaliin tai laitetilaan, kerro lyhyesti kuinka toimisit. *

Käyttäjä tuo sinulle muistitikun, jossa epäilee olevan viruksia, kerro lyhyesti kuinka toimisit. *

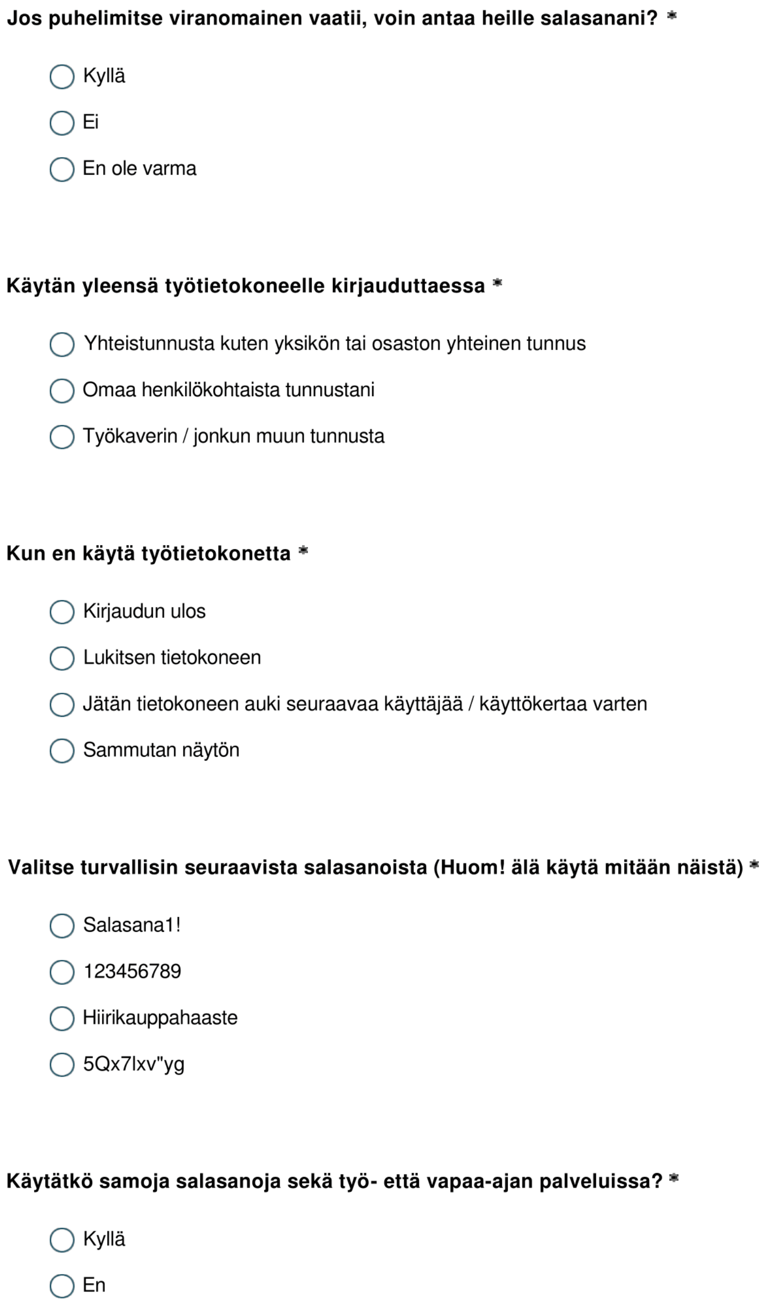
Valitse sopivin vaihtoehto kuvaamaan miten toimit eri tilanteissa

Jos puhelimitse ATK-tuki vaatii, voin antaa heille salasanani? *

○ Kyllä

○ Ei

○ En ole varma



Jos puhelimitse viranomainen vaatii, voin antaa heille salasanani? *

○ Kyllä

○ Ei

○ En ole varma

Käytän yleensä työtietokoneelle kirjauduttaessa *

○ Yhteistunnusta kuten yksikön tai osaston yhteinen tunnus

○ Omaa henkilökohtaista tunnustani

○ Työkaverin / jonkun muun tunnusta

Kun en käytä työtietokonetta *

○ Kirjaudun ulos

○ Lukitsen tietokoneen

○ Jätän tietokoneen auki seuraavaa käyttäjää / käyttökertaa varten

○ Sammutan näytön

Valitse turvallisin seuraavista salasanoista (Huom! älä käytä mitään näistä) *

○ Salasana1!

○ 123456789

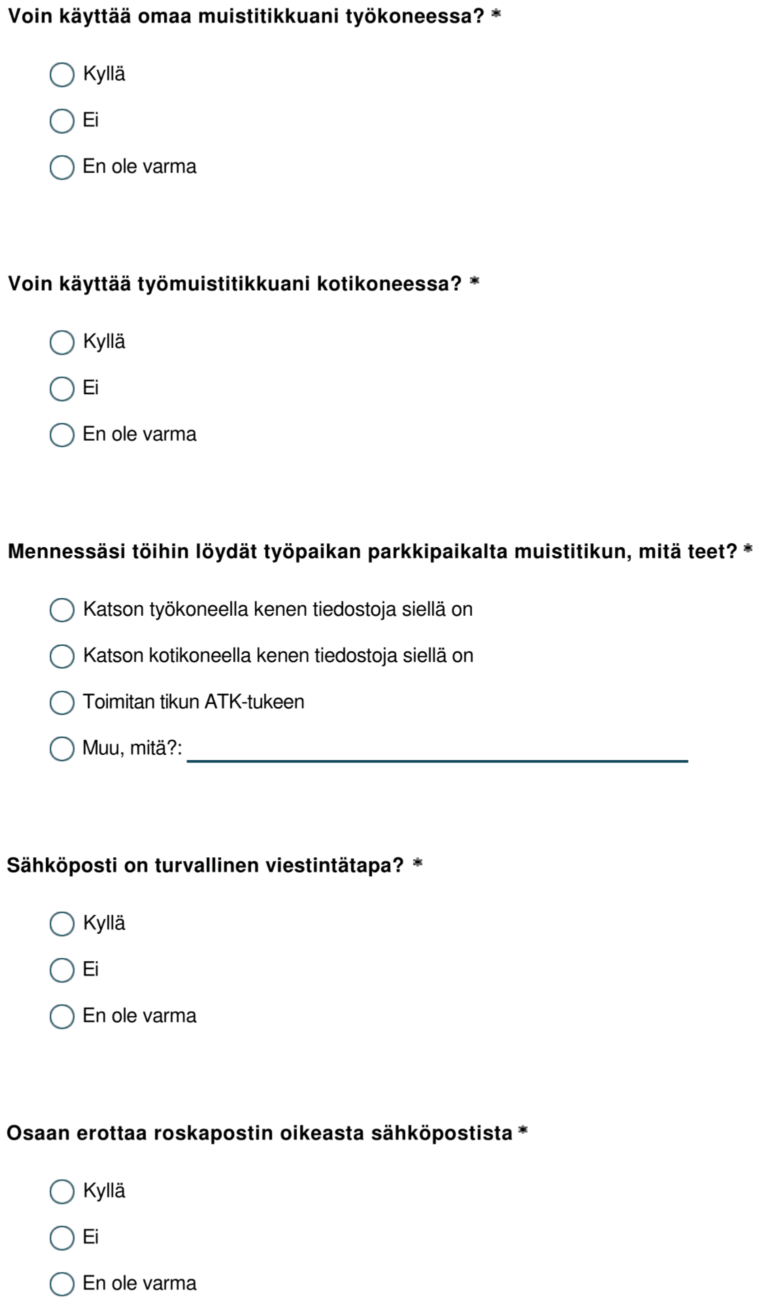
○ Hiirikauppahaaste

○ 5Qx7lxv"yg

Käytätkö samoja salasanoja sekä työ- että vapaa-ajan palveluissa? *

○ Kyllä

○ En



Voin käyttää omaa muistitikkuani työkoneessa? *

○ Kyllä

○ Ei

○ En ole varma

Voin käyttää työmuistitikkuani kotikoneessa? *

○ Kyllä

○ Ei

○ En ole varma

Mennessäsi töihin löydät työpaikan parkkipaikalta muistitikun, mitä teet? *

○ Katson työkoneella kenen tiedostoja siellä on

○ Katson kotikoneella kenen tiedostoja siellä on

○ Toimitan tikun ATK-tukeen

○ Muu, mitä?: ______________________________

Sähköposti on turvallinen viestintätapa? *

○ Kyllä

○ Ei

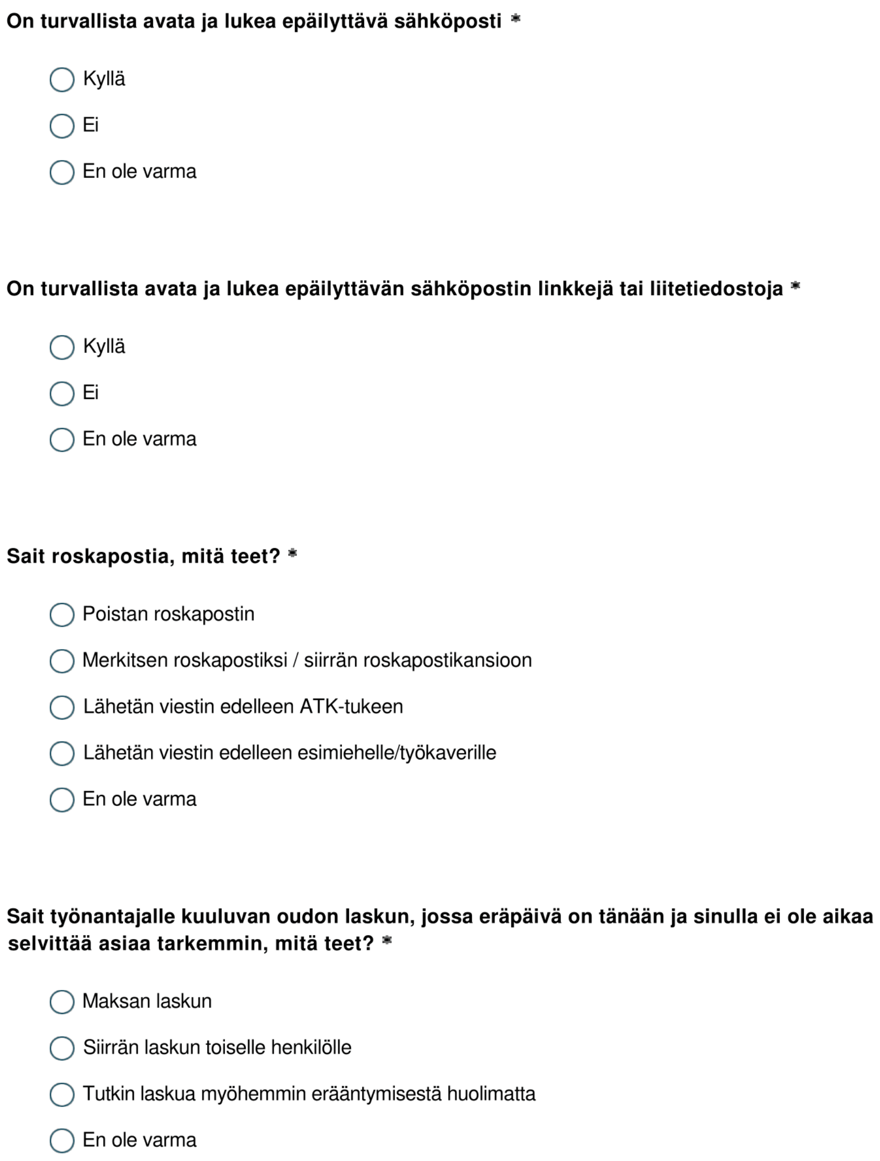
○ En ole varma

Osaan erottaa roskapostin oikeasta sähköpostista *

○ Kyllä

○ Ei

○ En ole varma



On turvallista avata ja lukea epäilyttävä sähköposti *

○ Kyllä

○ Ei

○ En ole varma

On turvallista avata ja lukea epäilyttävän sähköpostin linkkejä tai liitetiedostoja *

○ Kyllä

○ Ei

○ En ole varma

Sait roskapostia, mitä teet? *

○ Poistan roskapostin

○ Merkitsen roskapostiksi / siirrän roskapostikansioon

○ Lähetän viestin edelleen ATK-tukeen

○ Lähetän viestin edelleen esimiehelle/työkaverille

○ En ole varma

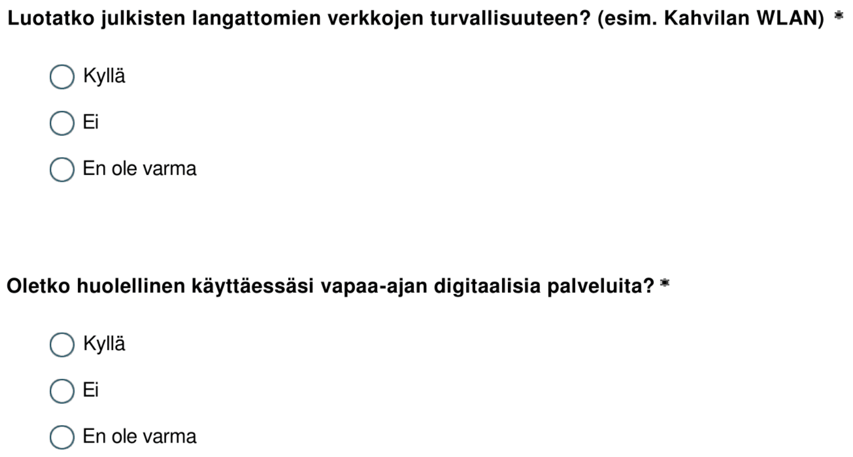
Sait työnantajalle kuuluvan oudon laskun, jossa eräpäivä on tänään ja sinulla ei ole aikaa selvittää asiaa tarkemmin, mitä teet? *

○ Maksan laskun

○ Siirrän laskun toiselle henkilölle

○ Tutkin laskua myöhemmin erääntymisestä huolimatta

○ En ole varma



Luotatko julkisten langattomien verkkojen turvallisuuteen? (esim. Kahvilan WLAN) *

○ Kyllä

○ Ei

○ En ole varma

Oletko huolellinen käyttäessäsi vapaa-ajan digitaalisia palveluita? *

○ Kyllä

○ Ei

○ En ole varma

Valitse sopivin vaihtoehto kuvaamaan tietämystäsi seuraavista aiheista *

	En tiedä lainkaan	Tiedän huonosti	Tiedän jonkin verran	Tiedän hyvin	En osaa sanoa
Mikä on päivitysten merkitys tieto- ja kyberturvallisuudelle?	○	○	○	○	○
Mitä ovat kiristyshaittaohjelmat ja miten ne leviävät?	○	○	○	○	○
Mitä ovat huijausviestit ja tietojenkalastelu?	○	○	○	○	○
Mikä on palvelunestohyökkäys?	○	○	○	○	○
Mitä ovat varmuuskopiot ja niiden käyttö?	○	○	○	○	○
Mitä riskejä on sosiaalisessa mediassa?	○	○	○	○	○
Mikä on tietoturvarajoitusten ja -ohjeistuksen merkitys?	○	○	○	○	○
Kuinka luottamuksellista tietoa tulee käsitellä?	○	○	○	○	○
Mikä on EU:n uusi tietosuoja-asetus ja kuinka se vaikuttaa minuun?	○	○	○	○	○
Mitä ovat tieto- ja kyberturvallisuuden tarjoamat mahdollisuudet?	○	○	○	○	○
Mitä tietoturvariskejä ja -vastuita liittyy ulkoistamiseen sekä laite- ja ohjelmistohankintoihin?	○	○	○	○	○
Mitä on informaatiovaikuttaminen?	○	○	○	○	○

Oletko esimiestyössä? *

○ Ei

○ Kyllä

Esimiehille tarkoitetut kysymykset.
Jos et ole esimiestehtävissä, ole hyvä valitse sivun alareunasta edellinen.

Valitse sopivin vaihtoehto kuvaamaan nykyistä tilannetta työssäsi *

	Täysin eri mieltä	Jokseenkin eri mieltä	Jokseenkin samaa mieltä	Täysin samaa mieltä	En osaa sanoa
Alaisillani on riittävät tieto- ja kyberturvallisuustaidot heidän työtehtäviinsä	○	○	○	○	○
Minulla on riittävät taidot opastamaan alaisiani heidän työnkuvaansa liittyvissä tieto- ja kyberturvallisuusasioissa	○	○	○	○	○

Valitse sopivin vaihtoehto kuvaamaan nykyistä tilannetta työssäsi *

	Täysin eri mieltä	Jokseenkin eri mieltä	Jokseenkin samaa mieltä	Täysin samaa mieltä	En osaa sanoa
Minulla on riittävät tieto- ja kyberturvallisuustaidot työtehtäviini	○	○	○	○	○
Tämä aihe on tärkeä ja siitä täytyy järjestää organisaatiossamme koulutusta	○	○	○	○	○
Tiedän mistä löydän organisaationi tietoturvaohjeet	○	○	○	○	○
Minua on ohjeistettu toimimaan erilaisissa tietoteknisissä häiriötilanteissa. Esimerkiksi jos koneellesi on tullut haittaohjelma tai työtehtävällesi kriittinen palvelu ei ole käytettävissä	○	○	○	○	○
Tiedän mistä saan lisää tietoa tai voin kysyä aiheeseen liittyvistä asioista?	○	○	○	○	○

Olen lukenut organisaationi tietoturvaohjeet? *

○ Olen lukenut

○ En ole lukenut

Minulle mieluisin tapa saada lisätietoa näistä asioista on: *

○ Tiedoittamalla. esim. sähköpostilla

○ Osallistumalla koulutukseen internetissä

○ Osallistumalla fyysisesti luennolle tai koulutukseen

○ En tarvitse lisätietoa näistä asioista

○ Muu, mikä? ____

Hienoa! Kaksi viimeistä kysymystä, joissa arvioit luottamustasi nykyisen ja tulevan maakunnan organisaatiosi tietojenkäsittelyyn.

