Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Weronica Nilsen

Security Culture in the Norwegian Health Care Domain

Master's thesis in Master in Information Security
Supervisor: Vasileios Gkioulos
Co-supervisor: Gaute Wangen
June 2021

NTNU
Norwegian University of Science and Technology

Weronica Nilsen

Security Culture in the Norwegian Health Care Domain

Master's thesis in Master in Information Security
Supervisor: Vasileios Gkioulos
Co-supervisor: Gaute Wangen
June 2021

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Security Culture in the Norwegian Health Care Domain

Weronica Nilsen

2021/06/01

Acknowledgements

I want to thank the following persons and institutions for their help during the master thesis.

Firstly, I want to thank my supervisors Vasileios Gkioulos and Gaute Wangen at NTNU for great help and feedback during the last two semesters. You have provided priceless help and motivation when it has been needed, and have provided resources to make this thesis as good as it can be.

I want to thank clinicians and other employees at Nord-Trøndelag Hospital Trust for their support and for contributing to data collection in this research project.
I also want to thank the participants from Østfold Hospital Trust for their contributions in the data collection to this research project.

Thank you, to the experts that took their time to participate in interviews which made great contributions to my thesis.

I also want to thank all the participants of the questionnaire, who took time off their busy days to answer my questions. Your contribution was highly appreciated. And a special thank you to all the administrative workers I have been in contact with, guiding me in the right directions when gathering participants to the questionnaire.

And lastly, I want to thank my husband Eirik and our daughter Alva for the patience and support during the last two years. I love you!

Abstract

Information security is an important aspect of everyday life for everyone, not only to security experts but also the users of electronic systems as the world becomes more and more digitised. Which means that the ability to recognise risk and threats is no longer just limited to automatic detection, but the users themselves needs to know how to recognise a threat and act accordingly when faced with it. This demands more digital security training and awareness training to recognise the threats the health care sector faces today. In other words, enhance the digital security culture within the health care sector.

The health care sector all over the world has of late been under attack from actors wanting to disrupt the work health institutions do and gain access to confidential patient information, and health care professionals themselves stands as first and most crucial defence against such attacks. They just have to be trained in such a fashion that they can recognise the potential risks and threats in order to avert and deter the attack.
However, the priority lies naturally with privacy, patient care and patient security rather than information security. But since the attackers have changed targets from hard targets to soft targets, i.e. the users, information security needs to be incorporated into their everyday work and in such a manner that does not constrain their work.
This master thesis main assignment was to discover to what degree health care professionals everyday work is affected by the digital security training, and if the knowledge and and awareness is transferred to their home setting.

The result from the research done with this thesis, show that the training given to health care professionals does not affect their work in such a degree as first anticipated as they are used to working with privacy in mind. There is certainly room for improvement regarding information security, and a new approach to the training could be the answer. The new approach could be a more customised training, meeting the health care professionals in their everyday work and not in a general way.

Sammendrag

Informasjonssikkerhet er et viktig aspekt av hverdagen for alle, ikke bare for sikkerhetseksperter, men også brukerne av elektroniske systemer etter hvert som verden blir mer og mer digitalisert. Noe som betyr at deteksjon av risiko og trusler ikke lenger bare er begrenset til automatikken, men brukerne selv trenger å vite hvordan de skal gjenkjenne en trussel og handle deretter når de står overfor den. Dette krever kursing om og bevisstgjøring på de truslene man ser i trusselbildet til helsesektoren i dag. Med andre ord, forbedre sikekrhetskulturen i helsesektoren.

Helsesektoren over hele verden har i det siste vært under angrep fra aktører som ønsker å forstyrre arbeidet helseinstitusjoner gjør og få tilgang til sensitiv pasientinformasjon, og helsepersonell står som første og mektigste forsvar mot slike angrep. De må bare trenes på en slik måte at de kan gjenkjenne de potensielle risikoene og truslene for å avverge og avskrekke angrepet.
Prioriteten hos helsepersonell ligger imidlertid naturlig nok på personvern, pasientbehandling og pasientsikkerhet i stedet for informasjonssikkerhet. Men siden angriperne har endret mål fra harde mål til myke mål, det vil si brukerne, må informasjonssikkerhet innlemmes i deres daglige arbeid og på en slik måte at det ikke begrenser arbeidet deres.
Denne masteroppgavens hovedoppgave var å finne ut i hvor stor grad helsepersonells jobbhverdag blir påvirket av denne digitale sikkerhetskursingen, og om de overfører den kunnskapen og bevisstheten hjem.

Resultatet av forskningen som er gjort med denne masteroppgaven, er at opplæringen som gis til helsepersonell ikke påvirker deres arbeid i en slik grad som først antatt siden de er vant til å jobbe med personvern i tankene. På informasjonssikkerhetsbiten er det absolutt rom for forbedring, og en ny tilnærming i opplæringen kan være svaret. En mer tilpasset tilnærming, møte helsepersonell i jobbhverdagen deres og ikke på en generell måte.

Contents

Figures

Tables

Chapter 1

Introduction

This chapter presents the topic covered by the master thesis project, a brief problem description about the topic, a presentation of the four preliminary research questions and the justification, motivation and benefits of writing this master thesis. It will also present how this master thesis would contribute to raising the awareness about the cyber security culture in health care.

1.1 Topic covered by the project

This research study will focus on the security awareness amongst health care professionals and how the security training affects them in their day-to-day business with patient care, both the positive and negative aspects. Furthermore, it will be attempted to identify potential gaps between the security training the health care professionals receive and what specific risks the sector actually faces.
Another side of the training, it would be interesting to see if it is possible to measure how they perceive the threat in their private sphere and if there are any difference in handling work related patients data and their own personal data.

1.2 Keywords

Health Care, Cyber Security Culture, Cyber Security Training.

1.3 Problem description

The focus of this master thesis will be on researching the cyber security habits of medical professionals and their awareness about the cyberthreats we are facing. The background for this is that we live in a country that has been spared for a lot of crime, political disturbances etc, which has led to a more relaxed attitude against protecting personal data as it seems. The protected environment we have resided in does not exists anymore, as we have seen time and time again recently. During the Corona pandemic, we witnessed an increased rate of both phishing

attempts [1] related to the corona pandemic and attempts to gain access to personal information with the help of digital signature ID and SMS - or smishing [1]. The latter example has been seen during the pandemic in Denmark [2]. There has been sent out text messages to the danish people, wanting them to disclose their secure and personal NemID [3] in order to exploit the information. The prediction is that the Norwegian people will be facing more personal attacks on their private sphere in cyberspace, and that the general populations security concept is not developed enough to withstand potential attacks. First line defence are the users[4]. The users need the motivation and knowledge to comply with the cyber security policies given by the organisation and it is the users who have to recognize the threat. The attacks that are most commonly used against health care providers are evolving, getting more exact and pinpointed, much due to the change in methods used by the attackers. The attacks seems to be less automated and more human operated, according to Microsoft[5].

Health care professionals oversee one of the nations most guarded assets: information regarding the health of their patients. This information is considered confidential and should only be accessed when necessary to give the patient the best possible care. The health care professionals are the first line of defence in protecting the patient's information. And the patients need to feel that their information is appropriately protected. Norway and Norway's health care system has had a few incidents with data breaches in the last couple of years, but all in all has been spared from the major attacks that has been seen around the world the last couple of years. Some examples are the ransom viruses Wannacry and Ruyk that managed to disrupted information flow and patient care in other countries such as The United Kingdom and The United States.

This research will address the security culture in the health care domain, focusing on how security training is conducted and how it is perceived among the health care professionals. It is important to understand what knowledge the health care professionals have about information security and their motivations to integrate this knowledge to their work. However, it would be natural to address the gap between the health care domain and information security as the motivation and priorities in these two domains tend to differ. Health care is about patient care first and foremost while information security is about keeping the information gathered safe from unauthorized access. The policies regarding how and where the patient information is treated could feel like a constraint on their way they have to work, shifting the focus from treating patients to treating information. This gap between domains can make it difficult to understand why cyber security awareness might be lacking on health care professionals.

To answer the research questions there will be performed personal interviews with information security professionals working in the health care domain to get

[1] `https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it`

an overview over the status of the threats they are facing in cyber space. It will also be conducted a survey amongst health care professionals to reveal their cyber security awareness and motivation to comply with information security policies enforced by their organization.

1.4 Justification, motivation and benefits

In a poll [6] conducted in 2019 by one of Norway's leading suppliers of eHealth platforms, DIPS, it was revealed that the health care professionals did not feel included in the digitization of the work place. The same poll reveals that both health care professionals and patients fear that their information could be misused or third parties could gain unauthorized access to the patients data. However, there has to be a motivation for the health care professional to comply with the information security policies and it would be interesting to see if the training they receive today (if they have received any training) provides this motivation or not.

My intentions with writing this thesis is to give the reader a chance to think about how cyber security is affecting every part of their lives, whether they are aware of it or not. On the other hand, it is also a clash of two domains, as a security expert would like the integrity, confidentiality and availability to be a priority, and the health care professionals prioritize the patients care first and foremost. There is a gap between these two domains that should be addressed, especially within the Norwegian health care sector.

1.5 Research questions

After a lengthy process, the possible research questions have been defined. The questions will remain in the same context as they are now, but will be even more detailed and scoped before submitting the master thesis agreement in January.

RQ1 - *What are the cyber security risks we are facing today in health care?*

RQ2 - *How does the cyber security training affect the risk awareness in the daily work of health care professionals?*

RQ3 - *To what degree do the cyber security training affect the risk awareness of the medical professionals in their private domain?*

1.6 Planned Contributions

This thesis will be written to research if the cyber security training among health care professionals has enhanced their risk awareness and to get insight in if the cyber security training they receive are transferable to their personal life. The point of this is to see if there are gaps in the training they receive and also see

how they act privately. It could also help address the training in other ways if the result yields unrevealed issues with security awareness and compliance, such as avoiding to follow the guidelines provided regarding information security in the work place.

As part of an agreement with one of the municipalities I contacted, they want to be presented with the findings of my research in order to see if they can use any of the findings to take measures if the findings indicates that it is needed.

1.7 Thesis outline

The thesis will consist of eight main chapters with several sections and some subsections.

- **Chapter 1 - Introduction**. An introduction to the thesis, problem description, research questions will be presented and a mention of planned contribution.
- **Chapter 2 - Background.** Some background information will be provided for the reader to more easily understand the content.
- **Chapter 3 - Related work.** In this chapter I will look into earlier work in the field and to topics that relate to my own topic.
- **Chapter 4 - Methods.** In this chapter the choices of methods are explained, and describe the steps taken to get the results.
- **Chapter 5 - Results.** Results from the data collection and analysis will be presented in this chapter.
- **Chapter 6 - Discussion.** The results will be discussed and put into context.
- **Chapter 7 - Conclusion.** In this chapter the conclusion will be presented.
- **Chapter 8 - Limitations and Future Work.** The limitations mentioned throughout the thesis will be explained in detail and the possible future work will be presented.

Chapter 2

Background

This chapter is written to present background information regarding important definitions that frame this thesis. It is important to define what is categorized as personal information and even more important, sensitive personal information and how the data in each category should be handled. It will also be attempted to describe the difference between risk awareness risk perception, as one determines behaviour and the other one do not. Furthermore, commonly used attack methods will be presented to give the reader an insight in how the attack methods differ from each other. There will a presentation of the most important policy-makers, guidelines, laws and regulations will be presented in order to understand the complexity behind information security in health care.

2.1 Risk awareness versus risk perception

Risk is something we have extensive knowledge about, i.e. risk and gain, how much can we risk to achieve what we want. We know there is a risk jumping out of an airplane with a parachute. The risk is that the jump could result in a fatal accident if the equipment fails. It is rare and most of the time this will not happen, but there is still a risk of it happening. The same risk is present it with opening an email and clicking a link or downloading an attachment without checking the legitimacy sender and the content. However, the chance of receiving a phishing email is much greater than the parachute not opening as 3 billion phishing emails are sent every day [1] versus approximately 21.3 skydiving fatalities per year[2] the last 10 years. Oklahoma Skydiving Center states that most of those fatalities does not come from faulty equipment, but rather experienced skydivers pushing limits and taking unnecessary risks, so the chances of a fatal equipment failure for a normal person skydiving under normal circumstances, is significantly lower.

[1] https://www.zdnet.com/article/three-billion-phishing-emails-are-sent-every-day-but-one-change-could-make-life-much-harder-for-scammers/

[2] https://oklahomaskydiving.com/blog/how-safe-is-tandem-skydiving/

Although when thinking about awareness and perception, they seem similar in many ways. They both relate to having some knowledge about a subject, know it exist and being able to understand how the threat can affect and how to avoid it. However, there are great differences between the two when addressing them in correlation to risk. Schmidt [7] says that awareness is connected to how we behave and being aware about how to behave in a given situation. It attributes to an action, on how to conduct one self to avoid the risk. This behaviour could correlate to past experience or social cues. Schmidt also states in his article that "The term "awareness" is only meaningful if it refers to a person's awareness *of* something" [7]. Health care personnel shows awareness for their field of work in how they conduct themselves among other colleagues. This is because of their training and that their colleagues belongs to the same "culture". They know that x has to be done to y if not will z happen. Training and social cues has been incorporated it into the bone marrow.

According to NIST-SP 800-50 [8] awareness is not training. Awareness is something that allows for the training to take effect. Awareness training could mitigate the possible individual differences in risk perception and the companies approach to training and with its own cyber culture can impact how the employees respond to the training. The awareness needs to raised in order to maintain a proper protection of the company's system and resources. The company needs to make the employees aware of the possible threats and vulnerabilities in order to keep the system safe.

2.2 Attack Methods

Gaining access to valuable information is one of the most common goal of the attackers. The information might not hold value for the attackers per say, the information is mostly valuable for the individual or company that the information pertains to. So, the attackers gaining access to information can be exploited in several ways. But in the end, the goal is to make the affected parties pay to regain access to their own information, or pay to stop it from spreading in public channels or the dark web.
This section will present several attack methods commonly utilized by attackers, especially on soft targets, but also on systems that have vulnerabilities.

2.2.1 Social Engineering

There are several ways for an attacker to gain access to a system. One of them is social engineering, or "cracking the human firewall" as the infamous Kevin Mitnick would call it [9, p. 4]. Social engineering is an effective way for the attackers to gain unauthorized access to what they perceive as valuable: the information the system contains. The methods used tend to vary, depending on who's the tar-

get. Using basic human interaction and exploitation of trust and/or errors, the attackers can manipulate the victims behavior in order to achieve their goal [3]. This section will present the most common method to shed some lights on how the attackers work and how efficient it can be.

Phishing

Phishing is an umbrella term used for attacks that manipulates the user to engage with the attacker in order to reveal valuable information.
Phishing is what it sounds like, it's a "bait and hook" method used by the attacker. They bait their victims into giving away information that could give them access to their computer, finances, social media or other personal information. They could even infect devices with malware.
If the phishing attempt happens in a work setting, the attackers could gain access to the company's system, and wreck havoc within the system, causing damage to the company data or infrastructure.

There are mainly two ways a phishing attempt could be arranged. Through spam (not targeted) or spearphishing (targeted) [4]:

1. Spam is usually not targeted at a specific individual, and is used to lure in as many victims as possible. The goal is to make money on the ones that fall for the scam by obtaining information about credit cards, bank accounts or passwords, or infect the target computer with malware [5]. Since this is a wide spread way of attack, it is highly effective as it is cost efficient.
2. Spearphishing is much more targeted towards specific individuals or organisations whose information the attackers deem valuable. The targeted attack is personalised to manipulate the victim into trusting the attackers to reveal the information they need. The initial target would normally not be individual first contacted, but acts as a mean to an end to gain access to the system in order to tap in to the company's resources [6].

When thinking about phishing, one traditionally thinks about suspicious emails with badly written language and strange URLs or attachments. But the attackers are not confined to emails in order to make contact with the victims, albeit it is a very effective and the most used phishing method [7]. As has been seen during the pandemic, there have been an increase in other methods, such as smishing (phishing through SMS) [8], vishing (phishing through telephone) [9], angler phish-

[3] https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering

[4] See footnote 3

[5] https://www.kaspersky.no/resource-center/threats/spam-phishing

[6] https://www.kaspersky.no/resource-center/threats/spam-phishing

[7] https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack

[8] https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it

[9] https://www.kaspersky.com/resource-center/definitions/vishing

ing (phishing through presenting as someone else)[10], extensive manipulation of search engine results[11] and ”typosquatting“ (exploits the chance of someone typing the wrong URL)[12].

There are other methods utilized by attackers. One of them is baiting[13] the victim by appealing to basic human drives, such as curiosity[10]. By leaving USB sticks infected with malware unattended at places people could find them is a good example on baiting. There is a large percentage of people who will try and access the drive to see what could be on it and try to locate the owner. If the device contains malware, connecting the device to a company or private computer that computer will most likely become infected with malware and give the attackers access to valuable information.
Another baiting method which the attackers might use is to offer free goods to the victim in an email attachment. This offered good could be posed as "free software" or similar, but is in reality an attachment infected with malware or software that does something malicious instead of what has been promised[14].

2.2.2 Malware

The word malware originates from the term “Malicious software”[11], and poses a major threat to computer systems. There are many types of different malware circulating out in the wild, such as keyloggers, spyware, Trojan horses, viruses and worms[11, p. 207-208]. They all work in different ways but the goal is the same: compromise confidentiality, integrity and availability in the victims systems. The danger about malware is that the user might not know they have been infected and are unknowingly sharing personal information with whoever is sitting on the other side of the information stream.

Ransomware

Ransomware is one of the most common methods used by attackers. The degree of how affected the victim gets depends on how malicious the attackers are, but they all want the same in the end: money. The attackers gain access to the victims systems by utilizing some of the methods mentioned earlier. One of the most basic ways attackers use ransomware, is scareware[15]. The attackers tricks the victims by using pop-ups or flashing alarms, which scares or intimidates them take action to mitigate the danger. The victims are presented with a solution, usually a dodgy software promising to clean the computer and restore it to the previous non-infected state. However, this is usually where the problems starts for the vic-

[10] See footnote 6
[11] See footnote 6
[12] https://www.kaspersky.com/blog/typosquatting-malware-infection-triggered-by-mistyping/4143/
[13] See footnote 3
[14] See footnote 3
[15] https://www.kaspersky.com/resource-center/definitions/what-is-ransomware

tim. Often, the software provided either does nothing or actually used to infect the computer with malware or create backdoors allowing the attacker into the system[16]. These types of attacks are usually small scale and affects individuals instead of large organisations.

Other types of ransomware is much more malicious and damaging. In 2019 and 2020, more and more public sectors globally has been targeted by an organisation of criminals of unknown origin. This ransomware was called Ryuk[17] and it mainly targets large companies with the means and resources to pay the ransom they demand, in cryptocurrency. The way they operate is to gain access to internal network and servers by using Phishing campaigns against the victims. The phishing campaign could contain one of several different types of malware to gain access to the victims , such as the Trickbot[18] and Emotet[19], disguised as links to malicious websites or attachments containing the malware. Once access is gained, the malware can lay dormant for some time before getting activated. But once activated, the Ruyk malware finds and encrypts stored data, and it can even find network drives and other resources to encrypt and render useless. As a precaution, it also disables important Microsoft Windows features that could save and restore the affected parts of the system to it's previous, non-encrypted state. This is to make sure that the companies can't fix the problem themselves, forcing them to pay the ransom.

The organisation behind Ruyk has been notorious in attacking schools in the US. It is speculated that it is much due to the fact that American schools lack proper cyber security measures[20], making them an easy target for the attackers. However, they have not shied away from attacking more vulnerable institutions, such as hospitals. Mid to late in 2020, several UHS[21] hospitals in the US experienced being targeted in a large cyber attack which halted patient care. Ambulances had to be rerouted to other hospitals and patients waiting for operations had to be relocated as well [22]. Having the attack disrupt important and life saving procedures is something that is one of the dangers with cyber attacks. In many cases, the EHR is not available for the ones that need it the most, the health care professionals that needs the information in order to treat the patient. This information could contain mentions of comorbidity that needs special attention or allergies to certain medications. Missing crucial information about these important aspects of a patient could be life threatening in a worst case scenario.

Furthermore, the thing that makes Ruyk so special is that it is most likely

[16] http://news.bbc.co.uk/2/hi/technology/8313678.stm
[17] https://en.wikipedia.org/wiki/Ryuk_(ransomware)
[18] https://en.wikipedia.org/wiki/Trickbot
[19] https://en.wikipedia.org/wiki/Emotet
[20] https://www.nytimes.com/2020/11/29/us/baltimore-schools-cyberattack.html
[21] Universal Health Services
[22] https://www.fiercehealthcare.com/tech/uhs-restores-it-service-to-hospitals-corporate-data-centers-following-massive-ransomware

human-operated unlike other forms of ransomware that seems to more machine-operated. By using actual human makes the attackers able to initiate more targeted and stealthy attacks[23]. The information that they gain access to could potentially be very valuable if sold on the dark web. Prices ranges from $1 for social security numbers, to $1,000 for a full patient record containing health information as well as data of birth, social security number and credit card information[24]. This information could be used to either threaten the victim to pay the attackers or the personal information get released or used in other malicious ways, like identity theft. Although the initial idea of stolen personal information might not be to use the data to steal an identity, it still promotes this fraudulent action [12].

Seemingly unrelated [25] specifically to Ruyk, investigations done by KPMG in the wake of the incident that occurred in Østre-Toten Municipality in January 2021 has revealed that the hackers have released sensitive personal information on the dark web [26].

2.2.3 Exploitation

As unfortunate as it is, we have witnessed lately that foreign forces has exploited several different types of zero-day vulnerabilities, e.g. Solarwinds and Microsoft Exchange, in order to extract information from Norwegian companies and the government. What defines a zero-day attack, is that it is a new and unknown exploit, generally surprising the cyber security community. This is where the problem lies. As it is a new threat, there is no way to protect against the unknown.
Solarwinds is a company that supplies IT network monitoring to many international companies and organisations, Pentagon and Norway's Government Pension Fund as well as Microsoft and the security firm FireEye among others[27]. The exploit was initially set in motion early in 2020, when Solarwinds were hacked. The attackers exploited the Orion platform and allegedly created a backdoor in order to infiltrate the victims. Solarwinds then disbributed the compromised version to their clients, who unknowingly used the software for several months before discovering the potential breach. Still, the exploit was not the only way that the hackers managed to infiltrate companies systems, they used many different techniques, utilizing legit softwares and other third party apps[28]. The aftermath of the breach is still not known as the hack was both complex and intricate, leaving the

[23] https://www.csoonline.com/article/3541810/ryuk-ransomware-explained-a-targeted-devastatingly-effective-attack.html

[24] https://techhq.com/2020/10/us-hospitals-brace-for-flood-of-ryuk-ransomware/

[25] as of 02.04.21

[26] https://www.ostre-toten.kommune.no/dataangrepet/31-03-21-personsensitive-data-er-pa-avveie.12471.aspx

[27] https://www.dn.no/teknologi/oljefondet/hacking/solarwinds/norways-11179-billion-nok-wealth-fund-affected-by-the-solarwinds-hack/2-1-964180

[28] https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T

incident management difficult.

The most recent zero-day is the Microsoft Exchange exploit discovered on March 3 2021[29], which comes in the wake of the Solarwinds attack. Although this attack was much larger and affected many more victims, the attack has not been getting as much media time as Solarwinds. This is due to the fact that it mostly affected small to medium sized organisations which hosted their Exchange servers on premises. This means that the organisations using the cloud-based Microsoft Exchange service were not affected. It is believed that the attackers have taken advantage of the pressure remote working has brought on during the pandemic, and thus attacked an area of the system which might have been overlooked[30]. However, security experts has not found any clear motivations for this attack, yet. Further investigation about the attack revealed that the attackers might have gotten their hands on a Proof-of-Concept attack code that Microsoft initially shared with antivirus companies affiliated with MAPP[31], a program that gives the companies early access to important security information[32]. When disclosing the incident, Microsoft released a patch that would mitigate future attacks on the affected Exchange servers, which leaves the responsibility to the individual companies to apply the patch and secure their own systems[33].

The potential ramifications from such attacks as these, are the loss of integrity, availability and confidentiality of the affected organisations information. In the health care sector, even lives could be in danger if important systems are disrupted and life saving components are missing, such as information about allergies the patient might have. If a patient has an allergy for a certain type of penicillin, it could be life threatening if the patient was given penicillin blindly.

2.2.4 Supply Chain Attack

In 2021, it is more likely than not that a company uses a third party service agent for parts of their online strategy. Many services that used to be hosted by the companies themselves has been outsourced to other companies that specialises in certain services (hardware or software), making them a service provider for the original company. When a third party provides these services to another company, they are working together in a so called ”supply chain“.

In a new report published in February 2021, NorSIS present supply chain attacks as an increasingly used attack vector[13]. They mention the use of non-

[29] https://www.businessinsider.com/microsoft-exchange-server-hack-why-cyberattack-matters-2021-3?r=US&IR=T

[30] See footnote 29

[31] Microsoft Active Protections Program

[32] https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/

[33] See footnote 32

secure cloud solutions, free and cloud-based software and the use of VPN on unauthorized equipment as some of the pitfalls for making the company vulnerable for an attack. This has become especially apparent during the last year with rapid digitisation and mandatory home office due to Covid-19, where companies has been forced to make decisions ad hoc, creating unnecessary vulnerabilities. NorSIS suggests[13] several measures that easily could be implemented to reduce the chance of a supply chain attack. Measures such as making sure proper password policies are in place, keeping devices updated and patched, monitoring and detection of the systems. It is also important to perform risk analysis in order to get an overview over the companies values, their value chains and vulnerabilities. However, this is not limited just to the company itself, it also applies to other companies in the supply chain and to the customers. Everyone has the responsibility to ensure that the supply chain stays intact.

These third party service agents could be large companies, such as Amazon Web Services (AWS), or they could be a smaller company, such as [24]7.ai[34]. In 2017, the American airline Delta Air Line was breached and had their customer data compromised[35]. [24]7.ai provided Delta Air Line with a chatbot service on their website in 2017 and 2018, and the attackers found their way into Delta Air Line system by exploiting weaknesses in the chatbot providers security measures. [24]7.ai also failed to inform Delta Air Line about the breach immediately, but rather waited five months to tell, leaving the Delta Air Line customers vulnerable for other types of attacks, such as social engineering[36]. Delta Air Line sued [24]7.ai Inc for negligence[37], claiming they had poor password policy and was lacking two-factor or multi-factor authentication for the employees to gain access to the source code. Delta also claimed in their lawsuit that the hackers managed to gain access to the source code for the chatbot by using compromised login credentials. By inserting malware into [24]7.ai's chatbot sourcecode [38] allowed the hackers to monitor the chats and collect the payment card information the customers entered upon completing the transaction in the chat. This shows how vulnerable a company and it's customers can be if one or more third party service providers lacks the proper security measures or are breaking the agreed-upon vendor compliance policy.

In Delta Air Lines case, approximately 825,000 customers information was exposed[39] in the attack. The attackers could also use other tools to cause harm to a company by targeting vendor in the supply chain, such as ransomware and DDoS

[34] `https://www.247.ai/`

[35] `https://www.wsj.com/articles/delta-sues-chatbot-provider-over-2017-breach-11565947801`

[36] Discussed in chapter 2.2.1

[37] See footnote35

[38] `https://www.mrwsystems.com/after-the-hack-delta-airlines/`

[39] See footnote35

attacks[40]. If something similar were to happen to a hospital, the service provided to the hospital by that vendor could be rendered unavailable. If that service is, for instance, a health record system it would not be possible for the health care professionals to gain access to important health information. The consequences if this happen could be disastrous, because without the correct information health care professionals can not give the best possible treatment to the patients and the patients safety is at stake.

2.3 Guidelines, laws and regulations regarding Information Security in health care

This section presents some of the laws and regulations that applies to information security in health care. The list is not exhaustive. The idea is that this section could be used as a tool to understand how eHealth works and what laws and regulations forms the Norwegian information security framework regarding eHealth.

- **Normen** [14]
  Normen is the national "Code of Conduct" for information security and data protection in health care. It is a holistic approach to a policy that include all sectors of the Norwegian health care organisation. "The Code" covers information security as it is regulated by Norwegian Law. It was developed by and for health care professionals with cooperation from the different trusts, the Ministry of Health and Care Services and NHN to ensure the completeness of the code of conduct[15]. "The Code" is planned used as a "best practice" for the organisations complying with the regulations addressed in "The Code". It also suggests how to best secure the organisations information by presenting practical guidelines regarding how to fulfill the requirements set in "The Code". However, it is not mandatory to comply to "The Code", but those who have entered into an agreement to follow it, have also agreed to comply with the guidelines given[16].

