jamk

Determining personnel's level of cyber security knowledge in Sasky Education Consortium

Juha Reijasto

Master's thesis
November 2021
Technology
Master's Degree Programme in Cyber Security

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Reijasto, Juha

Determining personnel's level of cyber security knowledge in Sasky Education Consortium

Jyväskylä: JAMK University of Applied Sciences, November 2021, 53 pages.

Master's Degree Programme in Cyber Security, Information Technology

Permission for web publication: Yes

Language of publication: English

Abstract

The subject of the research was to study how the personnel of the consortium of education associations understands the threats caused by cyber security and to find out the initial level of cyber security expertise. In addition, the aim was to develop a reference framework for the organization that it can use to improve the cyber security skills of the personnel in the future. The client was the Sasky Education Con-sortium.

The importance of cybersecurity has increased with globalization and digitalization and thus added challenges for the organization. However, to achieve a good level of cyber security, it is not enough for the organization to invest in software and hardware. Still, the competence and motivation of the personnel play a significant role in forming the level of cyber security.

The theoretical part deals in general with data protection and data security issues, legislation, the EU Data Protection and Regulation, and reference frameworks related to cyber security. In addition, the theory has addressed the impact of corporate culture in information security situations and the effect of psy-chology on personnel operations. Cybersecurity of hardware and software was excluded from the study. Similarly, students' cybersecurity competencies were left unaddressed. Quantitative research was used as the research method. An electronic survey was utilized in the personnel competence survey.

The findings of the study were compared with other similar studies. Based on the comparison, it was found that the results obtained are in line with previous studies. Based on the results, the consortium has needed to improve the cyber security skills of the personnel, the skills are mainly good, but some short-comings were also found.

In the big picture, an organization needs a culture change. Cyber security expertise must be in everyone's control to understand the impact of the choices made on overall cybersecurity. Thus, cybersecurity is a part of everyone's daily work, not a separate entity taken care of by the IT department or management. Further training and precise guidance can improve this understanding.

Keywords/tags (subjects)

Cyber security, employee survey, information security, privacy

Miscellaneous (Confidential information)

jamk

Kuvailulehti

Reijasto, Juha

Henkilöstön kyberturvallisuustietämyksen tason määrittäminen

Jyväskylä: Jyväskylän ammattikorkeakoulu. Marraskuu 2021, 53 sivua.

Master's Degree Programme in Cyber Security, Information Technology

Julkaisun kieli: englanti

Verkkojulkaisulupa myönnetty: Kyllä

Tiivistelmä

Tutkimuksen aiheena oli tutkia, miten koulutuskuntayhtymän henkilöstö ymmärtää kyberturvallisuuden aiheuttamat uhat ja lisäksi selvittää kyberturvallisuusosaamisen lähtötaso. Tavoitteena oli laatia organisaatiolle viitekehys, jonka avulla henkilöstön kyberturvaosaamista voidaan tulevaisuudessa parantaa. Toimeksiantajana oli Saskyn koulutuskuntayhtymä.

Kyberturvallisuuden merkitys on kasvanut globalisaation ja digitalisaation myötä ja siten lisännyt haasteita organisaatiolle. Hyvän kyberturvatason saavuttamiseksi ei riitä pelkästään organisaation panostus ohjelmistoihin ja laitteistoihin, vaan henkilöstön osaamisella ja motivaatiolla on merkittävä rooli kyberturvatason muodostumisessa.

Teoriaosassa käsiteltiin yleisesti tietosuojaan ja tietoturvaan liittyviä asioita, lainsäädäntöä, EU:n tietosuoja-asetusta sekä kyberturvallisuuteen liittyviä viitekehyksiä. Lisäksi teoriassa on käsitelty yrityskulttuurin vaikutusta tietoturvaan liittyvissä tilanteissa ja psykologian vaikutusta henkilöstön toimintaan. Laitteistojen ja ohjelmistojen kyberturvallisuus rajattiin tutkimuksen ulkopuolelle. Samoin käsittelemättä jätettiin opiskelijoiden kyberturvallisuusosaaminen. Tutkimusmenetelmänä käytettiin määrällistä tutkimusta. Henkilöstön osaamiskartoituksessa hyödynnettiin sähköistä kyselytutkimusta.

Tutkimuksessa saatuja tuloksia verrattiin muihin vastaaviin tutkimuksiin. Vertailun perusteella voitiin todeta, että saadut tulokset ovat samansuuntaisia aiempien tutkimusten kanssa. Tulosten perusteella koulutuskuntayhtymällä on tarpeita henkilöstön kyberturvallisuusosaamisen parantamiseen, ja osaaminen on pääosin hyvää, mutta myös joitakin puutteita havaittiin.

Isossa kuvassa organisaatio tarvitsee kulttuurin muutosta. Kyberturvaosaaminen tulee olla kaikkien hallinnassa, jotta ymmärretään tehtyjen valintojen vaikutus kyberturvan kokonaisuuteen. Kyberturvallisuus on siis osa jokaisen päivittäistä työtä, eikä erillinen IT-osaston tai johdon huolehtima kokonaisuus. Lisäkoulutuksella ja täsmällisellä ohjeistuksella tätä ymmärrystä voidaan parantaa.

Avainsanat (asiasanat)

Kyberturvallisuus, kyselytutkimus, tietoturva, tietosuoja

Muut tiedot (salassa pidettävät liitteet)

Contents

Figures

Tables

List of Abbreviations

CIA	Confidentiality, Integrity and Availability
DMP	Data Management Plan
DoS	Denial of Service attack
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
IOT	Internet of Things
ISMS	Information Security Management Systems
ISO	International Organization for Standardization
IT	Information Technology
JAMK	Jyväskylä University of Applied Sciences
KATAKRI	Information security audit tool for authorities
MITM	Man in the middle attack
NCSA	National Communications Security Authority
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NRA	National Regulatory Authority
OSINT	Open Source Intelligence
SA	Security awareness
SFS	Suomen standardoimisliitty ry.
SIEM	Security Information and Event Management
TRAFICOM	The Finnish Transport and Communications Agency
VAHTI	he Government Information Security Management Board
QM	Quality Management

1 Introduction

Awareness of cybersecurity is a theme that touches many businesses and people. There are numerous stories in the world about cybersecurity and the dangers associated with it. Cyber security issues come up almost daily in various media. Usually, cybersecurity comes up when something serious has happened.

The level of cyber security awareness must be high so that the company's operations and administration can be reached at all times. It is not enough for a company to spend on software and infrastructure to improve its cybersecurity; employees' skills and conduct are also essential aspects of the problem.

The importance of cybersecurity has grown with globalization and digitalization and thus increased challenges for the organization. To achieve a good level of cyber security, it is not enough for the organization to invest in software and hardware. Still, the competence and motivation of the personnel play a vital influence in the creating cyber security levels.

By mapping the level of cyber security knowledge of the personnel and getting acquainted with the challenges in the field, safe operating methods can be identified. Thus, a quick and inexpensive way to improve an organization's level of cybersecurity is to increase employee awareness of cybersecurity.

The subject of the study is to find out how the personnel of the consortium understands the threats caused by cyber security and to map the initial level of cyber security expertise. In addition, the aim is to develop a reference framework for the organization that can be used to improve the cyber security skills of the personnel in the future.

The subject of the study was raised in discussions with Sasky's personnel representatives, who revealed that the organization faces challenges in cyber security issues. As a result, solutions to the challenges were sought through the completion of the thesis.

The issue was addressed in two different ways; by reviewing previous research on the subject and through a personnel survey. The survey was conducted as a quantitative survey. Respondents from all organizational units and all personnel groups participated in the survey.

The work examined issues related to personnel activities related to cyber security. Hardware and software were excluded from the study. Similarly, students' cybersecurity competencies were left unaddressed.

1.1 Existing research

As background work for my work, I became acquainted with previous research related to personnel information management skills, which have been linked to information security and related training. From the existing research, I tried to find answers to the development of personnel skills and ensure good information management practices.

It should be in the minds of cybersecurity professionals to raise cybersecurity awareness among the public. Educating the public is essential for the adoption of cyber security practices (Bada et al. 2020). In a later survey of the impacts of cyber security awareness campaigns, Bada et al. (2020 preprint) sketched out five components that influence the viability of awareness campaigns. The primary is the proficient arrangement of the campaigns, and the second moment is the significance of not conjuring fear. The final variables are related to giving concrete, feasible steps in progressing cyber security and providing training. All of this should be done inside an appropriate social setting.

High-information training on cyber security has been found to influence behavior (McCrohan et al., 2010) but indeed, an elevated level of cyber security awareness does not fundamentally lead to critical execution of cyber security defensive measures (Zwilling et al., 2020). Straightforward recreations have been found to have the potential to assist teach individuals in cyber security, as seen in a ponder on teaching individuals on watchword security utilizing an Android application (Scholefield & Shepherd, 2019). For illustration, within the programs conveyed to children within the, Joined together Middle easterner Emirates and considered by Al Shamsi (2019), the substance of cyber security awareness programs ought to incorporate the recognizable proof of various online dangers. Indeed, although the test measure of that thinks about was exceptionally little, the

comes about were moderately uniform appearing that training, recordings, recreations, and blurbs all aid raise the cyber security awareness. (Al Shamsi, 2019.)

Gaps have been identified in European vocational and cybersecurity training, so education is also essential in the digital age (European Cyber Security Organisation, 2018). A consider of over 1200 healthcare experts in Finland appeared that cyber security awareness isn't sufficient and must be expanded (Haukilehto & Hautamäki, 2019). Individuals confronted with numerous notices and complicated counsel may forsake all endeavors for security and not stress approximately any cyber security threats. (Bada et al., 2020 preprint.)

Kruger & Kearney (2006) have examined a strategy based on social psychology research that can be utilized to familiarize employees with an information security mindset, behavior, and knowledge in a global mining company. They note that ignoring personnel for security reasons is one of the most significant security risks. The insignificant creation of a security program does not increase personnel's understanding of their role in ensuring security. Raising customer awareness and identifying hazards requires continuous and measurable action. Based on the survey, the strategy provided the administration with information on the level of information security. It was thus able to coordinate the critical improvement objectives for the information security areas. (Kruger & Kearney 2006.)

In her dissertation, Mari Karjalainen (2011) has created a metatheory for Information Security Education. She also says employees are one of the biggest threats to an organization's information security. She argues that in addition to an effective training method, it is crucial to understand employees' information security behavior. She defines the pedagogical requirements of information security education in the context of psychological, content, teaching methods, and learning assessment. In addition, she has created a theoretical framework to help understand the reasons for employees' security behavior. (Karjalainen 2011.)

The directing components of the hypothetical system for data security behavior are the social, organizational, and experiential measurements. Concurring to Karjalainen, at the corporate level, communication is the premise for advancing information-safe behavior so that employees get the esteem of data in their work. The transmission incorporates data security arrangement, verbal

communication, preparing, and the part and commitment of administration. It too covers directions, supervision, expenses, punishments, and coercive measures, the implies of which, in any case, Karjalainen considers to be robust in impacting employees' data security behavior. Information of the social measurement, which incorporates the organizational culture, society's standards, and the person's claim social foundation, makes a difference to plan a communication and instructive approach. In expansion, there's an ought to get it the behavior of employees through an experience-based measurement that covers their characteristics and past encounter, for case in connection to data innovation. All of these directing variables have an impact on a person's cognitive instruments. One of the main critical ways to diminish representative uncertainties and increment positive alter is the levelheaded measurement. For case, investigate appears that seen frameworks can have vital impacts on employees' data security behavior. In any case, paying consideration to this indirection and counseling gives less encounter with the trouble of the frameworks. It must too be sensibly illustrated that non-compliance with the rules has negative results, whereas the proper course of activity benefits one's claim work. In expansion, it ought to be caught on that an individual frequently does not make a choice to take after or not to take after security rules, but they are a portion of a person's behavior exterior of security behavior. Strategies are taken after since it is felt that it is as it were vital to do so; as a result, others take after them as well. (Karjalainen 2011.)

Previous research shows that document management, the promotion of information security, as well as the development of information management throughout the organization must involve all personnel from information processors to the management level. This requires training, commitment, and a conversational approach to ensure common understanding and benefit. Understanding how an organization's working models and worker characteristics influence the collection of data administration abilities can influence not as it were the amassed information but moreover the employees' inspiration and demeanor towards information security and data security.

1.2 Organization introduction

In 1966, the SASKY Municipal Education and Training Consortium (Sasky) was established. Sasky, which is owned by 13 municipalities in the Tampere region, offers VET in practically all fields at 12 separate school campuses throughout the region. Sasky additionally has two general upper

secondary schools, a civic institution, and a music institute that provide broad education. Sasky has recently expanded its services to include apprenticeship training, labor policy education, and prison education. There are around 7 000 students (6 000 VET) and 520 personnel members. Our VET is quite appealing; approximately 60% of potential applicants choose VET. (Sasky 2021.)

In expansion, the exercises advance the competitiveness of the business community and community well-being through their work-oriented and wide-ranging activities. Within the vision of the SASKY consortium of instructive regions, the motto is "Sasky knows how to create creative worlds - working together." Sasky Education Association's strategy towards 2024 states that SASKY follows good management and governance practices. This incorporates inside control and chance administration. (Sasky strategia 2021.)

1.3 Research objective

The subject was to study how the personnel of the consortium of education associations understands the threats caused by cyber security and to find out the initial level of cyber security expertise. The work aims to map the personnel's cyber security skills with a survey to increase the personnel's interest in the topic. Based on the study, suggestions were made to Sasky to improve security information. This includes, e.g., mapping how guidelines and general standards are understood and how an organization's policies and practices are recognized. Based on the results, suggestions for improvement will be developed to improve the competence of Sasky's personnel.

1.4 Structure of the research report

The background research was started by getting acquainted with the cyber security environment. News, articles, blogs, and cybersecurity works have been used as sources that provide a comprehensive picture of the dangers of cybersecurity and the ultimate challenges. The study was utilized as a data collection tool to make good use of the observation of both the study and the composed texture in the organization of the study. Quantitative research was chosen as a schematic technique because it was desired to elicit more reactions than the assembly thinking. Quantitative research provides a better understanding of cybersecurity information for all personnel.

The survey was conducted in the spring of April 2021 at the turn of April-May. The results were collected over a period of three weeks, after which they were analyzed and recorded. The thesis was mainly written only after the analysis of the questionnaire. After all the steps and results had been recorded in the thesis, the results and the analysis were handed over to Sasky. In the final stage, the company's feedback was processed into suggestions for further development.

The target group of the survey was the entire Sasky personnel. The personnel includes teaching personnel, supervisors, managers, support, and common services personnel—the people who participated in the survey work in 10 different units. The units are Hayo, Lupi, Mskk, Saso, Saty, Tpa, High school, Petejä or Music School, Common services and Information Management. Students were excluded from the survey.

1.5 Research questions

Discussions with Sasky's personnel representatives revealed that the organization faces challenges in cybersecurity issues. Solutions to the challenges were sought through the completion of the thesis. One important entity was the need to map the level of cyber security expertise of the personnel.

The research questions in this study were selected: How do personnel understand cyber security and its threats? What are the major gaps in personnel cybersecurity knowledge, and how are the gaps addressed?

The body of the question was drafted in such a way that it would consider the question in a way that maps the competence of the personnel. Question frames commonly used in audits are typically aimed at corporate management and IT departments, with very detailed content. For example, Traficom's cybermeter developed in 2020 served as a background for drafting questions. The question set should be updated based on the feedback received so that a regular survey is comparable with previous surveys. Personnel survey questions were carefully planned with Sasky's Safety Manager. Ideas for the survey questions were mapped from previous theses, research, Traficom's cybersecurity meter, and literature. These ideas were mirrored and further developed for the needs of the organization.

However, security or cybersecurity is not Sasky's main business, so the company did not consider it necessary to conduct a mandatory personnel survey, but the survey was based entirely on the voluntary nature of the respondents. The survey examined participants' security knowledge. The aim was to make the survey easy to answer so that the threshold for employees to participate in the survey would not become too high.