Luotan siihen, että omat luottamukselliset tietoni ovat turvassa nykyisessä organisaatiossani? *

○ En luota lainkaan

○ Luotan, mutta en täysin

○ Luotan täysin

○ En osaa sanoa

Luotan siihen, että omat luottamukselliset tietoni ovat turvassa tulevassa maakuntaorganisaatiossani? *

○ En luota lainkaan

○ Luotan, mutta en täysin

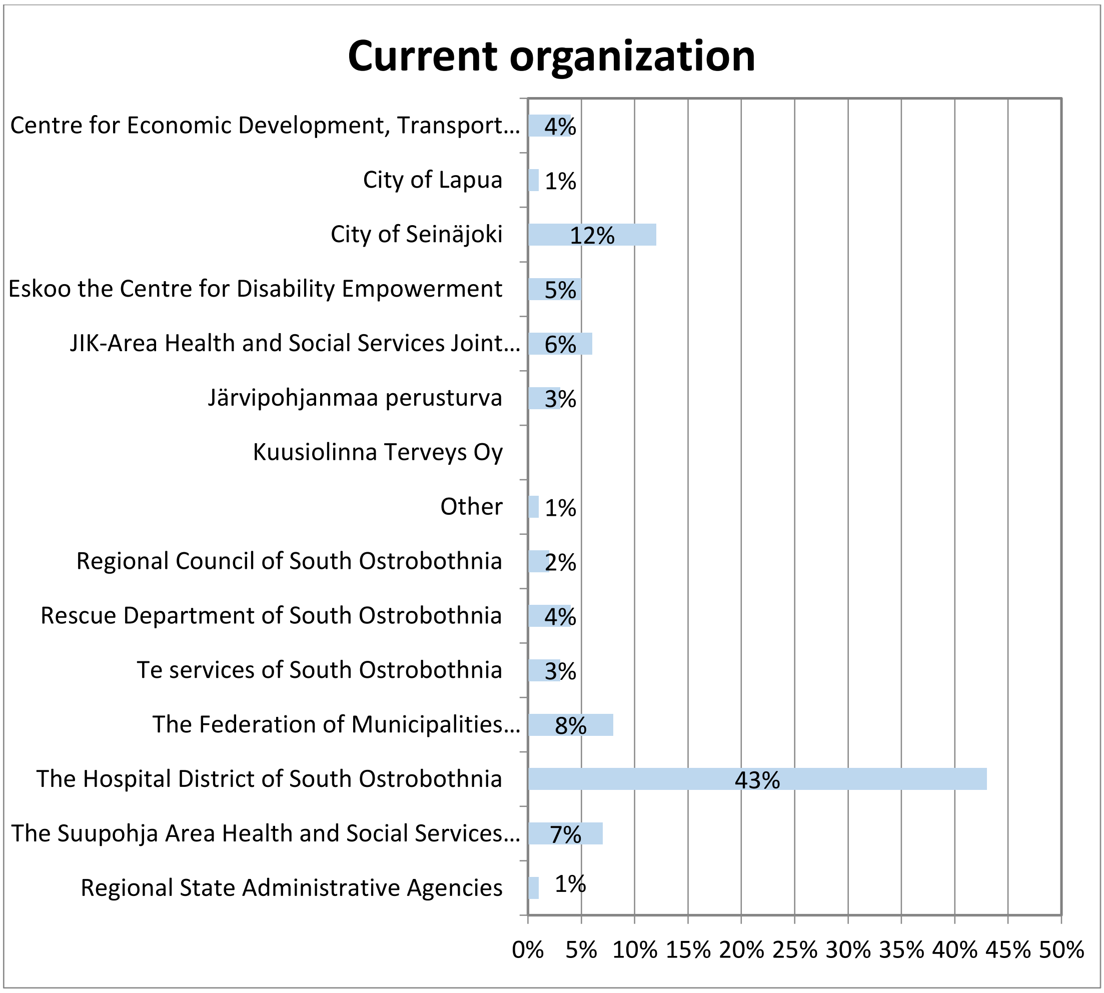
○ Luotan täysin

○ En osaa sanoa

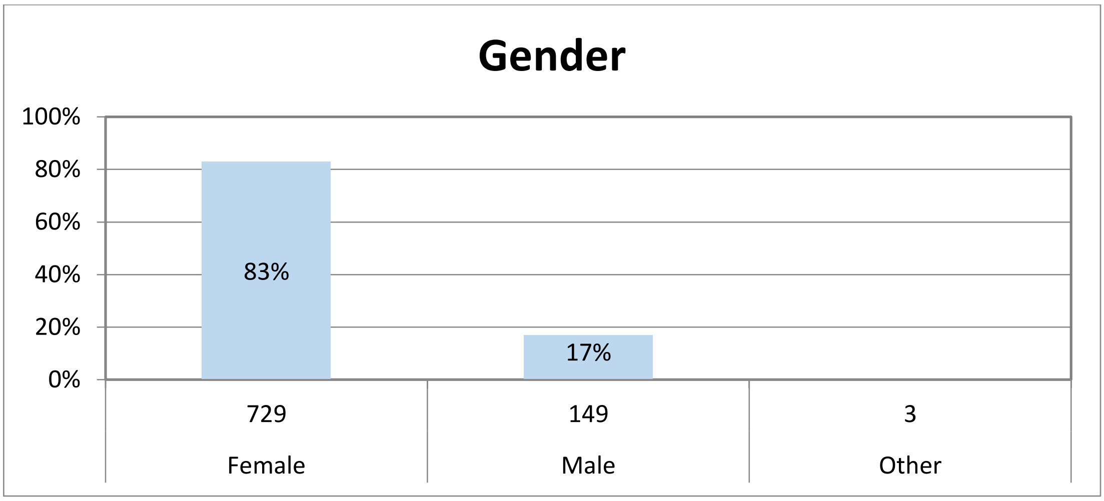
Mikäli haluat jättää palautetta, voit kirjoittaa sen alla olevaan tekstikenttään.

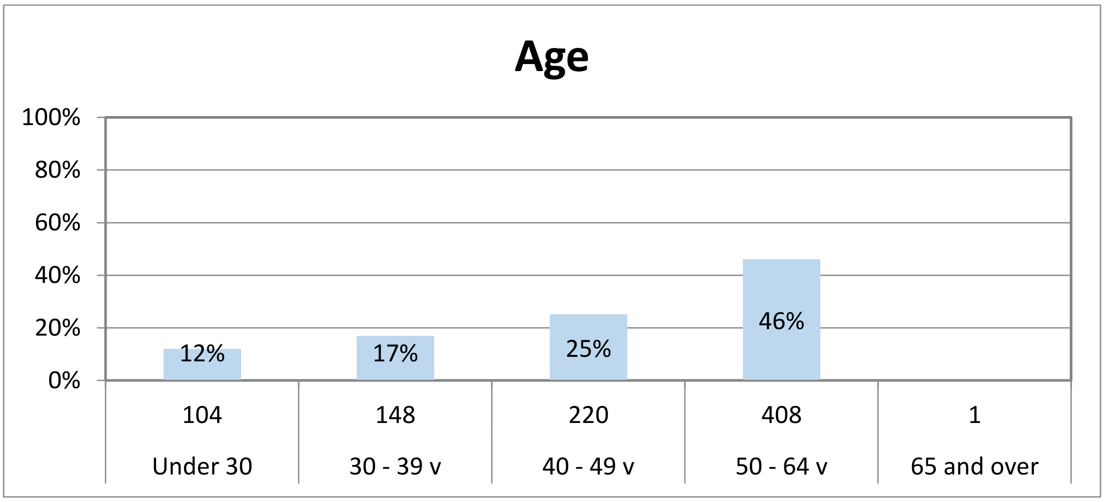
Lähetä vastauksesi painamalla Lähetä-painiketta.

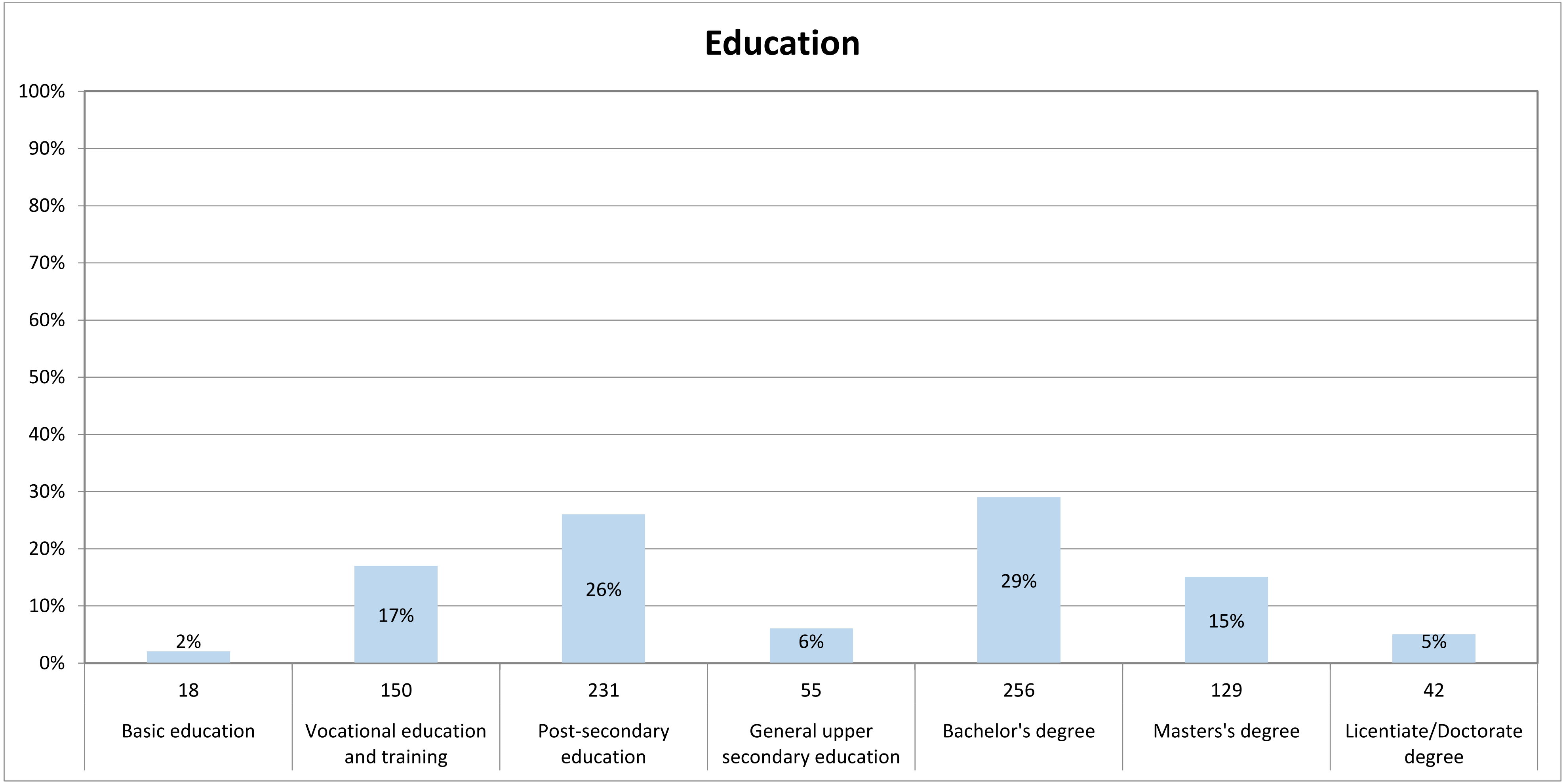
Appendix 8. Survey 3 results

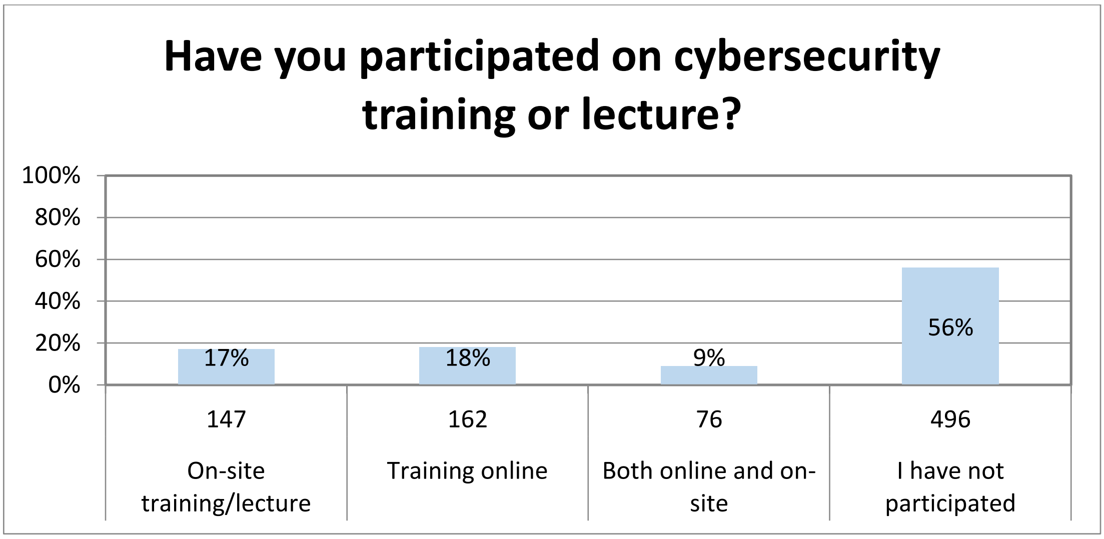


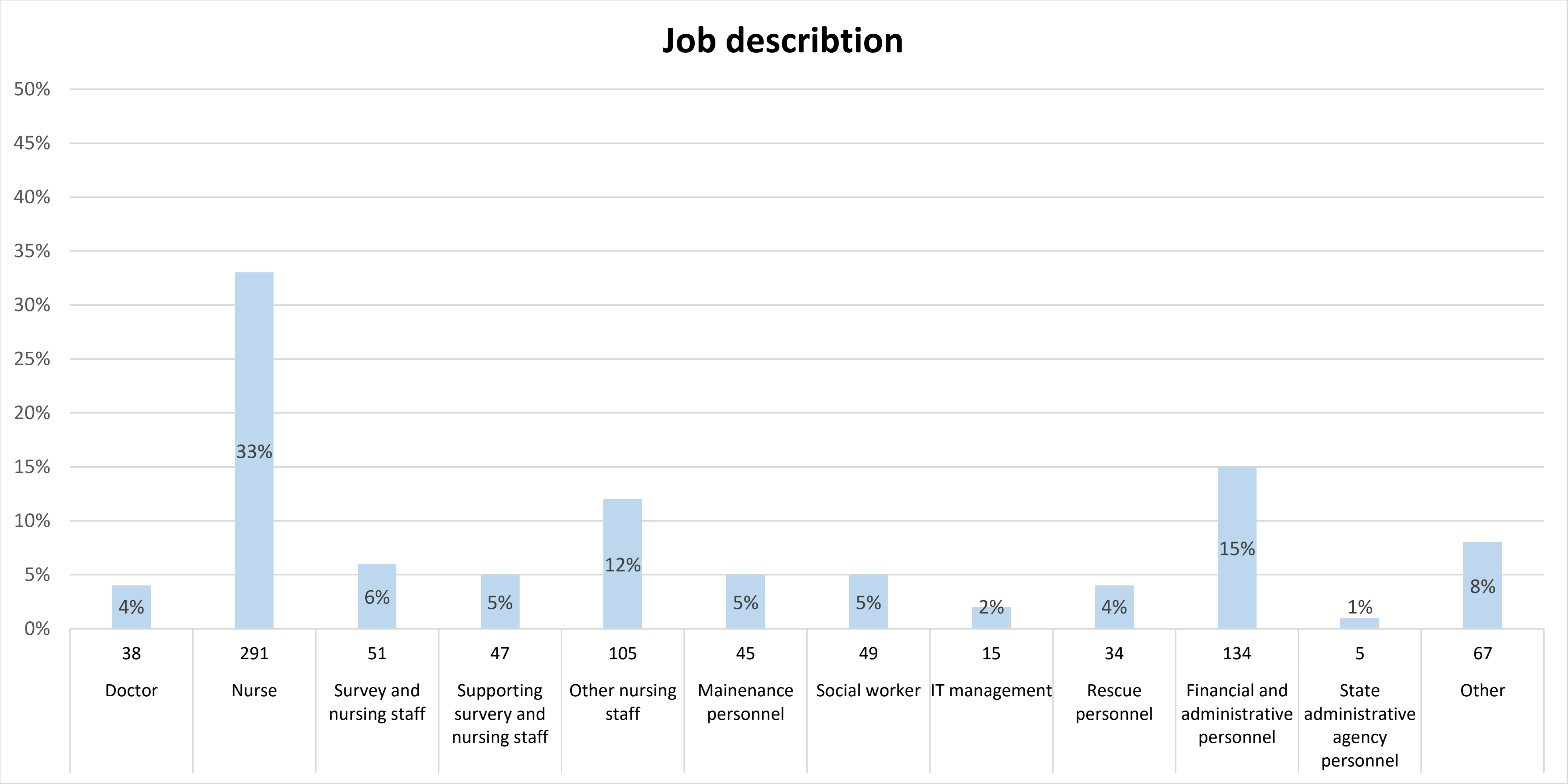
Organization	**Number of participants**
Centre for Economic Development, Transport and the Environment in South Ostrobothnia	36
City of Lapua	9
City of Seinäjoki	109
Eskoo the Centre for Disability Empowerment	47
JIK-Area Health and Social Services Joint Municipal Board	54
Järvipohjanmaa perusturva	22
Kuusiolinna Terveys Oy	1
Other	13
Regional Council of South Ostrobothnia	13
Regional State Administrative Agencies	11
Rescue Department of South Ostrobothnia	36
Te services of South Ostrobothnia	22
The Federation of Municipalities Kaksineuvoinen	71
The Hospital District of South Ostrobothnia	378
The Suupohja Area Health and Social Services Joint Municipal Board	59