- **ISO 27001** [17]
  ISO27001 are an International standard that is used in many organisations to ensure that "best practice" is implemented for the information security management system they handle. The standard provides requirements for the whole process, from establishing the system to maintaining and improving the system. The main focus in ISO27001 is to ensure that the information security management systems operates to preserve the confidentiality, integrity and availability by implementing controls and risk management processes. The importance of a well functioning and integrated information security management system is crucial when handling information, sensitive or not. As for the sensitive information that health is, it is even more

[40] Distributed denial of service attack, overload the targeted systems

crucial that the information security management system is able to withstand any potential issues that could endanger the confidentiality, integrity and availability.

- **SIKKL - Sikkerhetsloven** [18]
  Sikkerhetsloven, or the Security Act is a law regarding the safety and security of Norway's independence and interests, in compliance to Norway's basic legal principles and values found in a democratic society. In SIKKL, there are two chapters dedicated to information security: Chapter 5 - Information Security [19] and Chapter 6 - Information System Security [20].
  Chapter 5 - Information Security is focused on how the companies handling information should maintain a sound security level for confidentiality, integrity and availability. Which means that companies have to make sure that the information they handle should remain unknown to the unauthorized, not be altered or lost and only made available when only when it is needed. It is also necessary to categorize the information regarding the consequences unauthorized access to the information could do to the nation.
  Chapter 6 - Information System Security is focused on the systems on which the information is stored or handled. It is also stated that companies must monitor their information systems in order to prevent, uncover and deter incidents. Systems that handle personal information must comply to monitoring with methods and extent in which the information serves its purpose. Confidentiality, integrity and availability is also important regarding the information systems. Companies can also request that security authorities perform tests on their systems, so called penetration tests in order to get a clearer picture on the safety measures and controls of their information system. The same request can be made about how the information is being communicated and on how the security graded information is being handled.

- **POL - Personopplysningsloven** [21]
  "Personal information" law is a Norwegian Law that states what is permitted and not when handling personal information. It also states when and where the law is valid, and who can have their information handled.
  As of now, Norway is not a member of the European Union, but they still need to adhere to the laws and regulations implemented by the EU, which means that Norwegian data handlers need to comply with GDPR regardless of member status[22].
  The definition of personal information is information that can identify you as a person:
  - Name
  - Address
  - Phone number
  - Email

- Social security number
- Recordings (picture and voice)
- Biometric information
- Behavioral patterns, both physical and digital (shopping, smart watches, streaming)

Dynamic IP address and licence number falls under the classification personal information as long as it belongs to a private person and not a company or organisation, e.g. is used by more than one person.

Sensitive personal information is information that could be used against you by others. Initally it is prohibited to process these kinds of data, unless there are special reasons for it[41]. The following information is deemed sensitive:

- Race and/or ethnicity
- Political opinion
- Religion
- Philosophical belief
- Union membership
- Genetic information
- Biometric information
- Health Information
- Information about sexual relationships
- Information about sexual orientation

- **PJL - Pasientjournalloven** [23]
  The law dictates that all patients- and user data should be available and easy accessible for the health care professionals that need access to give the correct treatment and that the information should be guarded against unauthorized access. It is also important to secure the information in regards to the users privacy, the right to have access to information about their own health, patient security and the users availability to interact with the treatment.
  It is also stated that the health register can only be used when it is necessary to treat the patient, or for the administration to perform internal audits and quality control of the register. It is illegal to health care professionals to read or gain access to a users journal without just cause, and it could lead to reprimands as it did in a case from 2017 when a care professional accessed a patients journal without authorization[24] and blamed it on someone else using the computer and/or the health care professionals account. Even so, if another health care professional or someone else using the computer, they showed grave negligence in this case.

- **GDPR - Personvernforordningen** [25]
  GDPR is a fairly new regulation from the EU that involves the EU member

[41] `https://lovdata.no/dokument/NL/lov/2018-06-15-38/KAPITTEL_gdpr-2#shareModal`

countries, including the members of the European Economic Area which Norway is a part of[22]. Norway had strong protection of health information, even before GDPR with the help of the laws mentioned above. Still, the focus on information security that GDPR brought is second to none. With GDPR it became known that the individuals rights had been strengthened, which in turn meant that the individual could demand their information deleted, among other things. However, the user can not request their patient records deleted due to the fact that health care professionals need the records in order to treat the patient. The patients records needs to be available to the health care professionals in order to conduct proper treatment of the patient. Along with the several strengthened rights for individuals, it also became mandatory to have Data Protective Officers, which allows for better treatment of the large-scale sensitive data that we find in health care.

Chapter 3

Related work

This chapter will present five parts that I feel will help with understanding how the Norwegian health care sector focuses on cyber security. The first part will be a short overview of a recent report from NorSIS regarding the status of cyber security awareness in the general population and a recommendation from the Directorate of eHealth and Norsk Helsenett on how they recommend Norway should plan to enhance the cyber security competence and awareness in the Norwegian health care sector.
The second part will be a presentation of the report the Auditor Generals audit that was released in medio December 2020. This report is about how the four regional Norwegian health trusts plans to mitigate attacks against their digital infrastructure.
The third part, is an overview of the cyber security awareness in other countries. This is important in order to understand Norway's position amongst the countries with the best cyber security, it would be helpful to look to other countries and how they perceive cyber security and try to get an understanding in the measures they have applied to enhancing the cyber security culture.
In the fourth part, will be a short presentation of recent attacks of Norwegian resources.
In the fifth part, the information gathered about the original research question regarding courses and training will be presented. This includes the information gathered through interviews.

3.1 Security Awareness: Norway

NorSIS has since 2016 tried to map the Norwegian cyber security culture. By collecting information from a survey conducted during the first three quarters of 2020, NorSIS managed to give an overview of the Norwegian society's cyber security awareness. It would be useful to not only measure how health care professionals perceive the security risks at home and in the workplace, but also have an idea of how the Norwegian people in general perceive the risks. This measurement could be useful as it could help me (belonging to the information security

domain) understand the result I will get during my research and not make unreasonable assumptions about the status of cyber security awareness in the health care sector.

The 2020 report from NorSIS[26] was somewhat special, as Norway suddenly had to digitize due to the outbreak of Covid-19. The sudden change in how we had to work with and relate to the digital tools left the organisations with some headaches in how to solve security issues when a large part of their employees had to work from home. And the criminals knew how to exploit this situation. Solutions that were thrown together in a hurry left many vulnerabilities, such as users that normally were "safe" behind a firewall weren't anymore and had to assess themselves if the email they received was legitimate or not[27]. This resulted in a phishing attack using an "update" of the popular application O365 as a backdrop and with the attackers impersonating a sysadmin in order to get the users passwords and gain unauthorized access to the system [27]. This is just one of the examples why it is important to focus on cyber security and strengthen the awareness, not just in the separate domains but also in the whole of society.

3.1.1 Norwegian Society

As stated, the Norwegian society has this year faced many challenges due to the Covid-19 pandemic. The security culture seemed to get a boost during this situation, as people got to see how easy it is for criminals to exploit vulnerabilities in order to reach their goals. The report NorSIS released in 2020 revealed that there was an increase from earlier years in scepticism regarding using services online due to knowledge about hacking and threats[26, p. 28]. NorSIS sees this increase as worrying, as digitization is the future for both public and private sector. When looking at the status about knowledge and security education, it seems that organised training is not the main method of learning about information security. The participants state that they learn about information security from friends and colleagues, and in more informal settings rather than organised training and security experts[26, p. 35]. A large portion (70%) of respondents also stated that they did not receive organised training in cyber security the last two years[26, p.36]. In regards to attitude towards cyber security, it was quite interesting to read that 16% of the participants did break the rules regarding cyber security [26, p.41] and this is an increase from previous years[26, p. 42]. It would be interesting to see a study about why there is an increase in rule breaking: is it because of more or stricter rules making the users become indifferent to them or because the security culture becomes weaker in general?

3.1.2 Health Care

When looking at the recent NorSIS report[26], we can see the general status of how the Norwegian citizens perceive threats. As of November 2020, there had not been published any similar research regarding the health care sector. In medio December 2020 the Auditor General released a report regarding the state of

the information security in the Norwegian Health trusts, which will be presented in section 3.2. However, the Directorate for eHealth are currently working on a strategy for cyber security within the health care sector. Up until now there has not been any particular strategy specific for the health care sector. On commission from the Ministry of Health and Care Services, the Directorate for eHealth and Norsk Helsenett has cooperated in developing a recommendation for a joint strategy regarding cyber security adapted for the health and care services[28]. Cyber security is the foundation in patient care and privacy for both patients and the health care professionals, and with the increased need for digitization and increased risk for cyber attacks on health care systems it is vital that the general competency regarding cyber security is increased. This is something that is explicitly mentioned in the recommendation from the Directorate of eHealth and Norsk Helsenett[28]. When conducting the research for the recommendation, the issue about raised cyber security competency came up for discussion. Several actors feels that their biggest challenge regarding cyber security is the lack of said competency in all levels of the organisations[28, p. 26-27]. There already exists a platform for sharing information about threats and vulnerabilities through NHN and HelseCert. The recommendation explicit mentions the the training course KOMP-iS[1] to be used as a resource for training health care personnel in regards cyber security.

3.2 Auditor Generals audit of Norwegian Health trusts 2019-2020

In 2019 and 2020[29], the Norwegian Auditor General audited Norway's health trusts and the four regional ICT providers in order to measure the state of information security within the Norwegian health system. The Norwegian health system consists of 4 regions: South-Eastern Norway Regional Health Authority, Western Norway Regional Health Authority, Central Norway Regional Health Authority and Northern Norway Regional Health Authority[2]. All these different regions have little to no interaction with each other as they function independent of each other and are not part of the same system. This being the case, it made the audit both more difficult to do but in the same time easier as well. It made it more difficult because the work load gathering data was much higher than it would have been if the trusts resided under one main provider. On the other hand, the separated approach made the vulnerabilities much more clear and the single regional health trust, ICT provider or the local trusts that lacked the proper measures could be addressed directly.

The Auditor General utilized different methods in their approach to unveil vulnerabilities amongst the regional ICT providers and health trusts. It was a mixed

[1] `https://www.kslaring.no/local/course_page/home_page.php?id=44`

[2] Helse Sør-Øst RFH, Helse Vest RFH, Helse Midt-Norge RFH og Helse Nord RFH

approach with investigating management documents and testing the robustness of the trusts infrastructure. By retrieving management documents regarding how the system for information security is maintained throughout the regions, the Auditor General could reveal how the different trusts and ICT providers have focused their efforts on updating their routines and mitigation plans as technology evolves [29]. These documents also included risk and vulnerability analysis for all the trusts, internal security audit reports and detailed documents regarding how their ICT infrastructure had been build.
These documents were used as backdrops and preparation for the next step of the audit, the Auditor General's simulated attacks on the different systems. They did this in order to see how much information was available and how much control of the systems an attacker could gain. The result was not uplifting as only one of the regional trusts discovered the simulated attack[29, p. 21]. The rest did not discover it, which means the trusts lack monitoring in order to discover potential attacks. The methods used to simulate the attack were common attack methods, with no attempt of concealing network traffic or other disturbances an attacker would make during an attack[29, p. 21] on the trusts systems. They approached the system as any other attacker would, by establishing a pathway in to the system, mapping the ICT environment and gaining access to accounts with elevated authorization [29, p. 22-24].

Lastly, not only did the Auditor General test the individual regional health trusts ICT systems, they also wanted to address the issues regarding the findings about cyber security behavior in the documents gathered. The combined result from interviews, questionnaires and findings during the simulation led the auditors to believe that the behavior amongst employees in the trusts and ICT providers did not enhance the cyber security. Instead, this behavior was more likely to decrease the cyber security[29, p. 43]. The most pressing types of negative behavior mentioned is a weak password policy, creating unnecessary exceptions to established rules and access control, credential sharing, physical unauthorized access and negligence. The Auditor General performed a simulated phishing[29, p. 44] attempt towards some selected health care professionals to see how they would react. The email was constructed to handle a relevant issue at the same time as it would be obvious that the email was fake. That lead to a form that needed filling out and an attachment that could be downloaded. All in all, approximately 2300 email sent out to employees at the different trusts[3]. The result were not uplifting: 893(39%) of the receivers clicked the link provided in the email, 565(25%) filled out the form and 277(12%) downloaded the file attached. The information security personnel reported that only a handful of employees had contacted them to regarding the simulated phishing attempt. After interviews conducted regarding this matters, the employees stated that they did not know how to properly treat suspicious emails and some even lacked routines for reporting such emails[29, p. 46].

[3]The name of the trusts were redacted in the report

All of the regional health trusts provide information security training[29, p. 47], as part of the training the employee get when they start their new job or as a refreshment course provided as an e-learning course. The feedback from the employees is that they wish for a course more suited for the work they do and a more "hands-on" approach with the possibility to discuss relevant issues with colleagues and information security experts. The health trusts do utilize their own intranet in order to relay information they find useful regarding cyber security. However, this practice have left some trusts with other issues, such as the employees feeling flooded with information on the intranet and starting to ignore the information sent to them. The Auditor General concluded with that the behavior needed strengthening in order to build a stronger security culture among the employees, both health care professionals and the ICT employees connected to the trusts[29, p. 48]. Behavior is not as easy to affect as attention and both time and effort to change is needed to adjust it[30]. This means that short term solutions with having superficial e-courses and relaying information about information security without the possibility to learn or maintain focus on the issues does not work as well as systemic reinforcement of behavior[30]. The goal for the security training is not just well informed employees, but well informed employees that do the right things which in turn increases the security culture and the information security in the company[30].

3.3 Security Awareness: health care Professionals in other countries

As cyber security is perceived differently all over the world, the training in how personal sensitive health information should be handled and management are also perceived differently. One of the research questions addresses the security awareness in health care in Norway, but it would not make sense to address it if there is nothing to compare it to, in this case that would be: Poland, Denmark and England. There are a few reasons on why these countries have been picked as examples. For example, the NHS had to make changes in the wake of WannaCry. Denmark has a similar health care system as Norway, it would be interesting to see what they do differently and what they perceive as important focal points in regards to cyber security in health care. And last but not least, there has been conducted a similar study about security awareness in health care professionals in Poland which would be interesting to compare to the findings done in this thesis. In the following sections, the reasons for picking these countries will be explained in more detail.

3.3.1 Poland

In 2020, researchers Luiza Fabisiak and Tomasz Hyla presented the findings of their study on polish health care professionals and the measurement of their security awareness[31]. As in Norway, Poland has increased its use of electronic

medical documentation in regards to patient care. The Polish eHealth system consists of many different information systems, from electronic health records, electronic patient admissions and financial systems[31]. The importance of proper management of the systems, such as keeping the systems up to date, having the correct systems configuration and keeping the access to patients records to a bare minimum and only have access when needed, becomes apparent because these issues are something that could be fixed with technology alone. A much less focused part is the security training for the system users, as the users behavior often dictates how secure the system really is, i.e. password sharing, unlocked computers, BYOD[4], and not being critical enough about content on the internet. All these different risk elements can create new attack surfaces and increase the chances of unauthorized access to patient data. The researchers focused on conveying the important role the user has in health care cyber security, and not only focus on the training but also increasing the awareness of the users. Increasing cyber security awareness could help reduce many of the threats to cyber security the health care sector faces today [32].

The survey was administered to health care professionals in a multidisciplinary fashion, including doctors, nurses and midwifes, physiotherapists, lab assistants and medical administrators. They received a short survey consisting of 23 questions asking if they had cyber security training, about their usage, about their knowledge and how they would react in regards to a potential cyber incident. The results of this survey was not encouraging, as the average percentage of favourable answers resided between 36-50% (depending on the group measured) and the worst part was about their reactions to cyber incidents. The majority did not apply the knowledge obtained in previous cyber security training. For example, many would have trusted the sender of an email of they knew the name and position of the sender regardless of what they had been told earlier. As a result of this study, the researchers urged the Polish health care to take action and improve the cyber security training for the health care professionals, increase the frequency of the training and allow for collection of metrics in regards to whether or not the training has increased the awareness[33].

3.3.2 Denmark

Denmark has one of the best cyber security programs in the world, according to the research group Comparitech[34]. This is not surprising given the focus and attention the Danish Government has given cyber security in the Danish health care sector. Their strategy has been separated into four tracks: Predict, Prevent, Detect and Respond[4]. In these four strategy tracks, it seems that the focus for the health care sector are increasing the cyber security awareness in every level of the organisation, both for the management and the employees. The Danish Center for Cyber Security constantly monitor the threat against the health care

[4] https://en.wikipedia.org/wiki/Bring_your_own_device

sector and DCIS[5] acts as a hub and relays the assessment to the different sectors. This is to strengthen the presence of awareness in the sector. DCIS has also been given the responsibility to develop guidelines and policies that should be applied in the sector. The DCIS is also important when working towards strengthening the awareness among the health care professionals. DCIS believe that increasing the security awareness level for the health care professionals will strengthen the defence against cyber security incidents. It starts in health care programs in school by implementing courses on cyber security in the programs[4]. The training needs to continue after school and into the workplace. The authorities encourages local initiatives, but there are planned centralized health sector training packages to address the need for training. For the management, they focus on improving cyber culture, starting with identifying critical business processes and making sure that they have sufficient overview of risks and vulnerabilities within the health care sector. It is also important to have clear roles and responsibilities in case an incident happens. Especially in the health care sector, it is important to be able to take action quickly and know the respective responsibilities when it is needed.

3.3.3 England

Without going into too much detail about the actual attack, it can be established that the English health sector was hit pretty hard during the ransomware attack Wannacry[6]. This attack was allowed to happen because of the NHS lack in prioritizing keeping systems up to date as well as not making sure that hospitals connected to the NHS were following basic organisational cyber security standards[35].

In retrospect, this incident was not only caused by hackers disrupting the health care systems, utilizing a vulnerability which became known quite fast. The incident was allowed to happen because the recommendation about a Microsoft update patch which could have mitigate the attack, was not taken seriously. Not a single one of the 80 NHS organisations affected by the attack had applied the patch that came on April 17 2017[36]. And with the attack being initiated on May 12 2017[36], it should have been plenty of time to apply the patch and set up proper network firewalls. The attack was and is a good example of how the lack of good management and cyber culture can cause an entire organisation to be affected by attacks that could have been avoided if taken the right precautions and following standards. In the wake after WannaCry the NHS focused on improving the preparedness for the future. Some of the recommendations given in that regard, involved mandatory training to increase the cyber awareness for every level of the organisation.

[5]Decentralised Cyber Information Security unit

[6]`https://en.wikipedia.org/wiki/WannaCry_ransomware_attack`

3.4 Recent attacks on Norwegian eHealth Systems

On January 8 2018, the Norwegian organisation Sykehuspartner was alerted by HelseCERT about an advanced, targeted attack to the servers belonging to Helse Sør-Øst (South-Eastern Norway Regional Health Authority)[37]. Sykehuspartner confirms that there has been an incident regarding a web server. The initial investigations reveals that the attackers had been able to access more than anticipated, but they could not disclose what they had accessed. In a press release issued on January 16 2018 from PST it was speculated about foreign country's interference[38]. Moreover, in a press release from the minister of health a few days later, January 18 2018, it is stated that they feared sensitive health information had been stolen [39] during the breach.
Sykehuspartner stated, with the help of the security company mnemonic and HelseCERT investigations, that no medical records had been breached[40] in the attack. The investigation revealed that the attackers had been after information regarding an e-learning platform, which did not have any connection to patient information or patient treatment.
In retrospect, the way Sykehuspartner had prepared their systems for mitigating attacks, by implementing an analytic platform and IDS to all health trusts, allowed them to contain the threat quickly with a take-down, regain control and map the information accessed by the attackers.

More recently in August 2020, Helse Innlandet was breached[41]. This time the attackers chose to attack six web services that were supposed to be exposed to the internet. As with the attack on Helse Sør-Øst, Sykehuspartner managed to quickly contain the data breach and start the investigation. They soon discovered that the attackers had gained access through exploiting several vulnerabilities: a database server which had been configured wrong and poor validation of input data in a specific service called "Labhåndboka"[42]. The analysis also showed that it was possible to extract some patient data from a patient quality control service which is used to register discrepancies in regards to patient care and HSE on the workplace. There were approximately 25 patients affected from this attack[43]. As a precaution for the future, Sykehuspartner and Sykehuset Innlandet performed a mandatory password change for all their employees.

3.5 Courses and Training

This part was supposed to be answered as a part of my research questions, but as it will be stated later in Chapter 8.1 Limitations, it had to be moved to related works as the data was not sufficient to answer the research question in a scientific manner. As I have spent a fair amount of time on researching the topic and talking about it with the information security experts, I will present my findings in this section, because it is an important part of the raising of awareness about information security in health care.

After conferring with security experts working within the health care systems, the consensus is that the security training available for health care personnel is broad and general, and is mainly offered to new employees. The local security courses available lack the customization that might be needed in order to raise the needed awareness. There are also several arenas for information security coursing, such as **Leger i spesialisering**. Other arenas could be the trusts own intranet, focusing on nano-learning and small releases on information over time instead of a whole, superficial 15-minute course once a year.

3.5.1 The courses

- **PIIP and PIFF**
  However, other health trusts do have a more thorough approach, such as Oslo University Hospital (OUS). OUS have a program called PIIP and PIIF[7] which needs to be completed in order to work with Oslo University Hospital's systems. I was not able to talk to OUS about their course, but there are some available information about it online.
  There are certain requirements OUS demands from their employees, for instance, the employee must follow the hospital's safety instructions, and that the employee understands what behaviour is expected from them while working at OUS.
  PIIP[8] is offered to hospital personnel, including those who are hired on a short term contracts and temporary hires as well as other employees not doing clinical work. The course focuses not only on how to treat personal information according to rules and regulations and how to maintain the patients privacy, but also how to prevent unauthorized access to the trust's systems. It also teaches the employees how to report deviations and discrepancies in regards to information security.
  The course takes approximately 15 minutes to complete.

  PIFF[9] is a course developed by OUS and UIO and focuses mainly on researchers and others involved in health research in connection with OUS. The course is created to enhance the researchers knowledge about the rules and regulations regarding privacy and information security when doing research in health care. Furthermore, the course consists of 9 parts, all regarding subjects from OUS eHåndbok[10] and OUS' management system for quality and patient safety[11].
  The course takes about 90 minutes with a 15 minutes finishing exam.

[7] Personvern og Informasjonssikkerhet i Praksis/Forskning
[8] `https://oushf.wordpress.com/2018/07/19/ta-piip-beskytt-andres-privatliv/`
[9] `http://meddev.uio.no/elaring/ansattkurs/piff/index.shtml`
[10] `https://ehandboken.ous-hf.no/`
[11] `https://ehandboken.ous-hf.no/document/4`

- **KOMP-iS**
  The Norwegian Association of Local and Regional Authorities(KS) and Norwegian Health Net (NHN) uses a course developed by Helse Sørøst to educate their members. This course is mainly given to the municipalities and primary health care sector.
  The course consists of videos presenting different topics such as why information security is important, how does information security work, what are the managers and employees responsibility, and how the organisation should train their employees.
  The course utilizes several different means to impart the message about information security. Amongst these means are the "Value film", which presents the core values in the course. There are eight main values presented, which should be the focus when training the employees[12]:

  1. The employees should always log off when leaving their station/device.
  2. Never store patient information on removable storage, such as memory sticks.
  3. The employee should know how to conduct themselves on the internet.
  4. The employee should know what and who to share patient information with.
  5. The employee should not keep patient information on their e-mail.
  6. Never share passwords.
  7. The employee has control over the documents they are handling.
  8. The employee know their role and what information they should have access to.

  It also uses humor to help raise awareness and to create funny memories about the topic. They do this by including humorous short films. These short films have been created with the help of near and dear characters presented by actor Robert Stoltenberg. The characters, in traditional Robert Stoltenberg ways, challenge the health sectors take on information security in different ways.
  The course also allows for the participants to engage in discussions and let them reflect on the topics presented in the course.

  However, this course is meant for employees with managerial responsibilities and is not directly available for the employees. It is up to the organisation how they wish to go through with the training. NHN suggests the instructors divide the course into 3 x 45 minutes to maximize the learning experience[13].

- **NSM - Nasjonal Sikkerhetsmyndighet**
  NSM offers several courses, both physical (before Covid-19) and e-learning

[12] `https://www.statsforvalteren.no/contentassets/9bad1ed08e7e43dba1306768b34e2e00/kari-stofringsdal---kompis.pdf`

[13] See footnote 12

courses for license fees. They offer courses for ICT security as well as courses in other security aspects. One of the courses they offer regarding ICT security is "NSM's basic principles for ICT security" in which the basic principles is base for many control systems across Norway. This course contains:

1. a more thorough walk through of the principles and extra material
2. examples of basic principles and underlying measures
3. priorities of measures in the principles
4. use of principles in regards to cloud services
5. common misconceptions of ICT security
6. other relevant framework etc.

There are other courses available, such as a course about risk assessment and security clearance of ICT systems among other topics.

- **HEMIT**
  Central Norway Regional Health Authority, Helse Midt-Norge IT or HEMIT arranges an information security course through their quality control system, EQS, which is similar to a LMS (Learning Management System) to the four hospitals trusts belonging to the Central Norway Regional Health Authorities, as well as the hospital pharmacies (Sykehusapotekene).
  The use of EQS also allows the management to follow the progression of the courses and follow up on the employees that need to take the course.

  Tommy Kinnuenn, who works at Nord-Trøndelag Hospital Trusts, says that their course is mandatory for all new employees, and that they have a yearly goal of completion as well as a refresher every 2nd and 3rd year. The course progression should be followed up by a leader. The downside to offering the course to new employees, is that the employees who have been working in the trust after the course was implemented will not be offered the course.. He also states that the course provided to the employees is of a more general nature, offered to all employees across the organisation. When discussing the matter, Tommy Kinnunen says that physical meetings in the courses is difficult due to the size of the staff. They have approximately 3000 employees, so it is limiting how many that could be gathered at the same time in order to go through such a course.
  When talking to Tommy Kinnunen about his, he expressed wishes to change the course to make it more customized to the different roles in the hospital. He wants to meet the employee in their everyday work situation, make it more relevant and thus more likely to have an effect. An alternative is to buy a pre-made course from NorSIS, however, as he states, it is difficult to prioritize because he lacks his own budget.

- **Northern Norway Regional Health Authority and the Western Norway Regional Health Authority**

Unfortunately, neither of the two regional health authorities has disclosed much about their security training to the public. However, both of them did receive negative feedback about their information security from the report released by the Auditor General in December 2020 mentioned in chapter 3.2. In press releases from the health authorities they state that they have begun working on making improvements on their information security comply to today's standards. Northern Norway Regional Health Authority stated that they had plans to invest 1.2M NOK in projects regarding information security [14].

3.5.2 About courses from the interviews

I interviewed two security experts, Tommy Kinnunen who works as a CISO at Nord-Trøndelag Hospital Trust and another security expert working within a hospital trust in Norway (who wanted to remain anonymous).
Tommy Kinnunen has long experience from the field of information security. Having worked as a digital investigator for the police he started working as a CISO for a fish farming trust in 2010. In 2017 he established a consulting firm that offered consulting services regarding information security, among other things. He has also worked as academic administrator for information security (CISO) at Domstoladministrasjonen before he started working as CISO at Nord-Trøndelag Hospital Trust.

After speaking with the experts about information security courses in their trusts, it is clear that this is just the beginning of what is to come. Both of them have just begun working at their respective trusts, and wishes to make a change regarding how things are today. They both agree that the courses must be more adaptable, customized, in order to meet the employee in their every day work and make the information relevant for the role the employee has.
It is clear that the management needs to be more involved in raising the focus on information security. Tommy Kinnunen says that he knows that management in Nord-Trøndelag Hospital Trust has plans regarding this, other than just receive updates regarding status of measures done. The other security expert says that there is some work currently happening, and states that information security needs to be implemented at the top-level of management. If it's not well anchored at the top, one can not expect that the rest will follow.

On areas regarding future focus, the other expert wants to focus more on security culture and understanding of information security among health care personnel. This includes informing them about what they can and can't do with health data, which tools to use in treating data and, not to forget, make clear guidelines regarding the use of cloud services, which there has been some conflicting information about. It is also important to inform about laws and regulations that health

[14] https://helse-nord.no/nyheter/ikt-sikkerheten-ma-bli-bedre

care personnel has to relate to in every day work, such as Datatilsynet, helsepersonelloven and GDPR.