1.6 Limitations of the study

The thesis examines issues related to personnel behavior in cyber security issues. The work does not cover servers, hardware, and technologies, such as system programming or configuration. Instead, the work mainly focuses on the research of personnel activities in matters related to cyber security. Sasky's students are not in the scope of this study.

2 Infrastructure and cyber security

Today, the definitions of data protection and security have become more precise. The terms are the same worldwide. Similarly, the word cybersecurity is understood in a slightly different way in different contexts. There's no correct definition of the term digitalization or cybersecurity digitalization or cybersecurity. One of the world's leading research institutes, Gartner Inc., describes the terms as follows. "Digitalization is the use of digital technologies to change a business model and provide new revenue and value-producing opportunities; it is the process of moving to a digital business." (Digitalization, 2021.)

Cybersecurity is the combination of individuals, arrangements, forms, and innovations utilized by an undertaking to secure its cyber resources. Cybersecurity is optimized to levels that commerce pioneers characterize, adjusting the assets required with usability/manageability and the sum of hazard counterbalanced. Subsets of cybersecurity include IT security, IoT security, and information security. (Cybersecurity 2021.)

Cybercrime takes place across borders, in which case the laws of an individual country do not apply. The problem with these issues is the lack of laws worldwide, which has fortunately been improved; for example, the GDPR regulation of the European Union is a good example of this.

In many countries, there are organizations that take care of issues related to information security, data protection, and cyber security; in Finland this institution is called Traficom The Finnish Transport and Communications Organization is a specialist in permit, enlistment, and endorsement things. Traficom's mission is to construct associations that keep individuals, information, and products moving easily, safely, and economically. Traficom constructs unwavering operational quality by moving forward security when it comes to transport and advanced society and endeavor to supply quality and reasonable administrations within the transportation and associations segment. It ensures that people-centric and sustainable services will continue to be built in the future. (Traficom, 2021.)

The NCSA-FI is capable of security things related to the information exchange and dealing with classified data in electronic communications. The administrations of NCSA-FI back organizations' proactive security work and conceivable operational outcomes. In Finland, the obligation for our universal data security commitments has been separated among a few specialists. NCSA-FI is part of the Finnish security authority organization. The Service acts as the National Security Specialist (NSA) in Finland. (Traficom, 2021.)

2.1 Terminology

Data security rotates around the three essential standards: Confidentiality, Integrity, and Availability, also known as the Security Triad (CIA), which could be a show planned to direct arrangements for data security inside an organization. The CIA security triangle (see Figure 1) is a critical security concept since all security controls, instruments, and shields are executed to supply one or more of these assurance sorts. Vulnerabilities and threats are measured for their potential capability to compromise one or all the CIA set of three standards. Group of three is the premise for making an all-encompassing security arrangement to ensure all of the organization’s essential and delicate resources. All cyber-attacks can undermine one or more of the three parts of the CIA set of three. (OpenLearn, 2020.)

Figure 1. The CIA triad

For example, various scam attempts, personal privacy violations, spam, industrial espionage, piracy, computer viruses, cyber terrorism, and cyber warfare are considered threats to information security. Security threats include unauthorized access, unauthorized use of information, disclosure of confidential information, confusion of data, alteration of information, investigation of confidential information, copying of information, and destruction of information.

2.1.1 Confidentiality

Confidentiality (level of secrecy) or/and privacy is essential. All information by clients is secured and kept insecure. In an organization, information taken care of is intensely ensured, scrambled. There are restricted people who can get to clients' information. Get to must be limited to those authorized to see the information in the address. Every single activity is recorded fair perusing knowledge indeed. All activities can be followed afterward. Encryption is one way to guarantee secrecy, and a moment strategy is to get to control.

2.1.2 Integrity

Integrity involves keeping up the consistency, precision, and dependability of information over its whole life cycle. The information must remain intaglio to guarantee that unauthorized people cannot adjust the info (for case, by breaching privacy). In expansion, there are built-in instrument programs to distinguish any changes in information that might happen since the server crash. Record authorizations, get to controls, form controls are utilized to keep track of all activities, e.g., to avoid wrong changes. Approval of information is critical. Data that are modified by as it were authorized parties and there are no blunders in it, the data is dependable.

2.1.3 Availability

Availability means data is available, e.g., service is up and running. All downtime is critical for business. Security software such as firewalls guards against downtime and unreachable data due to malicious actions.

2.1.4 Authentication

Authentication is verifying the identity. In other words, prove to the system that you are the person you claim to be by showing some evidence—for example, entering a user id and password to log in.

2.1.5 Non-Repudiation

Non-Repudiation is a confirmation instrument that provides proof of the integrity and origin of data. A confirmation that the sender sent the message can be asserted to be genuine with high assurance. One case will be if the mail says Juha sends it at that point in the future, Juha can't claim that he did not initially send it. Advanced signature is utilized to guarantee non-repudiation. Non-Repudiation is a confirmation instrument that that gives verification of the judgment and beginning of information. Proof that the sender sent the message can be declared to be veritable with tall confirmation.

2.1.6 Asset

An asset is any information, gadget, or other components of an organization's framework that's profitable – regularly since it contains delicate information or can be utilized to get to such data. For case, an employee's desktop computer, tablet, or company phone would be considered an asset, as would applications on those gadgets. Moreover, basic frameworks, such as servers and back frameworks, are assets.

2.2 Cyber security awareness

In expansion to tending to the concepts within the CIA group of three, one of the purposes is to supply a thought-provoking way to see at cyber security inside a particular context, to raise awareness within the public on cyber security issues. There could be a requirement for this since,

as an illustration, cyber security abilities were lacking in a study of healthcare experts (Haukilehto & Hautamäki, 2019). Now and then, putting information at risk could be a choice, but in some cases, the reply "don't do it" isn't viable, and after that, it would be shrewd to at slightest have a few kinds of an interruption location system in place. Information is predominant in nearly all perspectives of life, from the private lives of individuals to the extensive commerce of organizations. A few of this data is delicate and should be kept secure, but it can be contended that securing all data is critical. The concepts related to data security can now and then be challenging to get, and thus demeanors towards obtaining information can be remiss. This will be an issue when users don't realize that their data is in peril and take more significant than average risks.

To get it, the contrasts between terms like cyber security and data security are critical. These two words, information security and cyber security, are by and expansive utilized as identical words in security expressing and make a portion of confusion among security experts. A few individuals think that cyber security is a subset of data security, whereas others think the inverse. In figure 2 there is a graph from the relationship between ICT security, cyber security, and information. In the diagram (Ciso platform 2016) right side diagram represent Cyber security - things that are vulnerable through ICT, it includes information, both physical and digital, and non-information such as cars, activity lights, electronic apparatuses, etc., whereas cleared outside speak to the data security - which comprises of data both computerized and analog. (Ciso platform 2016.)

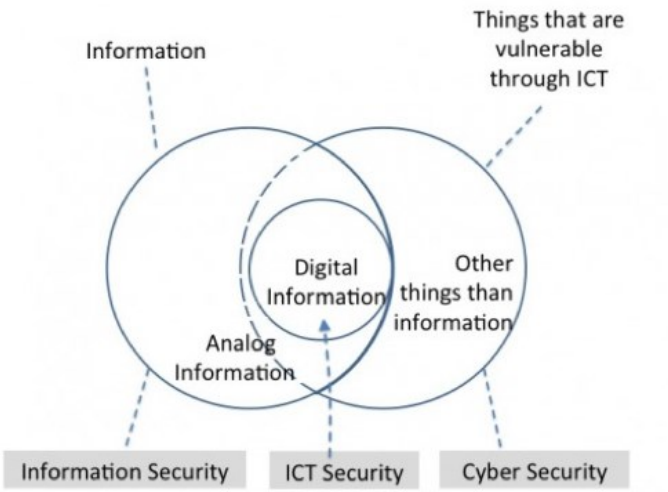

Figure 2. Relationship between ICT security, cyber security and information

2.3 Cyber threats

Cybersecurity causes harmful actions aimed at data corruption, data theft, or disruption of digital life. Cyber threats include computer viruses, data breaches, denial of service (DoS) attacks, and other attack vectors. The threat is the likelihood of a successful cyberattack aimed at unauthorized access, damage, destruction, or theft of information technology assets, computer networks, intellectual property rights, or other forms of confidential data. Cyber threats can come from trusted users within your organization or remotely by unknown parties (UpGuard 2021).

Cyber dangers come from various threat actors like organized wrongdoing organizations, hacktivists, disappointed insiders, programmers, common catastrophes, coincidental activities of authorized users. Typical threats include malware, spyware, phishing attacks, distributed denial of service (DDoS) attacks, ransomware, zero-day exploits, advanced persistent threats, trojans, wiper attacks, Intellectual property theft, theft of money, data manipulation, a man-in-the-middle attack (MITM attack) and unpatched software.

2.4 Cyber-security trends on 2021

Increasingly, everybody is moving towards an advanced organize, which moreover causes side impacts. Criminals want to benefit at the expense of others. More successful utilization of digitalization and data systems has expanded the dangers of cyber dangers in both the open and private divisions. Dr. Schröfl has said that cyber-attacks against EU countries have increased by more than 200%. (Hybrid CoE, 2020.)

Recent trends, the consequences of a worldwide pandemic, and cybersecurity statistics show a significant rise in hacked and breached data from previously unknown sources becoming more widespread in the workplace, such as mobile and IoT devices. COVID-19 has also increased the number of remote workers, increasing the risk of cyberattacks. Furthermore, according to recent security studies, most businesses have exposed data and poor cybersecurity policies, leaving them vulnerable to data loss. Therefore, companies must make cybersecurity knowledge, prevention, and security best practices a part of their culture to effectively combat evil intent. (Varonis, 2021.)

The near future looks somber for data security, says a modern NCSC-FI figure. Whereas the Vastaamo information breach turned the highlight on questions of safety and obligation within the setting of online administrations, this year will likely see more episodes. Numerous associations are developing accentuation on data security when building their online administrations, and regulators are looking to extend solidness. Despite these measures, we are improbable to dodge tricks or cyber assaults. Traficom's cyber top ten security forecast for 2021 is listed below. (Traficom 2021.)

1. "We will continue to witness unfortunate cyber incidents in 2021"
2. "More regulation, more stability"
3. "Differentiating between authentic and fake will become increasingly difficult"
4. "Much more time is needed until available know-how matches up to the challenges we face"
5. "Criminals will use cyber attacks to accumulate virtual currency"
6. "Remote work is here to stay, and so are the attendant risks"
7. "The competition for quantum-proof encryption will intensify"
8. "Fiercer competition among technological superpowers"
9. "State-level cyber influence operations will continue to become more numerous"
10. "Cyber security will finally feature on the agenda of top management"

2.5 Culture of security

The comment "Our safety department is getting more tools, but as an employee, I don't think I'm safe." and numerous other comparable words heard around the world. Often all these statements can be heard in the same company. Even though the best administration reserves the security work, gives the most recent, most compelling apparatuses, and bolsters these devices with an extraordinary security arrangement, but still does not accept that the company's data is secure. In reality, there's sufficient evidence that it isn't safe. Somewhere in the business of a company or government agency, something that should happen doesn't happen. Some or many people do not effectively support security. (Ross, 2011.)

The missing piece is a safety culture that can be defined as behavior patterns, beliefs, assumptions, attitudes. It is developed and learned, and it creates a sense of comfort. Culture develops a shared history as the group goes through everyday experiences. Similar experiences evoke specific responses that form expected and shared behaviors. These behaviors become unwritten rules, which become norms that are common to all people with the same shared history. (Ross, 2011.)

A culture is created whenever two or more people participate in a joint endeavor. The business environment has a behavior, beliefs, assumptions, attitudes, and practices that form a corporate culture. To the extent that information is part of this business, there is a safety culture. It may be weak, ineffective, disorganized, contradictory, unrecognizable, and haphazard, but it exists. It is recommended that the safety culture be strong, practical, well organized, and consistent. Even a company has many security components - personnel, software, hardware, procedures, policies, and standards - without a culture that binds them to the overall corporate culture, the best that can be hoped for is mechanical compliance with the data protection requirements standards. It is the minimum security that a company can tolerate. Security without culture is inadequate security.

Accomplishing a level of security does not happen in a self-produced and orderly way. It requires well-meaning individuals to need both positive and corrective steps to reinforce the safety culture to the required level, the level that administration extraordinary to have or ought to have within the intellect of the organization's administration. A security culture continuously exists, but a solid, compelling, and maintainable security culture requires work to construct and maintain. Culture cannot be actualized rapidly, as can security mechanics. There's no equipment to introduce or program to actualize. It includes making an attitude with the individuals who make up the company and its interatomic - between merchants, clients, other partners, and society. This attitude, points of view, and demeanors that direct behavior are a culture's substance that must be continuously planted, supported, and acknowledged. (Ross, 2011.)

2.6 Information security standard, laws, and legislation

Laws and regulations place restrictions on the management of an organization. The organization takes care of security matters within limits prescribed by law. Important law is the GDPR Privacy Regulation, which specifies in detail how personal data should be processed. On the security side, there are standards, recommendations, and frameworks to improve data security, but there is no binding legislation on data security and data protection. The Prime Minister of Finland Sanna Marin's government program has set goals for the development of national cyber security in connection with improving the situation, intensifying international cooperation and enhancing national coordination. In accordance with the Finnish Cyber Security Strategy, a cyber security development program has been prepared. (Valtioneuvosto 2021.)

A systematic approach that involves a process is called Information Security Management Systems (ISMS), technology, and people to protect and manage an organization's information through effective risk management. Laws, including EU GDRP, cover three key aspects: Confidentiality, Integrity, and Availability. (SFS-EN ISO/IEC 27000:2017.)

2.6.1 ISMS family of standards

The ISO 27000 arrangement collects all guidelines related to the data security administration framework and the ISMS family of measures. There's an organizational point of view focus in ISO 27001 and more focus on the individual in ISO 27002. Information Security Management System can be inspected against ISO 27001, which characterizes the review prerequisites. Comparing each standard, those outline together and are organized essentially. The difference is within the level of detail. ISO 27001 sets up what you must do but not how. ISO 27002 portrays how. The benefits of actualizing an ISMS will offer assistance to decrease data security dangers.

This standard describes details for requirements for the organization. In this document, there might be mentioned topic in one sentence, overall, about it. When the organization is planning an ISMS, it should focus on ISO 27001. Everything connected to the network is at risk for threat. The organization should be aware of possible threats, have a framework for identifying security risks, selecting controls, and continuously improve effectiveness. Also, legal and regulations need to be taken care of. Requirement standards are handled in ISO 27006 and ISO 27009 as well.

In ISO 27002 standards, there are described codes of practice for security controls. In this document, topics are explained thoroughly, in more than one sentence. The rest of ISO 27002, 3, 4, 5, 7, 12, 14, and TR 27008 and TR 27016 documents can be called guideline standards.

2.6.2 Vahti-instructions

The Ministry of Finance is responsible for leading and coordinating the development of information security in the Finnish public sector, especially in the central government. The Government Information Security Management Board (VAHTI), established by the Ministry of Finance, is responsible for the central government's information security operations, development, and coordination. In addition, VAHTI handles all-important significant government

information security policies and information security guidelines issues. In its work, VAHTI supports the preparation of government and treasury decisions and major government information security decisions. Furthermore, VAHTI aims to develop information security to improve the stability, continuity, quality, risk management, and emergency response planning of central government functions and promote information security to become an integral part of the operational performance of main government activities. (Vahti-instructions, 2021.)

2.6.3 Katakri

Katakri was created in 2009 as part of the government's internal security program. Authorities can use Katakri as an audit tool to assess an organization's ability to protect confidential information. Katakri itself does not establish information security requirements. Instead, it summarizes the minimum requirements under national law and international information security obligations. In this regard, the most important part of domestic law is the Central Government's Government Decree on Information Security (681/2010), which is an Act on Information Security and is protected to protect both domestic and international confidential information. . An important international source of information here is the Council Decision on Security Rules for the Protection of EU Confidential Information (2013/488/EU), which sets out the Security Basic Principles and Minimum Standards for the Protection of EU Confidential Information (EUCI). To guarantee straightforwardness, a source reference is continuously given in association with the necessities displayed in Katakri. (Katakri, 2015.)