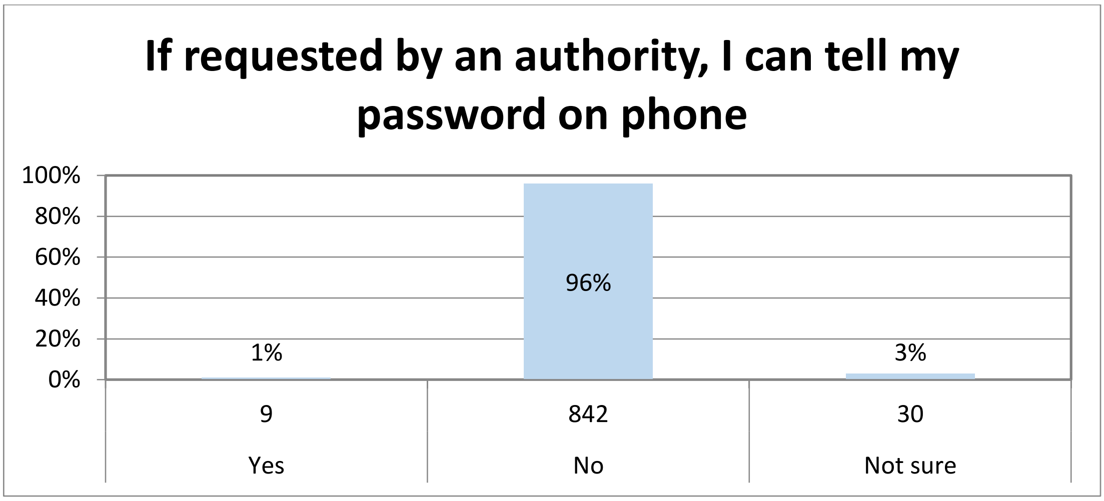

Gender
100%
80%
60%
40%
20%
0%
83%
17%
729
Female
149
Male
3
Other

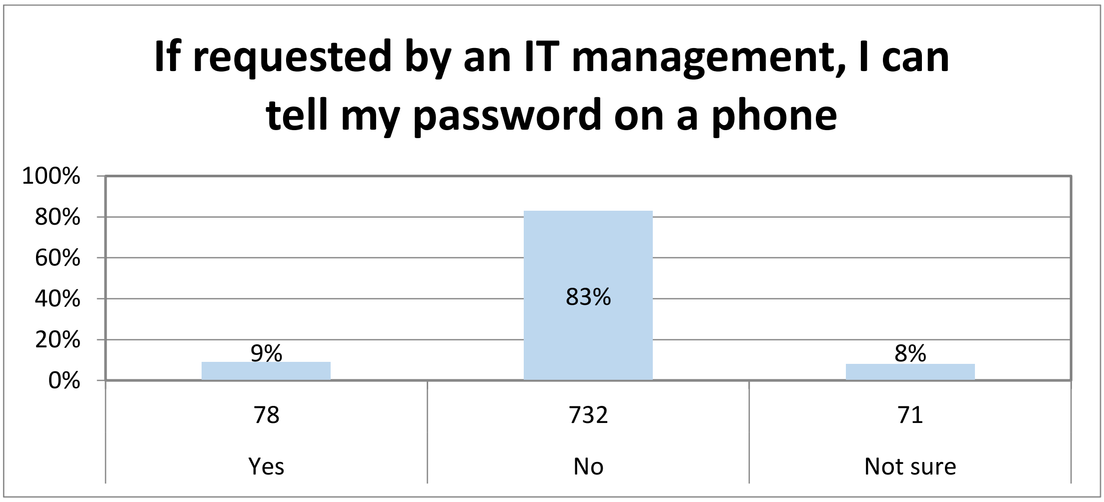

Age
100%
80%
60%
40%
20%
0%
12%
17%
25%
46%
104
Under 30
148
30 - 39 v
220
40 - 49 v
408
50 - 64 v
1
65 and over

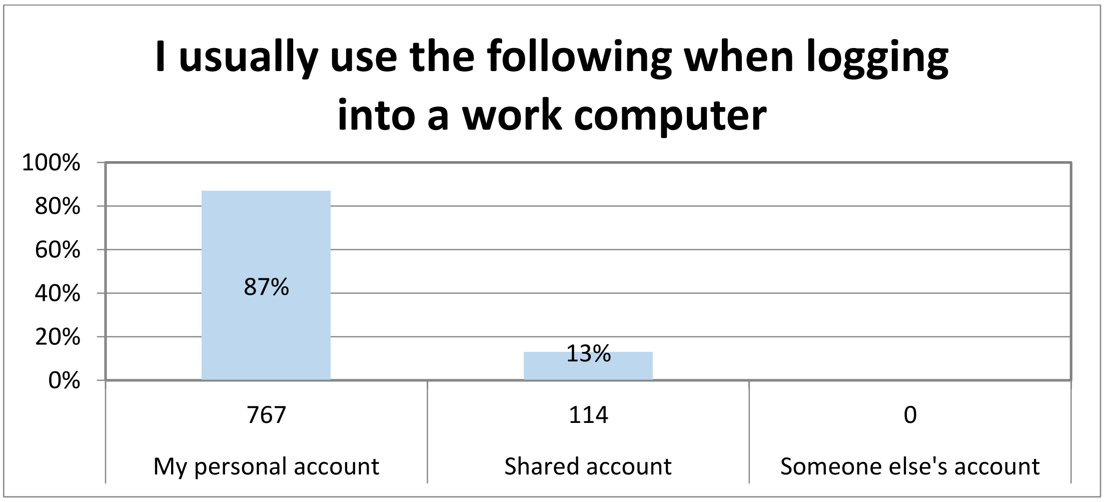

Education
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
2%
17%
26%
6%
29%
15%
5%
18
Basic education
150
Vocational education and training
231
Post-secondary education
55
General upper secondary education
256
Bachelor's degree
129
Masters's degree
42
Licentiate/Doctorate degree

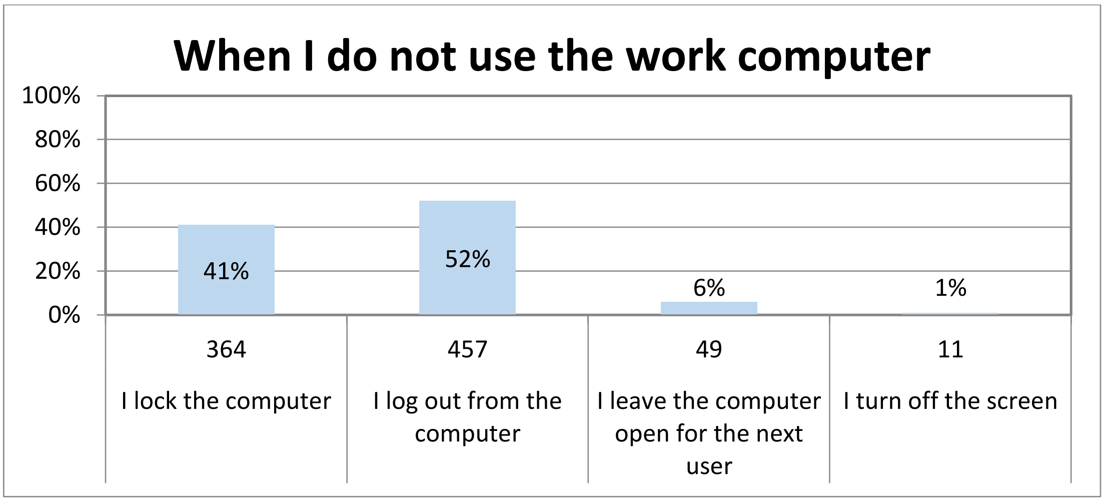

Have you participated on cybersecurity training or lecture?
100%
80%
60%
40%
20%
0%
17%
18%
9%
56%
147
162
76
496
On-site training/lecture
Training online
Both online and on-site
I have not participated

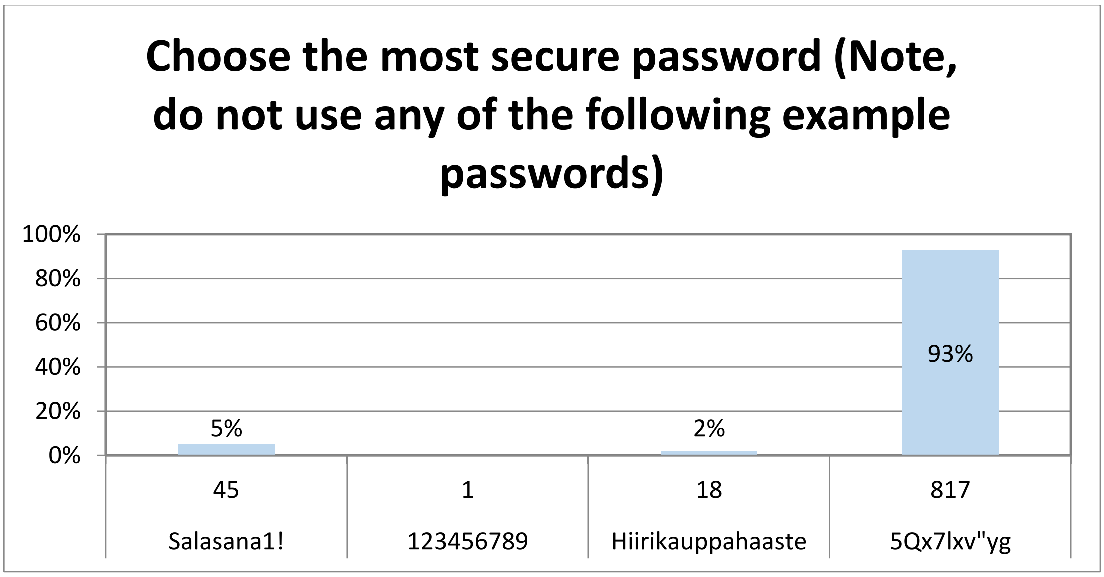

Job describtion
50%
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
4%
33%
6%
5%
12%
5%
5%
2%
4%
15%
1%
8%
38
Doctor
291
Nurse
51
Survey and nursing staff
47
Supporting survery and nursing staff
105
Other nursing staff
45
Mainenance personnel
49
Social worker
15
IT management
34
Rescue personnel
134
Financial and administrative personnel
5
State administrative agency personnel
67
Other

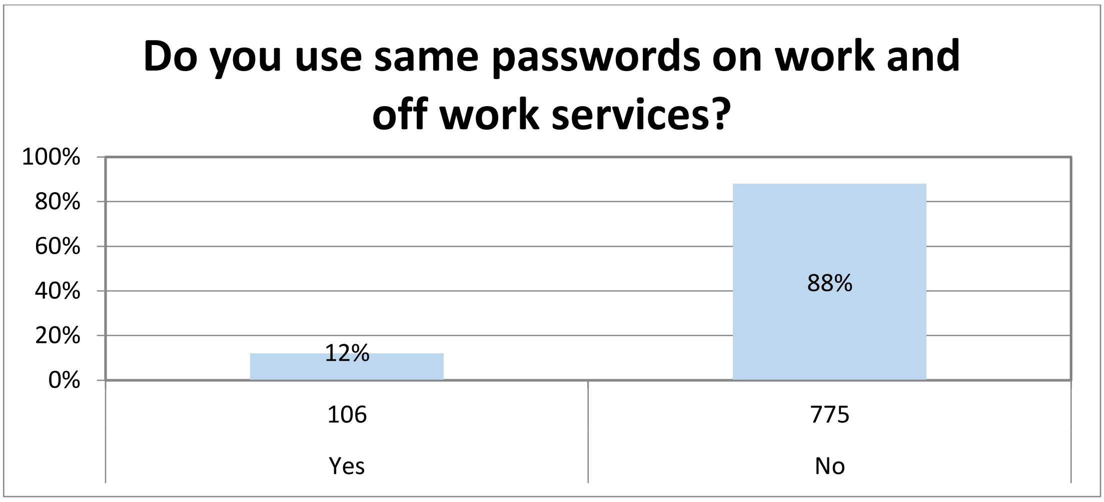

If requested by an authority, I can tell my password on phone
100%
80%
60%
40%
20%
0%
1%
96%
3%
9
842
30
Yes
No
Not sure

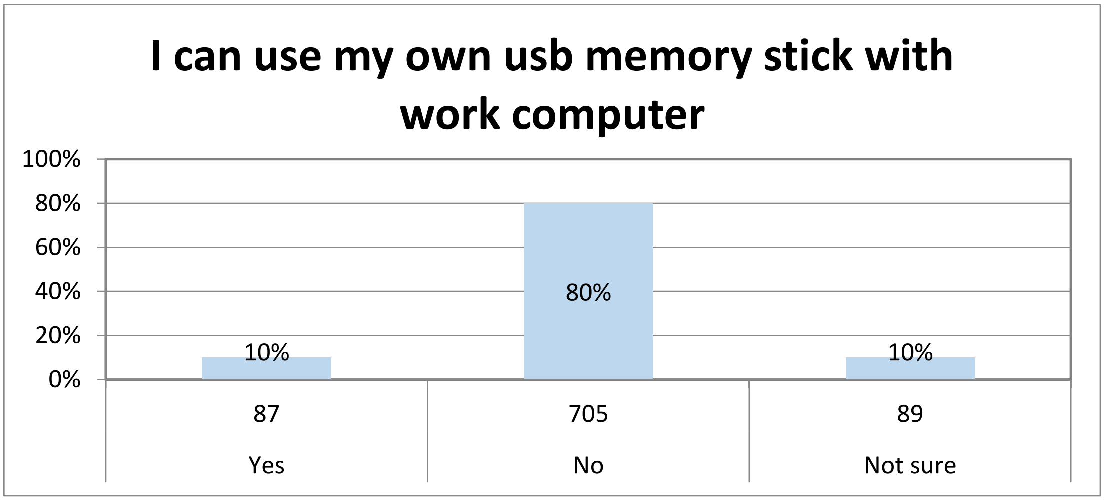

If requested by an IT management, I can tell my password on a phone
100%
80%
60%
40%
20%
0%
9%
83%
8%
78
732
71
Yes
No
Not sure

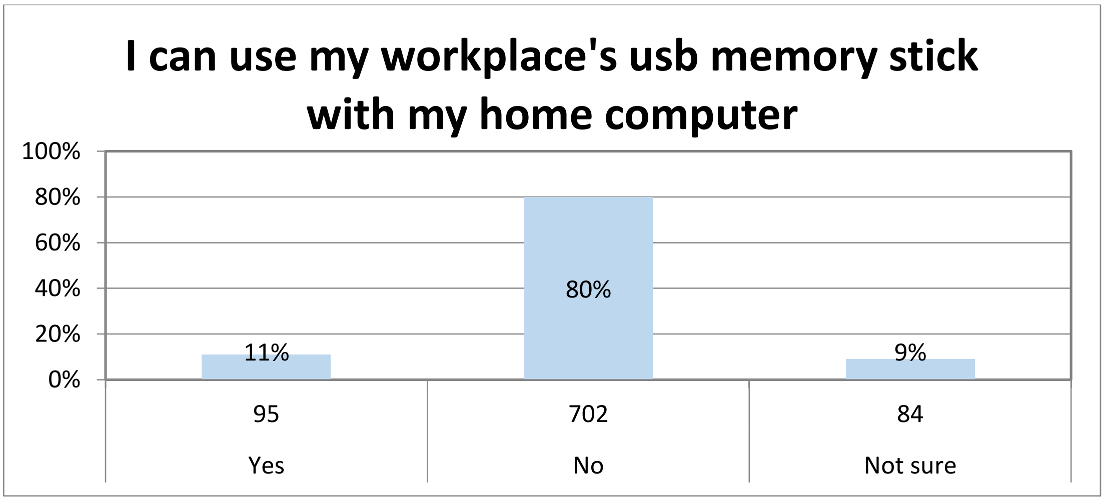

I usually use the following when logging into a work computer
100%
80%
60%
40%
20%
0%
87%
13%
767
114
0
My personal account
Shared account
Someone else's account