While both experts have different approaches to how they want to evolve and make information security more visible for health care personnel, they agree information security needs to mature within the health care sector. Tommy Kinnunen mentioned that he misses an overall strategy, like the National Cyber Security Strategy for Norway presented in 2019[15], which bases it self on NSM basic principles. Also, the maturity comes from knowledge development among all levels; individual level (the employee), group level (the organisation and internal environment) and lastly society (the environment surrounding the organisation, our partners etc.). The other expert feels that in order to gain maturity, the knowledge about information security needs to involve management and establish a minimum level of knowledge among the health care personnel in their trust.

Both experts agree on that the guidelines and recommendations regarding information security courses that exists today are good. Tommy Kinnunen mentions that while they are good, there is the challenge that the employees need to prioritize their time to manage to take the course and that the course needs to be implemented as an "education" that continues, develops and follows the technological development. The other expert thinks that there is a lot of decent offers out there, many presented during NSM's security month and you usually get what you pay for. Priorities and time is a more difficult matter.

[15] https://www.regjeringen.no/en/dokumenter/national-cyber-security-strategy-for-norway/id2627177/

Chapter 4

Method

In order to answer the research questions, research methods need to be applied. These methods are usually divided in two groups: Qualitative and Quantitative methods[44, p. 99].
The quantitative method is mainly used to explain the research by utilizing numerical data and standardized instruments. It is a more focused method than the qualitative method because the variables are known and are treated, and there are already established guidelines on how to conduct the process. The numerical data collected is usually analysed statistically and objectively, which decreases the possibility of researcher bias and the change of collecting bias data. One of the main reasons behind the quantitatively research method is to be able to collect as much data as possible to create a representative of the population.

The qualitatively method, however, has a more holistic approach to data collection. It is much due to the fact that instead of researching numbers the research are human beings, and humans are complex beings consisting of a lot of unknown variables. I need to be able to meet the participant where they are and not take them out of their own context. The data collected is often text-based and collected through observations or interviews. This makes the data I collect informative yet loosely structured depending on the context. The number of participants also tend to be low as it is not practical nor feasible to perform personal interviews to collect large amounts of data.

4.1 Mixed-method

Based on the presentation of the methods, I chose to utilize both the qualitative and the quantitative method, or a mixed-method design [44, p. 329]. The mixed-method will be ideal to use in this master thesis because it adds both qualitatively and quantitatively dimensions to the research questions. In addition to using the mixed-method, I continuously performed a systemic review of literature (literature review) during the process. The literature review proved to be useful to keep

up with the state of the art as well as showing interview participants that the interviewer was knowledgeable and able to understand the concepts and language during the interview.
The interviews were planned to be semi-structured[44, p. 160], and an interview guide and consent form was written before conducting the interviews. These documents were also a requirement to get the application from NSD approved to record the interviews.

It is known that by using a mixed-method approach the workload would be higher than by choosing either a qualitatively or quantitatively method. But by doing it this way, the different data is used to increase completeness of the research and increases the possibilities to triangulate the results of the research.

As initially stated, both qualitatively and quantitatively methods were conducted at the same time, with similar weighting to both the qualitative and quantitative data depending on the research question. In Appendix B - Questionnaire, Table B.1 is displaying how the different questions apply to the research questions.

The different methods and tools used will be explained more in detail in Chapter 4.3 Data Collection.

4.2 Applied Methods

This section contains the reasoning behind the choices of method applied to each research question. The target of the research is health care personnel and those who handle electronic health systems.

4.2.1 RQ1: What are the cyber security risks we are facing today in health care?

In order to answer this research question, there was conducted a risk assessment regarding the risks the health care sector faces today. It requires knowledge about the state of the art and a thorough literature review [44, p. 340] regarding the subject. The literature review will be important in the beginning of the project, but as cyber security is a dynamic field, the review will be ongoing throughout the process of the research period. The reason is to constantly be able to keep on top of what is state of the art. The literature review is also a tool to help the reader navigating best practises and laws and regulations regarding cyber security in the health care sector.

In order to get an accurate and real threat assessment regarding what the health care system faces, it would be natural to conduct interviews. It would be interesting to see what the people working with cyber security faces regarding threats on the health care system and what other countries health care systems

have been facing, such as the malware attacks on American hospitals[1], the malware Ruyk[2] has caused much damage and annoyance to the affected targets. Will the Norwegian health care sector be able to avoid attacks like this in the future? Is the training focused on learning the users to recognise these types of traps set up by the attackers? These are questions that could help answer research question 1.

4.2.2 RQ2: How does the cyber security training affect the risk awareness in the daily work of health care professionals? RQ3: To what degree do the cyber security training affect the risk awareness of the medical professionals in their private domain?

These two questions will be of a quantitatively nature and will be conducted as a two-part questionnaire. It is known that health care professionals do not have much spare time, it will not be an extensive questionnaire but the aim is to make it as concise as possible yet make it broad enough to pick up the nuances in the answers. It would also be important to learn the lingo to make the questions more easily relatable.

Among the questions presented is questioning if they handle data electronically and if they have had security training. There will be possibilities to measure the risk perception if the questionnaire distinguishes between those who have had training and those who have not. It will also be questions about how they would treat data in a work setting and in private - if there are any differences between the handling. It would also be interesting to see how the security measures imposed on the health care professionals have been perceived in their daily work and how much they evaluate the cyber security training in regard to Electronic Health Records [3] (EPJ) for example.

The quantitative approach in the online questionnaire will help collect data in a larger scale than the qualitatively data collection methods. It would take more time to conduct individual interviews in order to achieve the same amount of data to analyse. The data collected could also help pinpoint weaknesses in the hypothesis and could help to either confirm or disprove it. There are several positive aspects of using a quantitatively approach when answering these research questions. In order to achieve a valid collection of data which can be generalised for the intended population there has to be enough participants for the questionnaire.

4.3 Data Collection

The data collection was two parted: a questionnaire and interviews. This was the preferred methods as they dictated how the research questions were formed. The way the questionnaire was initially thought distributed was through social media

[1] https://www.wired.com/story/ransomware-hospitals-ryuk-trickbot/

[2] https://www.malwarebytes.com/ryuk-ransomware/

[3] https://en.wikipedia.org/wiki/Electronic_health_record

(Facebook) and with direct contact with the different health trusts in Norway. I made an email list over the major regional health trusts and the associated hospitals. The list contained 25 regional and local trusts in all. The email was conducted in such a manner that the trusts could either distribute the questionnaire them selves or I could do it if I got permission to do so. In this email I also requested the possibility to do interviews with information security personnel if possible.
I also sent emails to 30 municipalities, trying to check the media and contact municipalities that did not have a large outbreak of Covid-19 at the time. I did not request interviews with the municipalities. More about that in chapter 8.1 Limitations.

The result of the contact is seen in table 4.1. The missing numbers between the ones that initially responded and the actual numbers which responded yes or no was mostly the lack of follow up from both parties, but because of Covid-19 I kept track of the outbreak situations regarding the respondents areas and I did not want to keep pushing for answers from them, adding pressure to an already stressful situation.

Who?	Contacted	Responded	Responded Yes	Responded No
Trusts	25	8	5	1
Municipalities	30	8	4	2
Total	55	16	9	3

Table 4.1: Numbers of respondents

This result was something I expected and took in consideration when I performed my risk assessment. I am still happy with the result, seeing that the Norwegian health care was handling their third wave of Covid-19.

4.3.1 The Questionnaire

There are a lot of variables to consider when doing research and especially when it comes to doing research at this level. The ability to convinces the participants to participate in the study and to protect the participants from unwanted exposure of their personal data. After some research, I decided to use UiO's Nettskjema[4]. The reason behind this is that they promise complete anonymity, but also keep the respondents' privacy in mind if any personal information would be collected. Nettskjema also provides an easy and effective way to export the data to statistical tools and it is easy to see the results as it comes in. It is also a Norwegian product, which could be used to establish a more trustworthy impression in the respondent.

The questionnaire was initially meant to be distributed with an incentive (chance to win a gift card) to motivate the respondent to answer. However, this required

[4] https://nettskjema.no/

the respondent to voluntarily give up their e-mail address in order to participate in the drawing of the gift card and they would no longer be anonymous. After some thoughts and consideration, this option was discarded due to risk of having inaccurate, or worse, false answers because they feared for their privacy. The ”sensitive“ nature of some of the questions[5] also made the decision to make the questionnaire anonymous easier. I would rather risk getting fewer answers than risk getting false answers.

Further on, the strategy on collecting data was to do it two different ways: with the help of social media and direct contact with the hospitals and municipalities. There were some thoughts behind doing it this way. One was to create an easy way of controlling the samples, another way was to make sure that I would collect answers that were legit. When releasing the questionnaire in the wild on social media, I feared that it would reach someone who answered it regardless of they were a health care professional or nor. This was nothing I could control in a proper manner, so the way was to send a copy, an identical questionnaire, to the health care facilities I contacted directly. However, some of the participants required a presentation of the results, so in order to being able to accommodate their requests, I created identical questionnaires which was distributed. This way I could remain in control of the samples.

The questionnaire (found in Appendix B) was based on the questionnaire template issued by Digdir [6], which has been tested and used by companies and organisations. It was built up around 26 questions divided into five parts and included a finishing part where the participants could comment about either the questionnaire or general thoughts about the subject. It was calculated and tested that it would take just under 10 minutes to go through it. I was also interested in finding out if there were any differences in the answers between the participants who had received information security training and those did not receive it. The solution to achieve this became to replicate the questions already made and depending if the respondent answered *Yes/No* on the "trigger question" *Have you received information security training?* the questionnaire sent the respondent to the correct part of the questionnaire. This way, I had more control of the questionnaire and it was possible see if there were any differences between the answers without having to target the two different groups separately. The questionnaire was also tested and quality checked by health care personnel before releasing it, to make sure the questions and the language were relevant.

- **Part 1:**
  This part consists of questions regarding background information, if the

[5] Questions such as ”Have you ever deliberately violated the policies your employer has imposed on you in relation to information security¿‘ and ”Have you experienced feedback from colleagues that something you did posed a risk to information security¿‘

[6] `https://www.digdir.no/informasjonssikkerhet/veileder-kartlegging-av-digital-sikkerhetskultur/2142`

respondent uses electronic health systems (a criteria for advancing in the questionnaire), where the respondent works (primary health care, specialist health care or social health care) and finally if the respondent has gone through information security training or courses. The thought behind this part was to establish a foundation to compare the two groups of health care professionals with each other.

- **Part 2:**
  This part of the questionnaire consists of questions about the respondents' attitude towards information security and risk awareness.
- **Part 3:**
  This part of the questionnaire consists of questions about how leadership and controls is perceived by the respondents.
- **Part 4:**
  This part of the questionnaire consists of questions about the respondents' behaviour when using the internet, both at work and at home.
- **Part 5:** This part of the questionnaire consists of questions about where the respondent has received information security training from and what methods of training motivates learning.

Furthermore, the questionnaire consisted of different types of questions, ranging from the concise answers *Yes/No/I do not know* to Likert scale questions with answers like *Strongly Disagree/Partly Disagree/Partly Agree/Strongly Agree/I do not know*. The process will be explained in chapter 4.4 Data analysis.

During the initial phase of distributing the questionnaire, one of the supervisors came across a sponsored post on Facebook from another master student at NTNU. This newfound option to distribute the questionnaire to a targeted audience was tempting and had to be tried. The demography was Norwegians between the age 18 and 65, which met one or more of the criteria I specified. Among them were medicine and health as interests, and if they worked as a health care professional. Furthermore, I paid 700NOK for 10 days of promotion for my questionnaire. The promotion reached roughly 6200 people in the time period, and about 248 people clicked the link. The actual result from the promotion was 121 answers. The data collection period was between February 24th and April 26th for all forms.

The all over result from the questionnaire data collection ended up as can be seen in figure 4.2.

4.3.2 Interviews

The process started with doing the check with NSD if the project needed to be reported. As I wanted the possibility to record the interview if needed I had to report the project. As part of the requirement from NSD to get the approval I had to prepare an interview guide, which can be found in Appendix A. I also needed

Where?	No. of Answers
Social Media	141
Direct Contact	62
Contact 1	22
Contact 2	3
Sykehuset Østfold	110
Nord-Trøndelag Hospital	56
Total	394

Table 4.2: Numbers of respondents on the questionnaire

to add a consent form, which can be found in Appendix C. As it can be seen in the letter, there are differences between the numbers of research questions in the consent form and in the final thesis, but it will be addressed properly later in Chapter 8.1, Limitations.

As stated earlier in the chapter, I asked for interviews with information security professionals, and got responses from a few people who wanted to talk to me about the subject. After the respondent had agreed to an interview, we arranged a meeting on Teams. When inviting the participants, I added the information letter/consent form which also explained the thesis more in detail and what their participation would be.

I ended up not recording the interviews despite having approval from NSD to do so, as I thought it might lay some constraints on the participants. And I made a promise that if they were uncomfortable with any information they had given to me under the interview, I would not use it in the thesis. After the interviews, the information was re-written to the best of my abilities and sent to the participants for proofreading and approval of use.

4.4 Data Analysis

The data analysis has been conducted in SPSS for the analysis and excel for making the graphs. The graphs have been incorporated into the results in chapter 5 - Results, while the rest of the output from the analysis has been added as Appendix D page 135.
Initially, the answers were collected from Nettskjema.no and since there were 6 forms it had to be merged in to one big form containing every single case.

4.4.1 Descriptive analysis

I chose to perform a descriptive analysis of the data collected. Aarø[45, p. 13] states in his book that a descriptive analysis of a questionnaire will show characteristics of a whole populations or a sample of a population, and describes how the situation is in subgroups of the population. Subgroups could be divided into gender, age, education and so on.

On the ordinal and nominal data I have analysed, I have generally looked at the mean, because the answers has been very consistent with few selecting the answer “Do not know”. However, on the questions found in chapter 5.2.6, online activities and consequences, the amount of “Do not know” was actually so overwhelming that the results became severely skewed. To mitigate this problem, the category was presented in written and then visually when reporting frequencies in the first part of the analysis. The "do not know" category was removed from the dataset in order to be able to report the correct numbers for One-Way ANOVA. There will be a note in the text where this method has been applied, not to confuse the reader.

4.4.2 Bivariate statistics

Since my questionnaire consists of many Likert Scale questions, the analysis will consist of both nominal and ordinal measures, depending on the question. There has been critics about using bivariate analysis such as One-Way ANOVA on Likert scale questions, claiming it cannot be used for this type of analysis. However, the article written by Geoffrey Norman[46] has many clear and concise statements of why this is no longer true. The reporting of significance in this thesis will be sober none the less.

In regard to correlation, I have used the Pearson two-tailed correlation, seeing as my data is not monotonic. If it were monotonic, I would have used Spearman’s rho instead.

4.4.3 Hypothesis testing

In my significance testing of One-Way ANOVA, I have put gender as a factor. Furthermore, I have formed a hypothesis about the differences in the dependent variables and gender. The significance level was 0.05, meaning that there is no relationship between gender and answer if p=<0.5, or H0. If it is higher, then there is a relationship between the genders and the answers they have given., or H1.

Chapter 5

Results

In this chapter I will present the questions from the questionnaire and analyse them. They are divided into five parts, consisting of the same parts as the questionnaire: demographics, attitude and risk perception towards digital security, views on management and control in the workplace, behaviour and knowledge and motivation. The interviews conducted will not be presented in this chapter, as it felt more natural to address them in Chapters 3.5 and 3.5.2 in Related works, and in Chapter 6.1 Discussion - Research Question 1.

As I was determined to ask a segment of the population consisting of large population (health care professionals) I also needed to have a fairly large sample size. Numbers collected from SSB in March 2021, revealed that there were 452.051 people working within the health care sector at that time. With a wish to maintain a confidence level of 95% and keeping the margin of error low, at max 5%, I needed my sample size to be 384. In the end of the data collection, I had managed to get 392 answers, which means that my findings could be generalized for the intended population. However, as can be seen in table 5.1 12 responded that they did not use any form of EHR systems or handled patient information, so by default they could not finish the questionnaire (but they were still counted in the grand total). The end result was a sample size close to the limit to generalize the result.

Two respondents were removed from the data set. One was removed due to a glitch early in the data collection process, as there were an error in the questionnaire allowing the respondents to answer the questions about gender, age and work even though they answered “No” on the control question. This was fixed soon after the discovery, so no more errors were made.
The second was removed due to the fact that they had answered “Do not want to disclose” on the question on gender. This alone did not disqualify the respondent, but they were the only one choosing this option, making the analysis of the result unnecessarily complicated.

Furthermore, all the calculations made in SPSS has been added as an appendix, appendix D, SPSS Data sheet, on page 135.

5.1 Demographic and sample

As presented earlier in chapter 4 - Methods, the questionnaire was divided into two different sections, depending what was answered on the control question. The questionnaire started by asking whether the respondent was using an e-health system in their daily work or not. If the respondent answered ”Yes“ on the first question, they qualified to answer the rest of the questionnaire. If they answered ”No“ the questionnaire ended.

	Total	Percentage
Yes	380	96.9 %
No	12	3.1 %

Table 5.1: The total amount of respondents for the questionnaire

As can be seen in table 5.1, only 12 (3.1%) of the respondents the questionnaire reached answered no, which means that 380 (96.6%) started and finished the questionnaire. Nettskjema.no did not report that anyone had left the questionnaire before finishing it (even though it is most likely that something like that happened) even though it was a part of their statistics.

5.1.1 Gender distribution

At first glance, the gender distribution is quite skewed towards females. About 306, or 80.5%, of the respondents of the questionnaire were female and 74, or 19.5% male, as can be seen in table 5.2 and as a visual presentation in figure 5.1. However, when looking at statistics from Statistisk Sentralbyrå[1] (SSB) in table 5.3, this result is very close to the gender distribution working in health care in Norway. It should not come as any surprise that the majority leans towards females in health care as it has traditionally been a female dominated area for many, many years.

	Total	Percentage
Female	306	80.5%
Male	74	19.5%
Total	380	100%

Table 5.2: Gender distribution in the questionnaire

The gender distribution will also be used later in the presentation of the results, as part of the One-Way ANOVA analysis conducted. The distribution between the genders among the ones that had received security training (81.8% female and 18.2% male) and the ones that did not (78.3% female and 21.7% male), were quite similar to the original distribution.

[1] https://www.ssb.no/en/arbeid-og-lonn/statistikker/hesospers

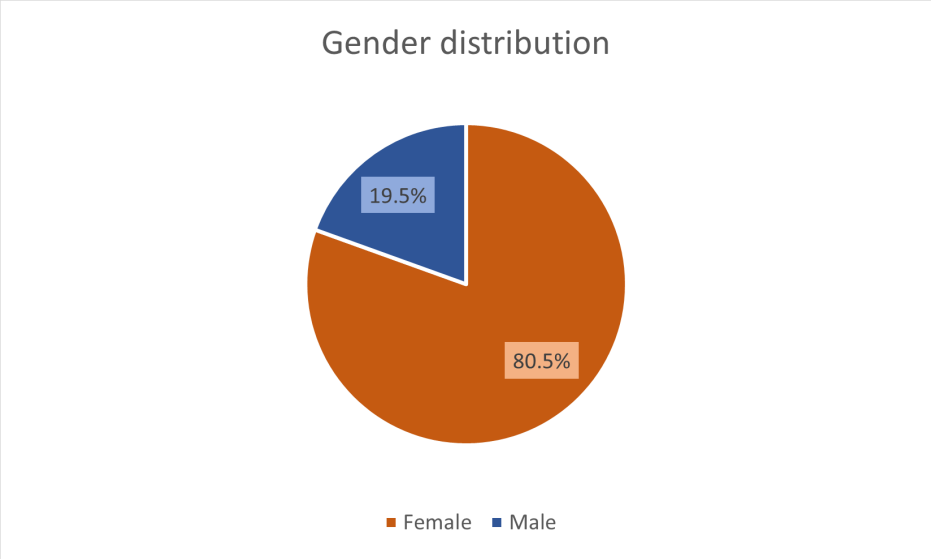


Figure 5.1: Sector diagram gender distribution

	2020	
	Total	Percentage
Persons with a health care education	569 630	100%
Male	91 521	16.1%
Female	478 109	83.9%
Employed with a health care education	452 051	100%
Male	77 456	17.1%
Female	374 595	82.9%
Employed with a health care education in health and social services	352 435	78%

Table 5.3: Gender distribution in Norway March 2021 (SSB)

5.1.2 Age distribution

The age distribution seen in table 5.4 and in figure 5.2, clearly states that the age groups 30-39, 40-49, and 50-59 are the most represented in this questionnaire. Perhaps not surprising, as many of the respondents who answered the questionnaire were recruited from Facebook, reached mostly females between 35 and 54. According to SSB[2] 41,5% working in health care are between the age 15-39, 36.1% are between 40-54 and 22.4% are 55 years or older, making it natural that these particular segments are more represented than others. The questionnaire also included two other categories, Under 20 and Over 70. No respondents

[2] https://www.ssb.no/statbank/table/12546/tableViewLayout1/

answered this, which is why the categories was omitted in the visual representation.

	Total	Percentage
20-29	56	14.6%
30-39	84	22.2%
40-49	108	28.4%
50-59	103	27.1%
60-69	29	7.6%

Table 5.4: Age distribution in the questionnaire

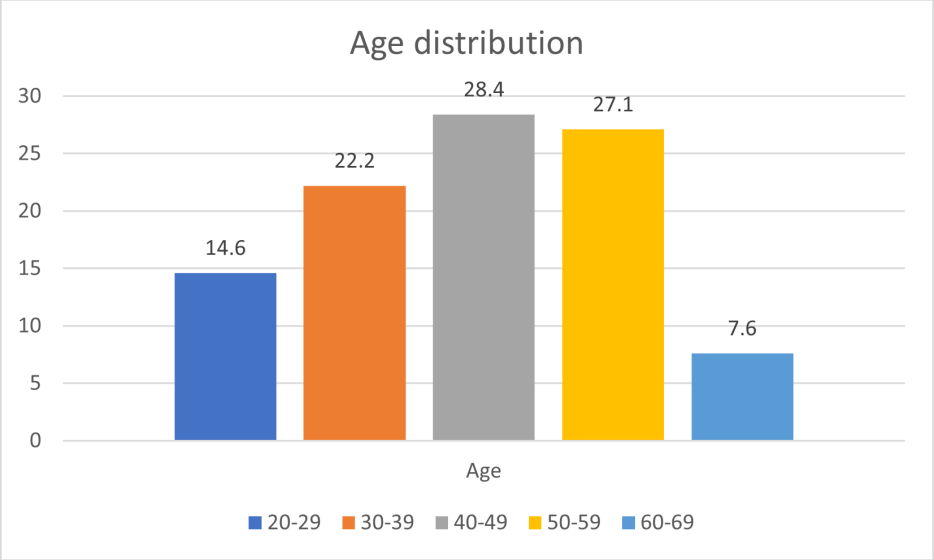


Figure 5.2: Age distribution of the respondents in %

5.1.3 Work distribution

The work distribution can be seen in table 5.5 and in figure 5.3. The results became skewed because I had more positive responses from hospitals participating than municipalities. This was also the reason I chose not to focus my research on the differences between where the respondents worked and rather focused on other aspects of my data. As can be seen in the visual representation, 56.6% of the respondents works in specialist health care and 38.4% works in primary health care. Social health care only had 1.3% of the answers and “Other” had 3.7%.

As mentioned, this question came with an option, “Other”, that allowed the respondent to type in where they worked if they felt that the categories did not suit them. Many of the answers came back actually belonging to the specified cat-

egories, but I did not change it because it would not make a significant difference to my analysis of the results.

	Total	Percentage
Specialist health care	215	56.6%
Primary health care	146	38.4%
Social health care	5	1.3%
Other	14	3.7%

Table 5.5: Work distribution in the questionnaire

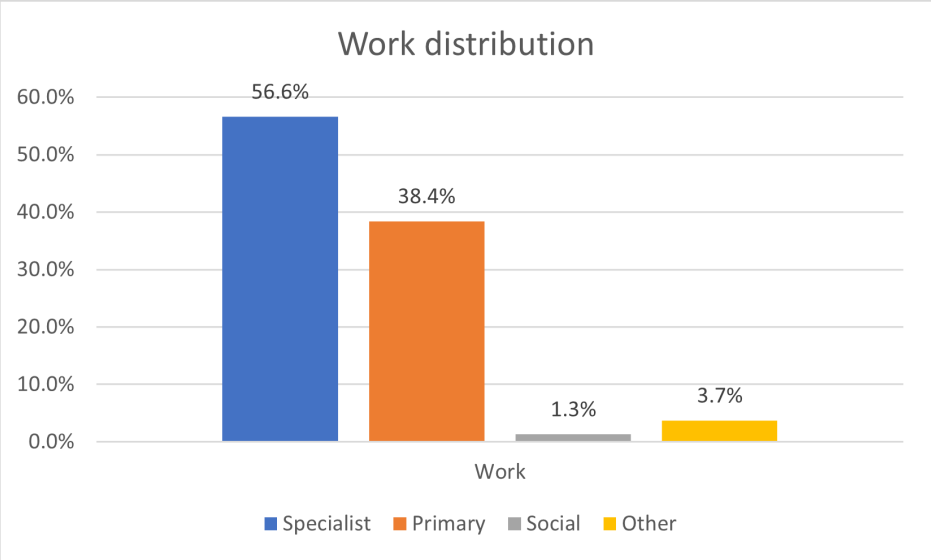


Figure 5.3: Work distribution

5.1.4 Security training

Whether or not the health care professionals had gone through any information security training was the key ingredient in my research, to reveal differences between the two groups. As can be seen in the visual representation in table 5.6 and in figure 5.4, almost 2/3, or 63.7% of the respondents have gone through courses or training regarding information security, while nearly 1/3, or 36.3% have not. This was as expected, regarding the feedback from health care professionals I have talked to outside this thesis.

When breaking down the statistics of training or no training, it would be interesting to see where the focus on training was highest. According to figure 5.5, Specialist health care sector has a 66%/34% distribution of received training or not. Meanwhile, the primary health care sector has 59.6% that have received train-

ing and 40.4% who has not. Social health care has a 40%/60% distribution and "Other", consisting of respondents from the three previous groups had 71.4% that said yes and 28.6% that said no to the statement.

	Total	Percentage
Yes	242	63.7 %
No	138	36.3 %

Table 5.6: The total amount of respondents for the questionnaire

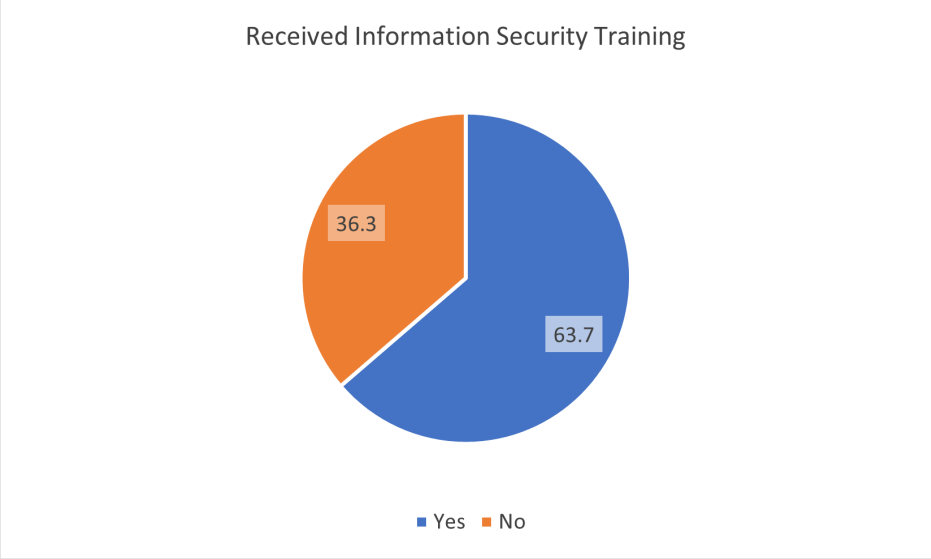


Figure 5.4: Distribution of Information Security Training

5.2 Attitude and risk perception to digital security

The reason for asking these questions in the questionnaire, was to make the respondent aware of certain aspects of information security that they might not think about every day. It was also asked early in the process in order to give the respondents the opportunity to get in the right "head space", to prepare them mentally for the rest of the questionnaire.

This part contains several sub-questions which addressed the attitudes towards digital security and reveal how the health care professionals perceive risks and threats.