2.6.4 How the EU tackles cyber threats

Cyberattacks and cybercrime are expanding in number and modernity over Europe. Moreover, this drift is set to develop advance within the future, given that 22.3 billion gadgets around the world are anticipated to be connected to the Internet of Things by 2024. (European Council, 2021.)

The EU is taking activities to address cyber security challenges like improving cyber strength, battling cybercrime, boos cyber discretion, strengthening cyber defense, boosting investigation and advancement, and ensuring a basic framework (European Board, 2021). The EU points to reinforce its security against cyber dangers and guarantee that businesses and citizens can benefit from dependable administrations.

The GDPR sets detailed company and organization requirements for collecting, storing, and managing personal data. This applies to both European organizations that process the personal data of individuals within the EU and external EU organizations that target EU residents (Your Europe, 2021).

The standards of information assurance measures are the rights of the information subjects, i.e., those having a place to the individual enroll, and the commitments of the information controller, i.e., the proprietor of individual information. Individual information assurance may be a crucial right of each human being, characterized by law and controls. It is the duty of organizations that prepare personal information to guarantee that their rights are regarded.

2.6.5 Cyber security framework, NIST

The framework uses businesspeople to guide cybersecurity activities and consider cybersecurity risks as part of an organization's risk management process. This framework is a set of cyber security activities that are benchmarks for performance and profitability. These references are shared in critical infrastructure sectors and provide detailed instructions for developing profiles for individual organizations. As a result, organizations can apply risk management principles and best practices to improve the security and resiliency of critical infrastructure, regardless of the magnitude of network security risks or the complexity of network security. (National Institute of Standards and Technology 2014.)

2.6.6 Cybermeter

Developed at NCSCFI (National Cyber Security Center), Cybermeter helps enterprise managers and organizations better control cyber risk and protect business continuity. Cybermeter, a tool developed at NSCSFI, enhances the capabilities of businesses, organizations, and society in general to prevent cyber threats. Cybermeter is a concrete tool that gives enterprise and organizational managers better control over cyber threats and provides a way to assess key features, processes, and dependencies. Social and organizational functions depend on digital services and systems. Digital operating environments are becoming increasingly vulnerable to cyber threats and interruptions, and interdependence increases the risk of operating interruptions. Preparation

requires cooperation between all parties and cross-sectoral understanding. This also helps protect Finland's overall cybersecurity level. (Cybermeter 2021.)

Cybermeter tool is designed for businesses to ensure preparedness for cybersecurity. The intention is that people familiar with cyber security will be audited. In connection with this work, focusing on mapping personnel competencies, this cybermeter tool was not used to determine personnel cyber security awareness.

3 Research

In development research, the goal is to bring about change (Kananen 2015). Developmental research is a set of different methods and is not considered a particular research method. In this study, an initial mapping is made, and suggestions for action can be made in the organization based on this. Where appropriate, it combines a quantitative and a qualitative research method (Kananen 2015). This study is the first mapping phase of development research.

The targets of this research plan are people, and data are collected through surveys. The data consists of survey responses. Two research methods, quantitative and qualitative, were considered to select the best research method. There is a clear difference in data processing between the two research methods. In quantitative studies, the data are numerical, and in qualitative studies, the data are not. However, these two research methods form a pair of methods that can be used alone or in combination to complement each other. (Koppa 2021.)

3.1 Qualitative and quantitave research methods

In contrast to quantitative studies of qualitative research, data are not numbers that attempt to answer probing questions that cannot be explained statistically, such as 'how' and 'why.' Qualitative research methods are ideal for gaining deeper information about a topic and help you understand people's reasons, motives, and answers (Kananen 2015, 70-71).

Quantitative survey methods are often used when measuring objects and statistically explaining the results (Koppa2010). Still, the current level of cybersecurity awareness, the reasons behind the level, and the search for answers to selected research questions that determine how to improve

awareness were considered insufficient to explain the results only statistically. For example, statistics and numbers may indicate what percentage of respondents know the correct answer, but quantitative research methods are not reliable ways to find and explain information about cybersecurity awareness levels and the reasons behind them.

3.2 Collection of research material

The data collection was carried out as a quantitative survey, which is well suited for collecting large-scale quantitative data and thus provides excellent support for research questions. Webropol was chosen as the survey implementation tool because this tool has been used in the company's previous research, and thus, the implementation environment had already been established. In addition, a familiar tool was considered to lower the threshold to participate in the study. The suitability of the Webropol tool for this survey was tested by first sending the survey to a smaller group of respondents.

The questions for the questionnaire were selected by familiarizing oneself with the need of the client; what questions can be used to map personnel cybersecurity skills and challenges. Thoughts on the questions were also gathered from the question batteries of other similar studies. There were originally 46 questions in the survey. Based on the feedback received, final questions were developed. The client hoped that it would take an average of 15 minutes to answer the questions. As a result, it was determined to cut the number of questions to 33. Keeping the survey reasonable was hoped to have a positive effect on the response rate.

The questions are divided in the results section into the following themes: Training and guidance, identification and assessment of cyber security risks, probability of cyber security threats, privacy, practical case studies, and managers.

3.3 Calculation methods

The following formulas have been used to subdivide the results. Average and standard deviation.

Average is

$$\bar{x} = \frac{\sum_{i=0}^{n} x_i}{\mathrm{n}}, \tag{1}$$

x_i is single observation, n is total number of observation.

Standard deviation is

$$s = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x})^2}, \tag{2}$$

where $\{x_1, x_2, \ldots, x_N\}$ are the observed values of the sample items, and $\bar{x}$ is the mean value of these observations, while the denominator N stands for the size of the sample: this is the square root of the sample variance, which is the average of the squared deviations about the sample mean.

This graph shows the distribution of observation values. The standard deviation is a measure of the variation in the observed values. The standard deviation of the observed values is the square root of the variance. In other words, a small standard deviation (variance) suggests that the observed values are centered around their center of gravity (arithmetic mean), and a large standard deviation (variance) implies that they are scattered.

3.4 Ethical Principles and Data Protection

This thesis work follows the ethical principles of the Jyväskylä University of Applied Sciences (JAMK) set out in JAMK staff (2018). The reason for these rules is to guarantee that the investigation delivered is of tall logical quality and a tall moral standard. (JAMK Staff 2018.)

The General Data Protection Regulation (GDPR) controls personally identifiable information collection, use, and storage. Since no personal information was collected, the data driving this thesis does not constitute a register and does not require special data protection protocols. (JAMK Staff 2018.)

Data management plan (DMP) was used to manage data and help others use data if shared (DMPTuuli, 2021).

3.5 Validation and reliability

Validity means whether the research has been done thoroughly, ie, whether the research is valid. Reliability assessments of quantitative and qualitative studies differ. Kananen (2015) defines qualitative research with five different criteria. Reliability criteria in qualitative research are Reliability, portability, dependence, confirmability, and saturation. Reliability means that the research results are truthful, i.e., they correspond to the phenomenon under study. Reliability, i.e., reality, and dependence, can be confirmed by peer review. (Kananen 2015.)

4 Results and Discussion

The questionnaire was sent to 579 people, of whom 183 replied, which gives the response rate 32%. Answering the questionnaire was voluntary. With the response rate quite low, the results need to be viewed critically. However, 183 responses were received, and responses were received from all units so that indicative interpretations could be made on the basis of the responses. Of the respondents, 21 were supervisors or directors, 97 were teaching personnel, and 65 were other personnel. The survey questions are in Appendix 1. Survey questions.

There is response percentage distribution by units in Figure 3. There were a total of 33 questions. There were 27 questions for the entire personnel and six additional questions for the supervisors.

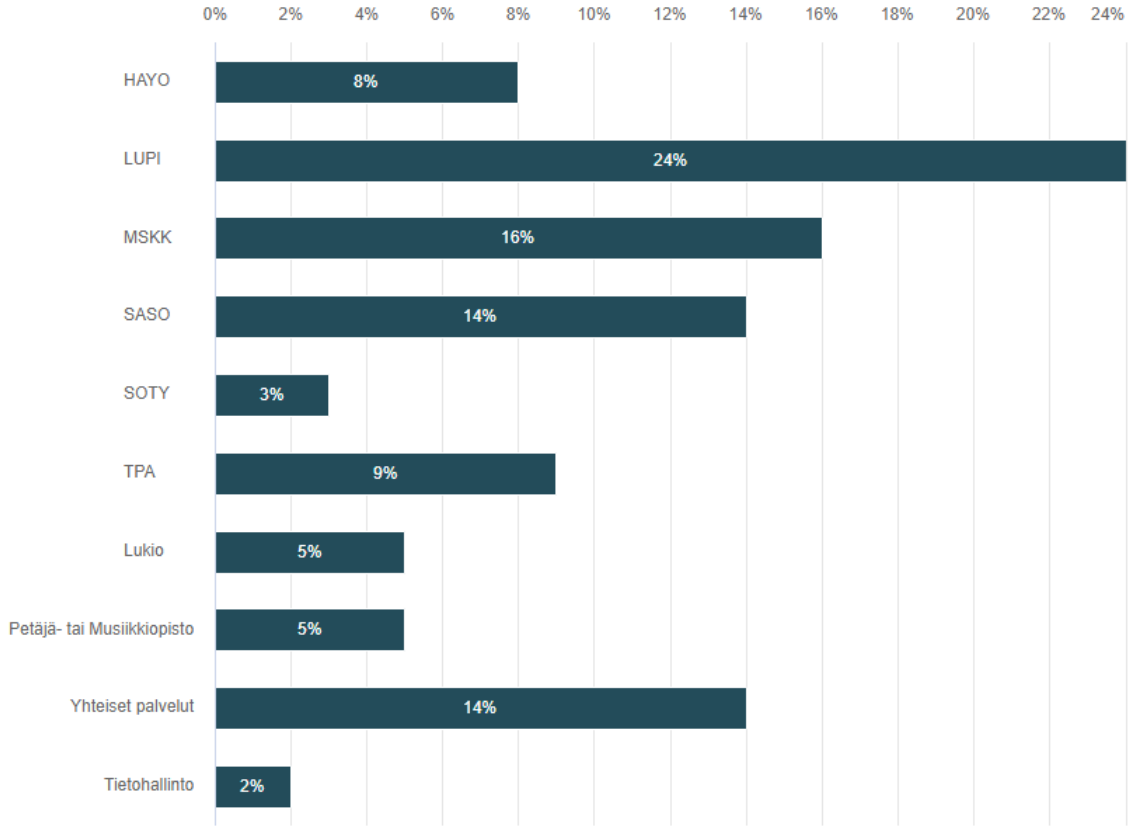

Figure 3. Percentage distribution of respondents by unit

4.1 Knowledge of terminology

Question 4 surveyed respondents' knowledge of basic cyber security terms; data privacy, security / cyber security, and security threat / cyber security threat. The answers showed that the knowledge was at a good level. According to the responses, respondents identified the terms as follows; privacy 98.3 %, cyber security 75.4 %, and cyber security threat 70.4 %.

Question 5 made statements related to basic terms. The aim was to find out how well the respondents knew the content and practical applications of the terms. The distribution of responses to correct cybersecurity claims are presented in Figure 4.

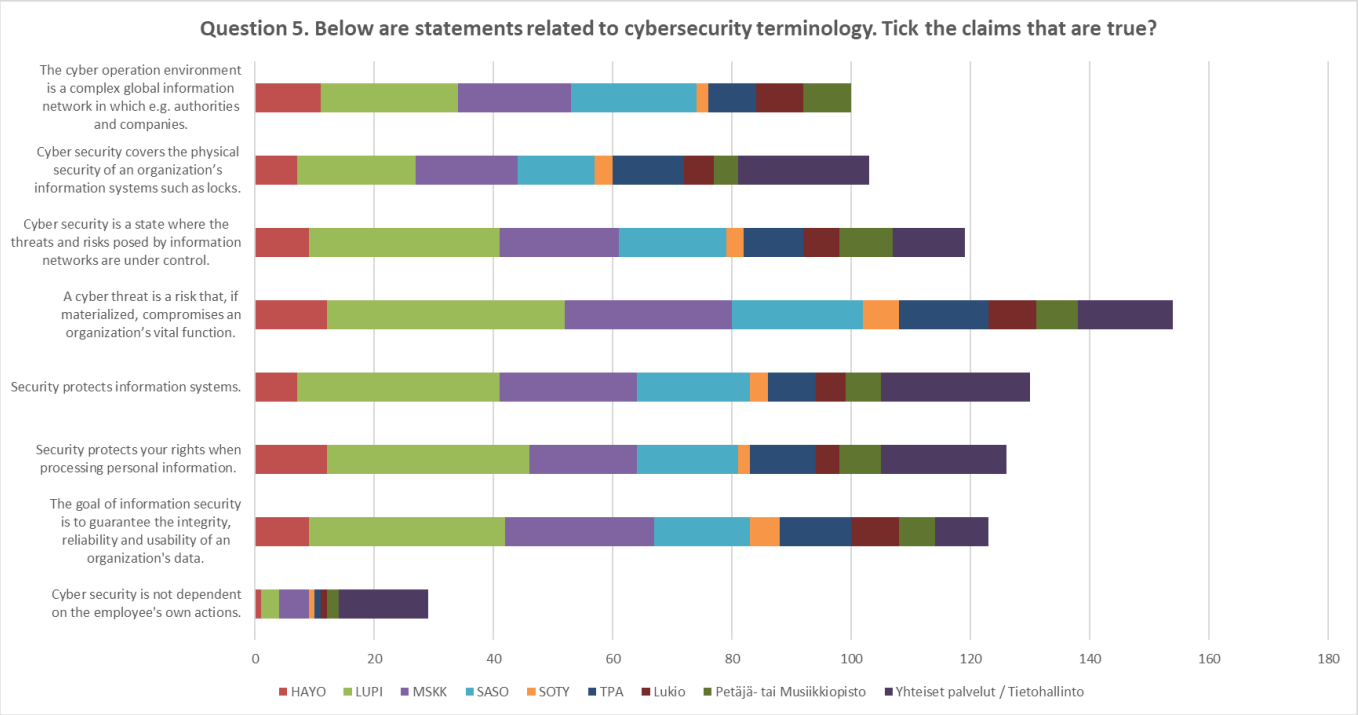

Figure 4. Distribution of responses to correct cybersecurity claims

The answers to question 5 showed that in quite a number of respondents, the terms were confused in practical situations. This is not likely to lead to threats, but the unfamiliarity of the terms should be taken into account in the form of instructions that are simple enough so that the use of the terms in the instructions does not cause misunderstandings.

4.2 Training and guidance

Question six mapped the previous cyber security training received by personnel. Question seven surveyed respondents' own perceptions of which subject areas they see a need for training.

Forty-four percent of respondents said they had received training in cybersecurity, and 25 percent of respondents had received training in the past year. Fifty-six percent said they had not received any cybersecurity training. Figure 5 shows the respondents' experiences of the need for training in different areas of information security. Respondents raised concerns about the security of smartphones. The distribution of responses to which security areas need more training is presented in Figure 5.