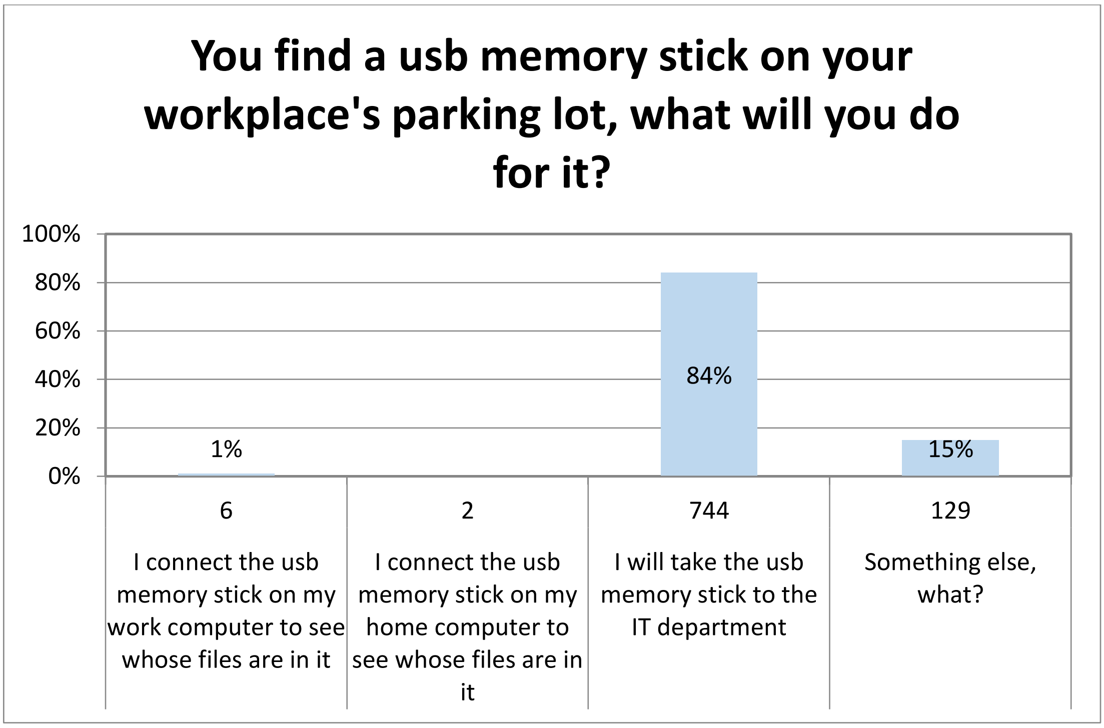

When I do not use the work computer
100%
80%
60%
40%
20%
0%
41%
52%
6%
1%
364
457
49
11
I lock the computer
I log out from the computer
I leave the computer open for the next user
I turn off the screen

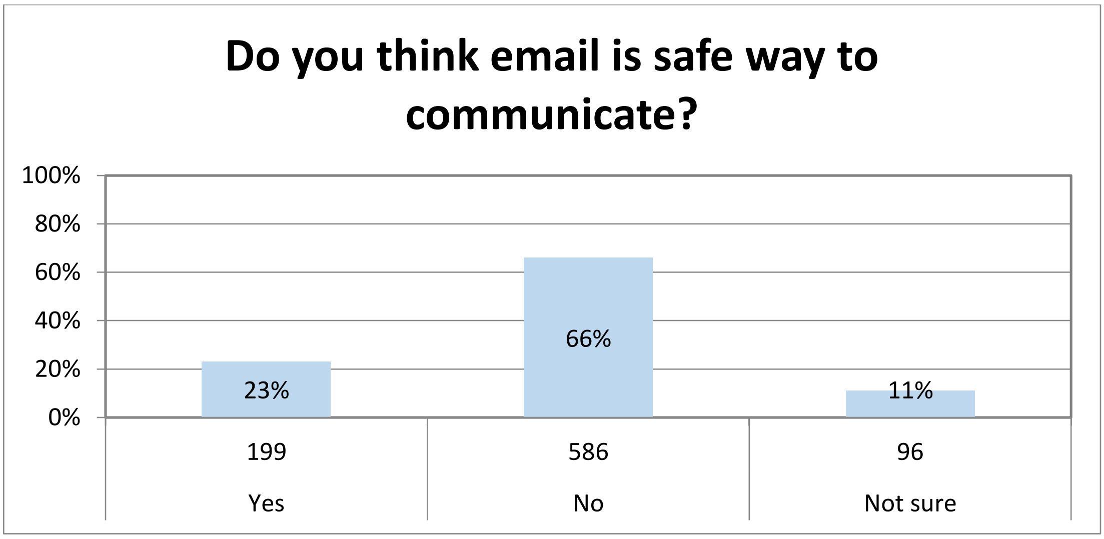

Choose the most secure password (Note, do not use any of the following example passwords)
100%
80%
60%
40%
20%
0%
5%
2%
93%
45
1
18
817
Salasana1!
123456789
Hiirikauppahaaste
5Qx7lxv"yg

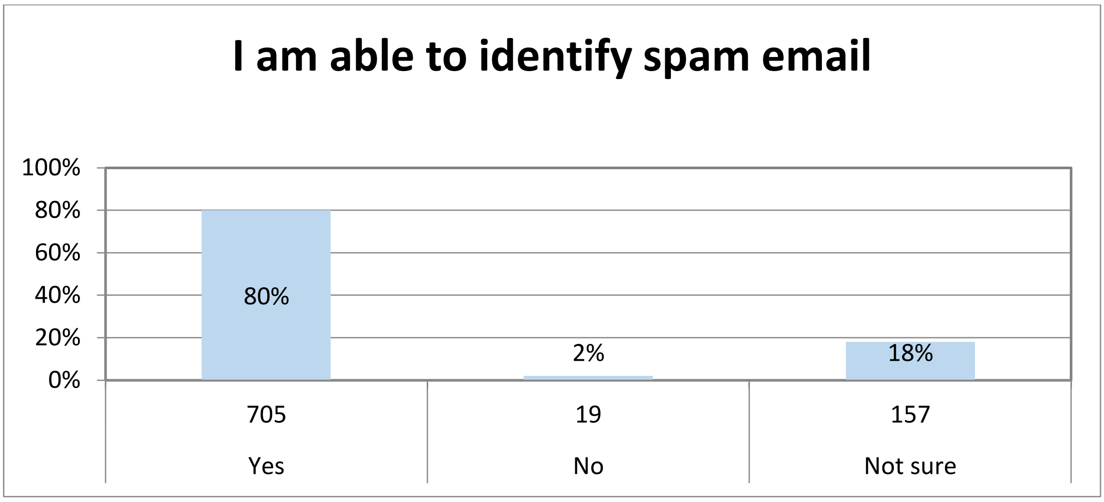

Do you use same passwords on work and off work services?
100%
80%
60%
40%
20%
0%
12%
88%
106
775
Yes
No

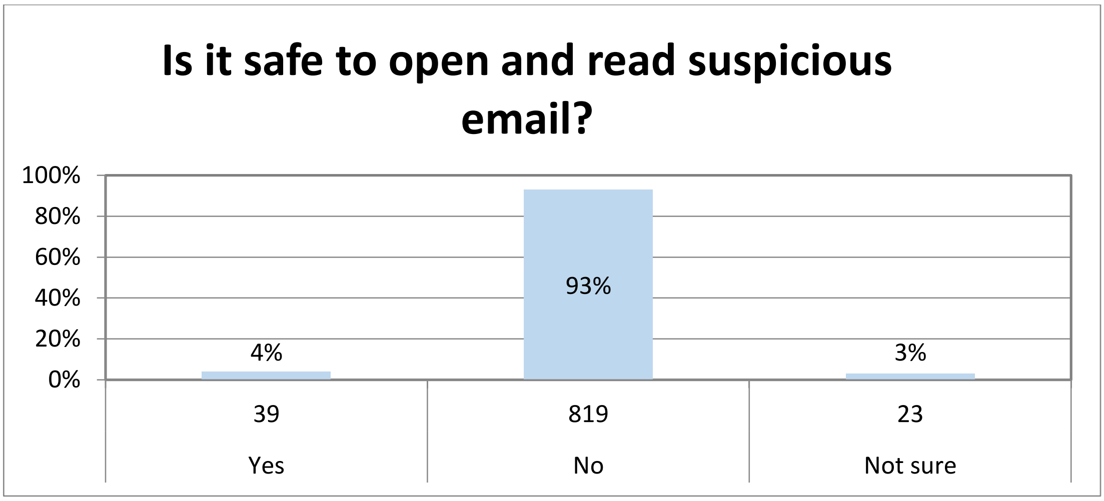

I can use my own usb memory stick with work computer
100%
80%
60%
40%
20%
0%
10%
80%
10%
87
705
89
Yes
No
Not sure

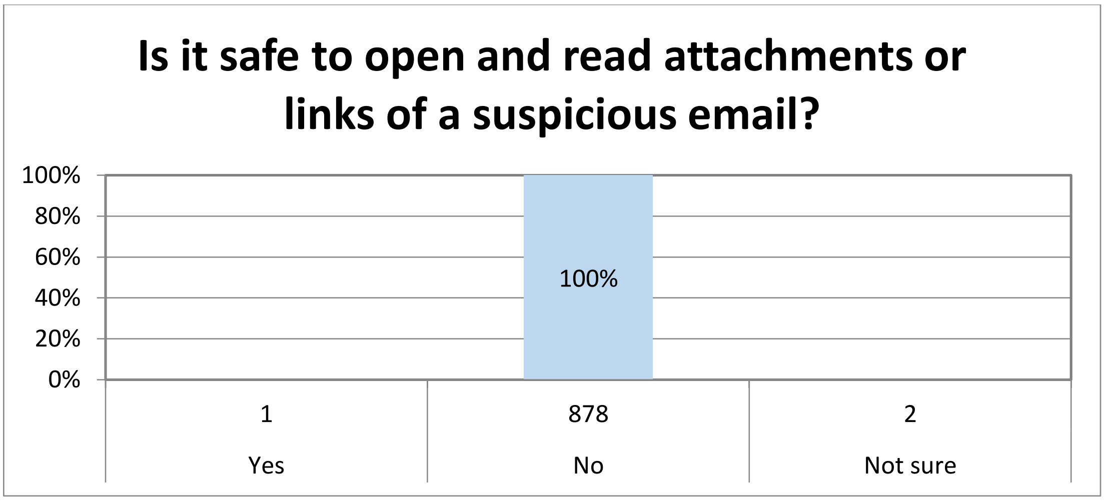

I can use my workplace's usb memory stick with my home computer
100%
80%
60%
40%
20%
0%
11%
80%
9%
95
702
84
Yes
No
Not sure

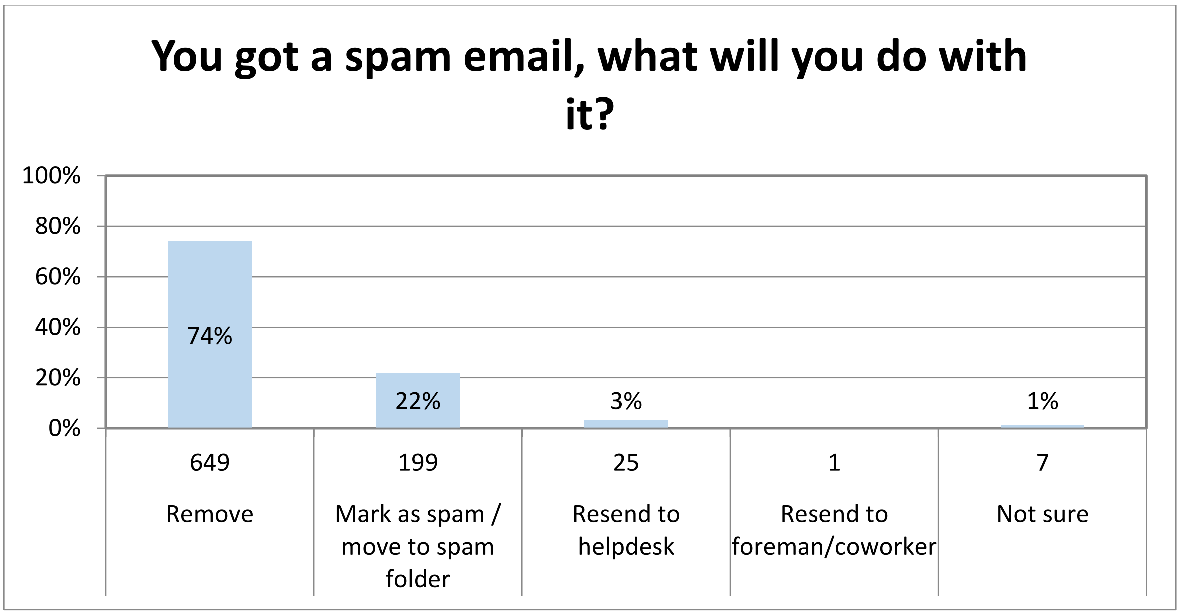

You find a usb memory stick on your workplace's parking lot, what will you do for it?
100%
80%
60%
40%
20%
0%
1%
84%
15%
6
I connect the usb memory stick on my work computer to see whose files are in it
2
I connect the usb memory stick on my home computer to see whose files are in it
744
I will take the usb memory stick to the IT department
129
Something else, what?

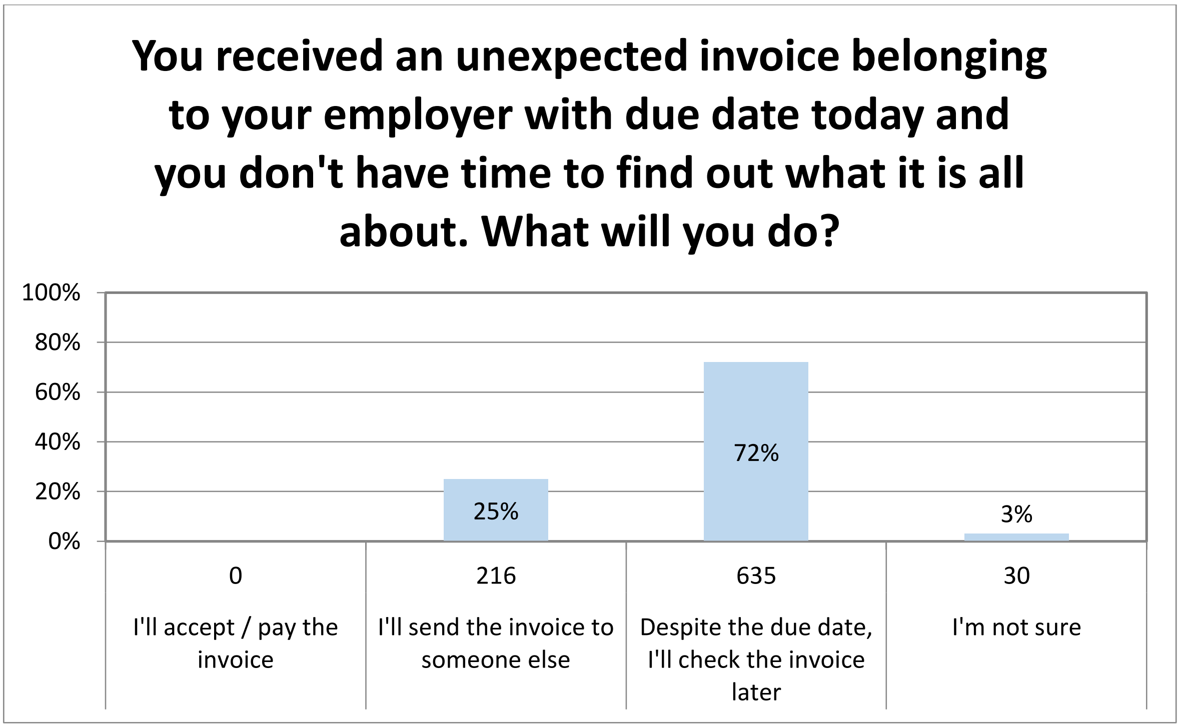

Do you think email is safe way to communicate?
100%
80%
60%
40%
20%
0%
23%
66%
11%
199
Yes
586
No
96
Not sure

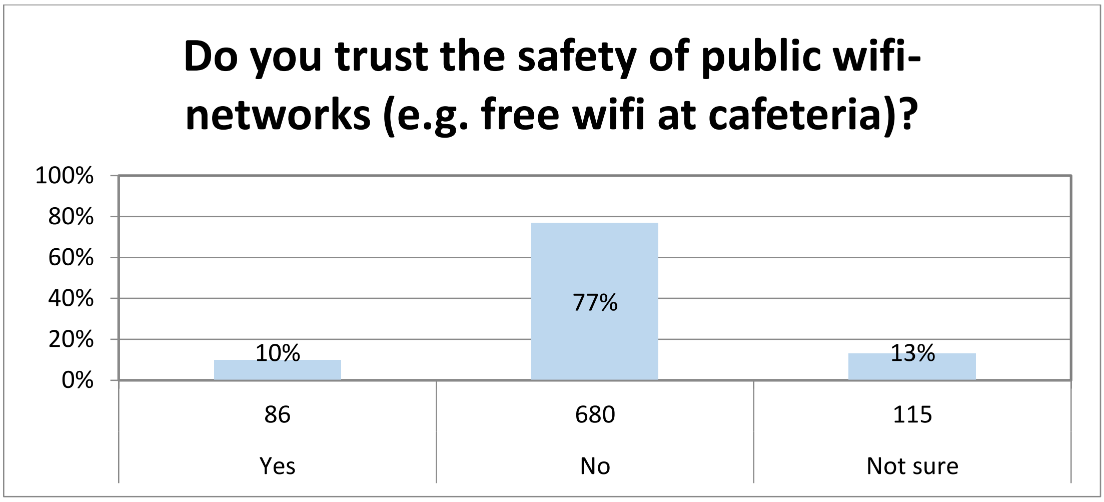

I am able to identify spam email
100%
80%
60%
40%
20%
0%
80%
2%
18%
705
19
157
Yes
No
Not sure