5.2.1 New Technology

The attitude towards new technology could reflect on the willingness to comply to new policies, the willingness to learn and adapt to new systems, just because

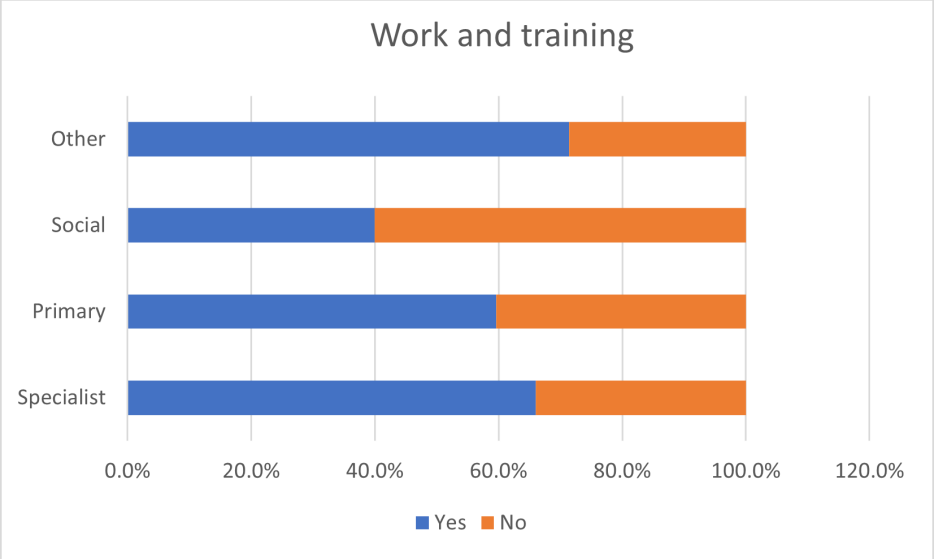


Figure 5.5: Work and Security training

it shows less fear for new elements of the work day and less threat to their work security, as Chao and Kozlowski pointed out in their study regarding employees perception on implementation of robotic manufacturing technology[47].

This question is about whether or not the health care professionals that had the training(n=242) were positive about introducing new technology into the workplace. As can be seen in figure 5.6, 82.2% agreed to the statement, and 16.1% partly agreed. While a large number of the respondents felt positive to new technology, 0.8% partly disagreed and the same amount disagreed to the statement. Among the women that had security training the mean was 3.77 (std.dev. .498), which makes the collective answer tilting from “partly agree” to “agree”. For the men, the mean was even closer to “agree” than the women at 3.91 (std.dev. .362.) A quick analysis with One-Way ANOVA, the result yielded a p-score of .087 between the women and men, which means a major significant difference between the genders.

In the personal domain, the amounts that were positive to new technology were a bit lower, 72.3% said they were positive to it, and the amount that partly agreed were a bit higher, 24.8%. About 2.1% partly disagreed and 0.4% disagreed to the statement. 0.4% did not know. Women were less positive to new technology at home than the men, with a mean at 3.65 (std.dev. .567). The men on the other hand, were more positive to new technology, landing at mean 3.95 (std.dev. .211). One-Way ANOVA could reveal a significant difference between the genders, were p= .000. There is a moderate correlation between being positive to new technology at home and at work, Pearson=.576 .

Meanwhile, the health care professionals that did not receive training (n=138) reported that 70.3% of them were positive towards new technology in the workplace, while 25.4% partly agreed to the statement. The ones that partly disagreed and disagreed to the statement were low in this segment as well, respectively 2.9% partly disagreed and 1.4% disagreed. Women had a mean of 3.68 (std.dev. .609) and men had 3.53 (std.dev. .629), which makes the women more positive to new technology at work. The significance between the genders were not as great as between those who had the security training, p=.262

At home, the health care professionals who did not receive training were 63% positive to new technology and 28.3% partly agreed. A fairly low percentage answered that they partly disagreed (5.1%) and disagreed (2.2%). Both women and men almost agreed on how positive they were to new technology, with the women's means of 3.56 (std.dev. .704) and the men's 3.57 (std.dev. .626). The correlation between being positive about new technology, but not by much, a moderately strong Pearson=.711.

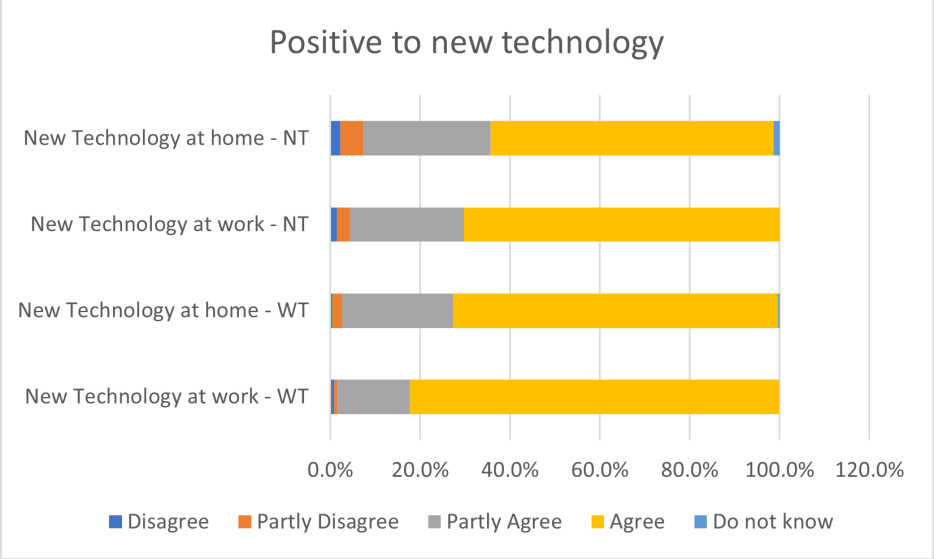


Figure 5.6: Positive to new technology

5.2.2 Risk and threats

When asking the health care professionals with training(n=242), questions about whether or not using the internet would pose an increased amount of risk at work and at home, there were similar answers given. As can be seen in figure 5.7 35.1% agreed to that there was high risk associated using the internet at work and 12.4 agreed to an increased risk at home. 44.6% partly agreed about the increased risk

at work and 50.8% at home. Those who partly disagreed about the use of internet at work (35.1%) and at home (27.3%) meant it did not come with an increased risk either places, while the ones that disagreed meant that is was a lower risk at work (7.9%) than at home (7%). Women reported a mean of 2.73 (std.dev. .899) at work and mean 2.83 (std.dev .848) at home. For the men the mean was 2.32 (std.dev. .740) at work and mean 2.43 (std.dev. .789) at home. These numbers reveals that the perceived risk is not that high or low as it reports means close to 2.5 (the middle). The p-score was p=.005 at work and 0=.004 at home. This tells us that there is a significant difference between women and men in regard to risk perceived at work and at home. Moreover, it has a moderately high correlation, Pearson =.694, which means there are some correlation to risk awareness regarding internet use at work and at home.

The health care professionals without training (n=138) did not agree on the fact that it was an increased risk to use internet on work and at home. When asked about it, only 5.1% agreed on it being higher risk at work and 9.4% at home. A larger amount partly agreed to the statement, 35.5% partly agreed it was an increased risk associated with using internet at work and 38.4% and at home. A higher amount partly disagreed on the increased risk regarding internet use at work (40.6%) and at home (36.2%) and 11.6% disagreed that there was any increase in risk either at work or at home. Women reported a mean of 2.64 (std.dev. 1.072) at work and mean 2.59 (std.dev. .996) at home. Men, on the other hand, had the mean of 2.27 and (std.dev. .691)) at work and mean 2.59 and std.dev. .858 at home. While One-Way ANOVA reveals that there are some significant differences to gender and the information about threat at work, p=0.46. Same as with training, there are a moderate correlation between perceived risk the use of internet at work and at home, Pearson=.695.

The respondents were asked about whether or not they had received sufficient information about digital threats both at work and at home. In a work setting, usually health care professionals receive this type of information from their employer, through appropriate channels, such as email and intranet.
As displayed in figure 5.8, a majority of the health care professionals that had received training agreed (37.2%) or partly agreed (34.7%) that they had received relevant and good information about digital threats at work, while 35.1% agreed and 43% partly agreed about the threat information at home. A lower amount partly disagreed (16.5%) or disagreed (11.9%) on the statement regarding work and similar regarding digital threats at home, where 15.7% partly disagreed and 6.2% disagreed. Women answered 2.98 (std.dev. .1.042) at work and 3.07 (std.dev. .873) at home. The men reported a mean of 2.93 (std.dev. .846) at work and 3.09 (std.dev. .858) at home. The p-score at work, p= .776 and at home, p=.862 tells us that there are no significance regarding gender and threat awareness.

The answers among the health care professionals that did not receive training can be seen in figure 5.8. A larger portion of them agreed or partly agreed that they had received good information about threats at home (19.6% agreed and 41.3% partly agreed) versus at work where only 8% agreed and 23.9% partly agreed to the same statement. However, the largest difference were the ones disagreeing about the statement. 14.5% claimed that they had a good information about the threats they could face at home, but 38,4% disagreed about the statement when it came to the workplace. Women answered at the mean 2.02 (std.dev. .1.032) at work and mean 2.57 with a (std.dev. .978) at home. Meanwhile, the men answered with a mean of 2.10 with a (std.dev.) .923 at work and 2.97 (std.dev. .809) at home. The One-Way ANOVA shows that there is significance between gender and the information about threats at home with p=.046.

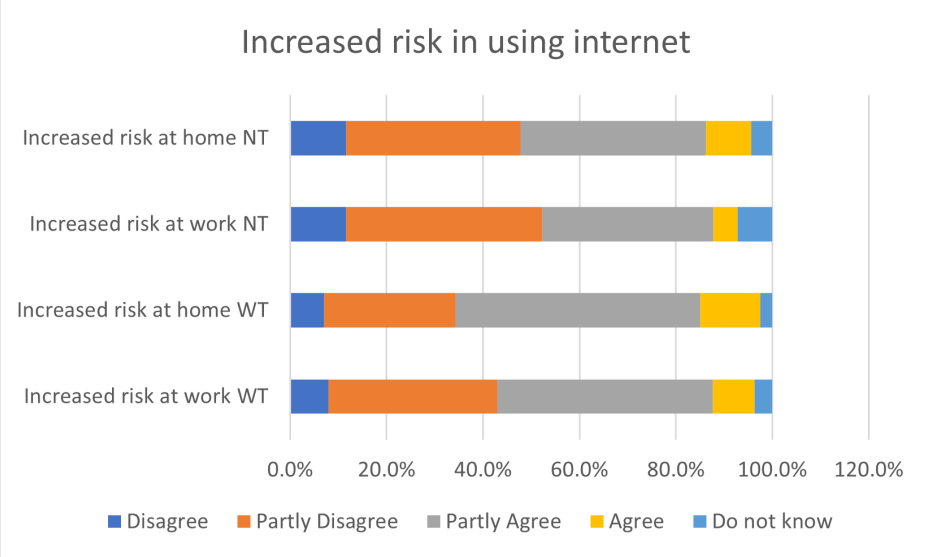


Figure 5.7: Increased risk in using the internet at work or at home

5.2.3 At work

Another segment of this question focused mainly on the workplace and their feelings towards having their ID potentially misused and how they feel regarding having online activities monitored by their employer at work.

On the statement whether or not the health care professionals was worried about their device or ID could be misused and connected to information security events, figure 5.14 shows that 11.2% of the ones that received training(n=242) felt worried about it, while 35.1% felt somewhat worried. There was a slightly larger percentage that partly disagreed (31.4%) or disagreed (18.2%), and 4.1% felt it was not relevant or they did not know how they felt about it. Women answered

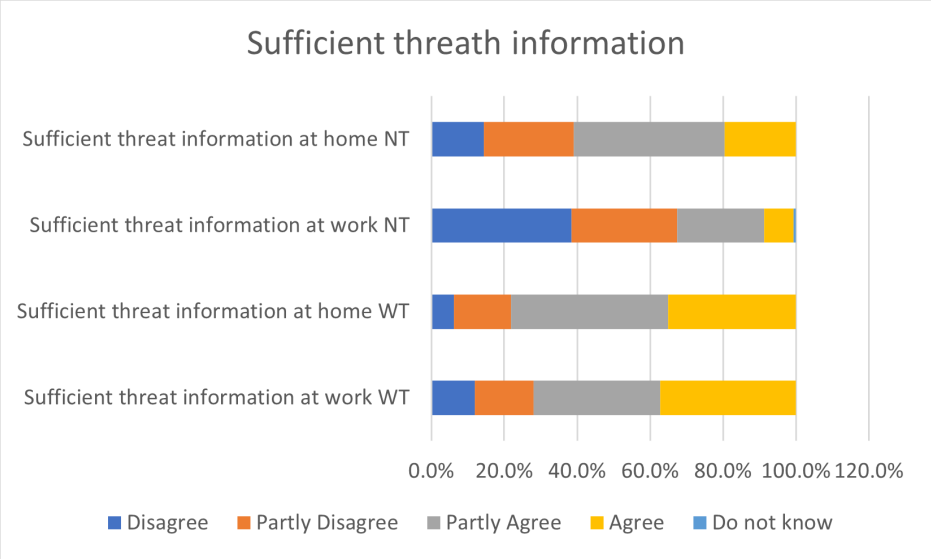


Figure 5.8: Have the respondents gotten sufficient information about digital threats

a mean 2.60 (std.dev. 1.060) which lands them somewhere in between partly disagree and partly agree. Men answered with a mean of 2.14 (std.dev. .878) which means they appear to be less worried about such events. One-Way ANOVA clearly states that there is a significance to gender and the level of worries presented, p=.007.
Amongst the other group, the health care professionals that had not received training, 10.1% felt worried about their device or ID being misused and 29% partly agreed to the statement as can be seen in figure 5.10. And similar to the ones that had received training, 30.4% partly disagreed and 18.8% disagreed. 11.6% did not know. The women without training reported a mean of 2.72 (std.dev. 1.296) which means that they favour parly agreeing to the statement. Men, on the other hand, reported a mean of 2.40 (std.dev. .932), again making them a little less worried about misuse of devices or ID. The significance seems to be less among the respondents without training. There was little or no correlations regarding this question and the other answers.

The respondents were also questioned about whether or not they had issues with their employer monitoring their internet activities while at work and if they had complete trust in their employer regarding their personnel file. In figure 5.9 The group that had received training agreed that they had no issue with either monitoring (54.1%) and had complete trust (55.4%) in their employer. On the other hand, a much lower percentage disagreed to the statement about monitoring (6.2%) and trust (2.5%). Regarding the answers, women reported a mean of 3.38 with a (std.dev. .892), which means that they are close to agreeing to the statement about monitoring. This makes them partly agree to the statement with

little significance to gender with p=.206. Men had a lower mean score at 2.93 (std.dev. .1.087), making them more sceptical to the employers monitoring than the women but not very sceptical. About trust the mean was 3.38 (std.dev. .779) and the men a mean of 3.32 (std.dev of .829.) This could also be seen in the One-Way ANOVA where p=.004, suggesting that there are significant differences between the genders and their opinion on monitoring. There is little or no correlation to the other answers in this section.

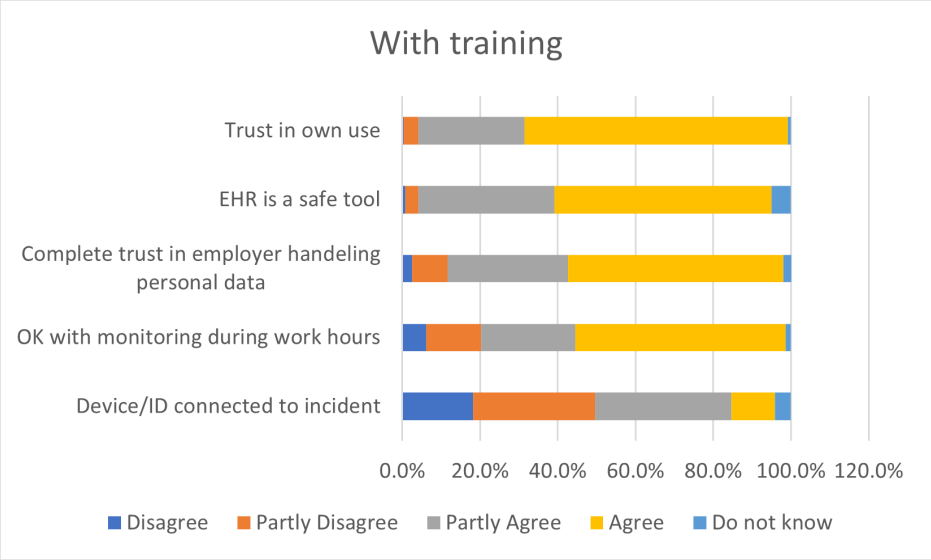


Figure 5.9: At work - With training

When addressing the group without training, 40.6% answered that they had no issue with the employer monitoring their activities, while 48.6% had complete trust in their employer. On the other side of the scale, 14.5% had issues with the monitoring and 6.5% had little trust in their employer handling their employee file. Among the women that do not have training, the mean was 3.03 (std.dev. 1.113), which makes them barely partly agreeing in the to the statement about monitoring. The trust in the employer were a little higher, with a mean of 3.37 (std.dev. .923). The men were more critical to the monitoring with a mean of 2.57 (std.dev. 1.135). The trust was a little higher among the men as well, with a mean of 3.07 (std.dev. 1.081). As with the ones that had received training, there were significance between gender and monitoring where p= .050, but less so when it comes to trust where p= .127. Pearson Correlation shows a moderately low correlation between the two variables about EHR and the safe use of EHR, pearson = .499.

On the questions about how the respondents felt that their EHR (EPJ) was a safe tool to use to treat patient data and if they felt secure in their use of the

tool 55.8% of the respondents who had received training agreed that EHR was a safe tool, while 35.1% partly agreed. 67.8% agreed they felt secure in their use and 27.3% partly agreed to that statement. Meanwhile, on the other side of the scale, 3.3% partly disagreed to the whether the EHR was a safe tool and only 0.8% disagreed. 5.3% stated it was not relevant or they did not know how they felt about it. It is similar for the ones that partly disagreed about their own use of the tools, where 3.7% partly disagreed while 0.4% disagreed. 4.1% did not know. There is not much difference between women and men regarding these questions. Both women and men felt similarly towards whether they perceived the EHR as a safe tool. Women had a mean of 3.61 (std.dev. .687) and men had a mean of 3.59(std.dev. .675) which means that they lean from partly agree to agreeing to the statement. According to the answers regarding how secure they felt in their own use, women were a little more confident than men, with a mean of 3.66 (std.dev .580) versus mean of 3.59 (std.dev. .622).

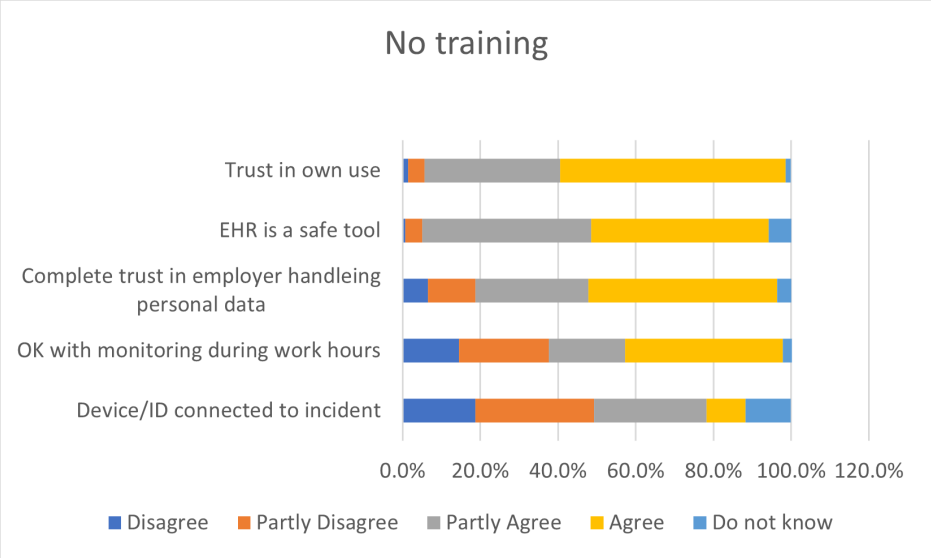


Figure 5.10: At work - No training

Among the ones without training, as seen in figure 5.10 45.7% agreed that EHR was a safe tool and 43.5% partly agreed, meanwhile 58% felt safe in their own use of EHR and 34.8% partly agreed to that. 4.3% partly disagreed with the statement about EHR being a safe tool and 0.8% disagreed to that. 5% did not assume it relevant or did not know. It was low percentages on the question about whether or not they felt secure in their own use of the system, 4.3% partly disagreed and 0.4% disagreed. 0.8% did not find it relevant or did not know. Both women and men felt safe that using EHR to treat patient data, respectively mean on 3.52(std.dev. .704) and 3.50(std.dev. .731), while there was a little gap in how secure they felt in the use of the EHR. Women felt more confident in their use,

with a mean of 3.57 (std.dev. .644). Men did not fall far behind with a mean of 3.40 (std.dev. .770). There were no significance between gender and how safe their EHR was perceived with p= .900, however there were more tendencies to significance considering gender and how secure the respondents felt using EHR, with p=.212. There is a moderately low correlation between EHR and safe use of EHR here as well, Pearson =.458.

5.2.4 Where is information security more important

How health care professionals see risk and how they perceive where they face the most threats, could be helpful in mapping how and where the threats come from. If someone thinks that information security is most vulnerable at home, how do they conduct themselves at work, and why do they feel that it is more important at home if that is the case? Is it because of all the security measures in place at work or is it because it is not their data that could at stake?

The though about this question was to check if the other answers that were set up as “at work” and “at home” actually reflected what they had answered on this question. It is easy to say something that “feels right” or seems “mandatory” to feel, but when push comes to shove it might not be the case after all?
The results of the question about where information security is most important can be seen in 5.11. The respondents had to choose between ”at home“, ”at work“, ”equally important“ or ”neither“. In both groups the answer ”equally important“ was dominant. In the group that had received training, 171 out of 242 (70.7%) answered this, while 26.9% answered ”at work“ and 2.5% answered ”at home“.In this case it is important to note that 1. means at home, 2. means at work and 3. means equally important. The women’s mean was at 2.68 (std.dev. .510) which places them between “at work” and that it is equally important.The men were not far off, with a mean of 2.70 (std.dev. .553). There were little significance between the genders and their answers, p=.748. There was low correlation between the variables.

In the group without training, there was a similar distribution. 107 out of 138, or 77.5% answered ”equally important“, while 20.3% answered ”at work“ and 2.2% answered ”at home“. No one answered ”neither“ from any of the groups. Women answered closer to “work” than men, with a mean of 2.78 (std.dev. .439) and 2.67 (std.dev. .606). There was more significance between women and men without training, p=.264, but it is not significant enough ($p<0.05$) to report it as being so. There was low correlation between the variables.

5.2.5 Feedback to and from colleagues

When asking the respondents about whether or not they had been given any feedback from colleagues about their actions being a risk regarding information security, 11.2% of the group with training (n=242) said yes while 88.8% said that they had not received such feedback as can be seen in figure 5.12. The women

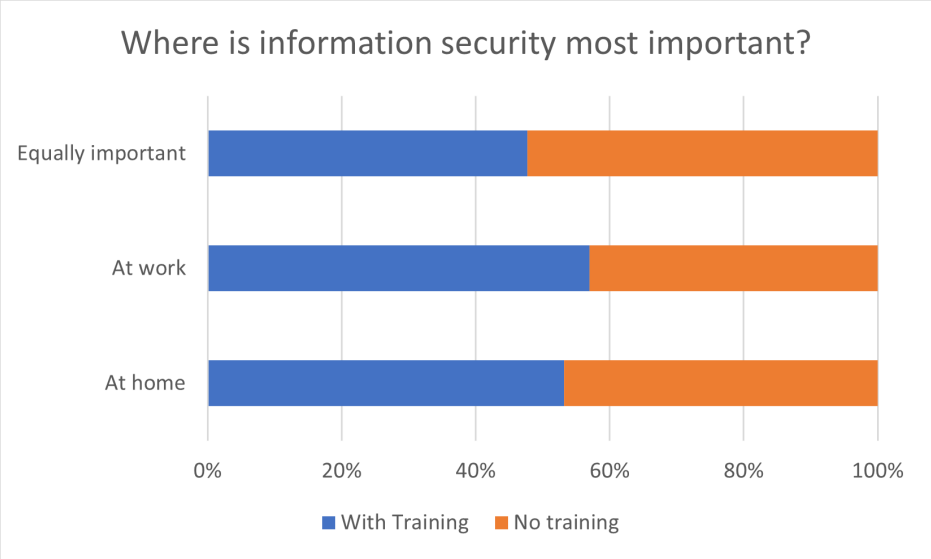


Figure 5.11: Where information security is most important

answered at a mean of 1.90 (std.dev. .302), which means most of them answered no on this question. The men had a mean of 1.84 (std.dev. .370) which means that some of them have had more feedback than the women in this case. There is some significance between gender and having said "yes" regarding the feedback, with p=.270, which is higher than the range of p<0.05.
In the other group, the ones that had not received training(n=138), 4.3% said that they had some feedback while 93.5% said they had not. 4.3% felt it was not relevant or did not know. Women without information security training reported a mean of 1.98 (std.dev. .273) and men close behind on 1.97 (std.dev .183). The result being that very few have gotten this feedback from colleagues. There is no significance between gender and feedback where p=.780.

On the question on how comfortable they were telling a colleague that their actions could pose as a risk for the company's information security, most of the respondents who had training were very comfortable (42.1%) telling their colleagues if they saw something and 33.9% said they were a little comfortable. Meanwhile, 19.8% were a little uncomfortable and 1.7% were very uncomfortable. 2.5% did not know. Women were a little bit less comfortable than men giving this type of feedback, with a mean of 1.94 (std.dev. 1.040) versus a mean of 1.77 (std.dev. 1.031). Some significance regarding gender and comfort level, p=.337, but not within the range of p<0.05.
In the group without the training 33.3% were very comfortable telling their colleagues and 34.1% were a little comfortable letting their colleagues know about the risk. 21.1% would tell, but felt a little uncomfortable about it, and 5.8% would feel very uncomfortable about it. 0.7% would not tell their colleague at all. Women

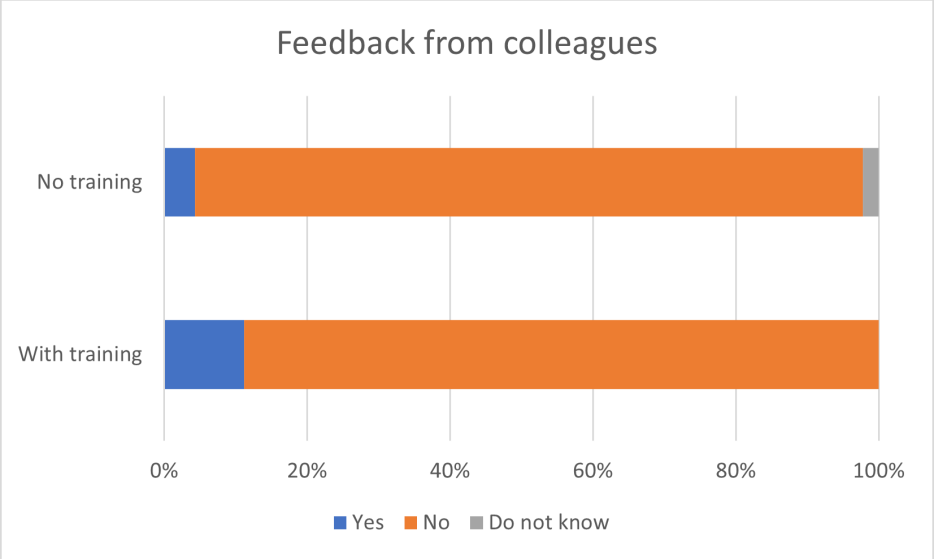


Figure 5.12: Feedback from colleagues

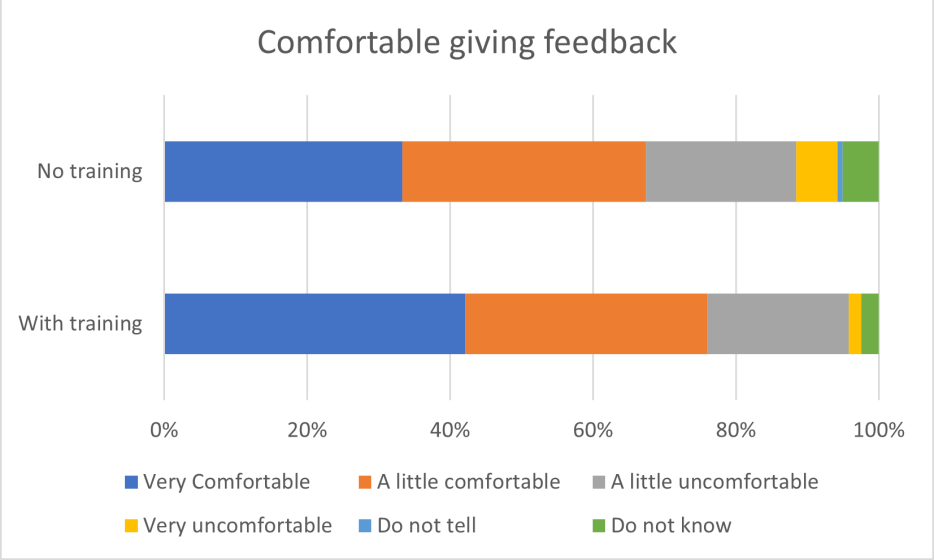


Figure 5.13: Comfortable giving feedback

without training shows more hesitancy regarding giving feedback to colleagues than women with training, with a mean of 2.30 (std.dev. 1.355), and the same with men at a mean of 1.93 (std.dev. .868). There was a higher significance regarding gender and feedback, p=.167, but it is still not low enough to report it as a significance. Within the respondents with no training, it was no correlation between comfort level to give feedback and received feedback.