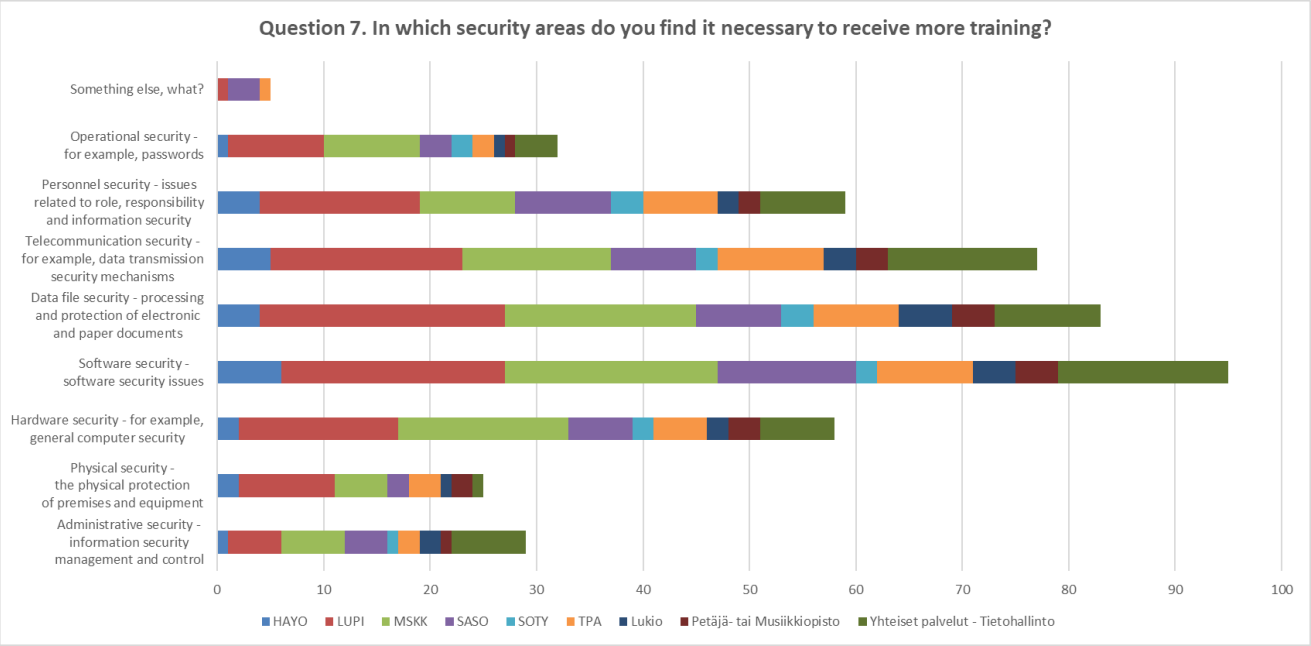

Figure 5. Distribution of responses to which security areas need more training

About half of the respondents saw the need for additional training in Software Security, Data File Security, and Telecommunication Security. One-third of the respondents also saw the need for training in equipment security and personnel safety. More effort should be put into implementing and introducing guidelines into the daily routine.

Questions 11 and 23 examined the personnel's knowledge of the current security guidelines and the respondents' opinions on the adequacy of the information and policies for cyber security threats. Figure 6 shows respondents' views on whether the organization provides sufficient information and guidance on information / cyber-security threats. Views on whether the organization provides sufficient information on threats presented in Figure 6.

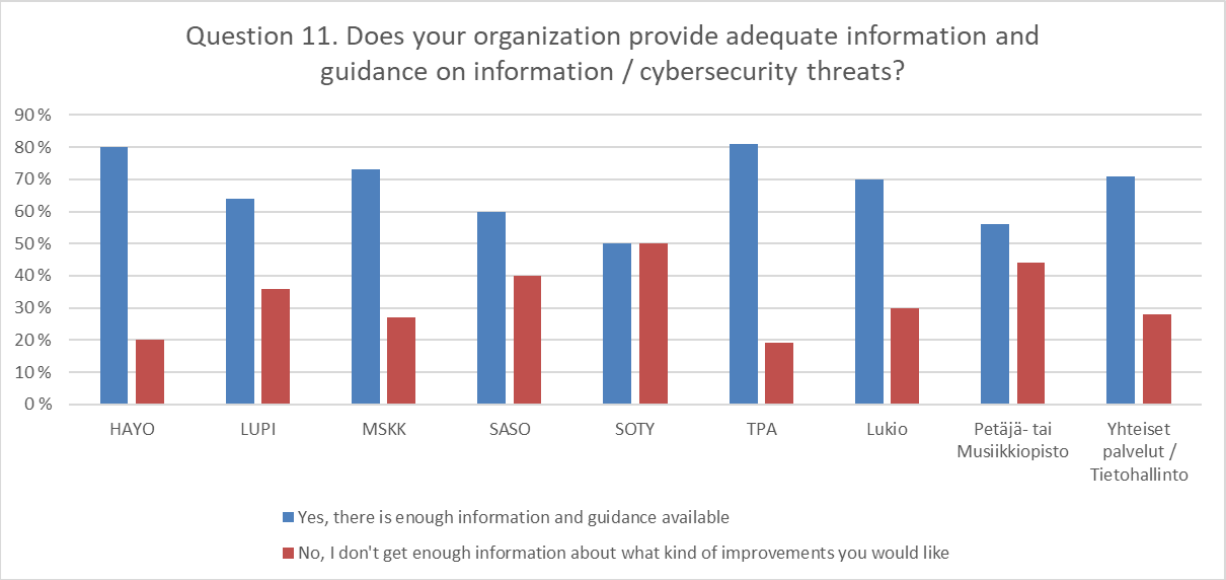

Figure 6. Views on whether the organization provides sufficient information on threats

Figure 7 shows that 87 percent of respondents say they know the organization's security guidelines well or reasonably. 13% of respondents are unfamiliar with the content of the security guideline, or the security guideline is completely unknown. In the overall picture, the situation is reasonable, but any person who does not know the instructions increases the risk of a security threat materializing.

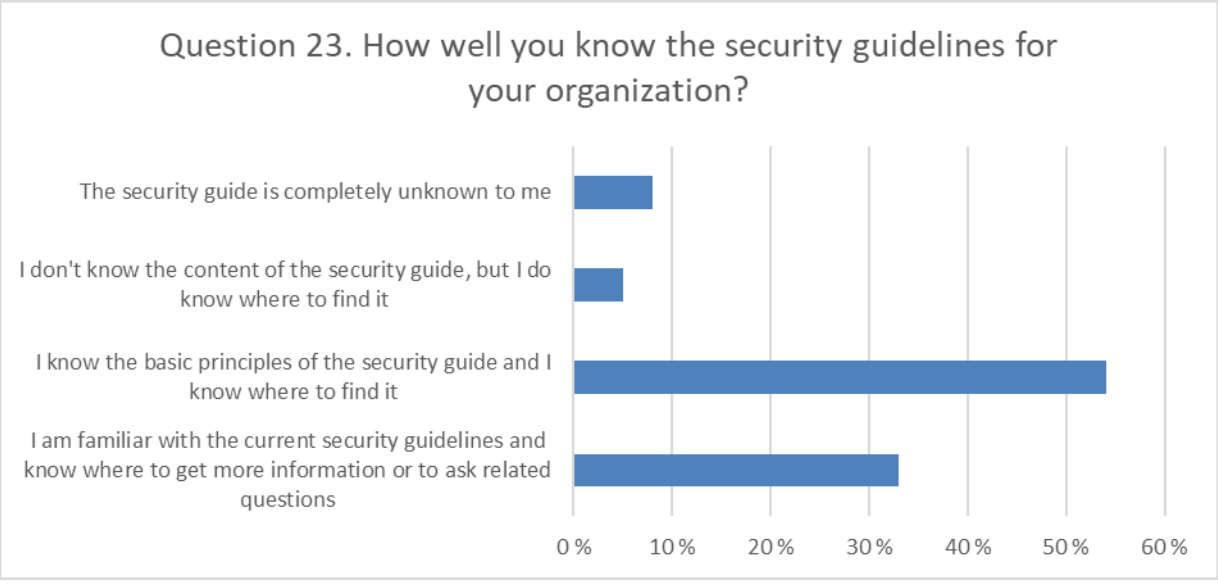

Figure 7. How well personnel knows organization guidelines

According to Figure 6, 68 percent of the personnel consider the security guidance provided by the organization to be adequate, and 32 percent would need improvements to the guidance. The need

for further training was highlighted in the open responses. The responses highlighted concerns about the implementation of security guidelines for one's own work and role. The guidelines should be sufficiently detailed and practical so that the guidelines do not remain too general, but the personnel outlines what the guidelines mean in their own practical work. One response summed it up as "finding knowledge – how to find and read information relevant to one's own work – what everyone needs to know, what they need to know in different roles, how relevant the information is presented, where resources are taken to learn knowledge and how to make use of it."

Question 10 asked personnel for their own views on their knowledge of various security / cyber security issues. The questions were related to typical cyber security threats. Table 1 shows the distribution as a percentage of personnel responses.

Table 1. Distribution of personnel's views on their expertise in typical cyber security threats

Question 10. Choose the most appropriate option to describe your knowledge of the following topics (1 = I don't know at all / 2 = I know badly / 3 = I know some / 4 = I know well / 5 = Can't say)							
	1	**2**	**3**	**4**	**5**	**Ave.(1)**	**Dev.(2)**
What is software updates importance for information and cybersecurity?	2,7	6	36,6	51,4	3,3	3,4	0,773605
What are tightening nuisance programs and how do they spread?	6	17,5	45,9	26,2	4,4	3,0	0,921669
What are scams and phishing?	0,6	4,9	36,6	54,6	3,3	3,5	0,666353
What is a denial of service attack?	6,6	22,4	37,7	29,5	3,8	2,9	0,966518
What are the risks on social media?	1,1	3,3	43,7	49,2	2,7	3,4	0,660095
How should confidential information be treated?	0	0	18	76,5	5,5	3,8	0,468163
What is information influence?	4,9	13,1	38,8	38,3	4,9	3,2	0,918651
What is identity theft?	1,1	2,8	27	65	3,8	3,6	0,644345

Figure 8 shows the average distribution of answers by the question on how the personnel's own view of their expertise in cyber security situations. The red line represents the average of all

responses. The average is on a scale of one (I don’t know at all) to four (I know well). On a question-by-question basis, the closer the averages are to the fourth value, it can be stated that the personnel's knowledge and skills are at a good level.

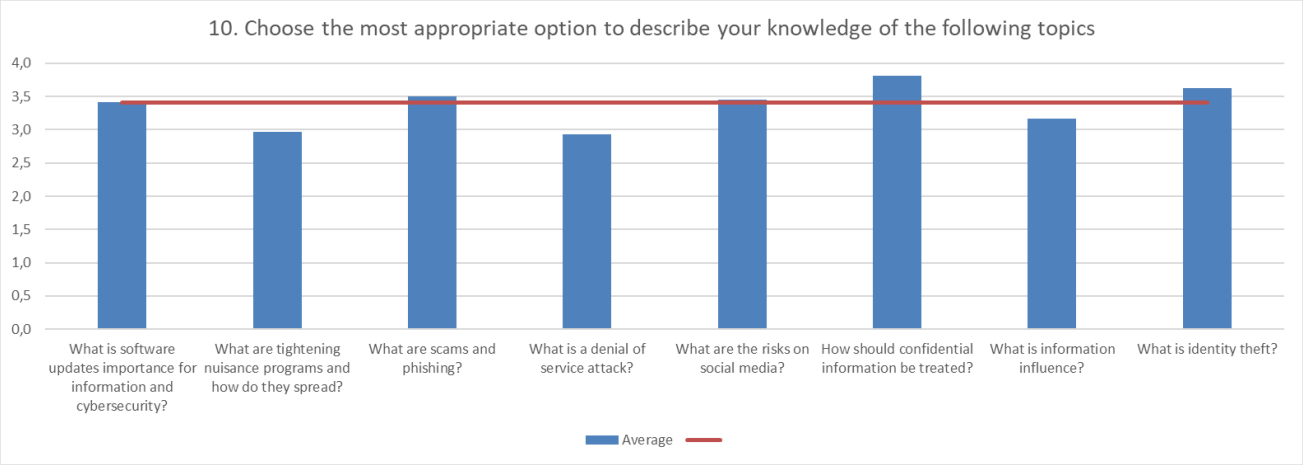

Figure 8. Views on knowledge of different topics

Figure 8 shows that knowledge is better than average (1) handling of confidential information, identity theft and fraudulent messages, and phishing. Outside the figure, it can be stated that although the knowledge of handling confidential knowledge is generally at a reasonably good level, 5.5 percent of the respondents had chosen the answer option, I can't say. It is quite worrying for the organization’s industry, considering that there is no knowledge of handling confidential information. It is also possible that the question has been misunderstood.

The weakest knowledge was about blackmail malware and its spread, as well as denial of service attacks. The reason for less knowledge may be that these issues are not perceived as critical for one's own job/industry.

Question 17 surveyed personnel knowledge of the rules for using websites. The distribution of responses is shown in Figure 9.

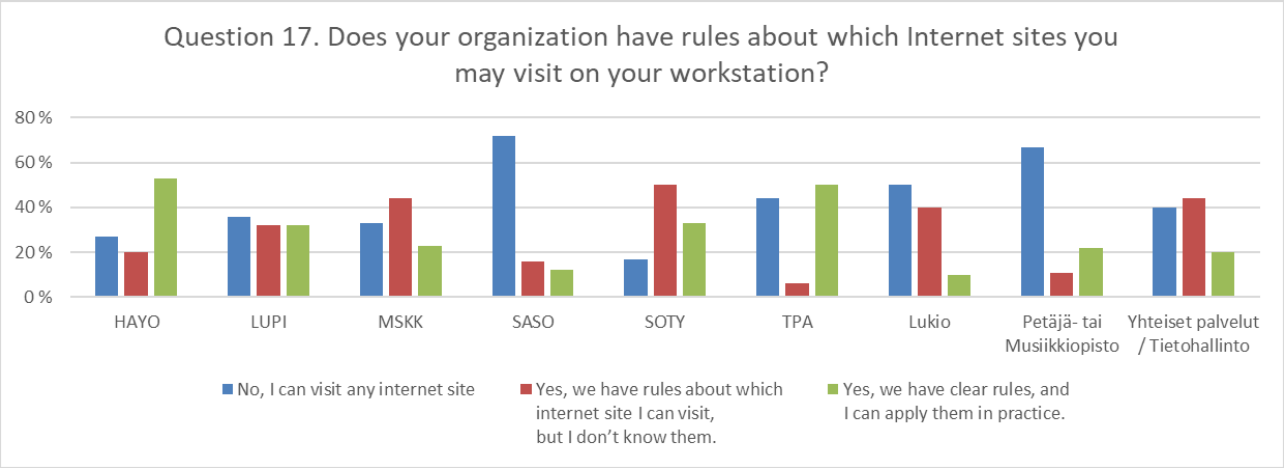

Figure 9. Views on whether the organization provides rules which internet sites are allowed

Forty-three percent of respondents believe that the organization does not limit which pages can be visited. Just over half of the respondents say that the organization has instructions on how to use the website. It should be noted in the result, however, that 30 percent of respondents who said the organization has instructions for banned websites do not know the pages are forbidden. Of the 183 respondents, only 51 said they knew which sites to visit. From the distribution of responses, it can be concluded that two-thirds of the personnel are not aware of the risks that a visit to different websites may pose. Raising the issue through orientation and training is particularly important.

4.3 Identification and assessment of cyber security risks

The following set of questions (questions 9, 12, 13, 14, 15, 16, 21) sought to find out what kind of cyber security threats or risk behaviors the personnel has observed in their work environment. Figure 10 shows the distribution of typical cybersecurity misconduct or situations encountered by personnel in the organization. Figure 11 shows how personnel behaves in different situations. Figure 12 shows how personnel uses ID card in daily business.