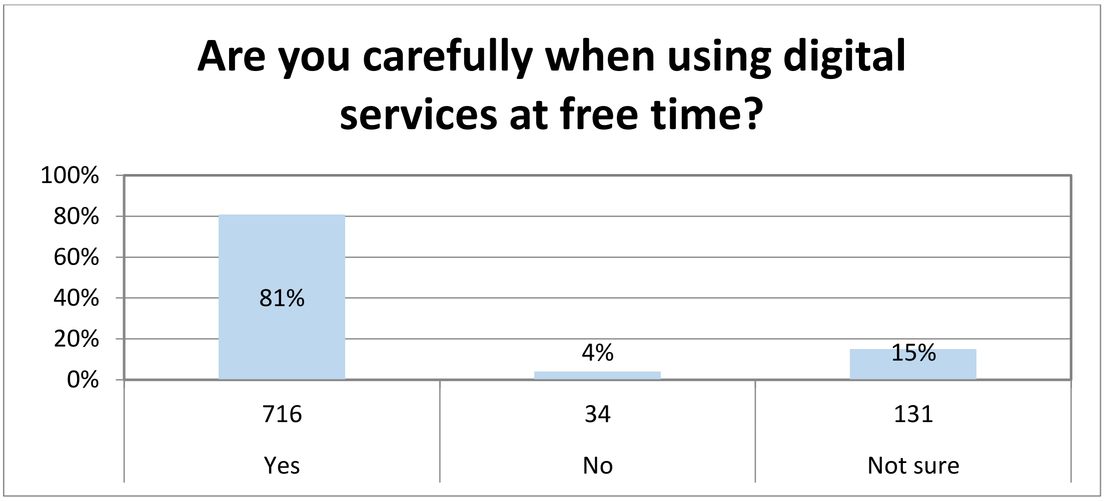

Is it safe to open and read suspicious email?
100%
80%
60%
40%
20%
0%
4%
93%
3%
39
819
23
Yes
No
Not sure

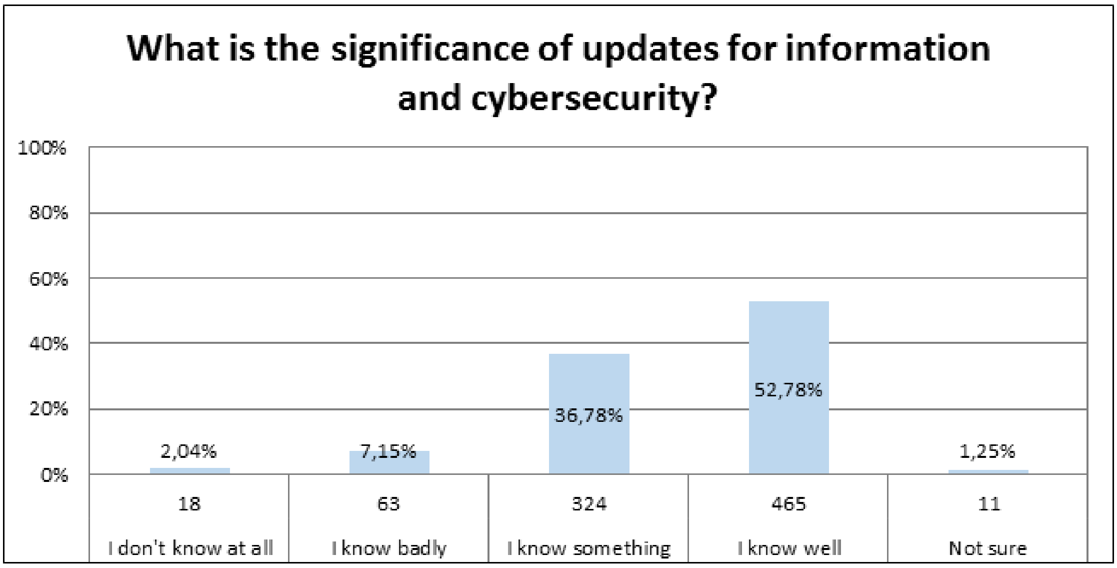

Is it safe to open and read attachments or links of a suspicious email?
100%
80%
60%
40%
20%
0%
100%
1
878
2
Yes
No
Not sure

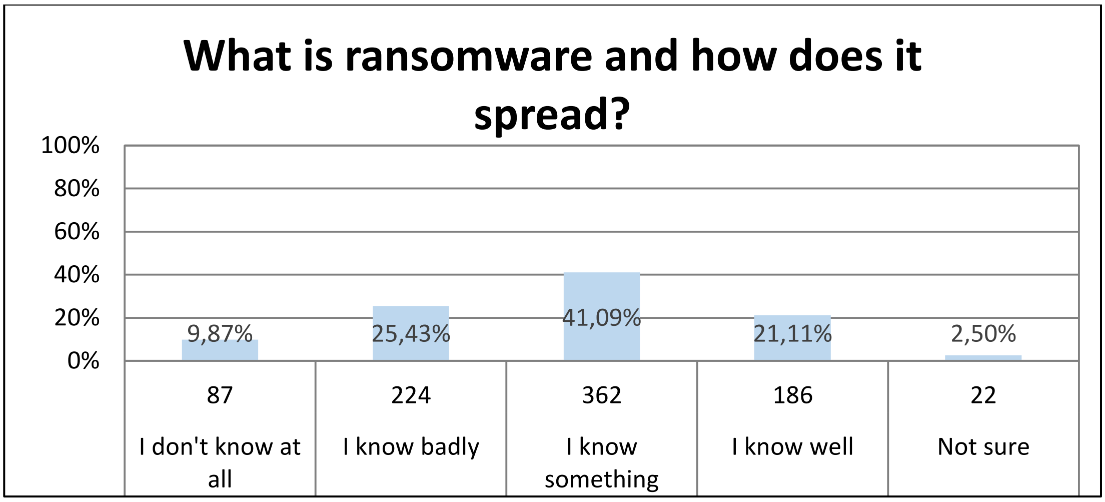

You got a spam email, what will you do with it?
100%
80%
60%
40%
20%
0%
74%
22%
3%
1%
649
Remove
199
Mark as spam / move to spam folder
25
Resend to helpdesk
1
Resend to foreman/coworker
7
Not sure

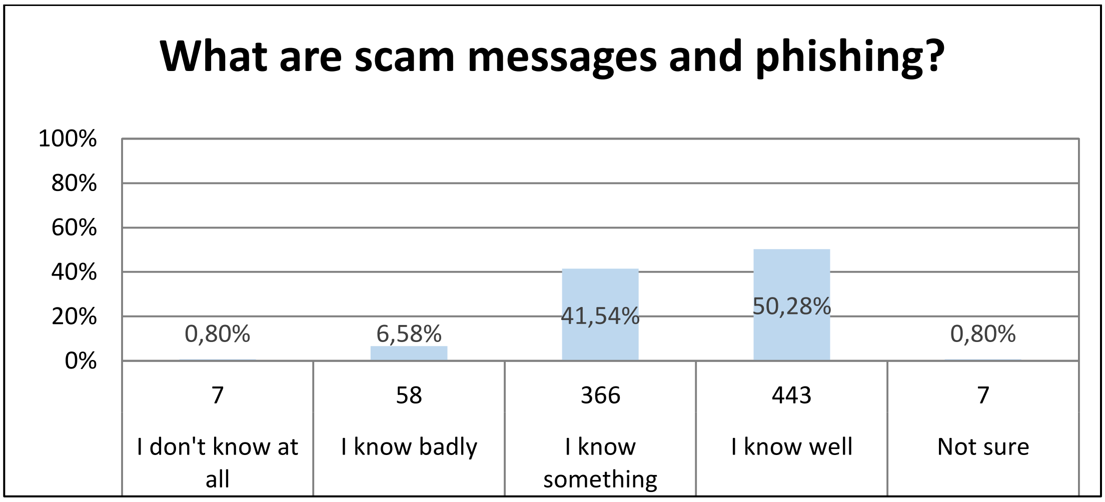

You received an unexpected invoice belonging to your employer with due date today and you don't have time to find out what it is all about. What will you do?
100%
80%
60%
40%
20%
0%
25%
72%
3%
0
I'll accept / pay the invoice
216
I'll send the invoice to someone else
635
Despite the due date, I'll check the invoice later
30
I'm not sure

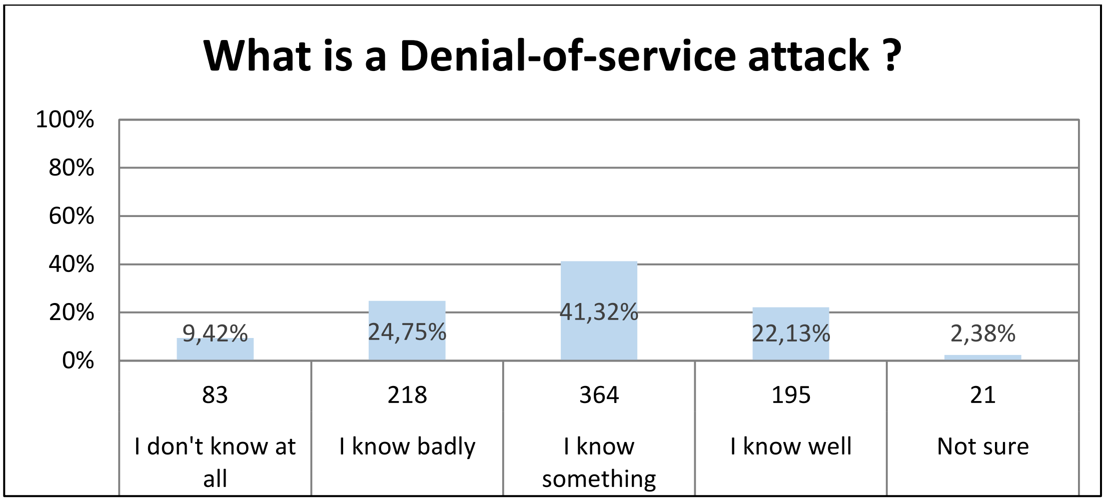

Do you trust the safety of public wifi-networks (e.g. free wifi at cafeteria)?
100%
80%
60%
40%
20%
0%
10%
77%
13%
86
680
115
Yes
No
Not sure

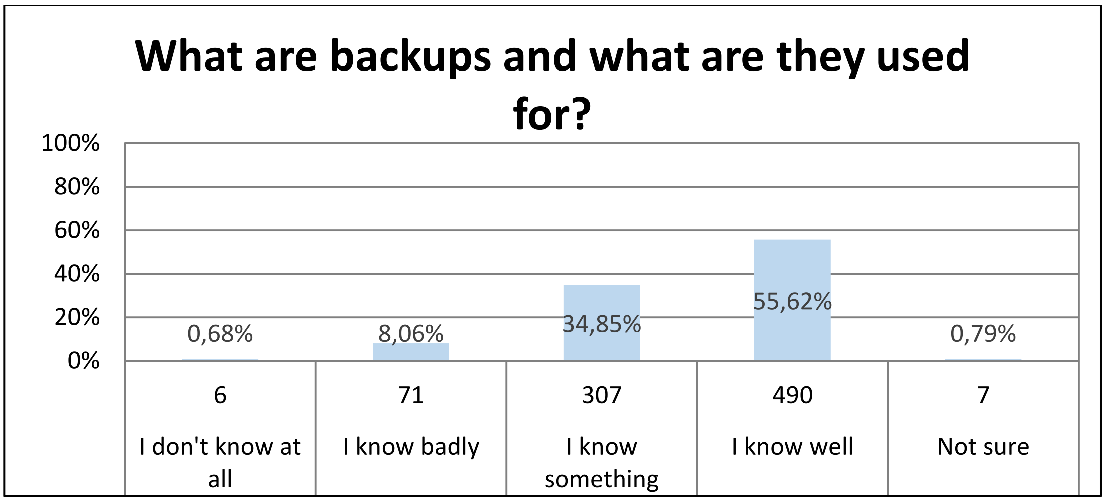

Are you carefully when using digital services at free time?
100%
80%
60%
40%
20%
0%
81%
4%
15%
716
34
131
Yes
No
Not sure

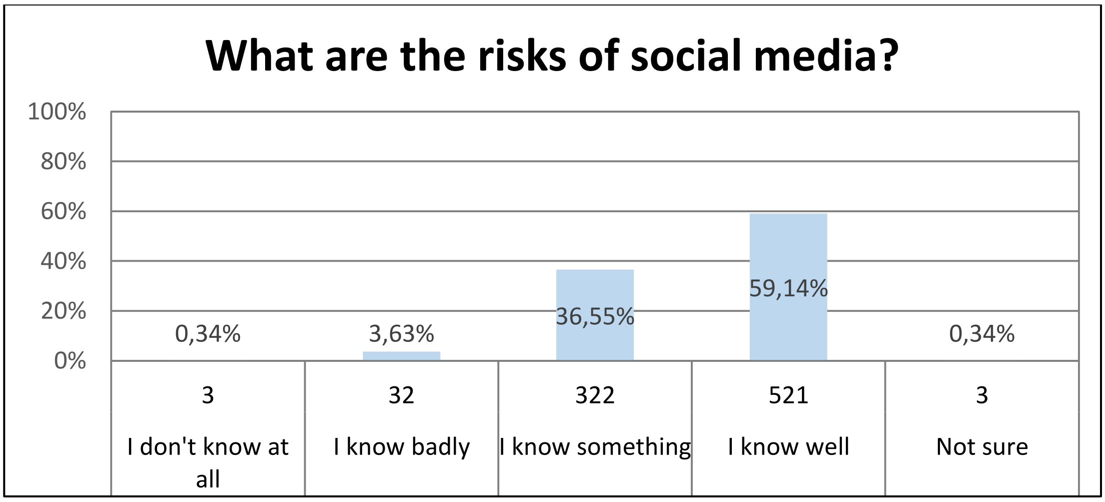

What is the significance of updates for information and cybersecurity?
100%
80%
60%
40%
20%
0%
2,04%
7,15%
36,78%
52,78%
1,25%
18
63
324
465
11
I don't know at all
I know badly
I know something
I know well
Not sure

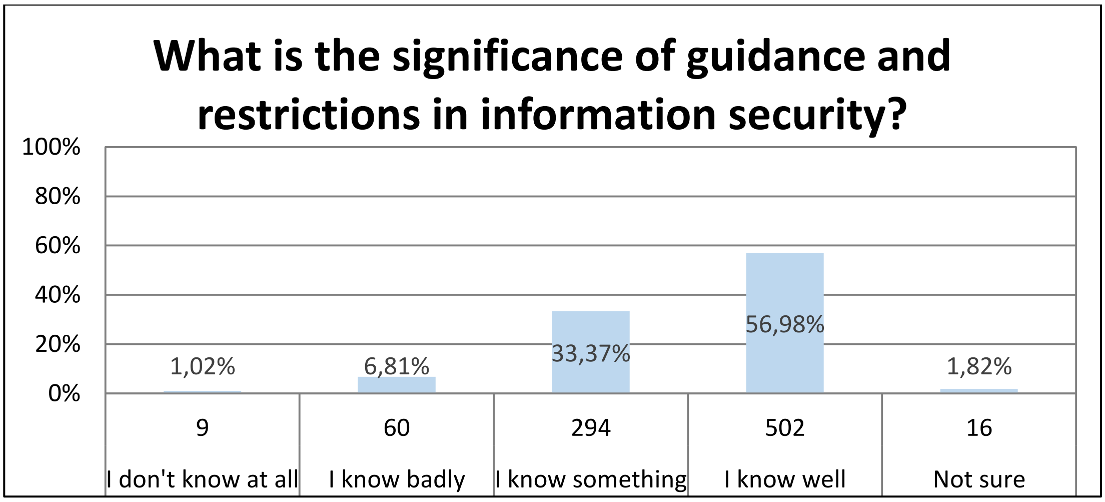

What is ransomware and how does it spread?
100%
80%
60%
40%
20%
0%
9,87%
25,43%
41,09%
21,11%
2,50%
87
224
362
186
22
I don't know at all
I know badly
I know something
I know well
Not sure

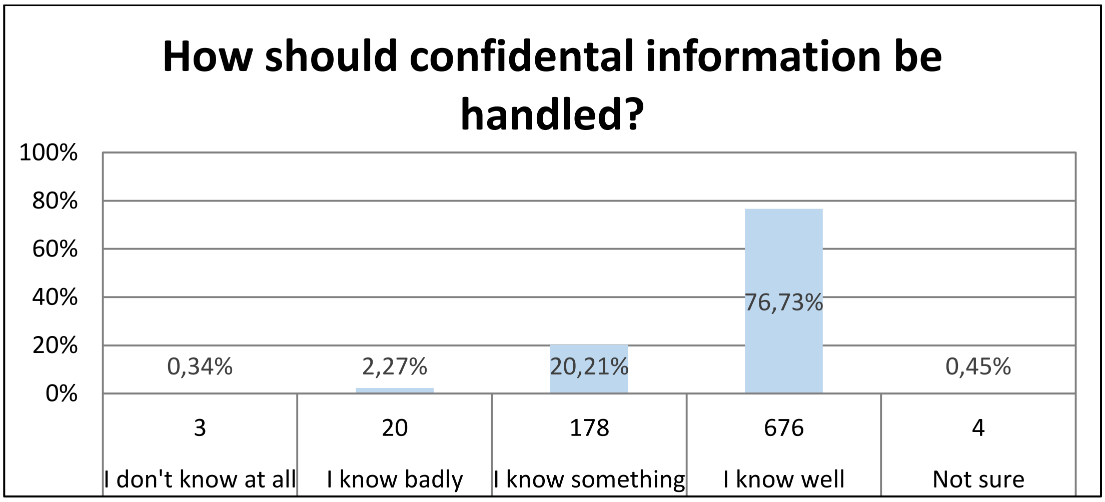

What are scam messages and phishing?
100%
80%
60%
40%
20%
0%
0,80%
6,58%
41,54%
50,28%
0,80%
7
58
366
443
7
I don't know at all
I know badly
I know something
I know well
Not sure