5.2.6 Online activities and consequences

These questions are regarding to which degree the respondent meant the different activities presented a risk, both at work and at home. The list of risks is something almost everyone faces every day, in some way or another. The other part was to assess threats to information security in connection to the workplace and to the respondents' own information security, their own private data.

Risk at work - with training

As can be seen in figure 5.14, "Borrowed passwords" was the activity that clearly imposes a greater threat among the ones with training, by 66.5%. The next risks, to a fairly large extent, were social media (36.4%) and e-mail (31.8%). However, there were a fair amount of people that did not know how "Smart Devices" (32.6%) or "Cloud services" (23.6%) would impose a risk at work.
Women answered lower than the men in regards to if borrowed passwords, with a mean of 3.35 (std.dev. . 980) versus 3.68 (std.dev. .800). The women answered with a mean of 3.05 (std.dev. 1.105) felt that social media imposes a larger threat than the men with a mean of 2.48 (std.dev. .939) did, but they almost agreed on the level of risk regarding e-mail where the women's mean was 2.41 (std.dev. .872) and the men's mean was 2.43 (std.dev. .846).

Figure 5.14: Potential risk at work - with training

Risk at home - with training

At home, seen in figure 5.15, the trend continued, with borrowed passwords that poses a greater risk at the largest extent, with 51.2%. The same goes for social media (42.1%) and e-mail (32.1%). Smart devices (29.3%) and cloud services (16.9%) were still the activities with the largest portion of "Do not know".
Women answered almost the same as at work, with a mean of 3.34 (std.dev. 1.095), however the men answered lower mean 3.16 (std.dev. 1.119), regarding borrowed passwords at home as less of a risk than at work. Women also meant that there was more risk with both social media with a mean of 2.80 (std.dev. .912) and e-mail mean of 2.45 (std.dev. .875) that the men on social media with a mean of 2.57 (std.dev. .974) and e-mail mean of 2.23 (std.dev. .937). There was some significance between the genders regarding storage (p=.070) and smart devices (p=.102) but not enough to report it as a statistical significance. There was also a moderate correlation about the risk of smart devices at work and at home (Pearson= .625), passwords at home and at work (Pearson = .607) and the risk of e-mail and social media at home (Pearson = .606).

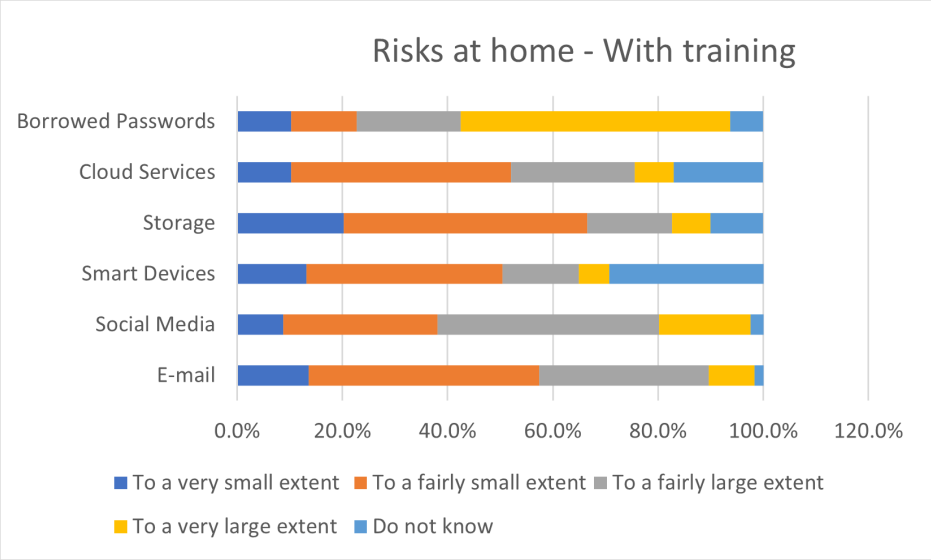


Figure 5.15: Potential risks at home - with training

Risk at work - no training

As seen in figure 5.16, "Borrowed passwords" did impose the largest risk among the health care professionals that did not receive training, at 48.6%. Again did social media (38.4%) come in second at a fairly large extent, but instead of e-mail came storage (26.1%) in at third. Smart devices and cloud services still have a large amount of "Do not know"- answers, 34.8% and 29%.
Women answered more towards "fairly small extent" at a mean of 3.34(std.dev. 1.153), while men leaned more towards "fairly large extent" at 3.60 (std.dev.

.675). Both women, with a mean of 3.81 (std.dev. 1.341) and men with a mean of 3.80 (std.dev. 1.341) agreed that storage was a fairly large risk at work. There was a statistical significance regarding gender and smart devices, with a p-score of p=.031.

Figure 5.16: Potential risk at work - no training

Risk at home - no training

In figure 5.17, we can see that there is similarities in the results among the ones without training regarding the risk at home. Borrowed passwords is still at the top by a large extent, 39.1%. Then social media (33.3%) and e-mail (26.6%) follows. As for the risk of borrowed passwords, women at 3.15 (std.dev. 1.281) see borrowed passwords at home a less of a risk than men at 3.37(std.dev. 1.159). When comparing the genders about risk and social media, they pretty much agree, women at 2.65 (std.dev. .998) and men at 2.63 (std.dev. 1.009).
There are some statistical significance regarding gender and smart devices, p=.014 and gender and cloud services, p=0.38. A moderately strong correlation could be found between smart devices at work and at home (Pearson =.716) and a moderately strong correlation between cloud services at work and at home (Pearson =.668). There is also a correlation between social media and e-mail at home (Pearson =.643) and cloud services and storage at home (Pearson =.614).

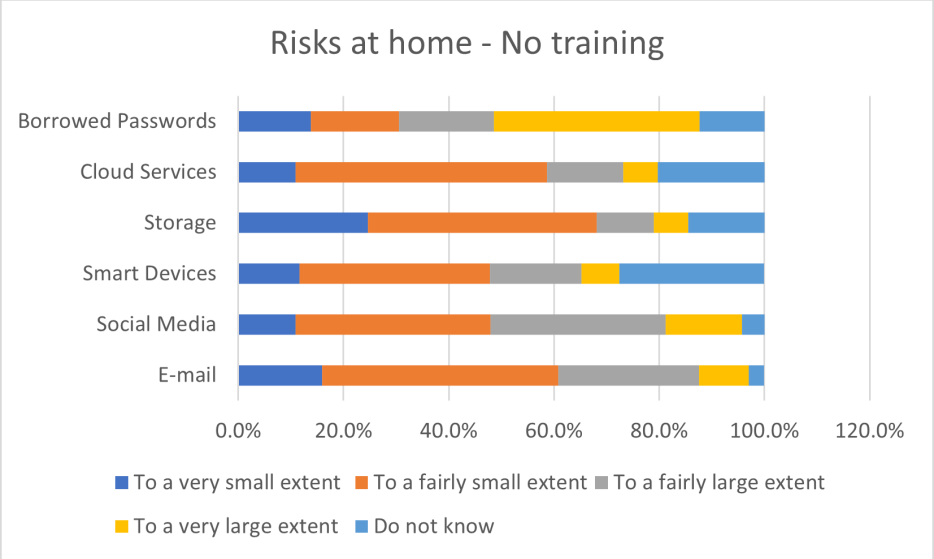


Figure 5.17: Potential risks at home - no training

Threats at work - with training

Over to how threat at work is assessed by health care professionals with training. As seen in figure 5.18 findings here are quite interesting, because there were no answers that “stood out” before the category “fairly large extent”, where we can find “Exploits of situations in society” at 28.5% as the largest threat. Covid-19 was used as an example in this case. It is, however, striking that there are so many who answered “Do not know” in this case. Is it not relevant for them, or do they not have enough knowledge about these threats in order to answer? 44.2% answered that they did not know about spearphishing and 42.1% said the same about supply chain attacks.

Disclaimer! Due to the fact that there were so many "Do not know"-answers to the questionnaire they had to be removed in order to perform a proper analysis. This will be discussed later in chapter 6 Discussion. This goes for all of the four following sections. Unlike the risk section, all the numbers will be presented and the new n-number will be given for each category.

Beginning with to what extent health care professionals with digital security training sees phishing (n=140) as a threat at work. Women answered a mean of 2.44 (std.dev. .925) while men felt an increased threat from it with a mean of 2.62 (std.dev. .925). About vishing (n=196) both women at 1.94 (std.dev. .902) and men at 1.93 (std.dev. .905) pretty much agreed that it was a fairly small threat. The same goes for spearphishing (n=135) where women answered 2.02 (std.dev. 960) perceived the threat a fairly small and men answered 1.91 (std.dev. .963) perceived it as very small.

On the question about ransomware (n=178), women reported a mean of 1.96 (std.dev. .969) and men 2.21 (std.dev. 1.048), placing this threat as very small to fairly small. Blackmail/extortion (n=177) got some of the same results, where women answered 1.96 (std.dev. . 992) and men answered 2.19 (std.dev. . 969) thinks that the threat is fairly small to very small. About exploits (n=177) of weaknesses in software and hardware, women reported a mean of 2.68 (std.dev. .942), which is a bit higher than what the men reported with a mean of 2.54 (std.dev. .977) leaving exploits more of a threat than ransomware and blackmail.
When asked about threats regarding misuse of ID (n=194), women perceived the threat as fairly low at a mean of 2.28 (std.dev. 1.014) and men a little lower at 2.12 (std.dev. .823) but still fairly low. Supply chain attacks (n=140) was almost unanimous reported from of both genders, women reported a mean of 2.31 (std.dev. .919) and men 2.30 (std.dev. .889) of a fairly low threat. A fairly relevant question of whether or not situations in society (n=181), such as Covid-19, could be exploited and seen as a threat, women meant that it could be perceived as a fairly low to fairly high threat with a mean of 2.77 (std.dev. . 867) while men answered a lower mean of 2.25 (std.dev. .840). And lastly, on the question about threats on infrastructure (n=195) women reported a mean of 2.53 (std.dev. 1.049) and men 2.34 (std.dev. .855) making the threat fairly low.

There is a statistical significance regarding gender and society, p=.001. There is a very strong correlation between blackmail at work and ransomware at work (Pearson=.918).

Figure 5.18: Potential threats at work - no training

Figure 5.19: Potential threats at home - no training

Threats at home - with training

When looking at 5.19, there is not many of the categories that is deemed a large threat at home, much like the answers about threats at work. The largest threat is exploits on a “fairly large extent”at 30,6%, followed by compromised ID at “a fairly small extent”. Spearphishing (34.7%), blackmail (33.9%) and ransomware (33.1%) were assessed as the lowest threats at home.
As could be seen in the previous part regarding work, there’s a large percentage that has answered “Do not know” on the questions. At first glance could the answer "spearphishing" be irrelevant at home, but if they use their work mail at home, it could easily become an attack vector as all the other, more relevant attack vectors. Supply chain attack (36.8%) still reigns highest among the “Do not know”, with phishing (35.1%) close behind.

At home, health care professionals with digital security training sees phishing (n=157) as a threat with fairly low impact. Women answered a mean of 2.29(std.dev. 1.011) while men felt an increased threat from it with a mean of 2.37 (std.dev. .883). Vishing (n=210) had women answering a mean of 2.24 (std.dev. 1.041) and men 1.95 (std.dev. .936) disagreeing. with results stretching from a fairly low threat to a very low threat. Both genders agree that spearphishing (n=154) was a very small threat, where women reported a mean of 1.68 (std.dev. .881) and men 1.53 (std.dev. .706).
On the question about ransomware (n=193), women reported a mean of 1.90 (std.dev. .978) and men 1.95 (std.dev. .854), placing this threat as very small. Blackmail/extortion (n=193) got some of the same results, where women (1.88/ std.dev. . 959) and men (1.86/std.dev. . 872) thinks that the threat very small as

well. About exploits (n=196) of weaknesses in software and hardware, women reported a mean of 2.54 (std.dev. .969), which is a bit higher than what the men reported with a mean of 2.64 (std.dev. .977) leaving exploits more of a threat than ransomware and blackmail.
When asked about threats regarding misuse of ID (n=206), women perceived the threat as fairly low at a mean of 2.20 (std.dev. .943) and men a little lower at 1.86 (std.dev. .823) as a very low threat. Supply chain attacks (n=153) had here as well an almost unanimous support from of both genders, women reported a little bit lower with a mean of 2.07 (std.dev. .943) and men 2.08 (std.dev. .841) of a fairly low threat. About the question of whether situations in society (n=195) could be exploited and seen as a threat, women meant that it could be perceived as a fairly low threat with a mean of 2.37 (std.dev. .978) while men answered a that it was a very low threat at 1.81 (std.dev. .773). Finally, on the question about threats on infrastructure (n=191) women reported a mean of 2.35 (std.dev. .970) and men 2.10 (std.dev. .855) making the threat fairly low in their eyes.

There is a statistical significance between gender and society, p=.001, and between gender and ID, p=.033. There were a few more correlations between the answers regarding home. For instance, there was a strong correlation between ransomware and blackmail (Pearson=.934), a moderately strong correlation between ransomware and spearphishing (Pearson=.676) and blackmail and spearphishing (Pearson =.670).
Meanwhile, there were some moderately strong correlations between phishing at work and at home (Pearson=.647).

Threats at work - No training

As with the previous parts of the threat-question, the health care professionals that did not receive training, none of the mentioned threat stood out as a very high threat to the information security in their workplace. As seen in figure 5.20, situations in society had the largest percentage in this case, with 13%. Exploits of software or hardware was perceived as a fairly large threat by 24.6% of the respondents, while situations in society came second on 23.9%. Compromised ID (31.9%) and attacks on infrastructure (27.5%) was seen as a fairly low threat by the respondents. Vishing and blackmail were perceived as a very low threat at work. Again, it is striking how many answered “Do not know” on the different threats listed in the question. On the question about phishing 50.7% answered “do not know”, similary on the question about spearphishing.

Still, all the “Do not know”’s have been removed in order to give a more correct report of the answers about the threats mentioned.

Starting at work, health care professionals with no digital security training sees phishing (n=68) as a fairly low threat. Women answered a mean of 2.30(std.dev.

1.008) while men felt an increased threat from it with a mean of 2.50 (std.dev. .859). About vishing (n=105) women reported a mean of 1.74 (std.dev. .853) and men 1.48 (std.dev. .653) perceived it as a very small threat. The same goes for spearphishing (n=68) where both women with a mean of 1.73 (std.dev. .918) and men at 1.65 (std.dev. .702) perceived the threat as fairly to very small.
On the question about ransomware (n=88), women reported a mean of 1.86 (std.dev. .982) and men 1.96 (std.dev. .878), placing this threat as very small to fairly small. Blackmail/extortion (n=86) got some of the same results, where women answered a mean of 1.88 (std.dev. .984) and men a mean of 1.95 (std.dev. .999) thinks that the threat is fairly small to very small. About exploits of weaknesses in software and hardware (n=93), both women and men agreed that the threat was fairly small. The women reported a mean of 2.45 (std.dev. .961) and the men 2.46 (std.dev. .932), leaving exploits one of the highest threats according to the respondents.
When asked about threats regarding misuse of ID (n=104), women perceived the threat slightly lower than the men at a mean of 2.06 (std.dev. .888) and men a little higher at 2.35 (std.dev. 1.018). The threat from a supply chain attacks (n=72) were fairly low. Women reported a mean of 2.21 (std.dev. .948) and men 2.11 (std.dev. .994). Whether or not situations in society (n=101), such as Covid-19, could be exploited and seen as a threat, women meant that it could be perceived as a fairly low to fairly high threat with a mean of 2.50 (std.dev. .983) while men answered a slightly higher mean of 2.56 (std.dev. .974). And lastly, threats on infrastructure (n=100) was perceived as fairly low. Women reported a mean of 2.27(std.dev. .936) and men 2.35(std.dev. .936).

There are no significance to report. There are, however, some correlations to report. There are moderately strong correlations between spearphishing and ransomware (Pearson=.651), supply chain and ransomware (Pearson=.670) and suppy chain attacks and blackmail (Pearson=.674). There is strong correlation is there between the answers given in regard to ransomware and blackmail (Pearson=.915).

Threats at home - no training

The respondents with no training agreed that exploits might be the biggest threat at home as well as work. In figure 5.21, it can be seen that 13.8% said it could impose a large threat on their own information security. Exploit (26.8%) and situations in society (23.2%) imposes a fairly large threat while misuse of ID at home (34.8%) is a fairly small threat. Supply chain attack was the category most did not know about, with 43.5%. Spearphishing also got a fairly high “do not know” ratio, with 42%.

Also here “Do not know“ removed from the dataset and the remaining num-

Figure 5.20: Potential threats at work - no training

bers analysed to make the answers more correct.

At home, health care professionals with no digital security training sees phishing (n=84) as a fairly low threat. Women answered a mean of 2.17(std.dev. 1.028) while men felt an increased threat from it with a mean of 2.38 (std.dev. .824) at home as well as at work. About vishing (n=113) women reported a mean of 2.11 (std.dev. 1.012) and men 2.11 (std.dev. .763). Women perceived it as a very small threat while men a fairly small threat. For spearphishing (n=80) where both women reported a mean of 1.66 (std.dev. 1.001) and men a mean of 1.59 (std.dev. .796) perceived the threat as fairly to very small.
On the question about ransomware (n=99), women reported a mean of 1.80 (std.dev. 1.037) and men 1.89 (std.dev. .832), placing this threat as very small to fairly small. Blackmail/extortion (n=98) got some of the same results, where women reported a mean of 1.79 (std.dev. 1.034) and men 1.96 (std.dev. .838) thinks that the threat is fairly small to very small where men saw it as an increased threat. About exploits of weaknesses in software and hardware (n=107), both women and men agreed that the threat was fairly small to fairly high. The women reported a mean of 2.53 (std.dev. .993) and the men 2.56 (std.dev. .934), leaving exploits one of the highest threats according to the respondents at home as well.
The knowledge about ID and threats regarding misuse of ID (n=111) is higher than the other categories. Women perceived the threat lower than the men at a mean of 2.25 (std.dev. .956) and men a little higher at 2.47 (std.dev. .956). On the other hand, threat from a supply chain attacks (n=78) were fairly low. Women reported a mean of 2.05 (std.dev. 1.042) and men 2.33 (std.dev. .913). Whether or not situations in society (n=105), such as Covid-19, could be exploited and

seen as a threat at home, women meant that it could be perceived as a fairly low threat with a mean of 2.23 (std.dev. .997) while men answered slightly lower 2.15 (std.dev. .974). And lastly, threats regarding infrastructure (n=103) were perceived as fairly low. Women reported a mean of 2.16(std.dev. .980) and men slightly higher at 2.31 (std.dev. .967).

There is some significance between gender and vishing, p=.063, but it is not low enough to report as a statistical significance. There were some correlations at home as well. It was a moderately strong correlation between blackmail and ransomware (Pearson=.704), spearphishing and ransomware (Pearson=.739) and lastly, a strong correlation between blackmail and ransomware (Pearson=.976)
There were some correlations between work and private as well. There is moderately strong correlation between spearphishing at work and at home (Pearson=.691), between spearphishing at work and supply chain attacks at home (Pearson=.629) and between blackmail at work and supply chain attacks at home (Pearson=.611).

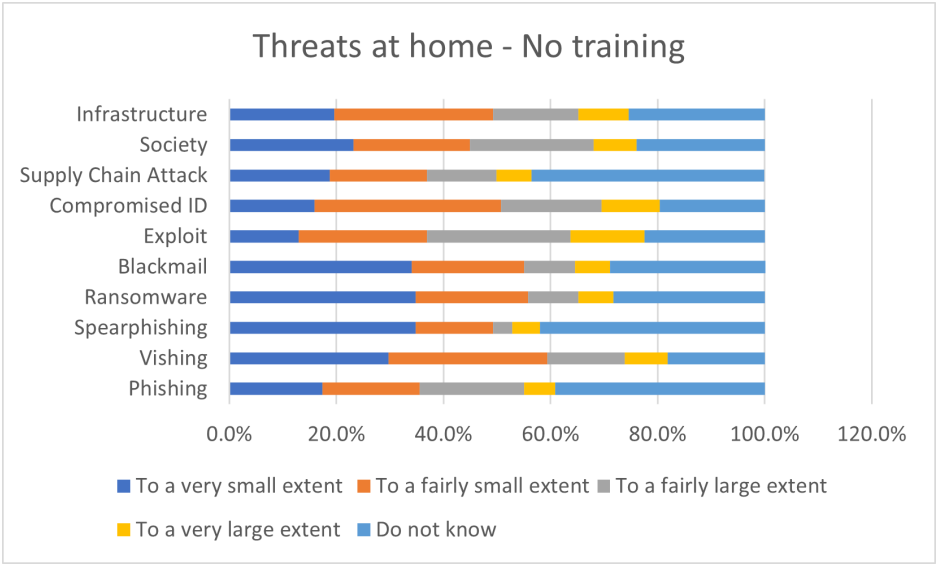


Figure 5.21: Potential threats at home - no training

5.3 Views on management and control in the workplace

How management relays information is an important aspect in how the employees learn and understand the importance of the information. If you fail to meet the employees where they are, the information you give seem less important and they will not learn. If the message is clear and relevant, there is a much higher chance

that the information will stick and mature. The background for this question was that if the health care professionals felt they had control over what guidelines and policies that they were expected to follow, or if they felt that they were missing some of it.

5.3.1 Overview - With training

On the question about whether or not the health care professional with training had sufficient overview over rules and guidelines in their workplace, 29.8% said that they had it to a very large extent, while 57% said they had to a fairly large extent. They also said that the guidelines that management had implemented were to a fairly low hindrance (46.7%) and a very low hindrance (43%). The focus on information security had not particularly changed the way they worked, they reported that 44.6% had a fairly small change and 20.2% had a very small change. 31% felt that they know to a small extent the procedure if they suspected a digital security incident, and the same amount knew the same procedures to a fairly large extent. 38.8% meant that the guidelines provided were presented clearly to them, while 42.1% felt that the management had set requirements to them in a fairly large extent. And 70.7% knew the consequences for breach of confidentiality to a large extent.
Women reported higher than the men regarding overview over guidelines, with a mean of 3.21 (std.dev. .680) versus 2.95(std.dev. .608), meaning the women had more overview than the men. Meanwhile, men reported higher than women when it came to the question if the guidelines was any hindrance, with a mean of 1.98 (std.dev. .821) versus 1.68 (std.dev. .840), making them more affected by the guidelines than the women. Women also reported a higher mean 2.30 (std.dev. .981) than the men 2.16(std.dev. 834) on how the focus on information security changed their way of working, making the women more affected. Men reported lower on the question regarding if they knew the correct procedures if suspecting a digital security incident with a mean of 2.23 (std.dev. .937) versus the women's mean of 2.55 (std.dev. 1.138). On the question regarding if the employer had presented the guidelines clearly, women, who reported a mean of 3.03 (std.dev. .958) meant that they had a better presentation of the guidelines than the men, who reported 2.84 (std.dev. .939). Women also meant that the management sets certain requirements to them regarding information security, with a mean of 3.28 (std.dev. .848) versus men with a mean of 2.91 (std.dev. .960). And finally, women, with a mean of 3.67 (std.dev. .628) knew better the consequences of a breach of confidentiality than the men 3.48 (std.dev. .628).
There were several aspects of statistical significance in this section. There is a significance regarding gender and how the overview over guidelines with a p-score p=0.21. There was also a significance regarding gender and if the guidelines created a hindrance in the workplace, p=0.35. Lastly, there is a significance between gender and the managerial requirements, p=0.12.
There is a moderate correlation between guidelines and requirements (Pearson

=-615).

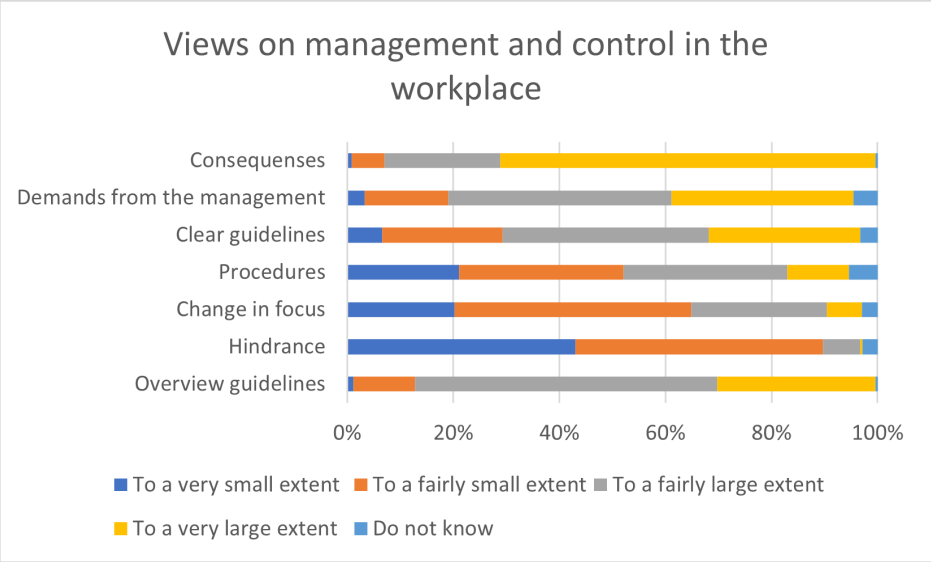


Figure 5.22: Views on management and control in the workplace - with training

5.3.2 Knowingly broken protocol - with training

When asked about if the respondents with training knowingly had broken protocols given to them by their employer, as can be seen in figure 5.23, 9.5% said yes, 84.3% said no and 6.2% did not know if they had broken any protocols or it was not relevant to them.
Women reported a higher mean than the men did, 2.01 (std.dev. .363) versus 1.77 (std.dev. .476). One-Way ANOVA reports a significance between the genders and the broken protocols, p=.000. No correlations to report.

5.3.3 Overview - no training

Furthermore, in figure 5.24, the question about whether or not the health care professional with no training had sufficient overview over rules and guidelines in their workplace, 42.8% said that they had it to a fairly large extent, while 30.4% said they had to fairly small extent. They also said that the guidelines that the management had implemented were to a fairly low hindrance (37.0%) and a very low hindrance (41.3%). On the question about whether information security had not particularly changed the way they worked, they reported that 51.4% had a fairly small change and 22.5% had a very small change. 39.1% felt to a small extent that they know the procedure if they suspected a digital security incident, and the same amount knew the same procedures to a fairly large extent. 23.2% meant

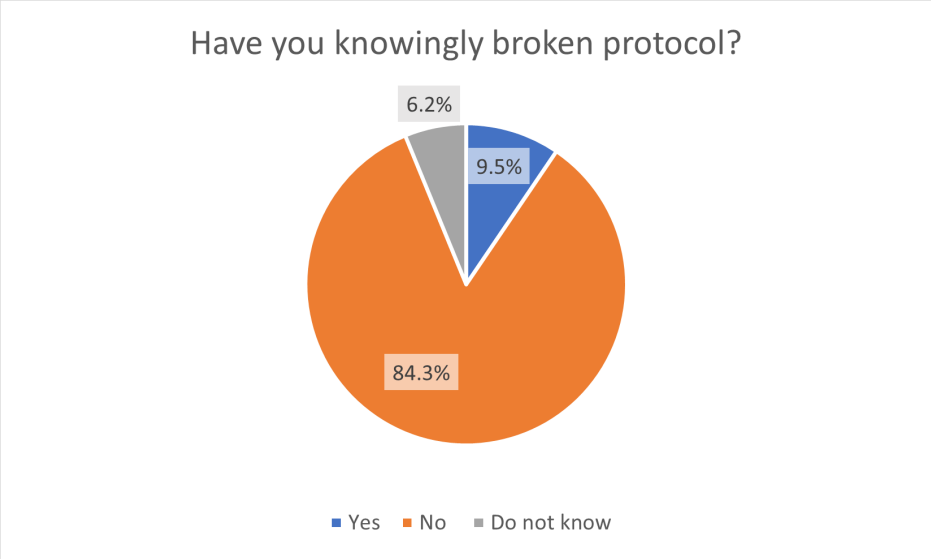


Figure 5.23: Knowingly broken protocol - with training

that the guidelines provided were presented fairly clearly to them, however, a larger amount meant that they had been presented in a fairly smaller extent, 32.2%. Meanwhile 35.5% felt that the management had set requirements to them in a fairly large extent. And 68.1% knew the consequences for breach of confidentiality to a large extent.