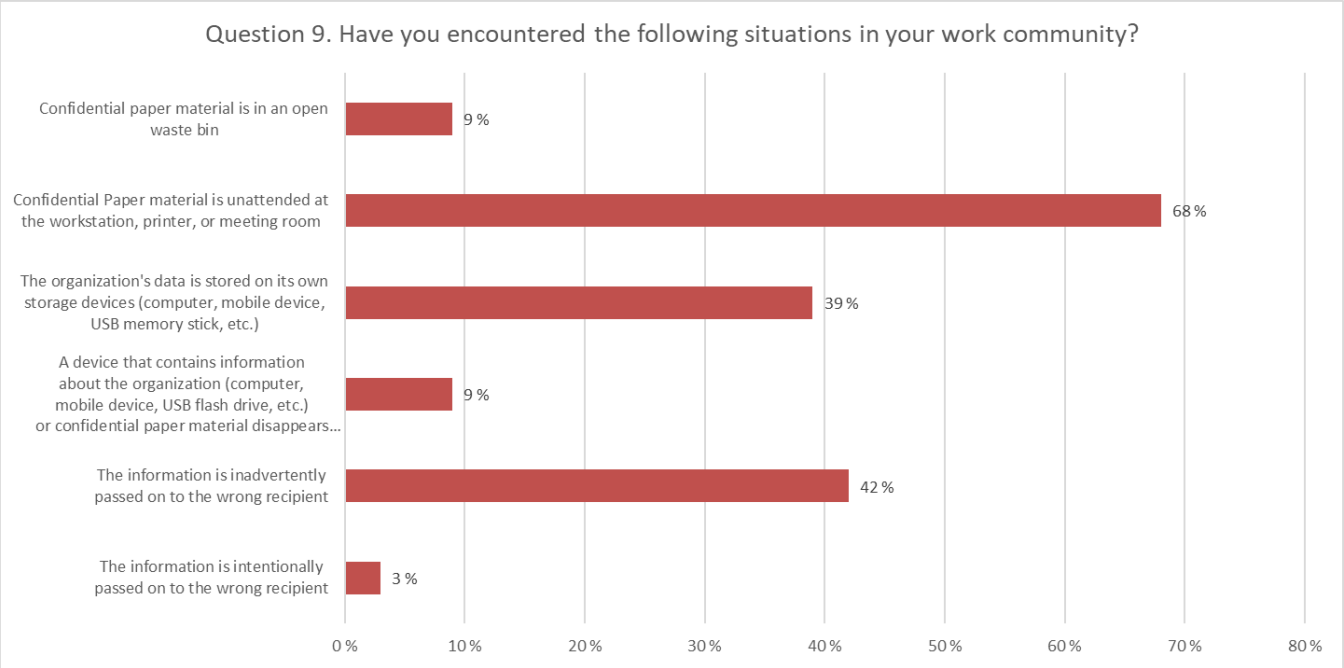

Figure 10. Distribution of typical cyber security situations in the work community

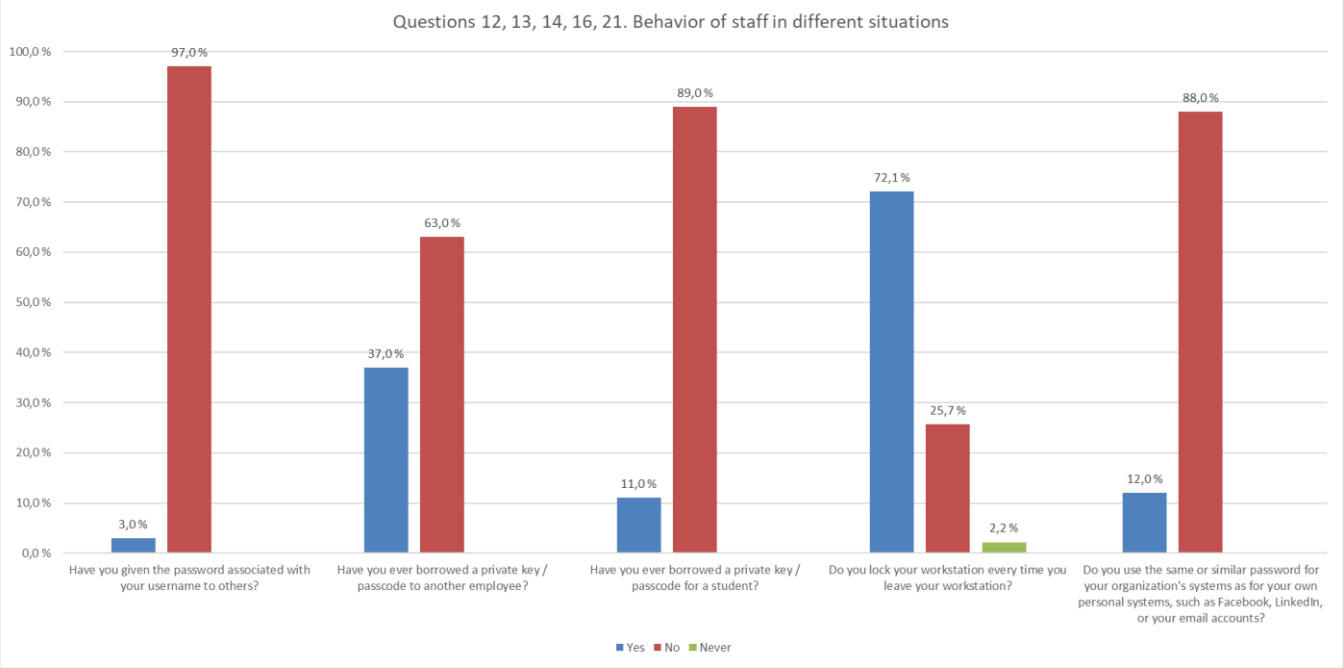

Figure 11. Behaviour of personnel in different situations

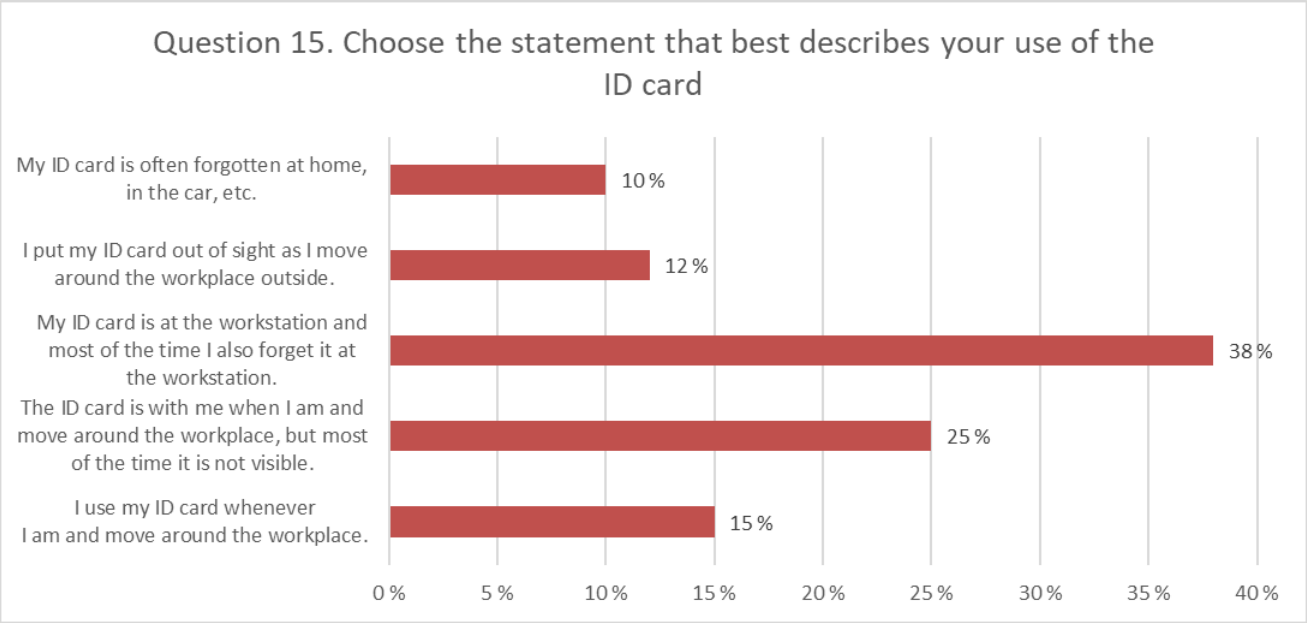

Figure 12. Breakdown of how personnel use ID cards

Question nine, which asked what kind of cyber security threat situations have been encountered in the work community, received 256 responses from 114 different respondents. Most often, respondents reported encountering a situation where confidential Paper Material is unattended at a workstation, printer, or meeting room. Seventy-seven people have come across this situation. According to the survey, 48 people have encountered a situation where information has been passed on to the wrong party. On the positive side, however, only three people have found the disclosure to have been intentional.

In general, it can be interpreted that the personnel of an organization has a correct understanding of how personal identifiers or tags should be used. However, any personal password that is passed on to another person is at risk. It can also be stated that the risk is increased by the access cards/keys placed or lent. Two percent of respondents reported not locking the machine at all. 88 percent of respondents reported using different passwords when logging in to the organization than for their own personal accounts.

Based on the answers, only 15 percents use the ID card correctly. An alarmingly large proportion of personnel needs guidance on how to use an identity card.

4.4 Probability of cyber security threats

Personnel was asked how likely various cyber security threats to occur in the coming year. Scam and phishing messages sent to the organization are considered to be the most likely to materialize. Just over a third of the respondents also considered other threats to be a potential risk to materialization. Only a few of the respondents had answered, I can't say alternative. About half of the respondents considered the realization of the threats to be rather unlikely. A person may not be able to imagine how their own actions will affect possible cyber security attacks. The organization should prepare for potential cyber security threats with a risk management plan and make plans for how to recover from a potential cyber security attack. Figure 13 shows the answer distribution of how likely cyber security threats will happen over the next year.

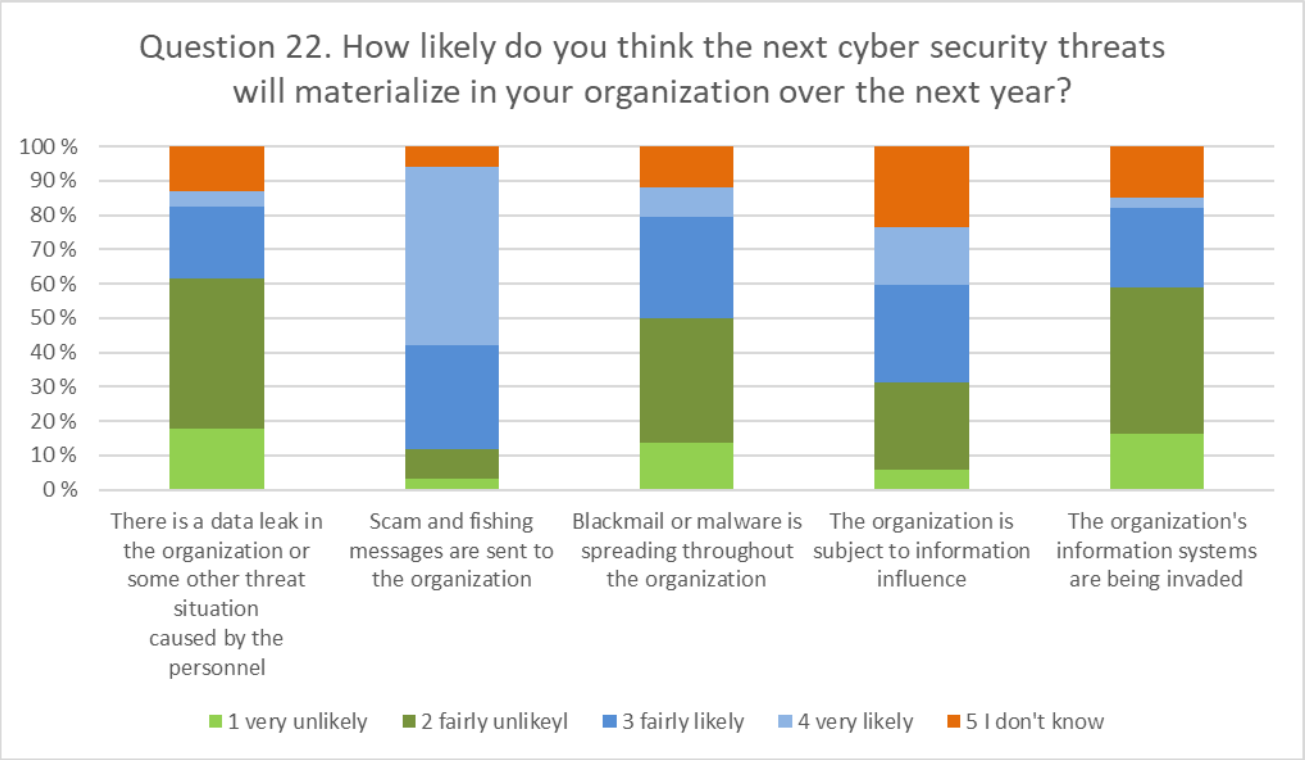

Figure 13. How likely cyber security treats will happen over the next year

Table 2 shows the distribution of responses to the statements. Respondents are most likely to see the threat posed by phishing and scam messages coming true in the coming year. About 82 percent of respondents agreed. On the other hand, the most unlikely alternative to the threat is seen by the respondents as a data leak in the organization or a threat situation caused by some other person. Cyber security surveys conducted in many different organizations have shown that the biggest threat to cybersecurity comes from either unintentional or intentional actions by

personnel. The personnel's own view is in great conflict with other research findings in the field. Even the insight of personnel can cause a false sense of security that personnel does not pose a cyber security threat. Respondents' views on how likely an individual threat is to materialize may be influenced by knowledge of threat situations, such as how much that threat has been featured in the media.

Table 2. Likelihood the cyber security situation will occur in the coming year

Question 22. How likely do you think the next cyber security threats will materialize in your organization over the next year? (1 = very unlikely / 2 = fairly unlikely / 3 = fairly likely / 4 = very likely / 5 = I don't know)						
	1	**2**	**3**	**4**	**5**	**Ave. (1)**
There is a data leak in the organization or some other threat situation caused by the personnel	18	43,7	20,8	4,4	13,1	2,1
Scam and phishing messages are sent to the organization	3,3	8,7	30,1	51,9	6	3,4
Blackmail or malware is spreading throughout the organization	13,7	36,1	29,5	8,7	12	2,4
The organization is subject to information influence	6	25,1	28,4	17	23,5	2,7
The organization's information systems are being invaded	16,4	42,6	22,9	3,3	14,8	2,2

4.5 Privacy

Question nine also included two data protection situation descriptions that respondents had encountered in their work. As shown in Figure 14, 7% of respondents had encountered a situation where personal data had been viewed without the need for a job. Nearly half of the respondents have encountered a situation where issues covered by student data protection are discussed with colleagues.

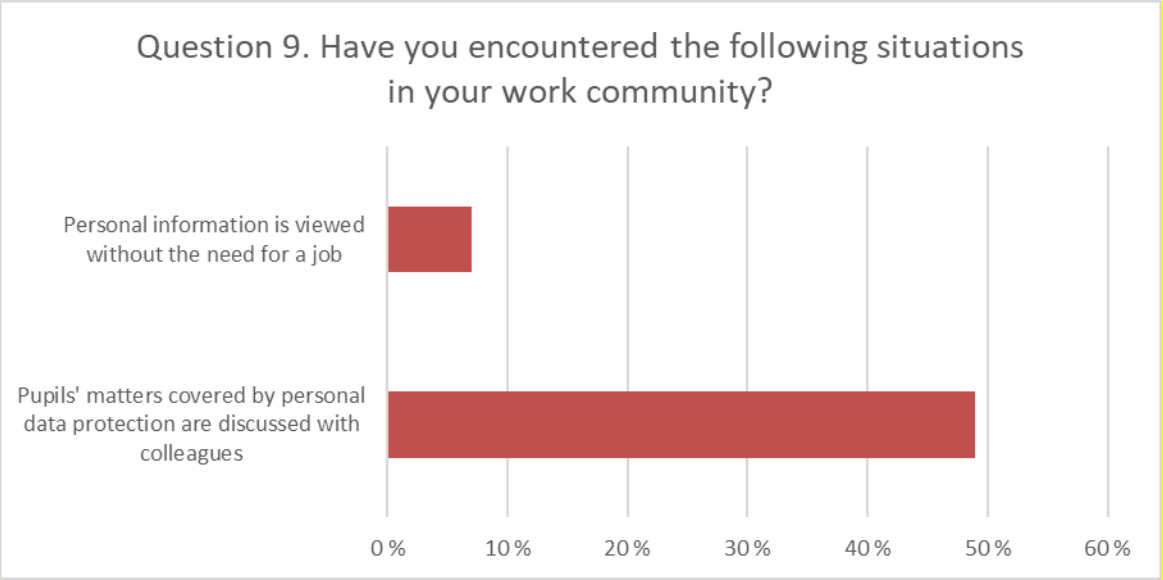

Figure 14 Distribution of typical privacy situations in the work community

Questions 18 and 19 found out how many of the personnel handle confidential information and whether the personnel handles it in external programs.