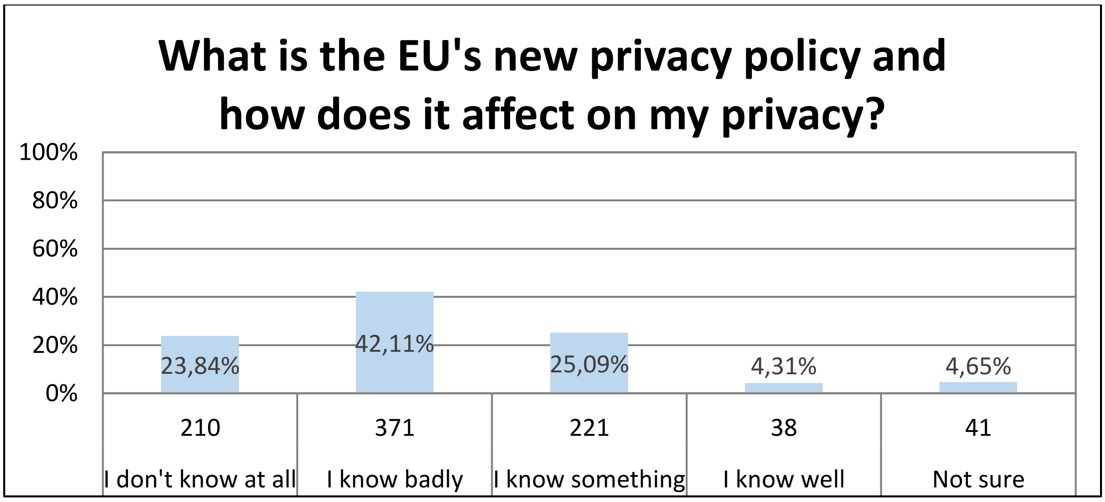

What is a Denial-of-service attack ?
100%
80%
60%
40%
20%
0%
9,42%
24,75%
41,32%
22,13%
2,38%
83
218
364
195
21
I don't know at all
I know badly
I know something
I know well
Not sure

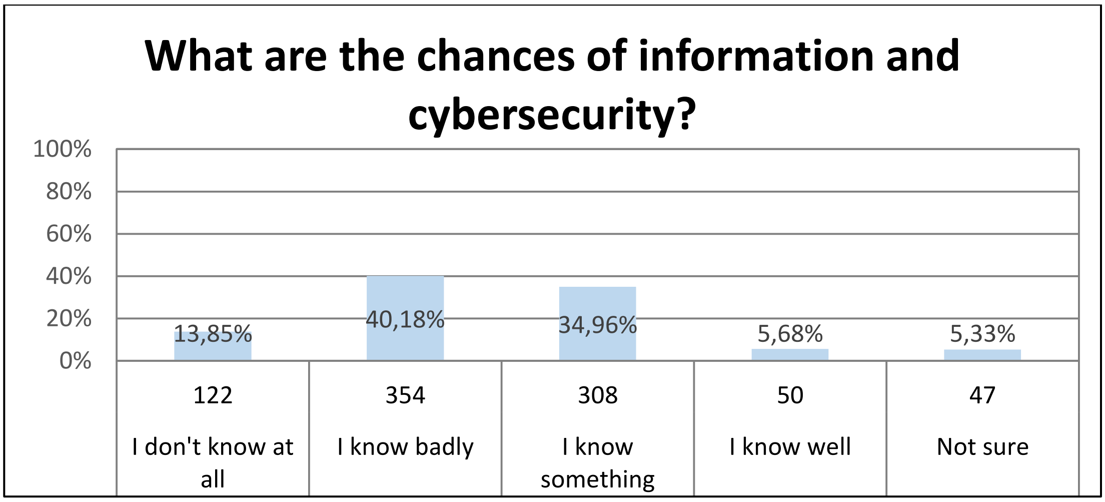

What are backups and what are they used for?
100%
80%
60%
40%
20%
0%
0,68%
8,06%
34,85%
55,62%
0,79%
6
71
307
490
7
I don't know at all
I know badly
I know something
I know well
Not sure

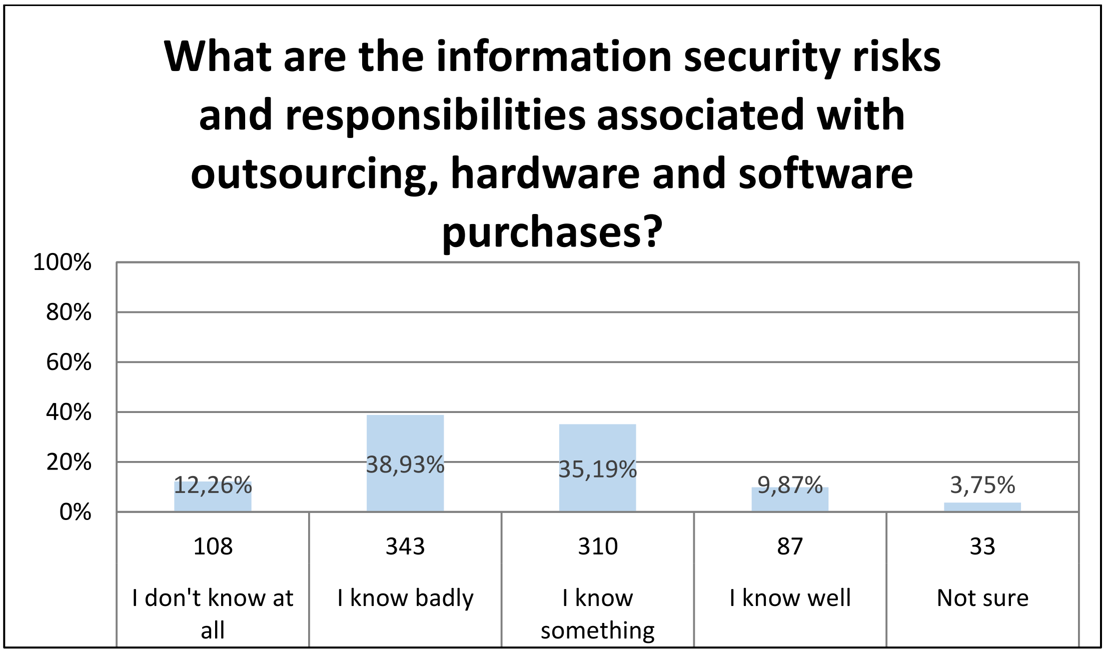

What are the risks of social media?
100%
80%
60%
40%
20%
0%
0,34%
3,63%
36,55%
59,14%
0,34%
3
32
322
521
3
I don't know at all
I know badly
I know something
I know well
Not sure

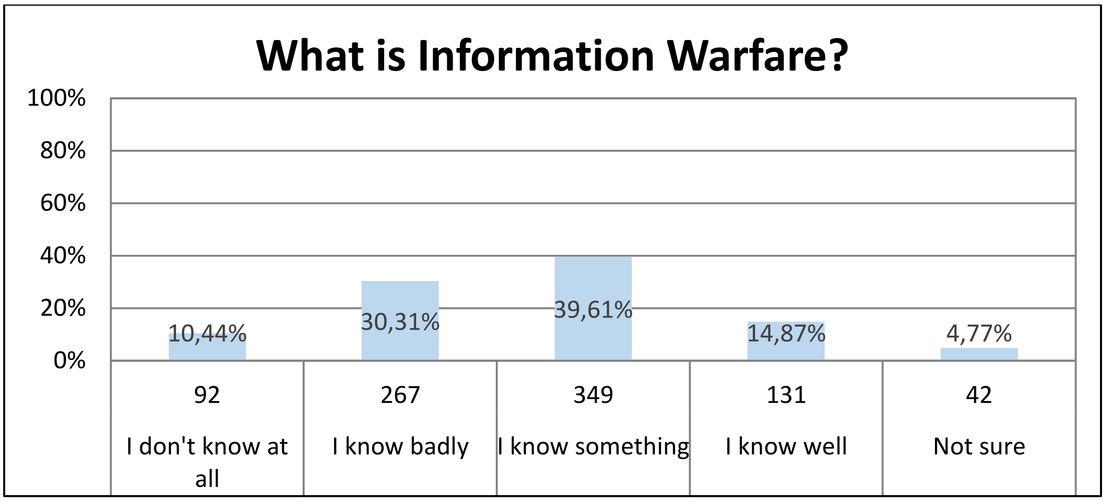

What is the significance of guidance and restrictions in information security?
100%
80%
60%
40%
20%
0%
1,02%
6,81%
33,37%
56,98%
1,82%
9
60
294
502
16
I don't know at all
I know badly
I know something
I know well
Not sure

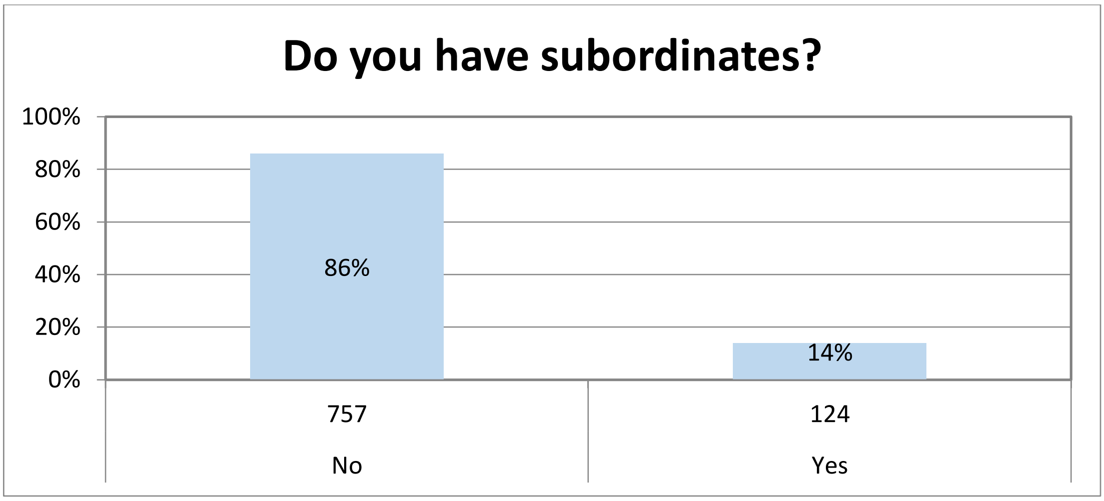

How should confidental information be handled?
100%
80%
60%
40%
20%
0%
0,34%
2,27%
20,21%
76,73%
0,45%
3
20
178
676
4
I don't know at all
I know badly
I know something
I know well
Not sure

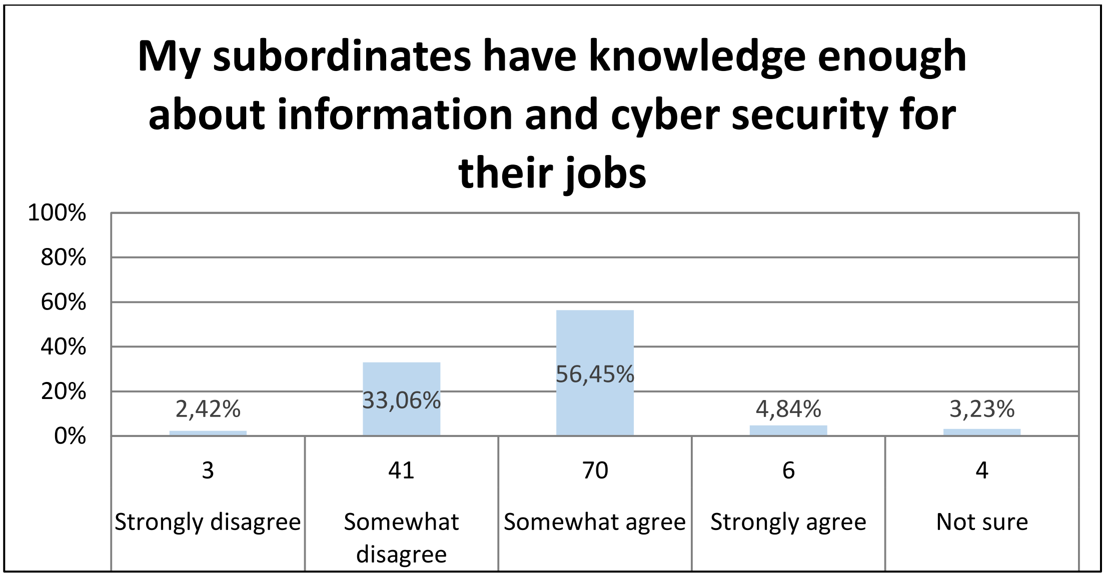

What is the EU's new privacy policy and how does it affect on my privacy?
100%
80%
60%
40%
20%
0%
23,84%
42,11%
25,09%
4,31%
4,65%
210
371
221
38
41
I don't know at all
I know badly
I know something
I know well
Not sure

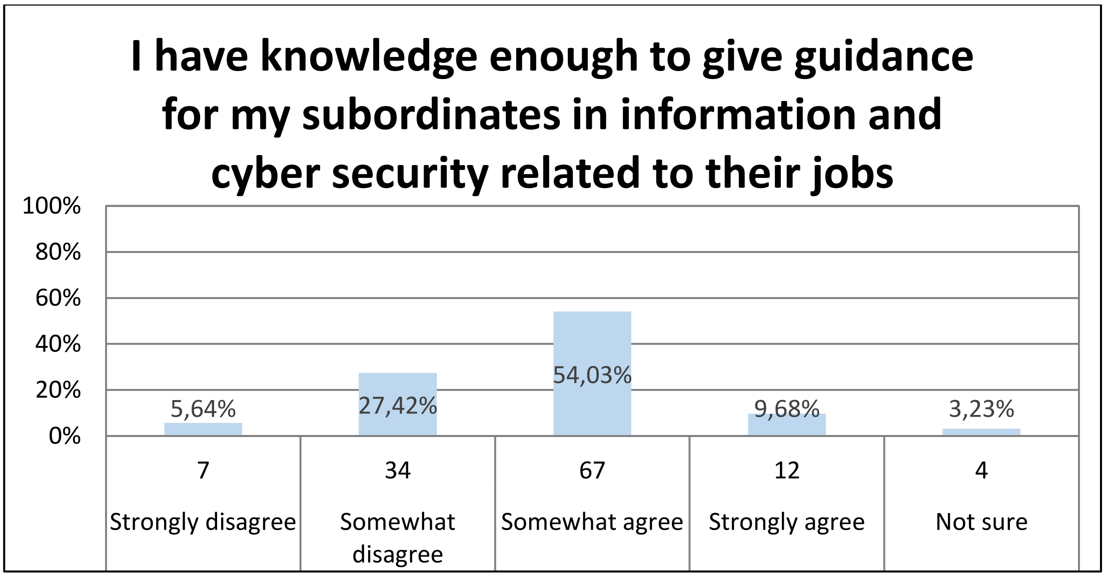

What are the chances of information and cybersecurity?
100%
80%
60%
40%
20%
0%
13,85%
40,18%
34,96%
5,68%
5,33%
122
354
308
50
47
I don't know at all
I know badly
I know something
I know well
Not sure

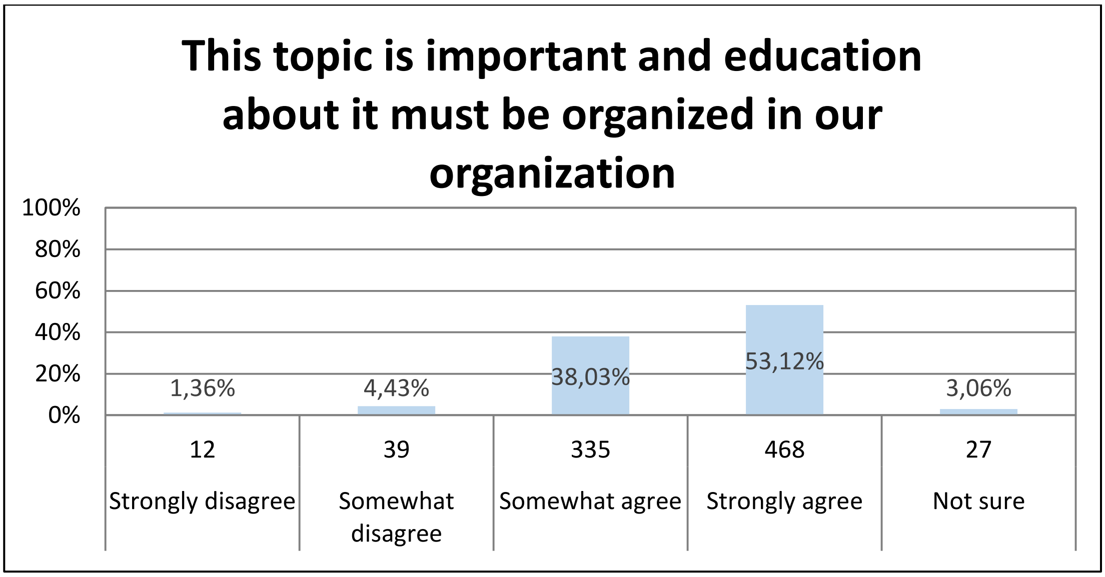

What are the information security risks and responsibilities associated with outsourcing, hardware and software purchases?
100%
80%
60%
40%
20%
0%
12,26%
38,93%
35,19%
9,87%
3,75%
108
343
310
87
33
I don't know at all
I know badly
I know something
I know well
Not sure