Women and men agreed regarding overview over guidelines, with a mean of 2.55 (std.dev. .990) versus 2.57 (std.dev. .728), reporting that they felt they had a fairly low overview over the guidelines. Meanwhile, men reported lower than women when it came to the question if the guidelines were any hindrance, with a mean of 1.90 (std.dev. 1.094) versus 2.17 (std.dev. 1.411), making the men less affected by the guidelines than the women. Women and men agreed on the change in focus the guidelines had entailed, where the women reported a mean of 2.25 (std.dev. 1.128) and the men 2.23 (std.dev. 1.135) on how the focus on information security changed their way of working.
Again, women and men agreed on the question if they knew the correct procedures if suspecting a digital security incident, with the men ahead a little bit with a mean of 1.87 (std.dev. .937) versus the women's mean of 1.84 (std.dev. 1.034). It is still a very low score, meaning the respondents has very little knowledge on those kinds of procedures. On the question regarding if the employer had presented the guidelines clearly, women reported a mean of 2.53 (std.dev. 1.315) meant that they had a better presentation of the guidelines than the men that reported a mean of 2.23 (std.dev. 1.194). The numbers suggest that they get the guidelines presented to them in a fairly clear manner. Women also meant that the management sets certain requirements to them regarding information

security in a larger degree than the men, with a mean of 2.67 (std.dev. 1.085) versus men with a mean of 2.23 (std.dev. 1.085). Lastly, men reported a mean of 3.67 (std.dev. .758), knew better the consequences of a breach of confidentiality than the women which reported a mean of 3.54 (std.dev. .756) in the same group.

There was no significance to report. There was a moderately low correlation between guidelines and requirements among the respondents with no training (Pearson=.473). The same tendencies could be seen among those with training as well.

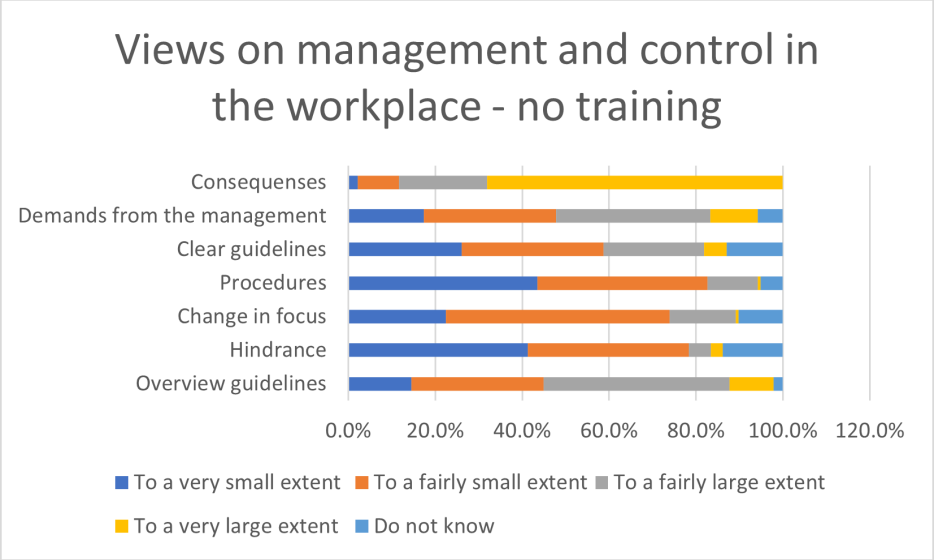


Figure 5.24: Views on management and control in the workplace - no training

5.3.4 Knowingly broken protocol - no training

When asked about if the respondents with no training knowingly had broken protocols given to them by their employer, as can be seen in figure 5.25, 6.5% said yes, 84.1% said no and 9.4% did not know if they had broken any protocols or it was not relevant to them.
Women reported a lower mean than the men did, 2.00 (std.dev. .362) versus 2.13 (std.dev. .507), which could mean that the men have lesser knowledge about whether they had broken policies. One-Way ANOVA reports no significance between the genders and the broken protocols, p=.106. No correlations to report here either.

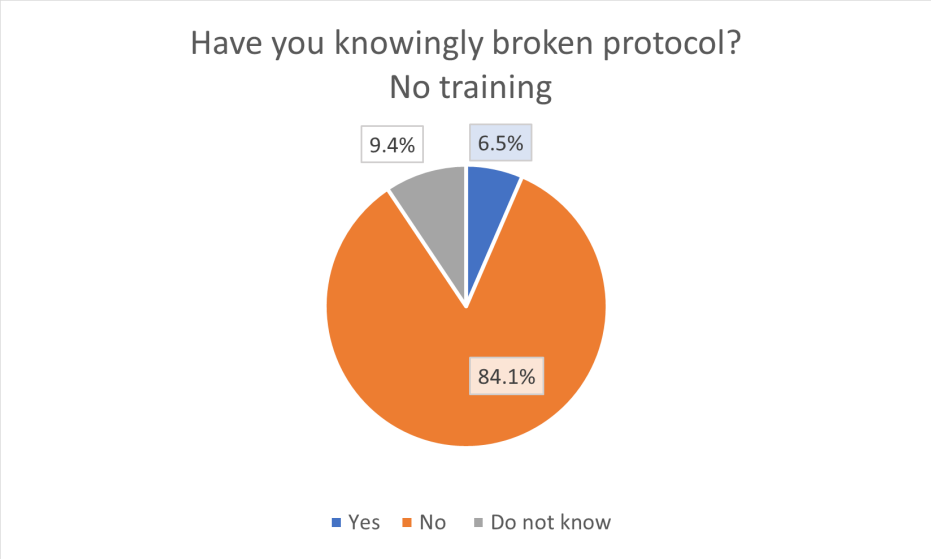


Figure 5.25: Knowingly broken protocol - no training

5.3.5 What affects the work

This question was left as an open answer, allowing the participants to write in their own words how the policies have affected their work.

With training

These are some of the comments from health care professionals with training.

- Automatic logged out of the system after X minutes.
- Lack of right of access stops us from building more experience, it lowers the patient safety.
- Not enough computers to do record keeping, too little time to do it.
- GDPR.
- Takes too long to log on to the system and change user. It is not always done in an emergency.
- Information regarding patient without relatives gaining insight in what you are doing.
- Difficult gaining access to external systems.
- The use of sound recordings.
- Outdated procedures gives outdated guidelines.
- Segmentation of the system (secure vs. unsecured) stops information flow (necessarily), but takes time to log on the different systems.
- Certain websites have been restricted.
- Slow system.
- Complicated systems that are not self-explanatory.

- No access to remote desktop.
- The storing of details from professionals matters.
- Restricted access to work e-mail and calendar at home. Missing crucial information because of it.
- Missing access on leader level. Have to ask about it, while it should be automatic.
- Not able to read e-mail outside work, have to use smart devices to gain access.
- Too many unrealistic scenarios presented versus the actual risk we are facing.
- Scanning of documents.
- The systems lack the ability to transfer personal data, especially when you can't use e-mail.

No training

- Limits the use of tools that would enhance my work.
- Logging on and off takes too long, especially in an emergency.
- Time consumption and extra work when documenting.
- Not allowed to read patient record before they move into the facility, we are not prepared well enough.
- Storing of pictures of wounds etc. on work phone. It threatens the patient security.
- Information does not share between programs, have to document double.
- No access to external websites.
- No storage of passwords.
- System do not allow cloud services, makes projects and educating difficult.

5.4 Behaviour

All of mankind have some sort of behaviour in a given context. Health care professionals as well. This question contains a list of things that checks how the respondents would react in a certain situation, to make the respondent think about their behaviour. The question focuses on the two groups at work and at home, to easier see where they think they have to control their own behaviour.

5.4.1 Online behaviour - with training

At work, most have some sort of guidelines to follow in regard to how they should behave when using technology and firewall to prevent incidents. Most do not have these restrictions at home, but they might be transferable from work. Health care professionals that have been through training, giving them some advantage on how to behave when using technology at work, but will the same training give them the same advantage at home?

At work

As can be seen in figure 5.27, 40.9% of the respondents with training usually check the website they are visiting at work, 43.5% always checks links and attachments in e-mails before opening them, and 48.3% always checks who the e-mail was sent from. 57.3% logs off or locks their device/ID before leaving, and the same amount (57.3%) has never used a personal device at work. 31.9% has never reported a suspicious e-mail.

On the question if the respondents check the legitimacy of a website before using it, women answered with a mean of 2.43 (std.dev. 1.014) while men answered a bit lower with 2.80 (std.dev. 1.069), meaning that women more often checked the website. Men also were a bit lower than the women on whether they checked links and attachments in e-mails before opening them, with a mean of 1.98 (std.dev. 1.023) versus the women who answered 1.88 (std.dev. .935).
When asking about if the respondents checked if the sender of the e-mail was legit, women reported a mean of 1.79 (std.dev. .926) answered a little lower than the men with a mean of 1.98 (std.dev. 1.067), that they were more likely to check it when receiving the e-mail. Women reported a mean of 1.48 (std.dev. .602) were also more likely to log off or lock their computer over men with a mean of 1.70 (std.dev. .904), but not by much. However, men, who reported a mean of 3.18 (std.dev. .995), was more likely to use private devices at work than women with a mean of 3.45 (std.dev. .815) and women, who reported a mean of 2.70 (std.dev. 1.317), reported more often suspicious e-mail than men who reported a mean of 2.77 (std.dev. 1.292).

There is a statistical significance between gender and checking the legitimacy of a website, p=0.35. There is also a statistical significance between gender and logging out/locking the device/ID. There is a moderate correlation between checking links and attachments and the sender at work (Pearson=.580).

At home

Figure 5.27, we can see that the results from the respondents with training that 43% usually checks websites before using them, while 52.5% always checks links and attachments in e-mails before clicking them. This is higher than they reported at work. 47.5% always checks the sender in an e-mail at home, and 31.4% sometimes logs off or locks their devices/ID at home. 53.3% has never used work devices at home, while 28.1% always report suspicious e-mails at home.

In regard to the question if the respondents check if a website is legit or not before using it, women answered with a mean of 2.17 (std.dev. .949) while men answered a bit lower with 2.36 (std.dev. .917), meaning that women more often checked the legitimacy of the website. Men also were a bit lower than the wo-

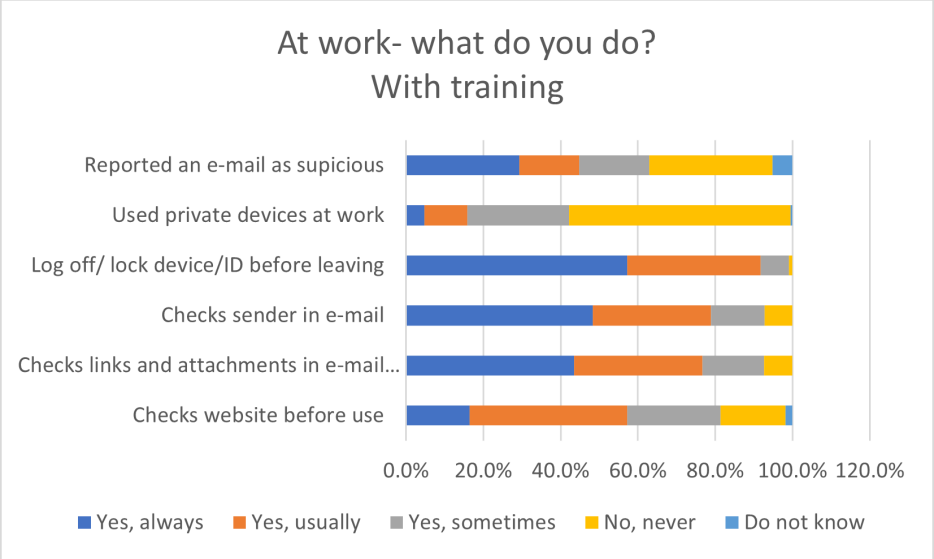


Figure 5.26: Behaviour at work - with training

men on whether they checked links and attachments in e-mails before opening them, with a mean of 1.82 (std.dev. .922) versus the women who answered 1.82 (std.dev. .771).
On the question about whether the respondents checked if the sender of the e-mail was legit, women reported a mean of 1.69 (std.dev. .827), answered a little lower than the men, who reported a mean of 1.95 (std.dev. .939), that they were more likely to check it when receiving the e-mail. Women, who reported a mean of 2.45 (std.dev. 1.059), were also more likely to log off or lock their computer over men, who reported a mean of 2.61 (std.dev. 1.083). Both genders answered "usually" to "sometimes". However, men, with a mean of 3.02 (std.dev. 1.067), was more likely to use work devices at home than women, who reported a mean of 3.38 (std.dev. .839). Meanwhile, women, who reported a mean of 2.40 (std.dev. 1.134) reported more often suspicious e-mail than men, with a mean of 2.45 (std.dev. 1.131).

There is a statistical significance regarding gender and whether they used private devices at work. There is also a moderately strong correlation between checking the sender of an e-mail and checking links at home (Pearson=.737). Furthermore, there is also a moderately strong correlation between checking the sender of an e-mail at work versus at home (Pearson=.743).

5.4.2 Online behaviour - no training

Having training could be an advantage at work, but still, common sense regarding patient security and privacy applies whether or not one has had any training.

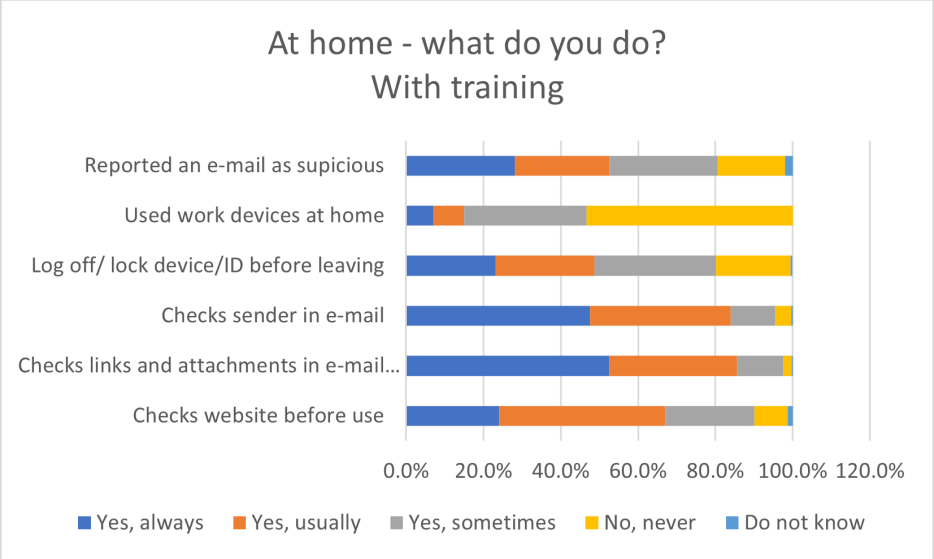


Figure 5.27: Behaviour at home - with training

At work

According to figure 5.28, 31.9% usually checks websites before visiting them at work, while 36.2% checks links and attachments in private e-mails. 45.5% always checks who has sent the e-mail and 55.1% locks or logs off their device/ID when leaving it. 62.3% has never used personal devices at work and 41.3% has never reported a suspicious e-mail.
About the question on whether the respondents check if a website is legit or not before using it, women answered with a mean of 2.36 (std.dev. 1.124) while men answered a bit lower with 2.67 (std.dev. 1.028), meaning that women more often checked the legitimacy of the website. Women and men agreed on the importance of checking links and attachments in an e-mail before clicking them, women with a mean of 2.12 (std.dev. 1.100) versus the men who answered 2.13 (std.dev. 1.150). Furthermore, on the question about whether the respondents checked if the sender of the e-mail was legit or not, women, who reported a mean of 1.91 (std.dev. .991) agreed with the men, who reported a mean of 1.90 (std.dev. 1.094), that they usually checked the sender. Women, with a mean of 1.61 (std.dev. .759) were also more likely to log off or lock their computer over men, with a mean of 1.67 (std.dev. 1.028), but not by much and both genders answered “usually” to “always”. In this case, women, who reported a mean of 3.38 (std.dev. .924) is more likely to use work devices at home than men, with a mean of 3.57 (std.dev. .858). Women, who reported a mean of 2.93 (std.dev. 1.134) reported more often suspicious e-mail than men, who reported a mean of 3.13 (std.dev. 1.445), they usually reports e-mails while men reports them sometimes.

There is a moderate correlation between sender and checking links at work

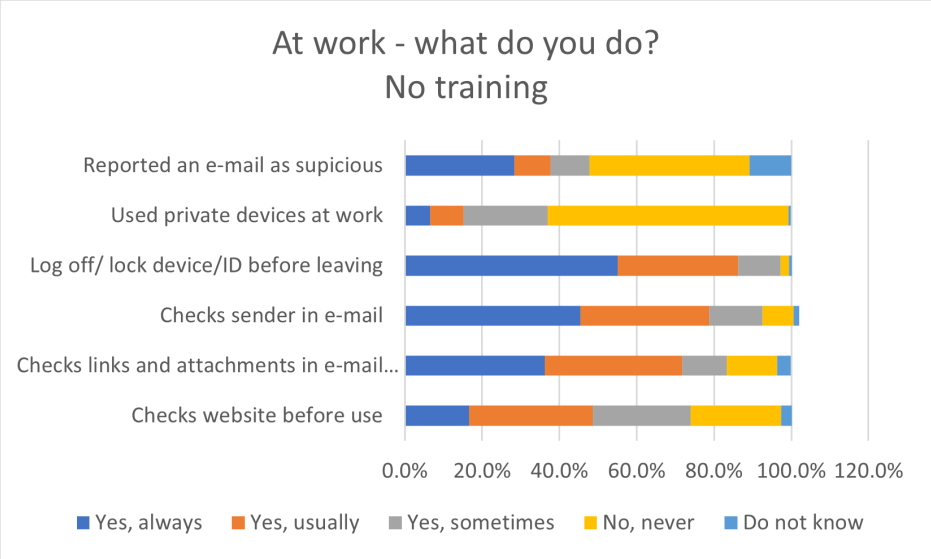


Figure 5.28: Behaviour at work - no training

(Pearson=.601).

At home

As can be seen in figure 5.29, 37.7% of the respondents that did not have training usually checks the website before they visit it. 52.5% always checks links and attachments before clicking and the same amount usually checks the sender in e-mails at home, which is much higher than at work. 31.9% the respondents sometimes log off/lock their devices/ID before leaving, while 66.67% has never used a work device at home. 33.3% always report suspicious e-mails.

On the question if the respondents check whether a website is legit or not before using it, women answered with a mean of 2.30 (std.dev. 1.016) while men answered a bit higher with 2.23 (std.dev. .858), meaning that men more often checked the legitimacy of the website than the women. Women and men agreed on checking links and attachments in an e-mail before clicking them, women with a mean of 1.67 (std.dev. .837) versus the men who answered 1.69 (std.dev. .922). When asking about whether the respondents checked if the sender of the e-mail was legit or not, women answered 1.68 (std.dev. .991) answered a little lower than the men who answered 1.77 (std.dev. 1.094), meaning that the women usually check the sender more often. Women who reported a mean of 2.50 (std.dev. 1.115) agreed with the men who answered 2.53 (std.dev. 1.008), that they "usually" log off or locks their devices at home. In this case, men answered 3.50 (std.dev. .777) that they are more likely to use work devices at home than women who answered 3.60 (std.dev. .770). Women, with a mean of 2.50 (std.dev.

1.384), reported more often suspicious e-mail than men did, with a mean of 2.83 (std.dev. 1.392), as women usually report e-mails while men reports them sometimes.

There is a moderate correlation between checking links and attachments and checking a website at home (Pearson=.594), as well as a moderately strong correlation between checking links and attachments and the sender of an e-mail at home (Pearson=.650).
Regarding correlations between work and home, there is a moderate correlation between checking the sender of an e-mail at work and at home (Pearson=.608).

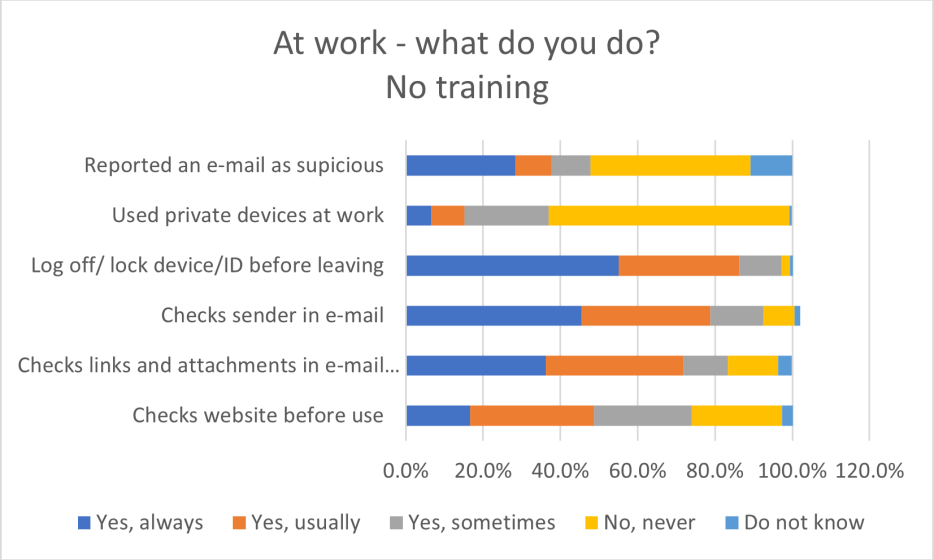


Figure 5.29: Behaviour at home - no training

5.4.3 Risk-posing actions

The list of risk-posing actions is not complementary, but it is something that a health care professional might have experienced on a day to day basis. This is more of a dilemma scenario, where the respondent discloses whether they have taken a “short-cut” to get the job done, unknowingly or not.

With training

Among the health care professionals with training 32.2% said that they had used the same passwords at work and at home. 8.7% said that they had sent patient data though e-mail, 1.2% had copied patient data unto a non-encrypted device and 1.7% had written details about work on their social media.

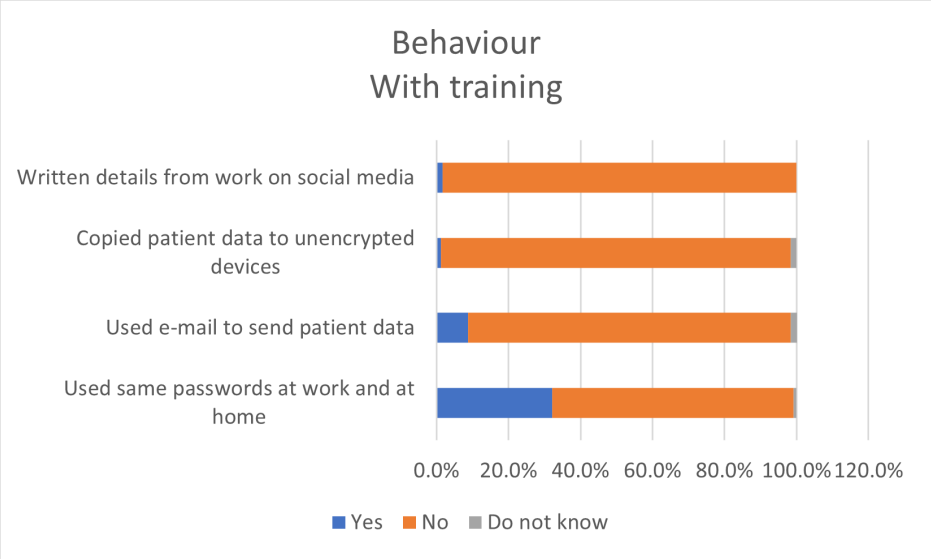


Figure 5.30: Risk-posing actions - with training

On the question of whether the health care professionals had used the same password at work and at home, women reported a mean of 1.66 (std.dev. .485) while the men reported 1.80 (std.dev. .462), meaning men more often than women did not reuse passwords. When asked if the respondent had used e-mail for sending patient data internally or externally, women reported a mean of 1.93 (std.dev. .483) while the men reported 1.91 (std.dev. .320), making them almost equally unlikely to send such information through e-mail. Women had almost never copied data to a non-encrypted device, with a mean of 2.02 (std.dev. .159) while men had done it to a small degree, with a mean of 1.95 (std.dev. .211). On the question about writing details on social media, all the men answered "No". With a mean of 2.00 (std.dev. .000) it could not have been a clearer answer. This makes the few that answered "yes" on this question women, with a mean of 1.98 (std.dev. .141).

There were statistical significance between genders and copy patient data, p= 0.033. No correlations to report.

No training

Among the health care professionals with no training, 40.6% had used the same password at work and at home, while 9.4% had send patient information through e-mail. 0.7% had used a non-encrypted device to copy patient data and 0.7% did not know if they had posted details from work on social media.

About the question on whether the health care professionals with no training

had used the same password at work and at home, women reported a mean of 1.58 (std.dev. .495) while the men reported 1.63 (std.dev. .490), meaning men more often than women did not reuse passwords. When asked if the respondent had used e-mail for sending patient data internally or externally, women reported a mean of 1.91 (std.dev. .493) while the men reported 1.93 (std.dev. .320), making them almost equally unlikely to send such information through e-mail. Women had almost never copied data to a non-encrypted device or did not know if they had, with a mean of 2.04 (std.dev. .190) while men had done it to a small degree with a mean of 2.00 (std.dev. .263). Again, on the question about writing details on social media, all men answered "No"! With a mean of 2.00 (std.dev. .000) it could not have been a clearer answer. This makes the few that answered "Do not know" on this question women, with a mean of 2.01 (std.dev. .096).

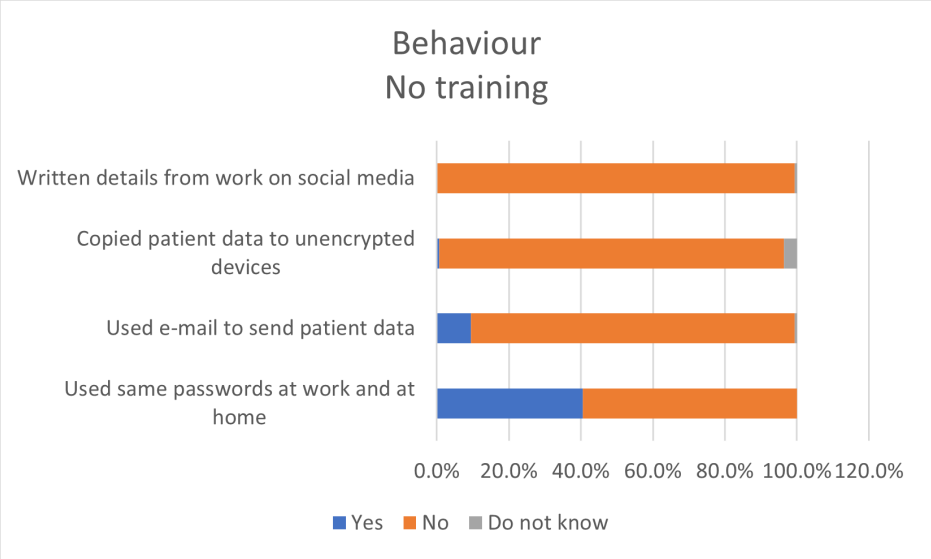


Figure 5.31: Risk-posing actions - no training

5.5 Knowledge and motivation

How information is presented is key for capturing the audience and relaying the information in a way that sticks. It is important to meet the audience where they are, and not make them come to you. In this section, the health care professionals were asked how they had learned about information security and how they would prefer to have the information presented to them. They were also asked about what they wanted to learn more about, apart from the generalized courses provided.

5.5.1 Training

With this question being a multiple-choice question, the analysis will be different. The question that was asked the respondents was "Where have you learned about information security?". The idea behind this question was to enlighten where a possible focus area could be.