Questions 18 and 19 found out how many personnel handles confidential information and whether personnel handle it in external programs. In Figure 15, 89 percent of respondents say they handle confidential information. 90% of respondents do not handle confidential information in external programs. A notable observation of the results is that none of the respondents who reported handling confidential information know whether they are handling it in external programs. It is also possible that the issue has not been fully understood correctly. However, based on the observation, attention should be paid to the guidelines on the handling of confidential information.

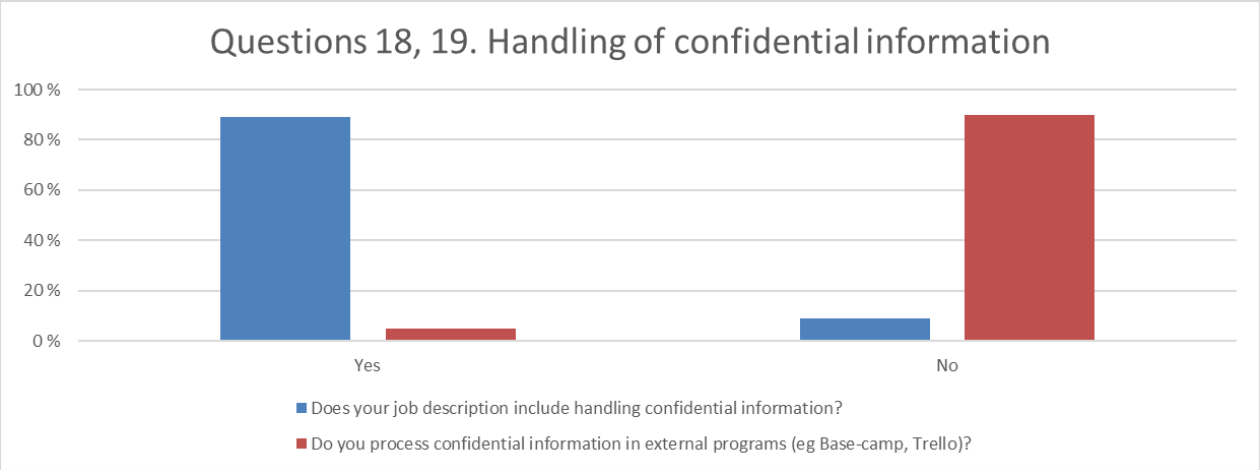

Figure 15. Privacy: Handling of confidential information

Question 20 mapped personnel knowledge of what communication channels they can use when communicating at work. Figure 16 shows the distribution of personnel knowledge of using different communication channels in work matters. Seventeen of the respondents said that a communication service provided by an external service provider, such as Gmail, can be used for communication at work. The question-making did not take a position on the content of work-related communication. The question set should have been more precise. For example, WhatsApp broadcasts promotional material for course offerings, which is also available on the organization's public website and does not pose a cyber security threat from the use of WhatsApp. If the content of the message includes students admitted to the course, the address and date of birth information is a privacy violation. There is no high risk in communicating public information, even if the communication channel is chosen incorrectly. Personnel should internalize which communication channel can be used for which content communication.

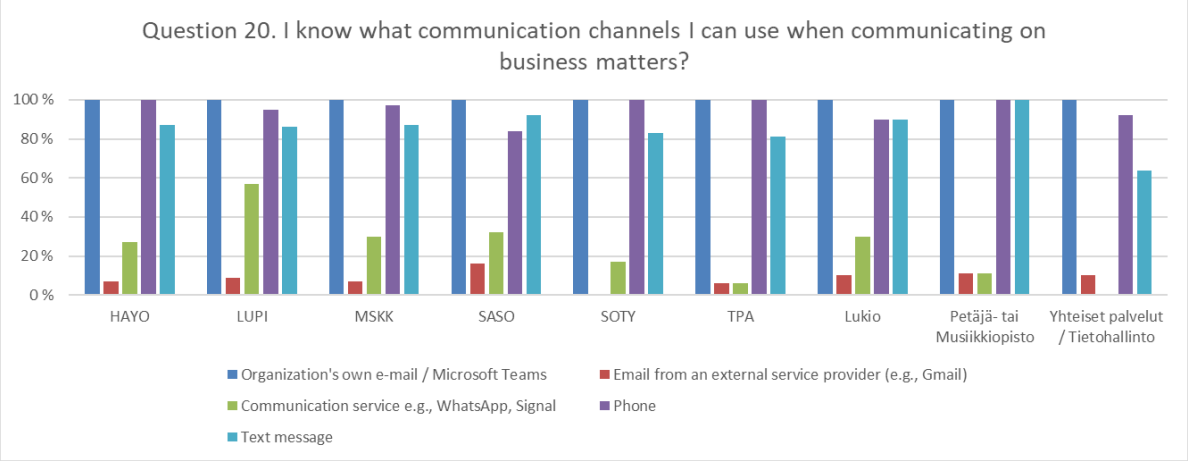

Figure 16. Privacy: Communication channels which can be used for business matters

4.6 Practical case studies

Questions 24-27 found out how personnel works in different practical situations. Figure 17 shows personnel responses by organizational unit, how they behave when they stop at a gas station and connect to the Internet for work. One hundred eighty-three people answered the question, of whom 77% stated that they would establish a secure (hotspot) connection via a mobile phone. 11% of the respondents could not answer the question. Similarly, 10 percent said they would use a different method. On the basis of the open answers, it can also be stated that there are employees who handle work matters only in the workplace.

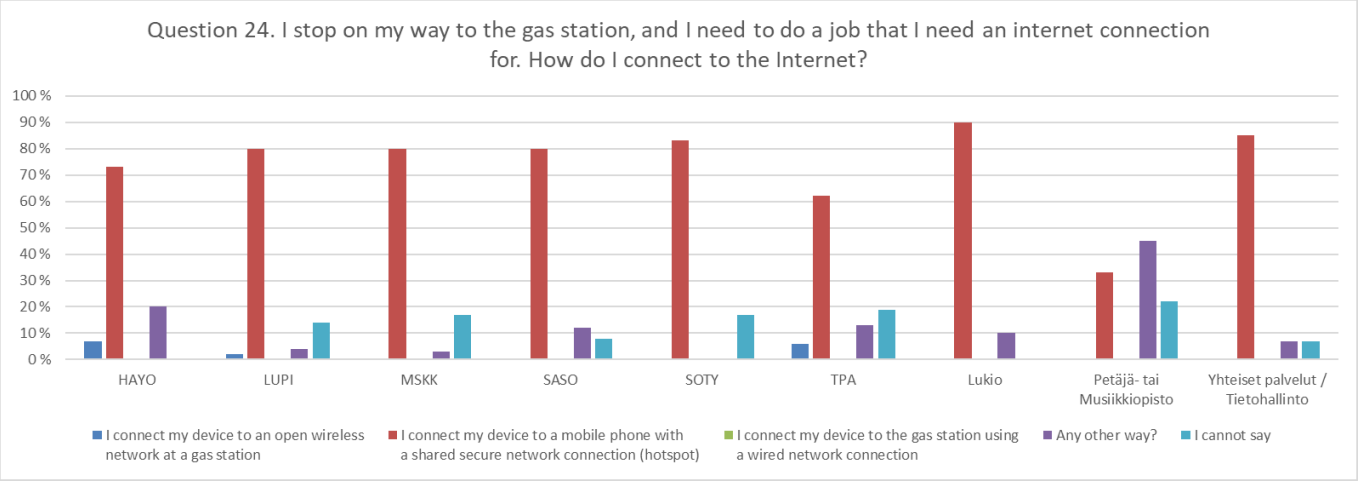

Figure 17. Distribution of how the personnel connect to the internet from gas station

Question 25 in Figure 18 found out how personnel acted when they found a USB stick in the ground in a school parking lot. The question was answered by 183 people, 91% of whom said they would take the USB stick and deliver it to the IT department. Similarly, 5 percent reported taking the USB stick they found to a lost property office. Three percent could not answer this question.

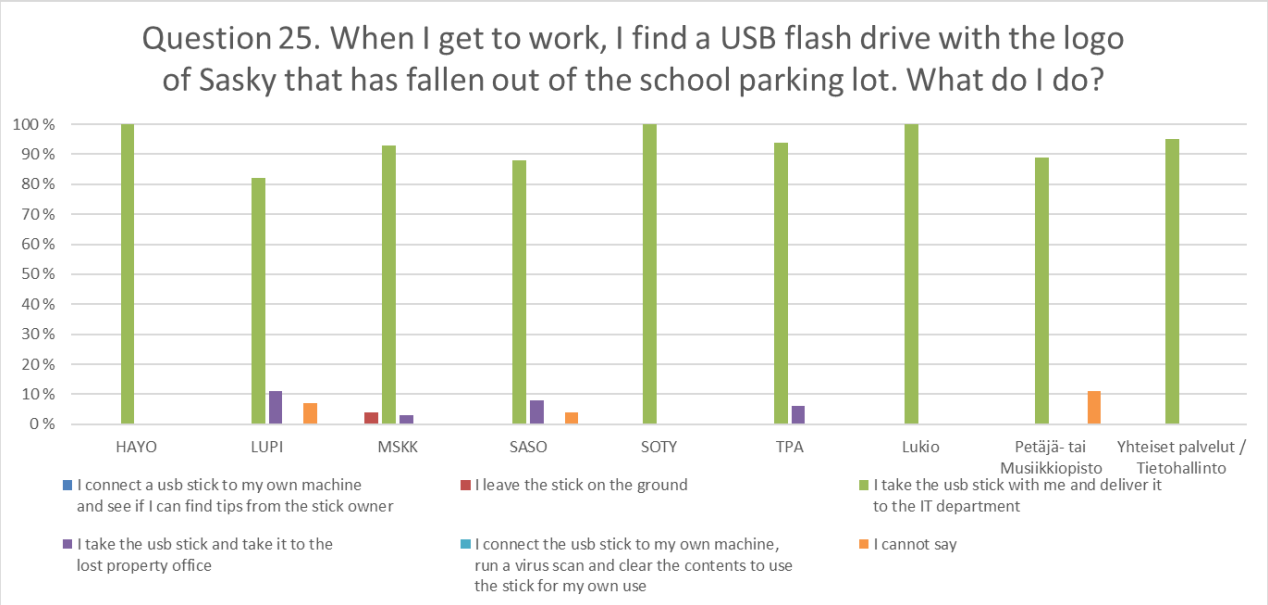

Figure 18. Distribution of what the personnel will do when they found usb stick

Question 26 in Figure 19 explained the actions of personnel in a situation where they receive an email from their co-worker and a link to a reflection site. This question was answered by 183 people, 54 percent of whom deleted the suspicious message. Correspondingly, 16 percent verified the authenticity of the sender's message. However, 17 percent opened the message to make their workday easier. An alarming number of respondents would have opened the link without verifying its authenticity from the sender or paying attention to the fact that the message may be contaminated.

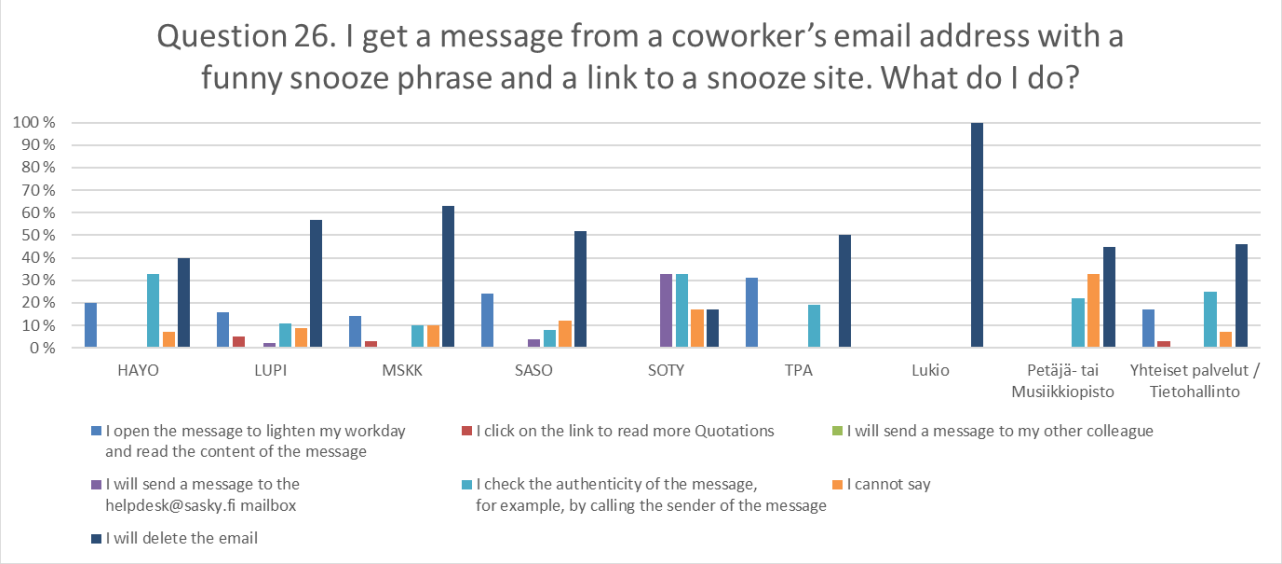

Figure 19. Distribution of personnel getting message from coworker's email address

Question 27 in Figure 20 of the example case explained how personnel would act if they receive a call from an IT support person who wants to remove the malware found on the machine. Of the 183 respondents, about 90 percent said they would end the call and suspect a scam. Similarly, about 10 percent allowed an IT support person to install a remote management program because the call had come from the IT department.

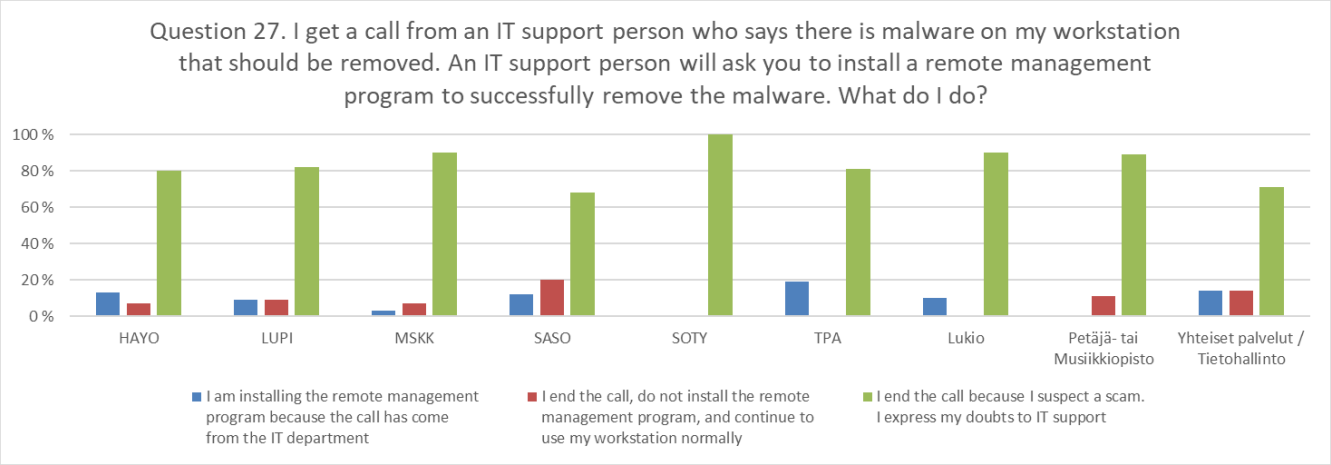

Figure 20. Distribution of how personnel respond to call from IT department

The vast majority of respondents identify cyber security risks and know how to act safely while minimizing the threats to the situation. However, it should be noted from the results that a small number of respondents would need improvements in their practices so that their actions would not undermine cybersecurity.

4.7 Managers

Questions 28-33 were put to the supervisors of the organization. Figure 21 shows the distribution of answers to the questions of how supervisors see the need to complete cyber attacks over the past year and whether compliance with employee security guidelines is monitored. Of the 21 respondents, 72 percent said safety guidelines were followed, 28% could not or did not want to answer the question.