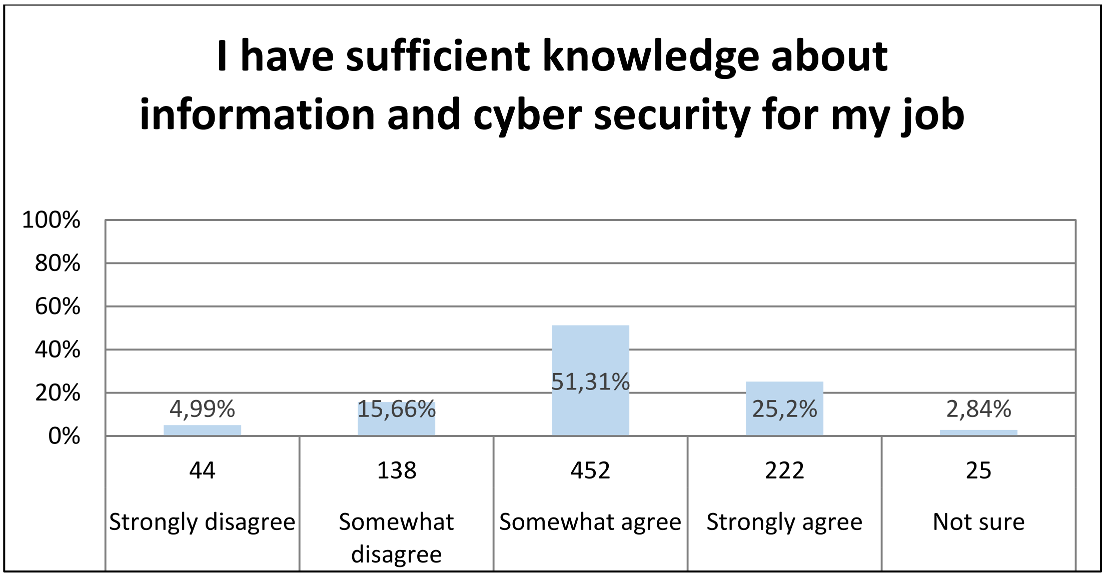

What is Information Warfare?
100%
80%
60%
40%
20%
0%
10,44%
30,31%
39,61%
14,87%
4,77%
92
267
349
131
42
I don't know at all
I know badly
I know something
I know well
Not sure

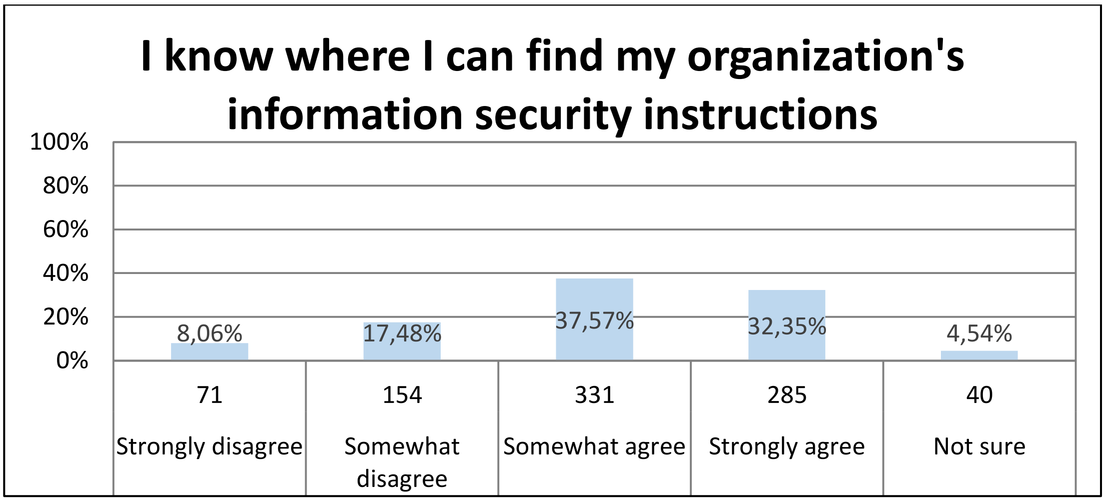

Do you have subordinates?
100%
80%
60%
40%
20%
0%
86%
14%
757
124
No
Yes

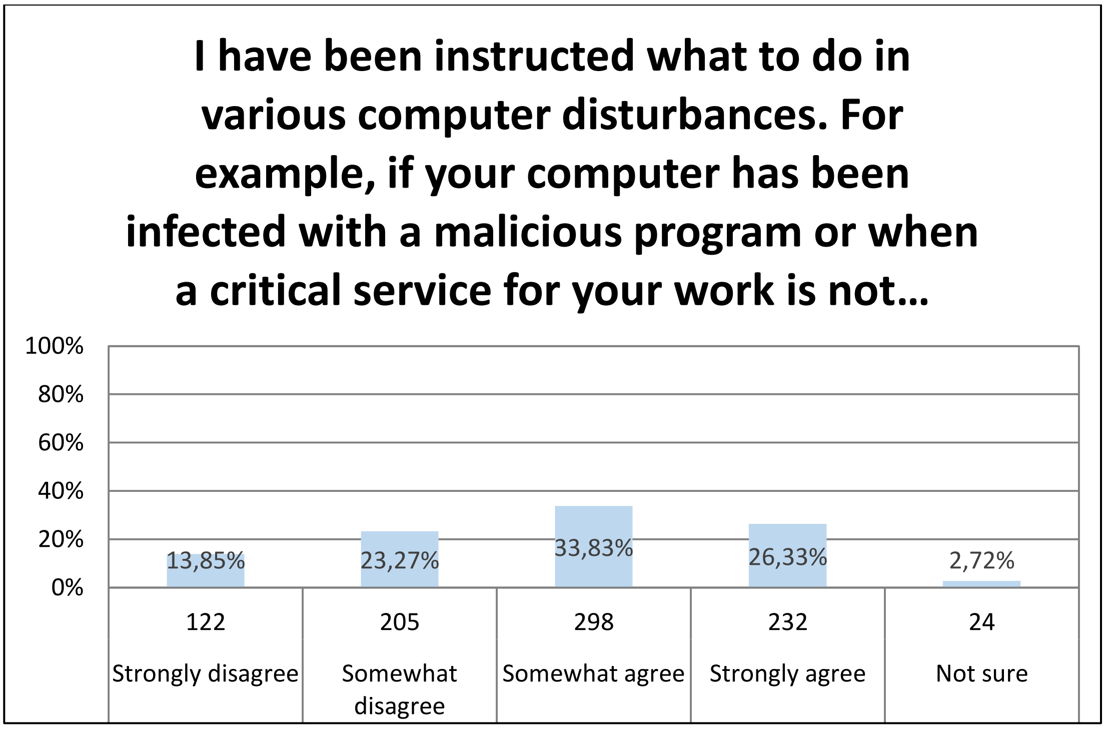

My subordinates have knowledge enough about information and cyber security for their jobs
100%
80%
60%
40%
20%
0%
2,42%
33,06%
56,45%
4,84%
3,23%
3
41
70
6
4
Strongly disagree
Somewhat disagree
Somewhat agree
Strongly agree
Not sure

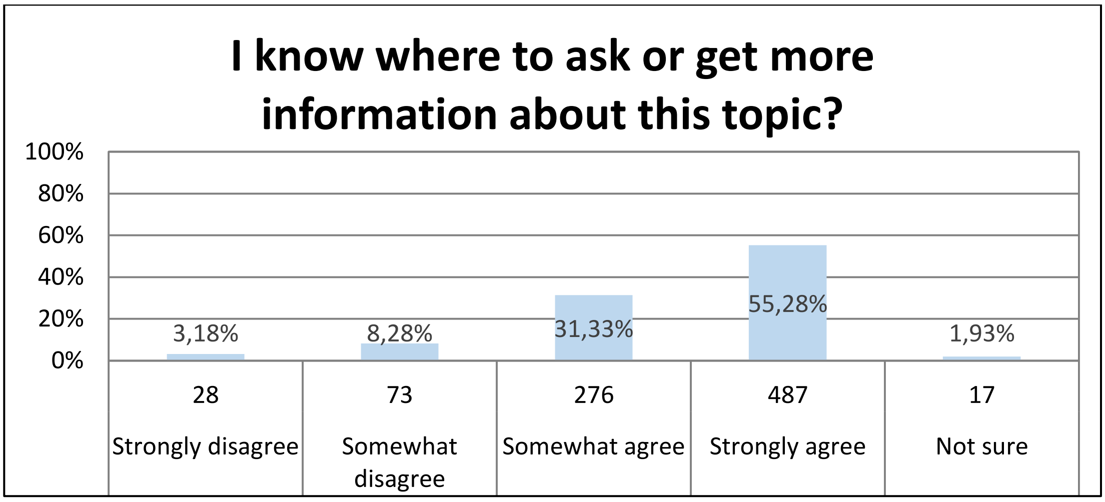

I have knowledge enough to give guidance for my subordinates in information and cyber security related to their jobs
100%
80%
60%
40%
20%
0%
5,64%
27,42%
54,03%
9,68%
3,23%
7
34
67
12
4
Strongly disagree
Somewhat disagree
Somewhat agree
Strongly agree
Not sure

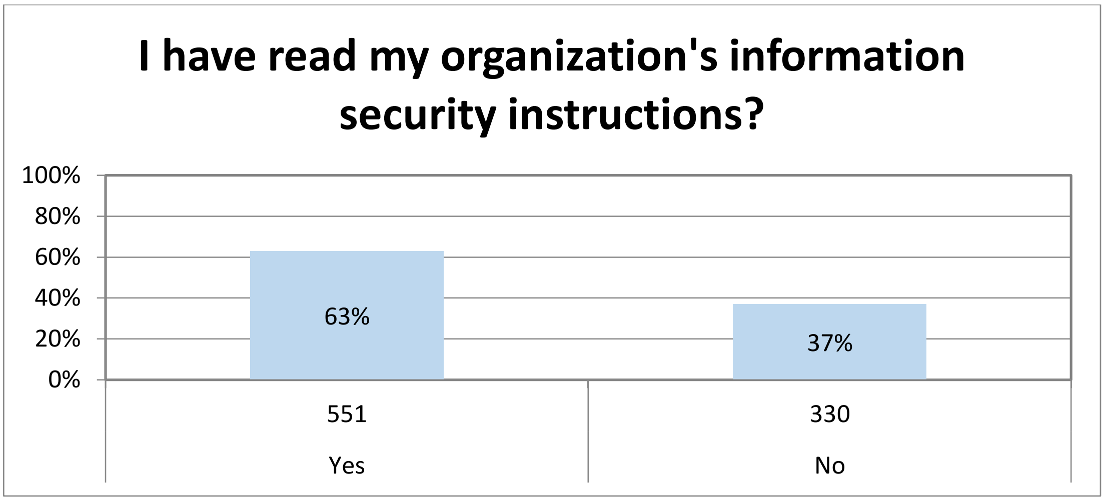

This topic is important and education about it must be organized in our organization
100%
80%
60%
40%
20%
0%
1,36%
4,43%
38,03%
53,12%
3,06%
12
39
335
468
27
Strongly disagree
Somewhat disagree
Somewhat agree
Strongly agree
Not sure

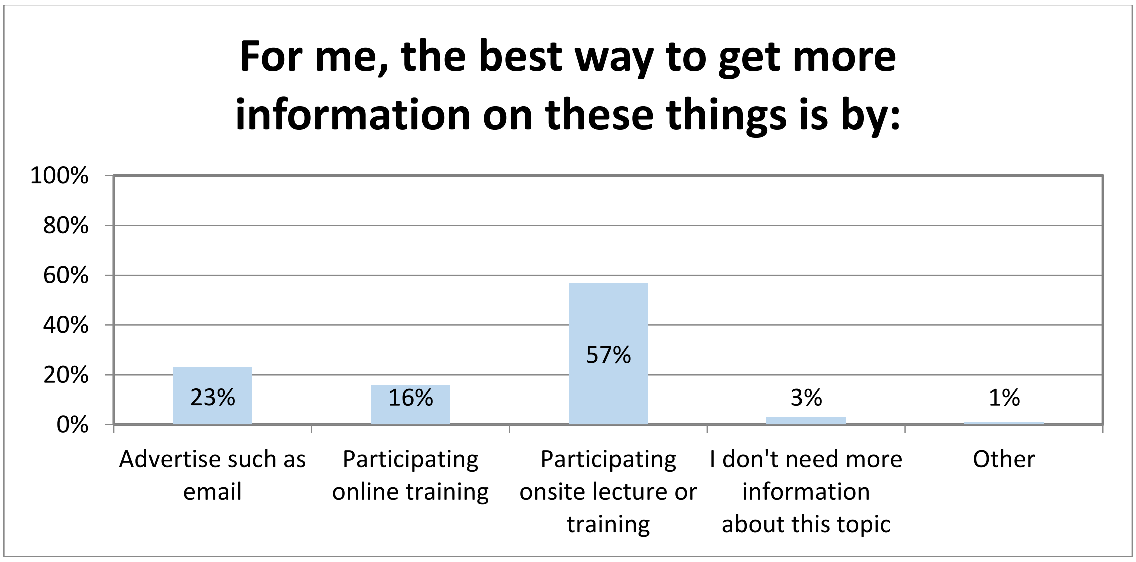

I have sufficient knowledge about information and cyber security for my job
100%
80%
60%
40%
20%
0%
4,99%
15,66%
51,31%
25,2%
2,84%
44
138
452
222
25
Strongly disagree
Somewhat disagree
Somewhat agree
Strongly agree
Not sure

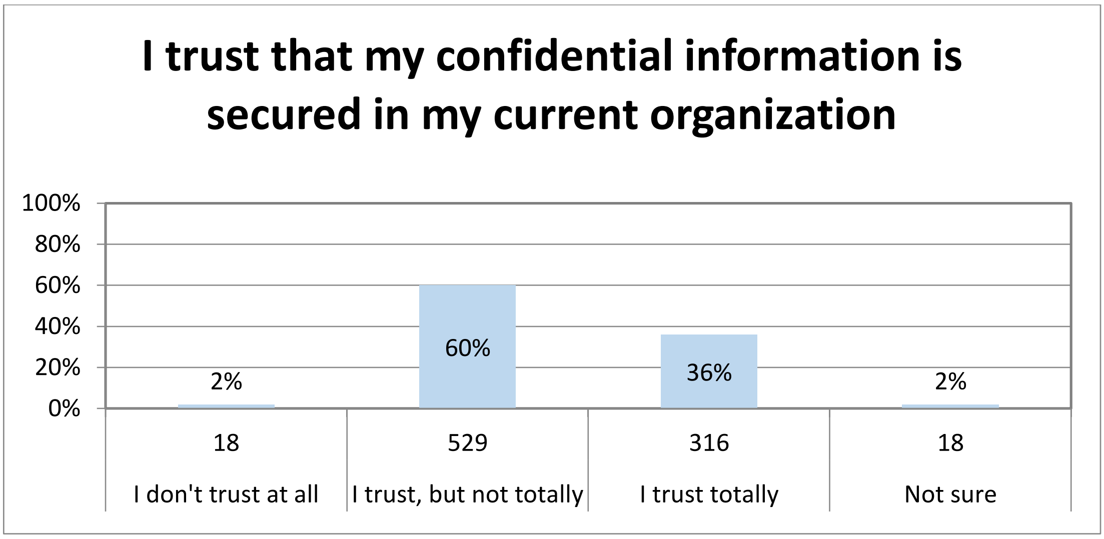

I know where I can find my organization's information security instructions
100%
80%
60%
40%
20%
0%
8,06%
17,48%
37,57%
32,35%
4,54%
71
154
331
285
40
Strongly disagree
Somewhat disagree
Somewhat agree
Strongly agree
Not sure

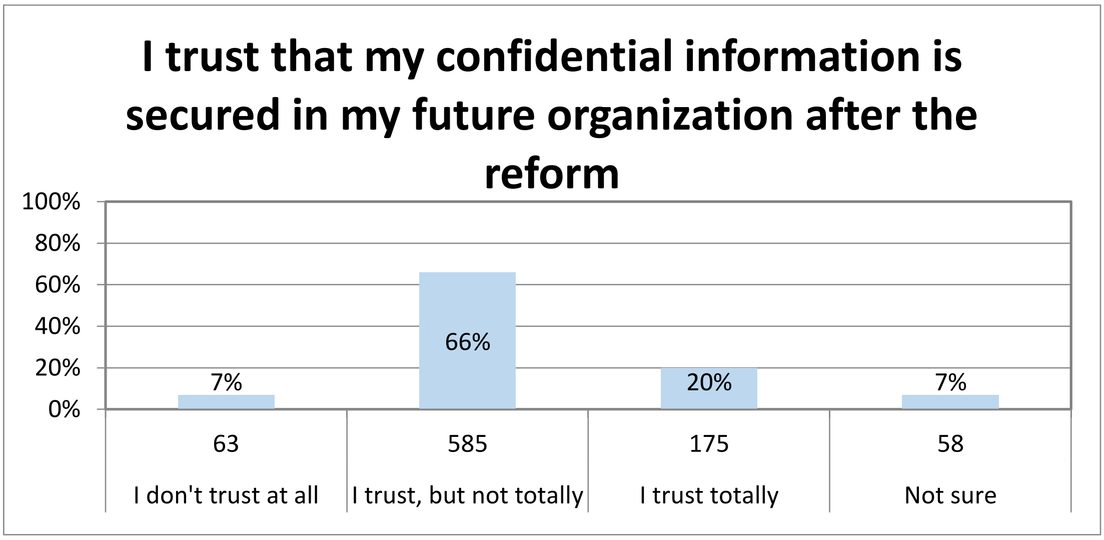

I have been instructed what to do in various computer disturbances. For example, if your computer has been infected with a malicious program or when a critical service for your work is not...
100%
80%
60%
40%
20%
0%
13,85%
23,27%
33,83%
26,33%
2,72%
122
205
298
232
24
Strongly disagree
Somewhat disagree
Somewhat agree
Strongly agree
Not sure


I know where to ask or get more information about this topic?