With training

As can be seen in figure 5.32, the respondents were given four common ways to increase knowledge used by both employer and employee which they could choose one or all four alternatives. The original size of the population which had received training were n=242. 85 respondents answered that they had gained knowledge by self-study, 149 by internal courses, 25 by external courses and 161 by having information given to them by their employer. All in all, health care professionals answered 420 times on those categories.

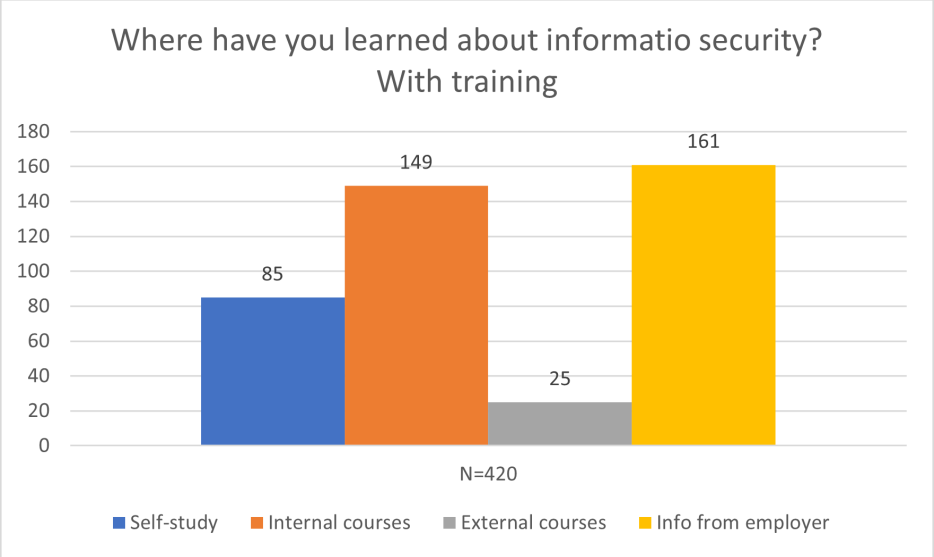


Figure 5.32: Learned about information security - with training

No training

The health care professionals that did not receive training was asked the same question as the ones that had received training. In figure 5.33 it can be seen that 87 respondents had gained knowledge by self-study, 14 from internal courses, 8 from external courses and 63 by their employer. The original population of health care professionals that did not have training was n=138 and they answered 172 times on this question.

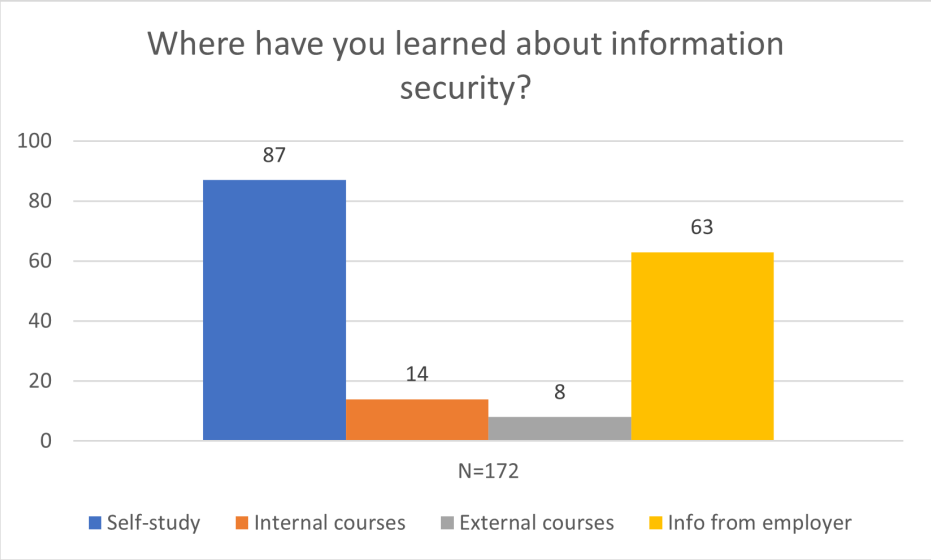


Figure 5.33: Learned about information security - no training

5.5.2 Training offered

This question asked the health care professionals if they had been offered a digital information security course the last two years. The security experts said that they were aiming to have their employees retake and refresh the course every year, which seems like a good plan. However, it seems that is not the case among many of the institutions that participated in this questionnaire.

With training

In figure 5.34, it can be seen that on this question the respondents answered that 55.8% of them had been offered training and participated, while 3.3% had been offered but had not participated. 35.1% had not been offered training and 5,8% did not know or it was not relevant for them.

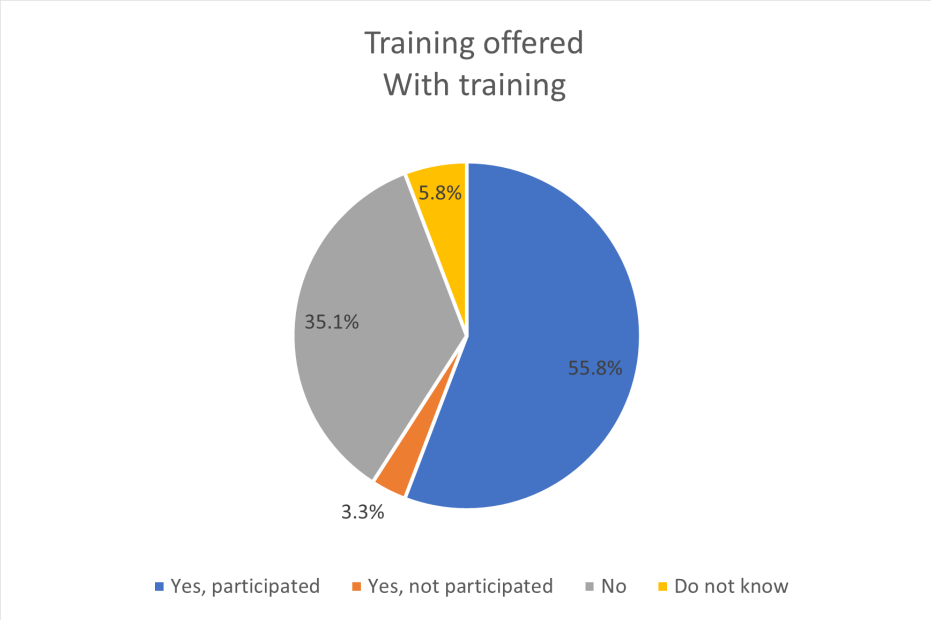


Figure 5.34: Offered training - with training

No training

As can be seen in figure 5.35, the respondents that haven't receive training, 5,1% answered that they had been offered and participated in a digital security course[3]. 3,6% said that they had been offered training but not participated, while 89.9% said they had not been offered training. 9,4% did not know if they had been offered training or not, or it was not relevant for them.

5.5.3 Tools to raise awareness

Courses and training in topic that is not fully customized to the work situation and field of interest could be seen as a chore and become something that "just needs to be done" in the eyes of some. The background for this question is to see what the health care professionals thinks might motivate their learning.

With training

In figure 5.36, the respondents have answered that customized e-learning courses could be the tool that motivates learning about information security the most, with 187 responses. In second place coursing with experts, or "fagdager", with 108 responses. Next, customized physical courses came at third place with 72 responses.

[3]More about that in 8.1 Limitations

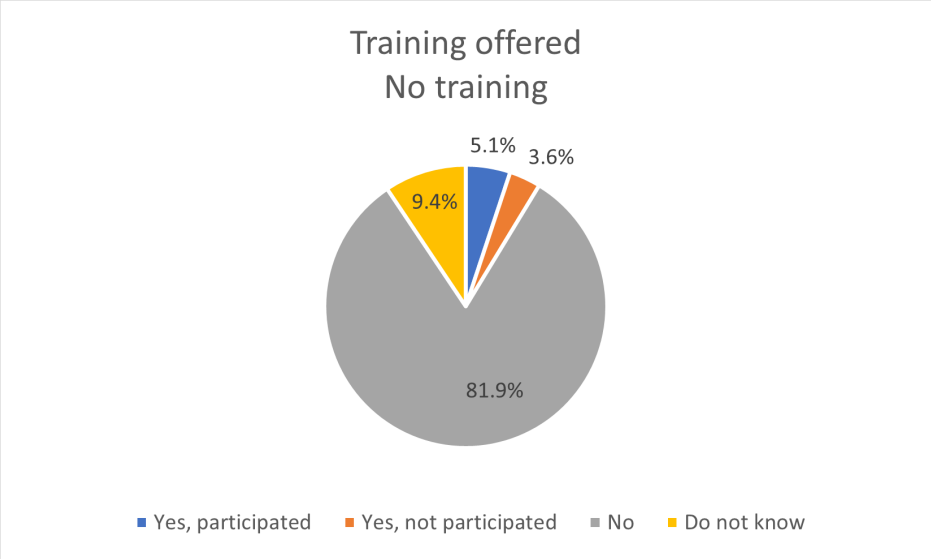


Figure 5.35: Offered training - no training

Films about the subject had 70 responses, while gamification had 39 responses. It was a total of 473 responses from the health care professionals with training.

No training

In figure 5.37, the respondents with no training answered very much the same as the respondents with training. Customized e-learning courses came first with 75 responses, while coursing with experts came at a close second with 68 responses. Customized physical courses came third here as well, with 55 responses, and film had 24 responses. Gamification was rated last in this group as well, with 6 responses. In total, there was 228 responses from health care professionals with no training.

5.5.4 Want to learn more about

The background for this question was to map fields of interest and what the health care professionals wanted to learn more about. I did get some feedback on not making this question mandatory because some did not want to learn more about the things listed in the question and felt that they had to answer something[4].

[4]More about that in chapter 8.1Limitations

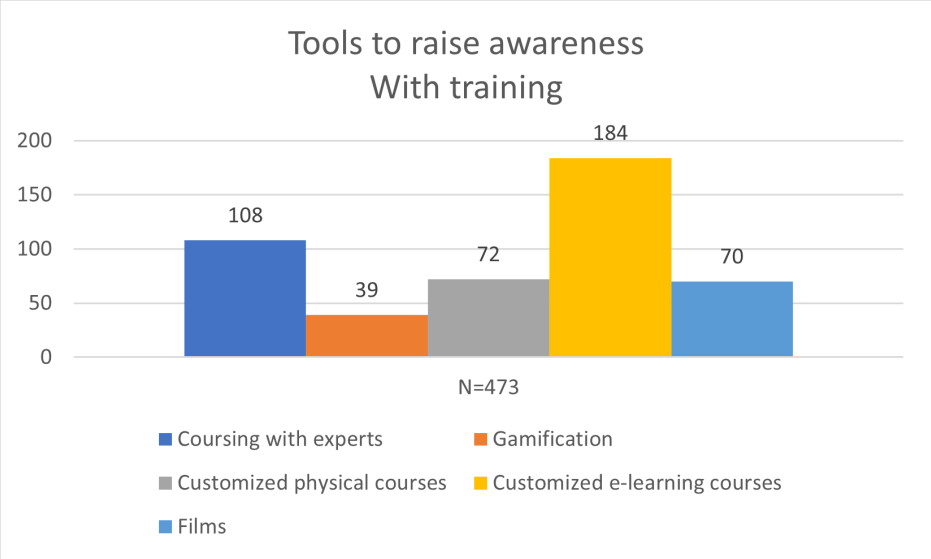


Figure 5.36: Tools to raise awareness- with training

With training

In figure 5.38, it can be seen that health care professionals want to learn more about information security at work (147), and more about information security at home (117). Furthermore, they want to learn more about how to report an information security incident (111), about cloud services (96), secure use of e-mail and lastly what courses that are available. One alternative was not answered by anyone in the group, and that was to learn more about how to treat patient information more more securely. There was 629 responses in total.

No training

Health care professionals with no training, had other priorities regarding what they wanted to learn more about. In figure 5.39, it can be seen that they want to know more about information security at work (96), then they wanted to know more about information security at home (63). In third came how to securely treat patient data (61). How to report information security (59) and information about available courses (59) had the same number of responses, while cloud services (53) and secure use of e-mail (47) came last. There were 438 responses in total.

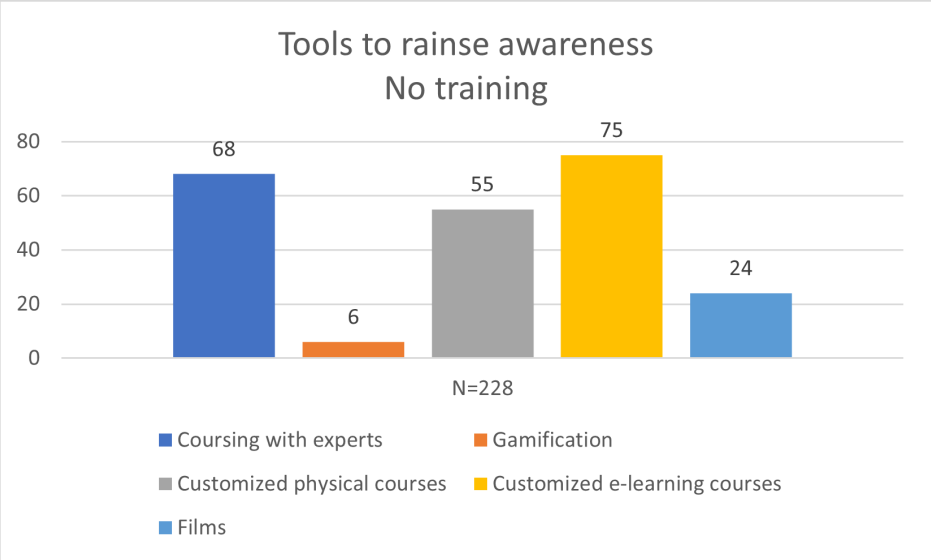


Figure 5.37: Tools to raise awareness - no training

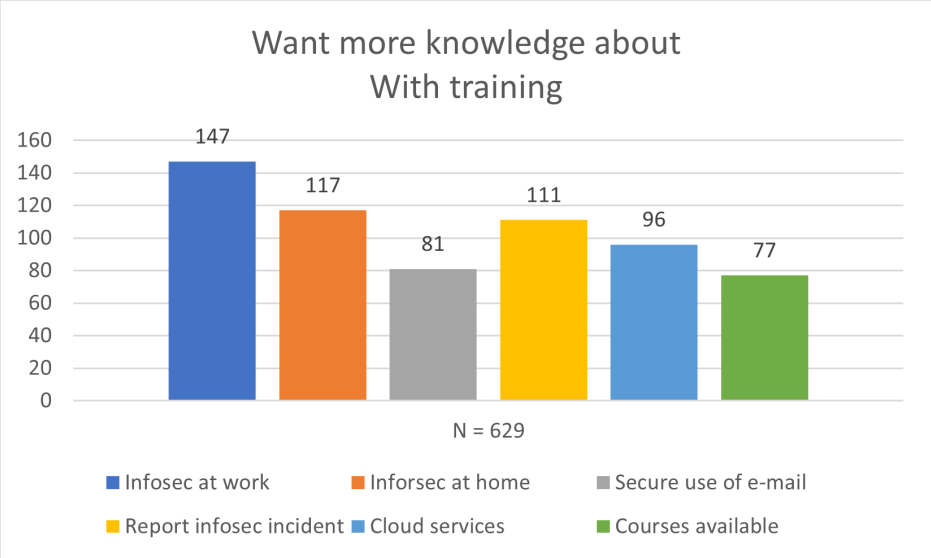


Figure 5.38: Want more knowledge about - with training

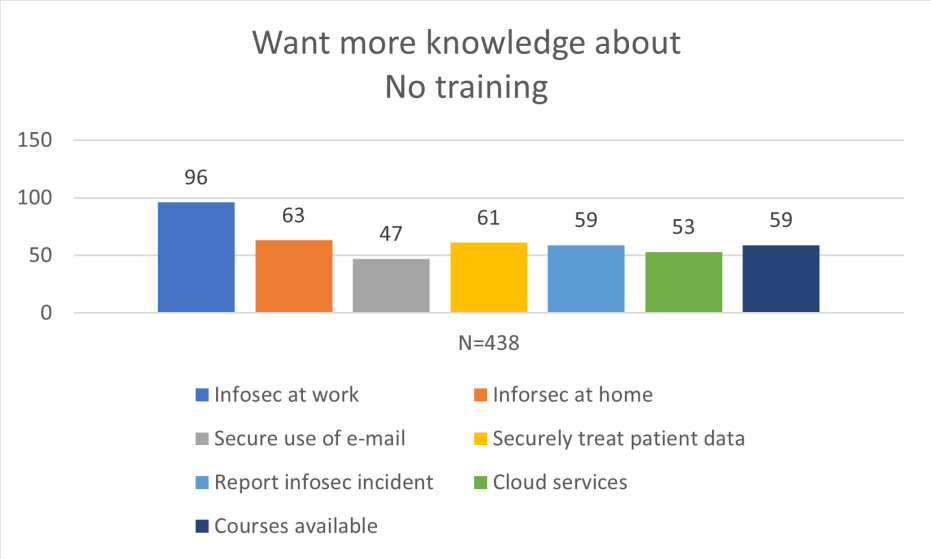


Figure 5.39: Want more knowledge about - no training

Chapter 6

Discussion

This chapter will be a discussion about the research questions and connecting the results found in chapter 5 Results to them. The research questions answered in this section is about the security threats the health care sector faces today, how the security training affects the health care personnel's everyday work, and if the training has had any effect at home.

6.1 Research Question 1 - What are the cyber security risks we are facing today in health care?

The first research question presented is a mix between nice discussions with security experts during the interviews and a literature review. However, there was a peculiar finding in some of the answers of the questionnaire which is best discussed in this section.

In the interviews conducted, the security experts had the same idea about which threats the health care sector is facing today, it pertains to the people using the systems. Tommy Kinnunen, CISO at Nord-Trøndelag Hospital Trust, felt that one of the biggest threats the sector faces today is wrong use of equipment and solutions. For instance, the increased use of home office during Covid-19 has removed the normally safe environment the employees are used to, which makes the employees more vulnerable. This, and that there are many different technological solutions available through the internet (shadow IT). These solutions enhance the challenge of controlling use and use within acceptable practice.
The other expert expressed a missing security culture among the employees that was the biggest threat. There is a lack of understanding about the threats the health care sector faces today and that this understanding is not deeply rooted in the everyday work. Health care personnel have absolute focus on patient safety, as it should be, but it leaves the information security focus behind. The expert thinks that much of the attitude shown towards information security has to do with the level of trust Norwegians have to each other and the state.

Both of the experts agree on that there absolutely is an external threat out there. Tommy Kinnunen mentions that e-mail clearly is an preferred attack vector for the attackers. E-mails containing malware or malicious links to malware is a challenge, because the attacker have developed their attacks and they are now very sophisticated and difficult to uncover.

In the questionnaire there were two questions that brought up common, specific named threats for the health care personnel to answer to what extent they considered them a threat, either at work or at home. In figure 5.18, the result from health care personnel with training can be seen. There is up to 44.2% that did not know whether or not spearphishing was a threat or not, and almost the same number of respondents answered the same about phishing. These named threats have been "buzz words" used by media and other security experts for years and should be known for a large part of the Norwegian population. Do they feel that it is not relevant for them and their work? As can be seen in figure 5.19 the percentage for "Do not know" is similar for the answers they gave about threats at home but a bit lower than the answers regarding work. It is the same type of result from the health care professionals that have not gone through training. Both figures 5.20 and figure 5.21 shows that the "Do not know" percentage of answers were quite high, as could be seen in the previous figures. These findings raise several different questions. Do these answers represent a lack of knowledge or have the question missed its purpose? Are these types of threats not relevant for the health care sector, or do they not know how it could affect them?
By looking at other answers, discussed later in sections 6.2 and 6.3 regarding the other research questions a clearer picture could form.

NorSIS' report from 2020 [26] has brought up a discussion about security culture among the Norwegian people in general. The findings in my thesis reflects the status of the general population's security culture. There is this general notion that since Norway is a small and imperceptible country in many ways, there is small chances of an attack in any form. This attitude towards the known threats out there could work as a threat in itself. When it comes to personal health data and patient information, they could be used for many things, for instance extortion or blackmail. There have been cases recently (also in Norway, Østre Toten municipality) where the hackers sold the information they gathered from breaches in health care systems on the dark web.

In addition to the previous report mentioned, the Norwegian Business and Industry Security Council (NSR) conducted and presented the Norwegian Computer and Data Breach Survey in 2020 [48]. In this report they have collected risk profiles and trends from several national organisations that have presented their own risk assessment. The result corresponds to the findings done in regard to this thesis and what the experts has determined the most prominent threats in

the health care sector.

6.2 Research Question 2 - How does the cyber security training affect the risk awareness in the daily work of health care professionals?

The discussion about this research question is based the answers given in the questionnaire distributed among health care personnel and my interpretation of the answers given. The questionnaire contained five parts regarding digital security, some parts were only questions about work and others about work and home. It was also deliberately set up to uncover potential differences between the health care personnel that had received training and the ones who had not received training by splitting the questionnaire in two depending on which answer they gave in the control question.

The overall impression that the health care personnel gave in their answers, regardless of training or not, was that the security culture within the health care sector is far from mature. For instance, the answers from the health care personnel with training regarding their usual tools and policies comes back as expected, such as e-mail, EHR and passwords. But when asked about cloud services as can be seen in figure 5.14, smart devices and storage, the answers reveal that the knowledge is lacking. A similar result could be seen in figure 5.16 regarding the health care personnel that have not received training, where the the known tools and policies has a certain recognition as risks while the more unknown were a bit more unreliable (according to the frequency of “Do not know”).

On the views of management and control in the work place, as could be seen in figure 5.22, most health care personnel with training had good overview and felt that they had a good follow up by management by having requirements set for them and they have gotten clear guidelines to follow. On the question about whether or not focus had changed with guidelines concerning digital security or if they felt that the guidelines have been a hindrance in their work, they expressed that it had not affected them much. In figure 5.23, 9.5% of health care personnel with training has knowingly broken protocol, but the actual percentage of this action is likely to be higher because of the nature of the questionnaire and the interpretation of some of the comments left in the questionnaire.
The health care personnel without training expressed a larger percentage of “Do not know” regarding the questions about change in focus and if the guidelines had felt as a hindrance on their work than the health care personnel with training, as can be seen in figure 5.24. On the other questions, health care personnel without training had an overall larger percentage of “To a fairly small extent” answered than the ones with training. They have fewer demands and requirements from

management, less clear guidelines from management and less knowledge about procedures regarding digital incidents. 6.5% admitted braking protocol knowingly among the health care personnel with no training. The numbers are possibly higher than reported in this case as well, due to the same reasoning as with the ones with training.

The recurring feedback from health care personnel with training in the questionnaire was that the procedures regarding EHR and other e-health systems took too much time to use. The logging on and off-part of the system uses valuable time and has shown to be a constraint during emergencies in which policies has been disregarded. They miss important information because they have trouble reaching their mail or calendar from outside of work or are forced to use smart devices in order to gain access, and they find it difficult gaining the right access to the correct systems. One felt that the procedures they had been presented was outdated even, and one meant that the scenarios they had been presented during training was irrelevant to the actual risk the health care sector faces.
There was feedback from health care personnel without training as well, still not as many as from the ones with training. Still, the issues seem to be time spent on logging on and off, and extra time spent documenting. There were mentions of not being allowed to read patient records before the patient moved in to the facility, which made the transfer preparations for said patient difficult.
Funnily enough, even though the health care personnel said that he guidelines was less of a hindrance to them, they had more comments on what was a hindrance to them versus the comments from health care professionals without training. 17.8% of health care professionals with training commented about hindrance and 10.1% without training commented. These statements clearly show that there is some sort of hindrance in regards to the work of a health care professional regardless of training.

The behaviour surrounding computer systems has a very strong effect on the user and their surroundings. Health care personnel with training was asked about their behaviour at work and how they acted in certain situations. For instance, 40.9% of the respondents with training checked the legitimacy of a website before further use, and 48.3% checks if the sender of an e-mail was credible or not. It is a surprisingly high number, also seen in the light of the Audit Generals report [29] where their phishing test revealed that 39% of the 2300 receivers of the mail clicked on the link provided, 25% revealed information and 12% downloaded attachments, which are quite high numbers seen in the light of scope of the test.
Of the respondents with training, 57.3% said that they always log off their device or ID when leaving their station, while 41.8% stated that they usually or sometimes log off. The respondents with no training reported that 55.1% always logs off and 48.2% usually and sometimes log off. This behaviour could explain why the mention of time consumption was so extensive.

When asked about risk posing activities such as writing details about work on social media, almost none of the two groups had done so. Similarly with the question about copying patient data to an unencrypted device as well. Some of the respondents answered that they had sent patient data via e-mail. The biggest percentage of risk posing actions were, however, reusing passwords at work and at home. The reuse of passwords seems harmless, but if a person uses their password from a streaming service at home for their use at work, and that service gets breached, attackers can use that password to gain access to the organisation's system. This question has one of the largest differences between the health care personnel that had training and the ones that did not. 32.2% of the respondents with training said that they had reused passwords, while 40.6% with no training said they reused password. More men than women, regardless of training, reused passwords.
Passwords are a double-edged sword on some instances. Employers enforce complex password policies making the employees change passwords often. While it makes the system much safer having a complex password policy, it complicates the everyday work for the users and shortcuts are created.

Security culture does not only include the individual attitude towards information security, but also how comfortable they are to give feedback to a colleague if they see something that is not by the book. In figure 5.13 it can be seen that most of the respondents with training answered that they were "very comfortable" or "a little comfortable", while a higher degree of respondents with no training answered that they were "a little uncomfortable" or "very uncomfortable". This is actually good news, as it shows that health care professionals have a low bar for telling their colleagues that what they are doing might be not OK in regards to policy.

6.3 Research Question 3 - To what degree do the cyber security training affect the risk awareness of the medical professionals in their private domain?

The discussion about this research question is similar to the previous, apart from discussing the results from the questionnaire which is about how health care personnel regards information security at home. The questionnaire contained questions making it possible to compare how the respondents answered about work and then at home.

In regard to whether or not the use of internet at home increases risk in some form, a smaller percentage of the health care personnel without training agreed to the statement than the ones who had training, 9.4% versus 12.4%, as can be seen in figure 5.7. On the question on they felt that they had sufficient information regarding threats at home, 35.1% of health care personnel with training agreed to the statement, while 19.6% of the ones without training agreed, as could be

seen in figure 5.8. This could show that health care personnel with training have managed to transform the information they had received during training to apply at home as well, and that they feel more confident in their knowledge at home.

Among the health care personnel that had received training, the risk seen in figures 5.14 and 5.15, the answers went from " a very large extent" and "a fairly large extent" at work, to "a fairly large extent" and "a fairly small extent" at home. The same can be seen regarding the health care personnel without training, in figures 5.16 and 5.17. The risks seem to have diminished in the transfer from work to home. And the training seems to not affect the perceived risk between work and home.
The trends continue when looking at the threats faced at work and at home. There is a shift between how each threat is perceived. Most threats have gone from a "fairly large extent" and "fairly small extent" at work to a "fairly small extent" to a "very small extent" at home among health care personnel with training. The result from the ones without training is pretty similar at work and at home, when looking at figures 5.20 and 5.19. In this case, the health care personnel answered a larger percentage of "Do not know" at work than at home, meaning that they do not have the knowledge and awareness to assess the threats in a work setting, but might be able to relate to them in private. However, as discussed in section 6.1, Research Question 1, the amount of "Do not know" in both groups, with and without training, in is very high, which supports the statement that there are some missing knowledge about the topic. It might not be a lack in knowledge about the specific threat, but the relevance of these types of attacks and the place they work. For instance, a phishing or spearphishing attack could lead to the loss of availability of the system or loss of integrity and confidentiality of patient data, even in a hospital with the correct measures in place.

In regards to behaviour at work and at home, the largest difference can be seen in figures 5.26 and 5.27 (with training), and figures 5.28 and 5.29 (without training) is that health care professionals, in both groups, in a much larger degree does not lock their devices or log off before leaving their devices at home. However, both groups check for suspicious links and attachments in e-mail in a larger degree at home. It is clear that health care professionals with training reports more e-mails at home than the ones without training. They also check websites before use in a larger degree. So, some of the behaviour the health care professionals that has received training have in a more controlled environment at work has been transferred to the behaviour they have at home.

To finish this discussion I leave with a comment that was received on the questionnaire: "Isn't it contradictory to send us this survey, with a simple link in a simple e-mail? I would not have clicked the link at home, to put it that way.".

Chapter 7

Conclusion

There should be no doubt that health care professionals have an important job, and they have a lot on their plate in regards to the information they handle on a daily basis. And, as stated earlier in the thesis, information security within the health care sector is far from mature. However, what is mature is their patient security, there should not be any doubt about that.