Of the 21 respondents, 72 percent said safety guidelines were followed, 28% could not or did not want to answer the question. 57% of respondents saw the need to prepare for cyber security

attacks changed over the past year. Nineteen percent did not see the need changed. Respectively, 24% of respondents could not respond to the necessary change.

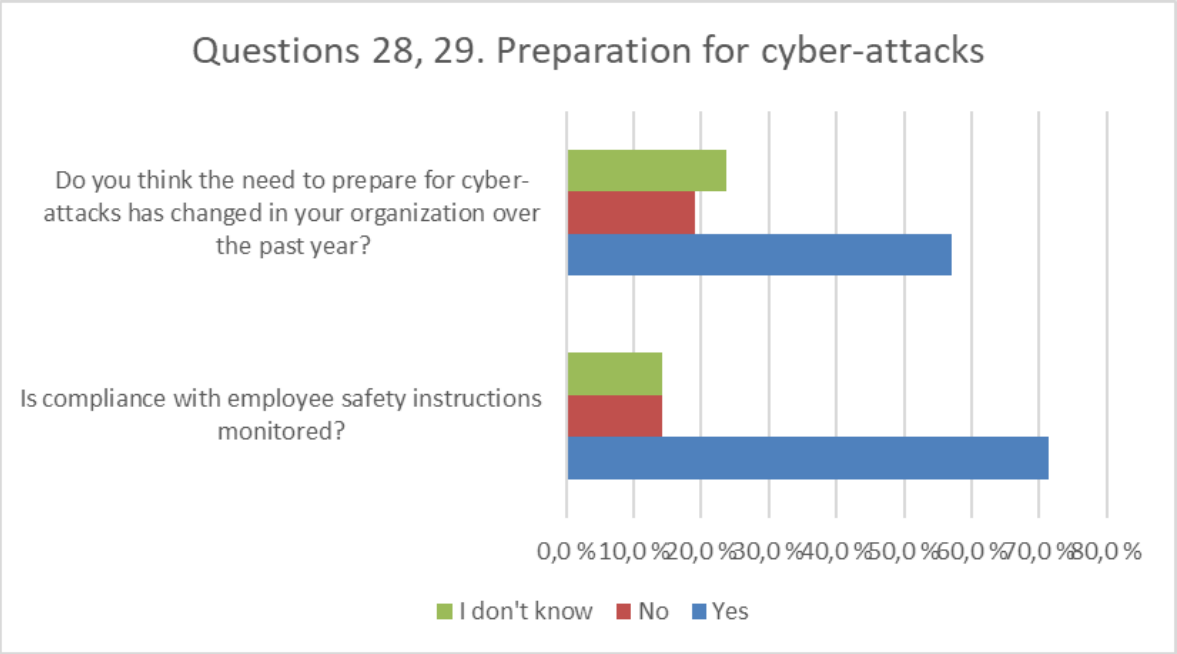

Figure 21. Distribution of preparation for cyber-attacks

Question 30 in Figure 22 explored how organizational security issues are resourced. Forty-three percent of respondents mentioned that things are handled alongside their own work. Thisrteen percent of respondents said a person had been hired for the job. In turn, Forty-three percent said this is not a one-person liability.

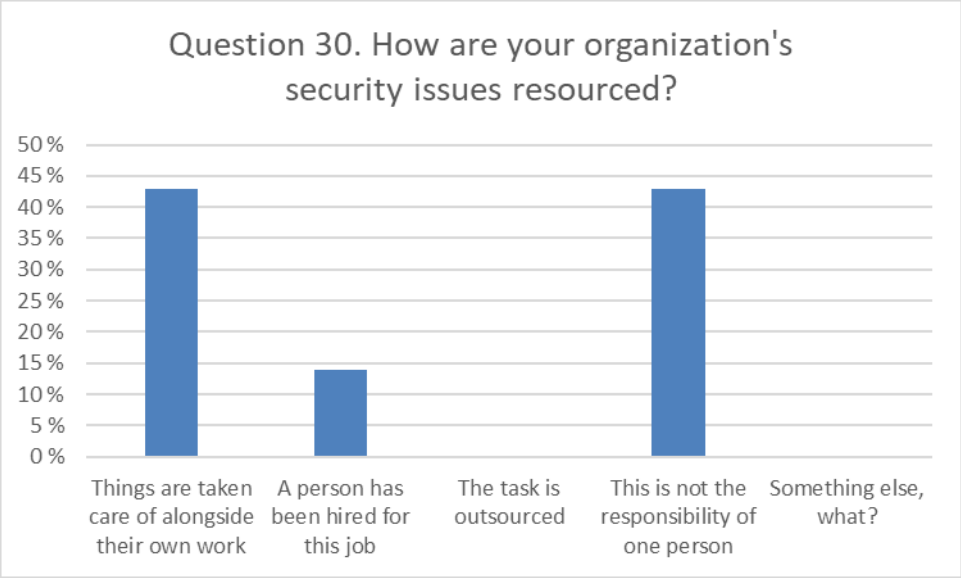

Figure 22. Distribution of how organization security issues resourced

Question 31 explored the importance that supervisors attach to the consequences of information / cyber attacks. Twenty-one answers were received to the question.

Table 3 shows the distribution of responses as a percentage. The options are on a scale of one to five, with one being completely irrelevant, two being fairly irrelevant, three fairly significant, and four highly significant. The fifth option is I can't say. The average is calculated between one and four on a scale.

42.9 percent of respondents considered the loss of real estate to be quite significant. 66.7 percent considered negative publicity to be very significant. 81% of respondents consider the invasion of privacy to be very significant. All of the consequences of the cyber attacks outlined in the question were considered by supervisors to be quite significant as well as highly relevant.

Table 3. Distribution of how managers consider the consequenses of cyber attacks

Question 31. How significant do you consider the consequences of the following information / cyber-attacks to be? (1 = Completely irrelevant / 2 = Fairly insignificant / 3 = Fairly significant / 4 = Very relevant / 5 = I don’t know)						
	1	**2**	**3**	**4**	**5**	**Average (1)**
Loss of real estate	14,3	4,8	42,9	19,0	19,0	3,2
Negative publicity	0,0	9,5	14,3	66,7	9,5	3,8
Violation of privacy (personnel or student)	0,0	0,0	9,5	81,0	9,5	4
Loss of income - direct or indirect	0,0	4,8	52,4	23,8	19,0	3,6
Business interruption	4,8	9,5	23,8	52,4	9,5	3,5
Criminal liability	0,0	0,0	19,1	71,4	9,5	3,9
Compensation to the customer	0,0	4,8	23,8	61,9	9,5	3,8

Question 32 in figure 23 found out what kind of disruption caused by cyber security threats the organization has prepared for. Twenty answers were received. Most respondents believe that the organization is prepared for various cyber security threat situations.

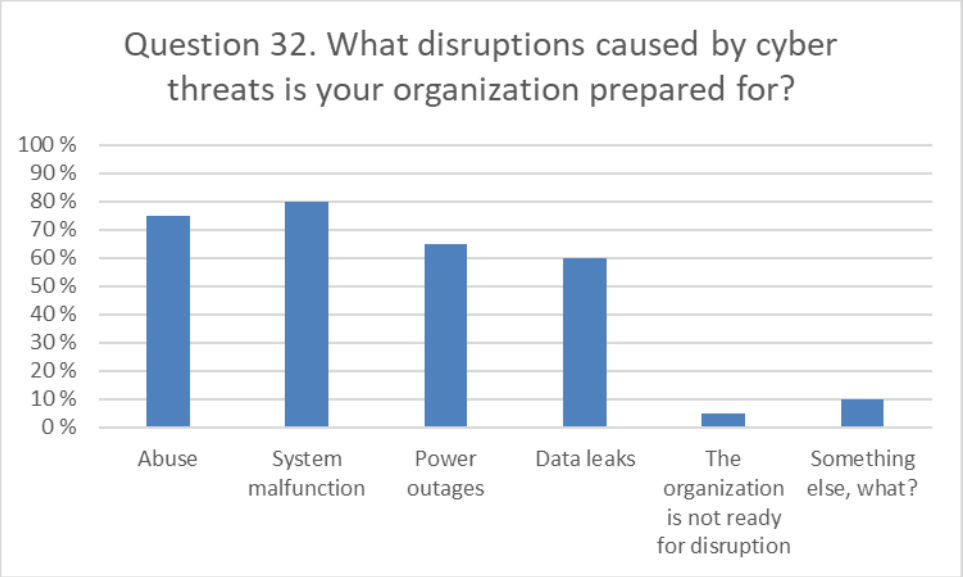

Figure 23. Distribution of which cyber threats the organization is prepared for

Question 33 in figure 24 explained how the organization's investments and their amount in information / cyber security are perceived. There were 21 respondents. 52 percent stated that investing in cyber security is vital to operations and that investment should be increased. Similarly, 48% felt that investing in cyber security is important and that the current investment will achieve an adequate level of cybersecurity.

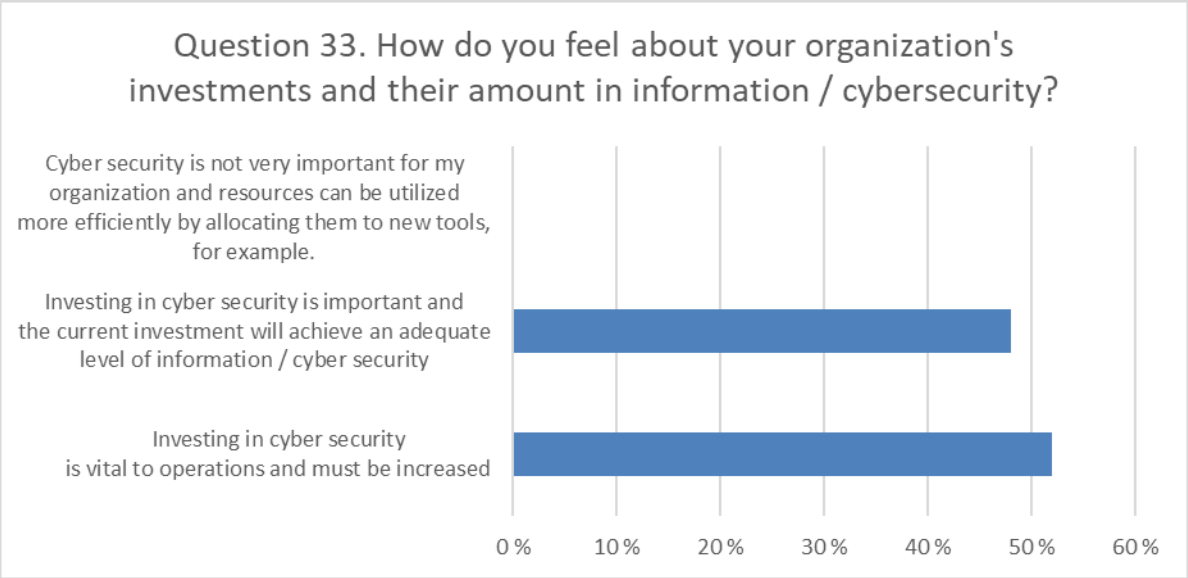

Figure 24. An opinion on how an organization invests and its amount in cybersecurity

Based on the questions addressed to supervisors, it can be stated that supervisors have a good understanding of the importance of cybersecurity. It can also be said that supervisors' perception of what the realization of threats means in practice.

4.8 Summary of results, challenges and areas for development

Based on the findings, that the company needs advice to improve cybersecurity guidance and training. The investigation revealed that personnel reported recognizing cybersecurity-related terms, but in practical situations, true/false claims were marked as true. The personnel's own understanding of the terminology is inconsistent with the actual knowledge. This should be taken into account when giving instructions so that the use of the terms does not cause misunderstandings.

The organization has a reasonable level of awareness and implementation of the security policy. Similarly, personnel understanding of the good practices in practical situations is good, but it should be noted that even a few people’s ignorances of common rules of the game or the wrong course of action can realize a security threat situation. The security guide should be easily accessible to everyone. The guide should be read in such a way that its content is known to everyone. Awareness can be raised through information sessions, coffee table bulletins, and by incorporating it into the induction of new employees.

There was a widespread need for additional training in cyber security. The development proposal is that the current data protection training will also address cyber security issues. Education should be kept simple enough and should not be made too laborious so that its benefits are lost and it becomes more challenging to absorb things. The training does not have to be a series of lectures a day, but things could be covered in smaller batches. For experienced individuals, cybersecurity issues should be brought up interestingly, as cyber security issues change over time. All personnel must stay up to date. The training should also sharpen the security classification of the data to understand how differently classified materials should be handled.

In Sasky's organization, the company's management is responsible for information security and data protection. Management should ensure that internal and external requirements are met. Developing security requires planning and resources from the organization. Instructions and materials for personnel should be simple enough for everyone to internalize the impact of their behavior on company safety. Poor security awareness can lead to risks being ignored, and security development can be classified as a less significant topic.

Personnel do not need to be cyber security experts but adopt safe practices as part of their daily work. For example, information management does not have to review the teleworking environment, as it does not necessarily improve data protection and security per se. Still, a better result is achieved by discussing issues and developing a corporate culture.

In the big picture, an organization needs a cultural change. Cybersecurity must be a ‘public skill’ so that everyone can understand the impact of their choices on public security. Thus, cybersecurity is not a separate matter handled by the IT department or management. It is the teacher's job to teach students (core business). Still, the organization should take care of the teacher's work environment and guide them to understand that everyone is part of the cybersecurity community. - How teacher choices increase cybersecurity. In subject teaching, it is also essential that teachers bring out the cyber security perspective so that new experts in the field can take care of cybersecurity in the future.

4.9 Comparison of results with previous research

At present, various studies and surveys related to cyber security are common. Companies and organizations on both the private and public sides commission theses, dissertations, commercial investigations, and research on the topic. This reflects the importance that organizations place on cybersecurity. Similar results can be observed from the results of several studies. The results of Sasky's survey are consistent with other survey results. It can be concluded from this that the challenges related to cyber security are similar regardless of the organization.

In her dissertation for the University of Oulu, Mari Karjalainen studies the improvement of employees' information security behavior. In his work, Karjalainen points out that one of the most critical problems of organizations is that employees neglect the established information security practices. She also notes that while the importance of safety training is recognized, the existing literature does not highlight the basic features and requirements of practical safety training. (Karjalainen 2011.) Based on the survey, Sasky's personnel also saw the need for additional cyber security training. When asked which areas of information security training are needed, the answers were widely divided into several regions. As Karjalainen stated, the content of the training is not ready. Challenges can be compiling training content that serves the need for training broadly enough.

According to the latest Digital Security Barometer of the Digital and Population Information Agency, disruptions in advanced administration are commonplace in Finnish working life. About 60 percent of the 4,690 respondents said they had to block their critical employment due to disruptions in computer services. Together with statistics on the incidence of disruption and the growth of cybercrime, these barometer results highlight the importance of digital security and related skills in working life and everyday life. More needs to be done to develop incompetence. Nearly 15 percent of respondents are concerned that the management of the supervisor's organization is not investing enough in advanced information security. (Tekniikka&Talous 2021.) Based on the answers to the survey, Sasky's personnel will quite likely see scams or phishing messages and information influencing the organization in the next year. Blackmail and the spread of malware in the organization were also seen as quite likely. Respectively, data leaks or intrusions into an organization's systems were seen as quite unlikely.

5 Conclusions

The thesis aimed to find out the level of cyber security knowledge of the personnel. The research questions were how personnel understand cyber security and its threats, the significant gaps in personnel cybersecurity information, and how the gaps are addressed. The client was the Sasky Education Consortium. The goal was to create a frame of reference for the organization to help develop personnel cybersecurity skills in the future. The theoretical part dealt with references to data protection, data security issues, legislation, the EU Data Protection Regulation, and data management. In addition, the theoretical part dealt with the effects of corporate culture in the field of information security, the impact of psychology on personnel activities. Cybersecurity of hardware and software was excluded from the study. Similarly, students' cybersecurity competencies were left unaddressed. Based on the research, reasonably comprehensive answers to the research questions were found, and based on them, and the organization is able to develop the cyber security skills of the personnel.