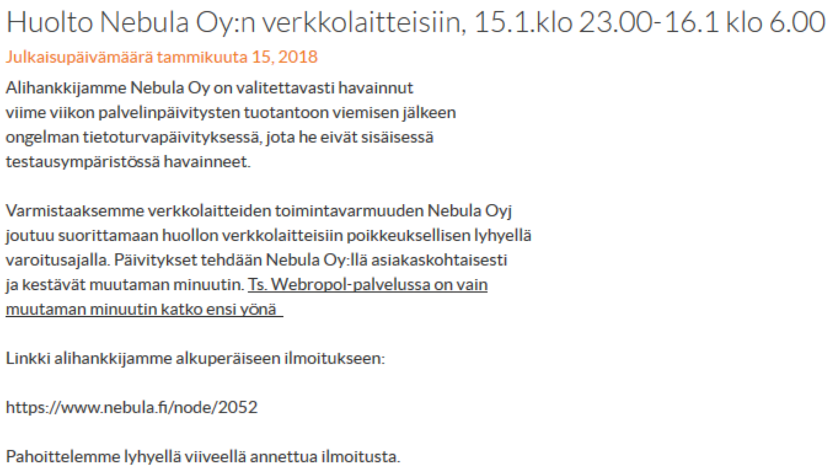

I have read my organization's information security instructions?


For me, the best way to get more information on these things is by:


I trust that my confidential information is secured in my current organization
100%
80%
60%
40%
20%
0%
2%
60%
36%
2%
18
529
316
18
I don't trust at all
I trust, but not totally
I trust totally
Not sure


I trust that my confidential information is secured in my future organization after the reform
100%
80%
60%
40%
20%
0%
7%
66%
20%
7%
63
585
175
58
I don't trust at all
I trust, but not totally
I trust totally
Not sure

Appendix 9. Webropol fault notifications captured in January 2018



Huolto Nebula Oy:n verkkolaitteisiin, 15.1.klo 23.00-16.1 klo 6.00

Julkaisupäivämäärä tammikuuta 15, 2018

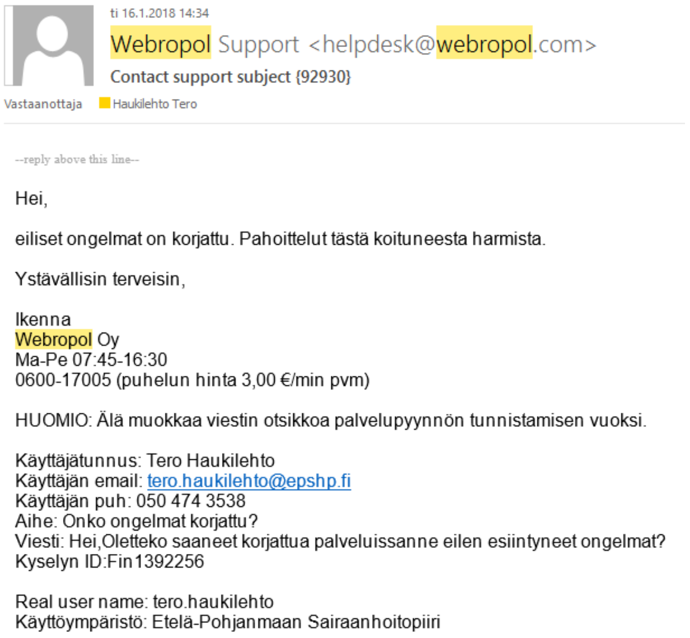
Alihankkijamme Nebula Oy on valitettavasti havainnut viime viikon palvelinpäivitysten tuotantoon viemisen jälkeen ongelman tietoturvapäivityksessä, jota he eivät sisäisessä testausympäristössä havainneet.

Varmistaaksemme verkkolaitteiden toimintavarmuuden Nebula Oyj joutuu suorittamaan huollon verkkolaitteisiin poikkeuksellisen lyhyellä varoitusajalla. Päivitykset tehdään Nebula Oy:llä asiakaskohtaisesti ja kestävät muutaman minuutin. Ts. Webropol-palvelussa on vain muutaman minuutin katko ensi yönä

Linkki alihankkijamme alkuperäiseen ilmoitukseen:

https://www.nebula.fi/node/2052

Pahoittelemme lyhyellä viiveellä annettua ilmoitusta.



ti 16.1.2018 14:34

Webropol Support <helpdesk@webropol.com>

Contact support subject {92930}

Vastaanottaja Haukilehto Tero

--reply above this line--

Hei,

eiliset ongelmat on korjattu. Pahoittelut tästä koituneesta harmista.

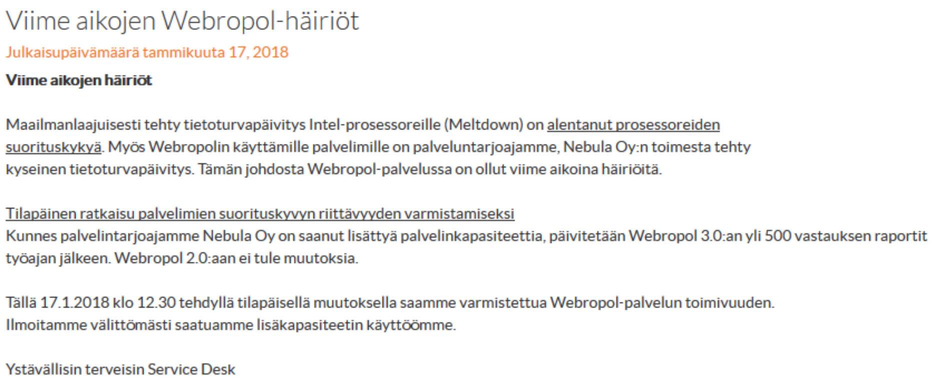
Ystävällisin terveisin,

Ikenna
Webropol Oy
Ma-Pe 07:45-16:30
0600-17005 (puhelun hinta 3,00 €/min pvm)

HUOMIO: Älä muokkaa viestin otsikkoa palvelupyynnön tunnistamisen vuoksi.

Käyttäjätunnus: Tero Haukilehto
Käyttäjän email: tero.haukilehto@epshp.fi
Käyttäjän puh: 050 474 3538
Aihe: Onko ongelmat korjattu?
Viesti: Hei,Oletteko saaneet korjattua palveluissanne eilen esiintyneet ongelmat?
Kyselyn ID:Fin1392256

Real user name: tero.haukilehto
Käyttöympäristö: Etelä-Pohjanmaan Sairaanhoitopiiri



Viime aikojen Webropol-häiriöt

Julkaisupäivämäärä tammikuuta 17, 2018

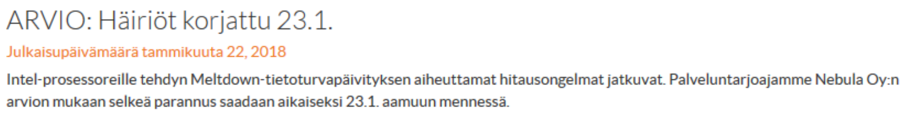
Viime aikojen häiriöt

Maailmanlaajuisesti tehty tietoturvapäivitys Intel-prosessoreille (Meltdown) on alentanut prosessoreiden suorituskykyä. Myös Webropolin käyttämille palvelimille on palveluntarjoajamme, Nebula Oy:n toimesta tehty kyseinen tietoturvapäivitys. Tämän johdosta Webropol-palvelussa on ollut viime aikoina häiriöitä.

Tilapäinen ratkaisu palvelimien suorituskyvyn riittävyyden varmistamiseksi
Kunnes palvelintarjoajamme Nebula Oy on saanut lisättyä palvelinkapasiteettia, päivitetään Webropol 3.0:an yli 500 vastauksen raportit työajan jälkeen. Webropol 2.0:aan ei tule muutoksia.

Tällä 17.1.2018 klo 12.30 tehdyllä tilapäisellä muutoksella saamme varmistettua Webropol-palvelun toimivuuden.
Ilmoitamme välittömästi saatuamme lisäkapasiteetin käyttöömme.

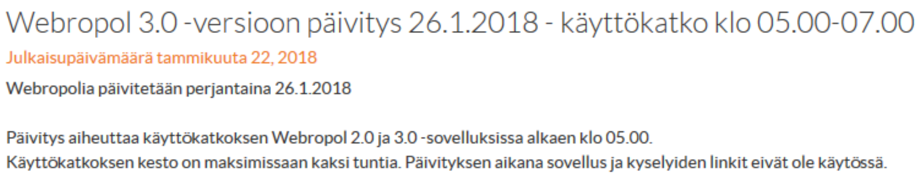
Ystävällisin terveisin Service Desk



ARVIO: Häiriöt korjattu 23.1.

Julkaisupäivämäärä tammikuuta 22, 2018

Intel-prosessoreille tehdyn Meltdown-tietoturvapäivityksen aiheuttamat hitausongelmat jatkuvat. Palveluntarjoajamme Nebula Oy:n arvion mukaan selkeä parannus saadaan aikaiseksi 23.1. aamuun mennessä.

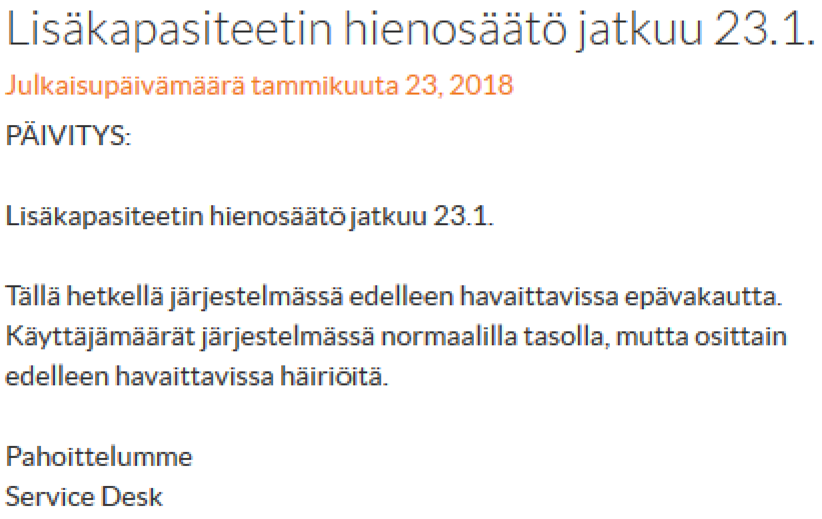


Webropol 3.0 -versioon päivitys 26.1.2018 - käyttökatko klo 05.00-07.00

Julkaisupäivämäärä tammikuuta 22, 2018

Webropolia päivitetään perjantaina 26.1.2018

Päivitys aiheuttaa käyttökatkoksen Webropol 2.0 ja 3.0 -sovelluksissa alkaen klo 05.00.
Käyttökatkoksen kesto on maksimissaan kaksi tuntia. Päivityksen aikana sovellus ja kyselyiden linkit eivät ole käytössä.



Lisäkapasiteetin hienosäätö jatkuu 23.1.

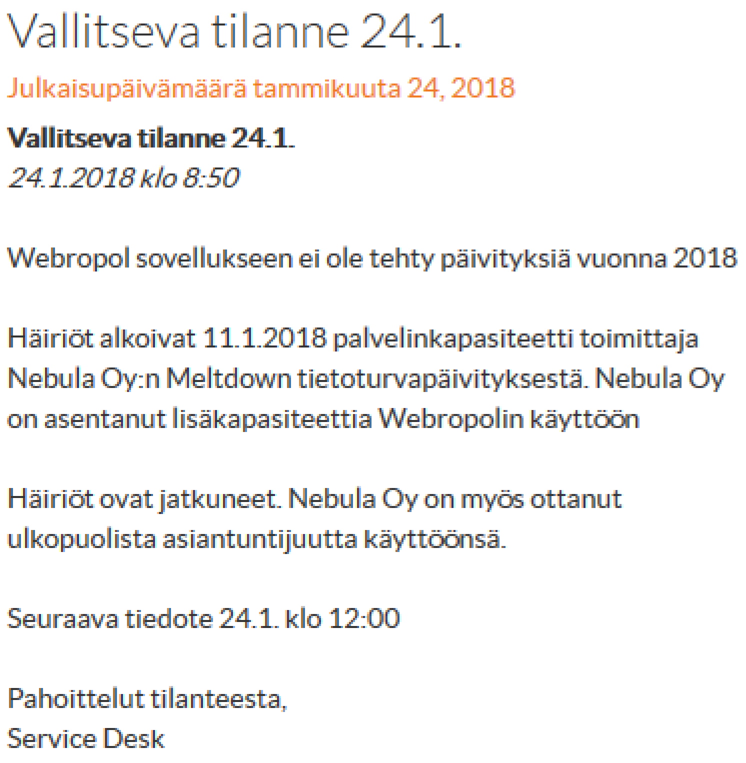
Julkaisupäivämäärä tammikuuta 23, 2018

PÄIVITYS:

Lisäkapasiteetin hienosäätö jatkuu 23.1.

Tällä hetkellä järjestelmässä edelleen havaittavissa epävakautta.
Käyttäjämäärät järjestelmässä normaalilla tasolla, mutta osittain edelleen havaittavissa häiriöitä.

Pahoittelumme
Service Desk



Vallitseva tilanne 24.1.

Julkaisupäivämäärä tammikuuta 24, 2018

Vallitseva tilanne 24.1.
24.1.2018 klo 8:50

Webropol sovellukseen ei ole tehty päivityksiä vuonna 2018

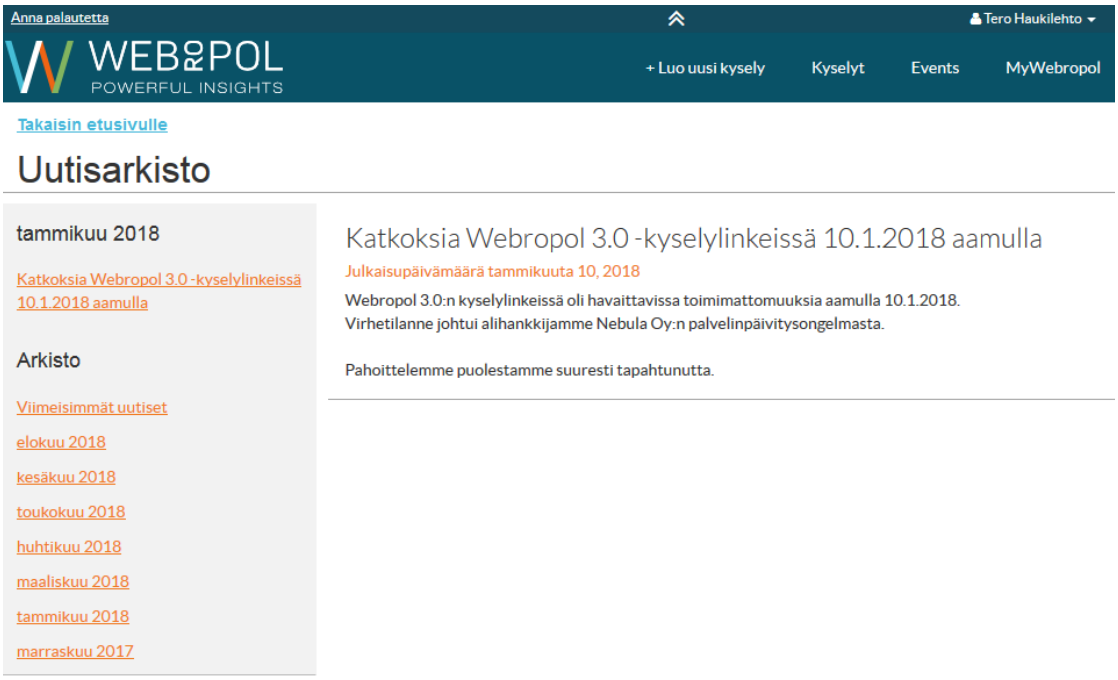
Häiriöt alkoivat 11.1.2018 palvelinkapasiteetti toimittaja Nebula Oy:n Meltdown tietoturvapäivityksestä. Nebula Oy on asentanut lisäkapasiteettia Webropolin käyttöön

Häiriöt ovat jatkuneet. Nebula Oy on myös ottanut ulkopuolista asiantuntijuutta käyttöönsä.

Seuraava tiedote 24.1. klo 12:00

Pahoittelut tilanteesta,
Service Desk

Appendix 10. Webropol fault notification in August 2018.



Uutisarkisto

tammikuu 2018

Katkoksia Webropol 3.0 -kyselylinkeissä 10.1.2018 aamulla

Arkisto

Viimeisimmät uutiset
elokuu 2018
kesäkuu 2018
toukokuu 2018
huhtikuu 2018
maaliskuu 2018
tammikuu 2018
marraskuu 2017

Katkoksia Webropol 3.0 -kyselylinkeissä 10.1.2018 aamulla

Julkaisupäivämäärä tammikuuta 10, 2018

Webropol 3.0:n kyselylinkeissä oli havaittavissa toimimattomuuksia aamulla 10.1.2018.
Virhetilanne johtui alihankkijamme Nebula Oy:n palvelinpäivitysongelmasta.

Pahoittelemme puolestamme suuresti tapahtunutta.