The whole of information security is extensive, and many sources deal with information security from the perspective of organizational management. For example, Traficom's cybersecurity meter is aimed at the organization as an IT security readiness measurement tool for the IT department.

The survey targeted the entire personnel. One hundred eighty-three responses were received, i.e., one-third of the target group responded to the questionnaire. The survey was answered from all units of the organization. The survey's results should be viewed critically, as the response rate was rather low, but one-third of the personnel's opinions can be used to draw indicative conclusions.

The selection of questions for the survey was made based on the needs of the employer and the corresponding surveys. The original set of questions was lightened to keep the time spent answering the questionnaire reasonable. It was estimated that many would not respond if the number of questions were large. When reducing the number of questions, more attention should have been paid to reformulating the remaining questions. Now the content of the questions did not fully cover the original target level.

Participation in the study was voluntary for personnel. It's unclear whether the number of people who responded would have been higher if the survey had been mandatory. In addition, the survey

was conducted in late spring at the turn of April-May when there was a rush in educational institutions at the end of the semester, when personnel may have prioritized other work before the survey. Looking back, the timing of the study was not optimal.

The questions of the survey should be specified on the basis of the answers, and the feedback received. Analyzing the results of the survey, it was stated that the question set needs to be clarified. For some questions, it may be unclear to respondents whether the question was about data protection or data security. In addition, the set of questions included items to which more detailed answers should be obtained. The questions should be modified so that there is no room for interpretation in the answers.

When considering the reliability of the results of the survey, it is necessary to take into account how well the questioning has been successful. That is, whether the respondent understood the question or whether the answer 'I don't know' because the question was not understood. In the 'I don't know' questionnaire, there were quite a few answers, from which it can be concluded that the questioning was successful and the questions were understandable.

As a development proposal, it is proposed to organize competence surveys annually or at least every two years. In this way, cyber security issues can be kept on the surface, and the development of the level of competence can be measured. Many companies have introduced an annual cyber security exam to ensure that personnel keep their skills up to date. One option is to add such a small-scale cyber security exam to the competency mapping.

In the digital age, cybersecurity can be a challenge for a company because the cybersecurity of a company is affected not only by hardware and software, but also by the abilities and motivation of employees. On the other hand, taking care of cybersecurity cannot unduly affect the work of employees, as it leads to non-compliance with cybersecurity policies or a decline in job performance. With technical solutions, it is possible to extend protection and reduce the risk posed by individuals. The challenges identified in the study should be mapped with a larger sample in order to draw statistically more reliable conclusions. To ensure an adequate level of security, management should have an appropriate understanding of security, including the improvement of personnel competence. It would be essential to understand the personnel perspective and to

make safety information available to personnel in a sufficiently comprehensible and straightforward form.

The organization must have a strategy to combat cyber security threats. Training should be organized so that cyber security awareness of cyber security threats becomes part of the personnel culture. The earlier cybersecurity is included in an organization's operational planning, the better the outcome is possible. Risk management, compliance with laws and regulations is integral part of decision-making.

The relevance of the work to the client is excellent. Although many cyber security level surveys and related studies have been conducted recently and can be used to make assumptions about the weaknesses and strengths of one's own organization, the equivalence of the results cannot be fully assured. Therefore, the mapping should be done on an organization-by-organization basis.

The study revealed that the organization does not have a cybersecurity assessment based on standards or a separate definition. A good topic for further research would be to find out to what extent ready-made standards and frameworks can be used for evaluation and whether there is a need for separate definitions. Following the selection of the definition to be used for evaluation, an audit should also be planned to verify the effectiveness of the evaluation method.

References

Al Shamsi, A. A. (2019). Effectiveness of Cyber Security Awareness Program for young children: A Case Study in UAE. International Journal of Information Technology and Language Studies, 3(2).

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672.

Ciso platform. (2016). Understanding difference between Cyber Security & Information Security - CISO Platform. CISO Platform. https://www.cisoplatform.com/profiles/blogs/understanding-difference-between-cyber-security-information

Cybermeter. (2021). Traficom. Finnish Transport and Communications Agency. https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter

Cybersecurity. (2021). Information Technology Glossary. Gartner. https://www.gartner.com/en/information-technology/glossary/cybersecurity

DMPTuuli. (2021). Data Management Tool. The Finnish Tuuli Project. https://dmptuuli.fi/plans

Digitalization. (2021). Information Technology Glossary. Gartner. https://www.gartner.com/en/information-technology/glossary/digitalization

European Cyber Security Organization. (2018 March). Gaps in European Cyber Education and Professional Training, March 2018. European Cyber Security Organization. https://ecs-org.eu/documents/publications/5fdb282a4dcbd.pdf

European Council. (2021). Cybersecurity: how the EU tackles cyber threats. European Counsil. https://www.consilium.europa.eu/fi/policies/cybersecurity/

Haukilehto, T., & Hautamäki, J. (2019). Survey of Cyber Security Awareness in Health, Social Services and Regional Government in South Ostrobothnia, Finland. In Internet of Things, Smart Spaces, and Next Generation Networks and Systems (pp. 455-466). Springer, Cham.

Hybrid CoE. (2020, October 21). Hybrid threats and the use of the cyber domain. The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/news/hybrid-threats-and-the-use-of-the-cyber-domain/

JAMK staff (2018). Ethical Principles for JAMK University of Applied Sciences Approved by the Student Affairs Board on 11 December 2018

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].

Karjalainen, M. (2011). Improving employees' information systems (IS) security behavior: toward a meta-theory of IS security training and a new framework for understanding employees' IS security behavior. University of Oulu.

Katakri. (2015). Information security audit tool for authorities. Ministry of Defence. https://www.defmin.fi/files/3417/Katakri_2015_Information_security_audit_tool_for_authorities_Finland.pdf

Kruger, H, Kearney, A. (2006). A prototype for assessing information security awareness. Computers & Security 25/2006, 289-296.

Koppa. (2021). Quantitative Research. Jyväskylä University. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/en/methodmap/strategies/quantitative-research

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. Journal of internet Commerce, 9(1), 23-41.

National Institute of Standards and Technology. (2014, February 12). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology. https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

OpenLearn. (2020). The CIA Triad. OpenLearn. https://www.open.edu/openlearn/ocw/mod/oucontent/view.php?id=104794&section=1.1

Ross, S. (2011). Creating a Culture of Security. Books24x7, Inc.

Sasky. (2021). SASKY Municipal Education and Training Consortium. Sasky. https://sasky.fi/english-site/

Sasky strategia. (2021). Sasky kohti vuotta 2024. Sasky. https://sasky.fi/wp-content/uploads/2019/12/Strategia-kohti-vuotta-2024.pdf

Scholefield, S., Shepherd L.A. (2019). Gamification Techniques for Raising Cyber Security Awareness. HCI International 2019. Florida, USA (arXiv preprint available https://arxiv.org/abs/1903.08454).

SFS-EN ISO/IEC 27000:2017. Information technology. Security techniques. Information security management systems. Overview and vocabulary. Helsinki: Finnish Standards Association. https://janet.finna.fi/Record/janet.318786. SFS Online.

Tekniikka&Talous. (2021, October 20). Tietokoneet tökkivät: Digiturvabarometrin vastaajista lähes 60 prosenttia on joutunut keskeyttämään tärkeitä työtehtäviä digipalveluiden häiriöiden vuoksi. https://www.tekniikkatalous.fi/uutiset/tietokoneet-tokkivat-digiturvabarometrin-vastaajista-lahes-60-prosenttia-on-joutunut-keskeyttamaan-tarkeita-tyotehtavia-digipalveluiden-hairioiden-vuoksi/f6107ade-6a0e-4592-8521-a9a98f13fcb8

Traficom. (2021). 10 cyber security developments to look out for in 2021. Finnish Transport and Communication Agency.
https://www.traficom.fi/en/news/10-cyber-security-developments-look-out-2021

UpGuard. (2021, August 12). What is a Cyber Threat? UpGuard.
https://www.upguard.com/blog/cyber-threat

Vahti-instructions. (2021). Suomidigi. Blog.
https://www.suomidigi.fi/en/ohjeet-ja-tuki/vahti-instructions

Valtioneuvosto. (2021). Valtioneuvoston periaatepäätös kyberturvallisuuden kehittämisohjelmasta. Goverment and ministries.
https://valtioneuvosto.fi/hanke?tunnus=LVM006:00/2021

Varonis. (2021, March 16). 134 Cybersecurity Statistics and Trends for 2021. Article.
https://www.varonis.com/blog/cybersecurity-statistics/

Your Europe. (2021). Data protection under GDPR. Your Europe.
https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. Journal of Computer Information Systems, 1-16.

Appendices

Appendix 1. Survey questions

1. Select your unit

2. Respondent group. I am

- Director or supervisor
- Teacher or teaching or tutoring personnel
- Other personnel (other than those mentioned above, common services, support personnel)

3. Age?

- Less than 30 years
- 31-40 years
- 41-50 years
- 51 years or older

4. Do I know the following terms?

- Privacy
- Security / cyber security
- security threat / cyber security threat

5. Below are statements related to cybersecurity terminology. Tick the claims that are true

- The cyber operation environment is a complex global information network in which e.g. authorities and companies.
- Cyber security covers the physical security of an organization’s information systems such as locks.
- Cyber security is a state where the threats and risks posed by information networks are under control.
- A cyber threat is a risk that, if materialized, compromises an organization’s vital function.
- Security protects information systems.
- Security protects your rights when processing personal information.
- The goal of information security is to guarantee the integrity, reliability and usability of an organization's data.
- Cyber security is not dependent on the employee's own actions.

6. When was the last time you received cyber security training or completed cybersecurity courses?

- Less than 6 months ago

- 6-12 months ago
- More than 12 months ago
- Never

7. In which security areas do you find it necessary to receive more training?

- Administrative security - information security management and control
- Physical security - the physical protection of premises and equipment
- Hardware security - for example, general computer security
- Software security - software security issues
- Data file security - processing and protection of electronic and paper documents
- Telecommunication security - for example, data transmission security mechanisms
- Personnel security - issues related to role, responsibility and information security
- Operational security - for example, passwords
- Something else, what?

8. Select the devices you have connected to the Internet

- Desktop computers
- Laptops
- Tablet computers
- Smartphones
- Smart TVs
- Printers
- Scanners
- Wireless communication devices
- What else

9. Have you encountered the following situations in your work community?

- The information is intentionally passed on to the wrong recipient
- The information is inadvertently passed on to the wrong recipient
- Pupils' matters covered by personal data protection are discussed with colleagues
- Personal information is viewed without the need for a job
- A device that contains information about the organization (computer, mobile device, USB flash drive, etc.) or confidential paper material disappears on a business trip
- The organization's data is stored on its own storage devices (computer, mobile device, USB memory stick, etc.)
- Confidential Paper material is unattended at the workstation, printer, or meeting room

- Confidential paper material is in an open waste bin

10. Choose the most appropriate option to describe your knowledge of the following topics

(1 = I don't know at all / 2 = I know badly / 3 = I know some / 4 = I know well / 5 = Can’t say)

- What is software updates importance for information and cybersecurity?
- What are tightening nuisance programs and how do they spread?
- What are scams and phishing?
- What is a denial of service attack?
- What are the risks on social media?
- How should confidential information be treated?
- What is information influence?
- What is identity theft?

11. Does your organization provide adequate information and guidance on information / cyber security threats?

- Yes, there is enough information and guidance available
- No, I don't get enough information about what kind of improvements you would like

12. Have you given the password associated with your username to others?

13. Have you ever borrowed a private key / passcode to another employee?

14. Have you ever borrowed a private key / passcode for a student?

15. Select the statement that best represents your ID card usage?

- I use my ID card whenever I am and move around the workplace.
- The ID card is with me when I am and move around the workplace, but most of the time it is not visible.
- My ID card is at the workstation and most of the time I also forget it at the workstation.
- I put my ID card out of sight as I move around the workplace outside.
- My ID card is often forgotten at home, in the car, etc.

16. Do you lock your workstation every time you leave your workstation?

- Yes, I always lock my workstation.
- I will not lock my workstation if I leave only for a short time.
- No, I don't lock my workstation at all.

17. Does your organization have rules about which Internet sites you may visit on your workstation?

- No, I can visit any internet site
- Yes, we have rules about which internet site I can visit, but I don’t know them.

- Yes, we have clear rules, and I can apply them in practice.

18. Does your job description include handling confidential information?

- Yes / no / I don’t know

19. Do you process confidential information in external programs (eg Base-camp, Trello)?

- Yes / no / I don’t know

20. I know what communication channels I can use when communicating on business matters?

- Organization's own e-mail / Microsoft Teams
- Email from an external service provider (e.g., Gmail)
- Communication service e.g., WhatsApp, Signal
- Phone
- Text message

21. Do you use the same or similar password for your organization's systems as for your own personal systems, such as Facebook, LinkedIn, or your email accounts?

22. How likely do you think the next cyber security threats will materialize in your organization over the next year?

(1 = very unlikely / 2 = fairly unlikely / 3 = fairly likely / 4 = very likely / 5 = I don’t know)

- There is a data leak in the organization or some other threat situation caused by the personnel
- Scam and phishing messages are sent to the organization
- Blackmail or malware is spreading throughout the organization
- The organization is subject to information influence
- The organization's information systems are being invaded

23. How well you know the security guidelines for your organization?

- I am familiar with the current security guidelines and know where to get more information or to ask related questions
- I know the basic principles of the security guide and I know where to find it
- I don't know the content of the security guide, but I do know where to find it
- The security guide is completely unknown to me

24. I stop on my way to the gas station, and I need to do a job that I need an internet connection for. How do I connect to the Internet?

- I connect my device to an open wireless network at a gas station
- I connect my device to a mobile phone with a shared secure network connection (hotspot)
- I connect my device to the gas station using a wired network connection
- Any other way?

- I cannot say

25. When I get to work, I find a USB flash drive with the logo of Sasky that has fallen out of the school parking lot. What do I do?

- I connect a usb stick to my own machine and see if I can find tips from the stick owner
- I leave the stick on the ground
- I take the usb stick with me and deliver it to the IT department
- I take the usb stick and take it to the lost property office
- I connect the usb stick to my own machine, run a virus scan and clear the contents to use the stick for my own use
- I cannot say

26. I get a message from a coworker's email address with a funny snooze phrase and a link to a snooze site. What do I do?

- I open the message to lighten my workday and read the content of the message
- I click on the link to read more Quotations
- I will send a message to my other colleague
- I will send a message to the helpdesk@sasky.fi mailbox
- I check the authenticity of the message, for example, by calling the sender of the message
- I cannot say
- I will delete the email

27. I get a call from an IT support person who says there is malware on my workstation that should be removed. An IT support person will ask you to install a remote management program to successfully remove the malware. What do I do?

- I am installing the remote management program because the call has come from the IT department
- I end the call, do not install the remote management program, and continue to use my workstation normally
- I end the call because I suspect a scam. I express my doubts to IT support

Following questions were targeted to managers

28. Is compliance with employee safety instructions monitored?

- Yes / no / I don't know

29. Do you think the need to prepare for cyber-attacks has changed in your organization over the past year?

- Yes / no / I don't know

30. How are your organization's security issues resourced?

- Things are taken care of alongside their own work
- A person has been hired for this job
- The task is outsourced
- This is not the responsibility of one person
- Something else, what?

31. How significant do you consider the consequences of the following information / cyber-attacks to be?

(1 = Completely irrelevant / 2 = Fairly insignificant / 3 = Fairly significant / 4 = Very relevant / 5 = I don’t know)

- Loss of real estate
- Negative publicity
- Violation of privacy (personnel or student)
- Loss of income - direct or indirect
- Business interruption
- Criminal liability
- Compensation to the customer

32. What disruptions caused by cyber threats is your organization prepared for?

- Abuse
- System malfunction
- Power outages
- Data leaks
- The organization is not ready for disruption
- Something else, what?

33. How do you feel about your organization's investments and their amount in information / cybersecurity?

- Investing in cyber security is vital to operations and must be increased
- Investing in cyber security is important and the current investment will achieve an adequate level of information / cyber security
- Cyber security is not very important for my organization and resources can be utilized more efficiently by allocating them to new tools, for example.