The conclusion has been divided into a separate conclusion for each of the research questions, as well as an overall conclusion for the thesis.

Research Question 1
The digital threats that the health care sector faces today has changed from direct attacks such as DDoS and exploit of vulnerabilities to the soft targets within the sector, the users. The external threat from foreign actors is still present by all accounts, but those types of attacks are so sophisticated that it is difficult to uncover for a health care professional, and it is not their job to do so. They can, however, be taught to recognise attempts made by attackers to themselves and their colleagues.
The digital development in the health care sector has been enormous on its own, but the pandemic has accelerated the development further by force. This development has left some issues in its wake, such as wrong use of equipment and decisions made ad-hoc regarding how to best solve the issues at hand, e.g., home office.
There is also an issue with a missing security culture among health care professionals, and a lack in awareness about the threats the health care sector actually is facing. A lack of awareness does not equal a lack in knowledge, but it's a lack in being aware how the threats presented could affect the users, both at home and at work.

Research Question 2
Even though guidelines should state what is allowed or not allowed to do at work, several of the answers from both groups of health care professionals prove that

they do not follow them religiously. There could be several reasons for this: there is a lack of knowledge, understanding and awareness regarding digital information security among the health care professional with and without training, time constraints or unclear guidelines. However, the health care professionals that have received training had some areas that they showed more knowledge than the one without any training, but the overall answers were not that different.

At the start of this thesis, the notion was that health care professionals had been affected by the training they had received. Now at the end, it is clear that the security training has not affected the as much as first anticipated. This could be because information security (not to be confused with privacy or patient security) is far from mature within the health care sector. And by that I do not mean that they should feel that the guidelines and policies regarding information security should feel as a constraint on their work, but they should have felt a change in routines or in the way they work. However, they are used to working with the patient's privacy in mind, but information security is much more than just privacy.

Research Question 3
Health care professionals have managed to adopt some of the habits and behaviours from work to home, according to the results. Still, both risks and threats have been deemed "less serious" at home, both by those who had received training and those without training. One of the factors could be that the awareness of what type of system and information they are handling at work and at home. There was an increase in checking websites and e-mails at home, showing that they have a trusted system at work that should pick any discrepancies if there are any.
Not surprisingly, the opinion from the start of the thesis changed in this regard as well to a certain degree. The differences between health care professionals that had received training was perceived to have had more of an effect at home than it actually had, when comparing them to the ones that did not have the same training.

As mentioned before, information security within the health care sector needs maturing. However, it seems that after the audit performed by the Auditor General in 2019-2020 (presented in Chapter 3.2 Background), actions have been made by all the regional health trust in order to turn around and start making changes.
Security culture among health care professionals seems to be at the same level as information security regarding maturity. However, there are some aspects with the security culture that seems to surpass the information security in many ways. There is a large percentage of health care professionals that have little or no issue with telling colleagues they are doing something that poses a risk to the information security, which usually means that they are confident about what is right and wrong in regard to information security.
It is also clear that my questionnaire has revealed that there is some sort of a cog-

nitive dissonance going on between knowledge about digital threats in the health care sector and the thought about how the threats can affect them.

Chapter 8

Limitations and Future Work

As in most research there are areas that could be improved, which has been mentioned throughout the thesis. These areas will be addressed more thoroughly in this chapter.
Also, research is never done, which leads to ideas that others (or me) could build upon and evolve into new and interesting studies. I have mentioned a few suggestions for future work in this chapter.

8.1 Limitations

Not all goes as planned during research, this research project included. There were some minor hiccups during this process, which will be addressed in this chapter. Most of the limitations was foreseen in the risk assessment done during the research pre-project done during the fall semester and addressed there, so I was prepared on a few setbacks.

8.1.1 Application to do research

Many municipalities and hospitals require an extensive application to do research with them, also when the research do not include patient or health data. This was something I was not aware of. The applications took a good amount of time, to write and to get approval. Had I known this, I would have started applying in the beginning of the semester and not have to spend time during the data collection period to do it.

8.1.2 No interviews from municipalities

When I sent out my invitations to join in the data collection, as stated earlier in Chapter 4.3 Data Collection, I sent e-mails to about 30 municipalities and 25 hospital and regional trusts. In the e-mail to the hospital and regional trusts I included a request for interviews with a security expert and/or CISO while that request was

omitted to the municipalities. The reason behind this was that I assumed that municipalities in a much lesser degree had a security expert on hand and perhaps not a centralised department for information security. In hindsight, I should have included the request to the municipalities as well, as my assumptions could have led me to not getting more interviews.

8.1.3 Reducing research questions from 4 to 3

Unfortunately, I had to reduce the amount of research questions from 4 to 3. The research question that was "cut" was "What cyber security training is available for health care professionals today?". The reason for this action was the lack in answers from the main providers of digital security training, such as KS, and OUS. To be more precise, a representative from OUS did answer and said that they could not participate in this research project. Because of the lack of providers participating, I felt I could not defend having a research question that could not be verified by the providers of the courses. After talking to my supervisors about the issue and with their blessing, I removed the question from the other research questions and into Chapter 3.5 instead.

8.1.4 Mandatory questions

After reading feedback comments on my questionnaire about particularly one of my questions, I realised that the feedback was completely correct and I should have thought about it on beforehand. In part 5, question 26 I asked about what the respondents wanted more information about and listed some of the most common topics I could think of. I did not consider that the list was not exhaustive and that some of the respondents did not want to know more about the topics listed and information security in general. I could have resolved this differently and kept that question voluntary.
Although no specific comments about mandatory questions regarding the rest of the questionnaire, I assume that there were other questions that could have been voluntary as well.

8.1.5 Covid-19

My questionnaire was released 26th of February, just before the third wave of Covid-19 hit Norway. Knowing this, the municipalities and hospitals I contacted in regard to the questionnaire and interview was carefully picked. However, some of the municipalities and hospitals who I contacted suddenly got more Covid-cases during the process and had to decline participation.
Despite having picked one of the worst times to do research on health care professionals, the result of 394 respondents was surprising and shows that with some elbow grease and many hours of administrative duties, great results can be made even during a pandemic.

8.1.6 Wrong answers

My questionnaire started with a control question as one of the first questions, where the answer decided what direction the questionnaire took. That question was "Have you undergone information security training?". If the respondent answered "Yes" their answers would be compared to others who answered "Yes", and "No" would be compared with the respondent said "No". However, question 24 for both groups was "Have you been offered training or information security courses in the last two years?" and while the respondents had answered "No" on the control question, 5.1%, or 7 respondents, answered that they had participated in digital security training the last two years. This is something I should have seen before I started the data analysis and corrected, but as it was discovered too late in the process I chose not do anything about it. The amount that had answered incorrectly was so small I felt it would not have much significance to the result of my research questions.

8.2 Future Work

This thesis has given an overview over the state on information security in the health care sector, but there are several areas that could be looked into at a deeper level.

Research methods to increase security culture
For now, the security culture in the Norwegian health care sector is far from mature. Which should not come as a surprise as security training is not yet offered to a large part of health care professionals working within the Norwegian health care sector. However, training alone will not increase the security culture, awareness campaigns and other methods in order to keep the employees motivated could be of great value.

The effect of the training
This thesis did not research the effect of the training, rather how the training affected health care professionals in their everyday work. The possibility to test the employees before and after a course could reveal how much effect the training had, and reveal weak spots in the training, making it possible to adjust the training accordingly.

Customised training
Security experts has already stated that they want to meet their employees in their everyday work situation, they want to make the training more relevant to the role and knowledge level. The solution could be to start developing methods to easily map the level of knowledge of and adapt to the different roles they have in the hospital. This is something that lies close to my heart and I hope I can work with in the future.

Bibliography

[1] Datatilsynet, *Phishing hvordan beskytte virksomheten*, (Accessed 2/10/2020), Oct. 2020. [Online]. Available: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/phishing---hvordan-beskytte-virksomheten.

[2] C. F. C. Security, *The Cyber Threat Against Denmark*, (Accessed 23/02/2020), Jul. 2020. [Online]. Available: https://cfcs.dk/en/cybertruslen/threat-assessments/the-cyber-threat-against-denmark/.

[3] N. E. Larsen, *NemID in Denmark | IT-Politisk Forening*, (Accessed 2/10/2020), Jan. 2012. [Online]. Available: https://www.itpol.dk/notater/NemID.

[4] P. C. F. for the Healthcare Sector, *Cyber-og-informationssikkerhed-uk.pdf*, https://sum.dk/~/media/Filer%20-%20Publikationer_i_pdf/2019/A-strengthened-collective-cyber-and-information-security-effort/Cyber-og-Informationssikkerhed-UK.pdf, (Accessed on 10/10/2020).

[5] H. I. Security, *Microsoft shares preventable human-operated ransomware insights*, https://healthitsecurity.com/news/microsoft-shares-preventable-human-operated-ransomware-insights, (Accessed on 11/03/2020), Mar. 20.

[6] DIPS, *Ny meningsmåling om helsedigitalisering | dips*, https://www.dips.com/no/ny-meningsmaling-om-helsedigitalisering, (Accessed on 10/12/2020), Jun. 2019.

[7] K. Schmidt, 'The problem withawareness': Introductory remarks onawareness in cscw',' *Computer Supported Cooperative Work (CSCW)*, vol. 11, no. 3, pp. 285–298, 2002.

[8] M. Wilson and J. Hash, *Nist sp 800-50, building an information technology security awareness and training program*, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf, (Accessed on 03/03/2021), Oct. 2003.

[9] K. D. Mitnick, *The art of deception : Controlling the human element of security*, eng, Indianapolis, Ind, 2002.

[10] C. Kidd and B. Y. Hayden, *The psychology and neuroscience of curiosity*, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4635443/pdf/nihms722442.pdf, (Accessed on 02/23/2021), Nov. 2015.

[11] W. Stallings and L. Brown, *Computer Security: Principles and Practice*. Pearson Education Limited, 2018, vol. Fourth Edition - Global Edition, ISBN: 978-1-292-22061-1.

[12] W. Roberds and S. L. Schreft, 'Data breaches and identity theft,' *Journal of Monetary Economics*, vol. 56, no. 7, pp. 918–929, 2009, ISSN: 0304-3932. DOI: https://doi.org/10.1016/j.jmoneco.2009.09.003. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0304393209001214.

[13] NorSIS, *Norsis_trusler_trender_2021_digital.pdf*, https://norsis.no/wp-content/uploads/2021/03/NorSIS_Trusler_Trender_2021_Digital.pdf, (Accessed on 04/09/2021), Apr. 21.

[14] D. for e-helse, *Normen*, https://ehelse.no/normen, (Accessed on 10/10/2020).

[15] D. for e-helse, *Om normen - ehelse*, https://ehelse.no/normen/om-normen#Styringsgruppe, (Accessed on 11/24/2020).

[16] D. for e-helse, *Normen – norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren - ehelse*, https://ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren, (Accessed on 11/24/2020).

[17] ISO 27001:2017, *Information Technology, Security Techniques, Information Security Management Systems*. ISO, Geneva, Switzerland.

[18] J. og beredskapsdepartementet, *Lov om nasjonal sikkerhet (sikkerhetsloven) - lovdata*, https://lovdata.no/dokument/NL/lov/2018-06-01-24, (Accessed on 02/08/2021), Jan. 18.

[19] J. og beredskapsdepartementet, *Lov om nasjonal sikkerhet (sikkerhetsloven) - lovdata*, https://lovdata.no/dokument/NL/lov/2018-06-01-24#KAPITTEL_5, (Accessed on 02/08/2021), Jan. 18.

[20] J. og beredskapsdepartementet, *Lov om nasjonal sikkerhet (sikkerhetsloven) - lovdata*, https://lovdata.no/dokument/NL/lov/2018-06-01-24#KAPITTEL_6, (Accessed on 02/08/2021), Jan. 18.

[21] J. og beredskapsdepartementet, *Lov om behandling av personopplysninger (personopplysningsloven) - lovdata*, https://lovdata.no/dokument/NL/lov/2018-06-15-38?q=Personopplysningslove, (Accessed on 10/10/2020), Jul. 2018.

[22] N. D. of eHealth, *Implementation of gdpr in health care sector in norway - ehelse*, https://ehelse.no/personvern-og-informasjonssikkerhet/implementation-of-gdpr-in-health-care-sector-in-norway, (Accessed on 11/16/2020).

[23] H. og omsorgsdepartementet, *Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven) - lovdata*, https://lovdata.no/dokument/NL/lov/2014-06-20-42?q=pasientjournalloven, (Accessed on 10/10/2020), Jan. 2015.

[24] *Gikk inn i pasientjournalen til underordnet uten grunn – advarsel til sykepleier | helsetilsynet*, https://www.helsetilsynet.no/tilsyn/tilsynssaker/2019/gikk-inn-i-pasientjournalen-til-underordnet-uten-grunn-advarsel-til-sykepleier/, (Accessed on 11/16/2020), Sep. 19.

[25] E. Commission, *Regulation (eu) 2016/679*, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504, (Accessed on 10/10/2020), May 2016.

[26] B. Malmedal, *Nordmenn-og-digital-sikkerhetskultur-2020-web-1.pdf*, https://norsis.no/wp-content/uploads/2020/10/Nordmenn-og-digital-sikkerhetskultur-2020-web-1.pdf, (Accessed on 11/21/2020).

[27] NorSIS, *Se opp for svindel-e-post med falsk office365-oppdatering - norsis*, https://norsis.no/se-opp-for-svindel-e-post-med-falsk-office365-oppdatering/, (Accessed on 11/21/2020).

[28] D. for e-helse, *Anbefaling om strategi for digital sikkerhet - ehelse*, https://ehelse.no/aktuelt/anbefaling-om-strategi-for-digital-sikkerhet/_/attachment/download/429fc44c-275f-4638-89f4-6c56cba19f30:4ff499bbb5b0d3996095b830ec0a8be477f6827a/Strategi%20for%20digital%20sikkerhet%20i%20helse-%20og%20omsorgssektoren.pdf, (Accessed on 11/21/2020).

[29] Riksrevisjonen, *Riksrevisjonens undersøkelse av helseforetakenes forebygging av angrep mot sine ikt-systemer*, https://www.riksrevisjonen.no/globalassets/rapporter/no-2020-2021/undersokelse-av-helseforetakenes-forebygging-av-angrep-mot-sine-ikt-systemer.pdf, (Accessed on 01/28/2021), Dec. 2020.

[30] K. Munkejord and B. Sund, *Når ansatte er et mål for cyberkriminelle - magma*, https://www.magma.no/nar-ansatte-er-et-mal-for-cyberkriminelle, (Accessed on 02/02/2021), Feb. 20.

[31] T. Hyla and L. Fabisiak, 'Measuring Cyber Security Awareness within Groups of Medical Professionals in Poland,' Jan. 2020, (Accessed 2/10/2020). [Online]. Available: http://hdl.handle.net/10125/64215.

[32] J. Rajamäki, J. Nevmerzhitskaya and C. Virág, 'Cybersecurity education and training in hospitals: Proactive resilience educational framework (prosilience ef),' in *2018 IEEE Global Engineering Education Conference (EDUCON)*, 2018, pp. 2042–2046. DOI: 10.1109/EDUCON.2018.8363488.

[33] I. Winkler, *Security awareness: 7 elements of a successful program | cso online*, https://www.csoonline.com/article/2133408/network-security-the-7-elements-of-a-successful-security-awareness-program.html, (Accessed on 11/18/2020), Jun. 17.

[34] P. Bischoff, *Which countries have the worst (and best) cybersecurity?* https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/, (Accessed on 11/20/2020), Mar. 20.

[35] G. Martin, S. Ghafur, J. Kinross, C. Hankin and A. Darzi, *Wannacry—a year on*, https://www.bmj.com/content/361/bmj.k2381.full, 2018.

[36] W. Smart, *Lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf*, https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf, (Accessed on 11/18/2020), Jan. 18.

[37] C. Jacobsen, *Lærdommer etter angrepet mot helse sør-øst*, https://ehelse.no/normen/presentasjoner/_/attachment/download/873e1a33-b003-43df-950e-14c6b014b7cd:a878183a24f43fefc54138e61dbeb4d0946d977b/1300_jacobsen_angrep_mot_HSO.pdf, (Accessed on 11/18/2020), Nov. 18.

[38] PST, *Etterforskning av nettverksangrep mot datasystemene til helse sør-øst*, https://pst.no/alle-artikler/pressemeldinger/etterforsking-av-nettverksangrep-mot-datasystemene-til-helse-sor-ost/, (Accessed on 11/20/2020).

[39] NorSIS, *Hackingen av helse sør-øst - oppsummering - norsis*, https://norsis.no/hackingen-helse-sor-ost-oppsummering/, (Accessed on 11/20/2020).

[40] H. S.-Ø. HF, *Informasjonssikkerhet og personvern er styrket etter datainnbruddet - helse sør-øst rhf*, https://www.helse-sorost.no/nyheter/informasjonssikkerhet-og-personvern-er-styrket-etter-datainnbruddet, (Accessed on 11/18/2020).

[41] S. I. HF, *Dataangrep mot sykehuset innlandet hf - sykehuset innlandet*, https://sykehuset-innlandet.no/om-oss/aktuelt/nyheter/dataangrep-mot-sykehuset-innlandet-hf#berorte-tjenester, (Accessed on 11/20/2020).

[42] S. I. HF, *Oppdatering dataangrep - sykehuset innlandet*, https://sykehuset-innlandet.no/om-oss/aktuelt/nyheter/oppdatering-dataangrep, (Accessed on 11/20/2020).

[43] S. I. HF, *Analysearbeidet etter dataangrepet mot sykehuset innlandet er avsluttet - sykehuset innlandet*, https://sykehuset-innlandet.no/om-oss/aktuelt/nyheter/analysearbeidet-etter-dataangrepet-mot-sykehuset-innlandet-er-avsluttet, (Accessed on 11/20/2020).

[44] P. D. Leedy, *Practical research : Planning and design*, eng, Boston, 2015.

[45] L. E. Aarø, *Fra spørreskjemakonstruksjon til multivariat analyse av data : En innføring i survey-metoden*, nob, Bergen, 2007.

[46] G. Norman, 'Likert scales, levels of measurement and the "laws" of statistics,' *Advances in health sciences education*, vol. 15, no. 5, pp. 625–632, 2010.

[47] G. T. Chao and S. W. J. Kozlowski, 'Employee perceptions on the implementation of robotic manufacturing technology,' eng, *Journal of applied psychology*, vol. 71, no. 1, pp. 70–76, 1986, ISSN: 0021-9010.

[48] N. Sikkerhetsråd, *Mørketallsundersøkelsen 2020 - norwegian only*, `https://www.nsr-org.no/uploads/documents/Publikasjoner/Morketalls-2020-web.pdf`, (Accessed on 05/21/2021), 2020.

Appendix A

Interview Guide

Intervjuguide «Digital Sikkerhetskultur innen Helsevesenet»

1. Hvilke trusler mener du utgjør den største faren for helseforetak i 2021?

2. Har du oversikt over de ulike kursene som tilbys helsesektoren?
    a. Er disse tilpasset hver de ulike arbeidsfeltene vi finner innenfor helsesektoren eller er de mer generelle?
        i. Hvis generelle: Føler du at en tilpasset tilnærming til opplæringen hadde vært mer gunstig for utviklingen av en solid sikkerhetsatferd?
        ii. Hvis tilpasset: Føler du sikkerhetskulturen forbedret seg etter de fikk tilpasset opplæring?

3. Får helsepersonell i deres foretak tilbud om kursing i informasjonssikkerhet?
    a. Hvis ja, er det obligatorisk å gjennomføre treningen/kurset?
        i. Takker mange ja til kursing?
    b. Er dette en del av opplæringen eller får de tilbud om det etter hvert?
    c. Hvor ofte må de gjenta kurset?
    d. Hvordan metode mener du oppnår best effekt på informasjonssikkerheten?
        i. Kurs
            1. Fysisk
            2. E-læring
        ii. Trening
        iii. Testing
        iv. Workshops
    e. Hvis nei, tror du at de ansatte har et behov for en sånn type kurs eller trening?

4. Hvilke metoder bruker dere i forbindelse med kartlegging av sikkerhetskultur i foretaket?

5. Under normale forhold (non-covid), kjører dere testing på de ansatte for å sjekke om infosec-treningen har fungert?
    a. Hvis ja, hvilke metoder bruker dere?

b. Hvis nei, er det noen grunn til at det ikke blir prioritert?

6 Føler du at helseforetakene fokuserer nok på sikkerhetskultur blant helsepersonell?
   a. Mener du at det prioriteringen deres er riktig eller hadde du ønsket endringer i forhold til det trusselbildet vi ser i dag?
   b. Hvordan informerer dere de ansatte om eventuelle trusler eller hendelser?

7 Har dere rutiner for rapportering av mistenksomme eposter?
   a. Hvis ja, er det mange ansatte som bruker det?
   b. Er metoden for rapporteringen enkel og lett tilgjengelig?
   c. Hvordan håndteres disse i ettertid? Får de ansatte beskjed om funnene?
   d. Hvis nei, hvorfor har dere ikke rutiner for rapportering?

8 Synes du at de anbefalingene angående kursing innen informasjonssikkerhet og sikkerhetskultur som eksisterer i dag er gode nok?
   a. Hvis ja, ser dere noen effekt av dette etter gjennomført kurs?
   b. Hvis nei, har du noen meninger om hvordan de kan gjøres bedre?

9 Hvilke fokus bør helseforetakene ha for å øke den digitale bevisstheten til de ansatte i helseforetakene?
   a. Bedre passordpolicy
   b. 2FA/MFA/Biometri
   c. Deling av tilganger
   d. Tilgangsstyring
   e. Overvåking av personell
   f. Begrense fysiske tilganger
   g. Konsekvenser for ureglementerte hendelser

10 Involveres lederne i prosessene rundt kursingen?
   a. Hvis ja, har dere sett en effekt av det?
   b. Hvis nei, hvorfor ikke?

Interview guide “Digital security culture in health care”

1. What threats do you think pose the greatest danger to health care companies in 2021?

2. Do you have an overview of the different courses offered to the health care sector?
    a. Are these adapted to each of the different fields of work we find in the healthcare sector or are they more general?
        i. If general: Do you feel that a customized approach to training would have been more beneficial to the development of a solid security behavior?
        ii. If customized: Do you feel the security culture improved after they received customized training?

3. Are health professionals in their company being offered information security training?
    a. If so, is it mandatory to complete the training/course?
        i. Do many accept the training?
    b. Is this part of the tutorial or do they get offered it eventually?
    c. How often do they have to repeat the course?
    d. How do you think you have the best effect on information security?
        i. Course
            1. Physical
            2. E-learning
        ii. Training
        iii. Testing
        iv. Workshops
    e. If no, do you think your employees have a need for such a type of course or training?

4. What methods do you use when mapping safety culture in the enterprise?

5. Under normal conditions(non-covid), do you run testing on the staff to check if the information security training has worked?
    a. If so, what methods do you use?

b. If no, is there any reason why it won't be prioritized?

6 Do you feel that health care companies are focusing enough on safety culture among healthcare professionals?
   a. Do you think that their priority is right, or did you want changes in relation to the threats we see today?
   b. How do you inform your employees of any threats or incidents?

7 Do you have routines for reporting suspicious emails?
   a. If so, are there many employees who use it?
   b. Is the method of reporting simple and easily accessible?
   c. How are these handled afterwards? Are employees notified of the findings?
   d. If no, why don't you have reporting practices?

8 Do you think that the recommendations regarding training in information security and security culture that exist today are good enough?
   a. If so, do you see any effect of this after completing the course?
   b. If no, do you have any opinions on how they can be done better?

9 What focus should health enterprises have in increasing the digital awareness of health care workers?
   a. Better password policy
   b. 2FA/MFA/Biometrics
   c. Sharing permissions
   d. Access management
   e. Monitoring of personnel
   f. Restrict physical accesses
   g. Consequences for unruly events

10 Are the leaders involved in the processes around the training?
   a. If so, have you seen an effect of that?

b. If no, why not?

Appendix B

Questionnaire

Velkommen til denne spørreundersøkelsen om Digital sikkerhetskultur i helsevesenet.

Hvem har laget undersøkelsen og hva handler den om?

Mitt navn er Weronica Nilsen, og jeg er masterstudent på NTNU i Gjøvik hvor jeg studerer informasjonssikkerhet. Min masteroppgave handler om digital bevissthet og sikkerhetskultur innen helsevesenet. En del av den går ut på å kartlegge bevisstheten rundt digital sikkerhet i jobbsammenheng og privat. En annen del omhandler å kartlegge om de retningslinjer og policyer som er pålagt helsepersonell påvirker jobbhverdagen.

Spørreundersøkelsen

Spørreundersøkelsen består av 26 spørsmål delt opp i 5 ulike kategorier og selve undersøkelsen vil ta i underkant av 10 minutter å gjennomføre.

- Del 1 er bakgrunnsinformasjon, om du bruker digitale helsesystemer, arbeidstilhørighet og om du har gjennomført informasjonssikkerhetkurs eller -trening.
- Del 2 handler om holdninger og risikooppfattelse.
- Del 3 handler om oppfattelse av styring og kontroll.
- Del 4 handler om atferd i forbindelse med bruk av internett på jobb og hjemme.
- Del 5 handler om hvor kunnskapen om informasjonssikkerhet kommer fra og om hvilke metoder motivere læring for deg.

Anonymitet og deltakelse

Undersøkelsen er helt anonym, men alle spørsmålene er obligatoriske bortsett fra tekstsvar som er helt frivillig å svare på. Et annet viktig aspekt er at siden spørreundersøkelsen er anonym, vil det være helt umulig å slette dine svar etter du har levert inn. Innlevert svar vil da bli behandlet som samtykke for deltakelse. Du står helt fritt til å avbryte spørreundersøkelsen når du måtte ønske før den blir sendt inn. Da vil alle svar du har levert, bli slettet.

Kontakt

Hvis du har noen spørsmål eller kommentarer angående oppgaven eller ønsker å lese oppgaven etter den er ferdig, kan du kontakte meg på epost weronicn@stud.ntnu.no. Oppgaven vil bli veiledet av Vasileios Gkioulos (vasileios.gkioulos@ntnu.no) og Gaute Wangen (gaute.wangen@ntnu.no).

Tusen takk for hjelpen!

Del 1 - Bakgrunnsinformasjon

1. Bruker du elektronisk pasientjournal eller andre digitale helsesystemer?

- Ja
- Nei

Del 1 - Bakgrunnsinformasjon

2. Kjønn

- Kvinne
- Mann
- Ikke-binær
- Ønsker ikke svare

3. Hvor gammel er du?

- Under 20
- 20-29 år
- 30-39 år
- 40-49 år
- 50-59 år
- 60-69 år
- Over 70 år

4. Innen hvilken helsetjeneste jobber du?

Hvis du ikke finner riktig helsetjeneste, legg det til under annet.

- Spesialisthelsetjenesten
- Primærhelsetjenesten
- Sosiale tjenester
- Annet

5. Har du gjennomgått informsjonssikkerhetstrening?

Informasjonssikkerhetstrening vil si interne eller eksterne aktiviteter i form av styrking av informasjonssikkerheten i regi av arbeidsgiver/oppdragsgiver.

- Ja
- Nei

Del 2 - Holdninger og risikooppfatning til digital sikkerhet

6. Hvor enig er du i følgende påstander?

Dette er dine subjektive holdninger til digitalisering og informasjonssikkerhet.

Helt uenig / Delvis uenig / Delvis enig / Helt enig / Vet ikke

- Jeg er positiv til ny teknologi i jobbsammenheng
- Jeg er positiv til ny teknologi privat
- Det er høy risiko forbundet med å bruke internett på jobb
- Det er høy risiko forbundet å bruke internett privat
- Jeg har fått god informasjon om digitale trusler på jobb
- Jeg har fått god informasjon om digitale trusler privat
- Jeg er engstelig for at min datamaskin eller ID kan kobles opp mot sikkerhetshendelser
- Jeg har ingen problemer med at arbeidsgiver overvåker nettaktiviteter på jobb
- Arbeidsgiver har min fulle tillitt når det kommer til behandling av min personalmappe
- Elektronisk pasientjournal er en trygg måte å behandle pasientdata
- Jeg føler meg trygg i bruken av de elektroniske systemene vi har på jobb

7. Hvor er det viktigst å tenke på informasjonssikkerhet?

- Privat
- På jobben
- Det er like viktig
- Ingen av de er viktig
- Vet ikke

8. Har du opplevd at kolleger har gitt deg tilbakemelding om at det du gjør utgjør en risiko for informasjonssikkerheten?

Det kan være at du har fått tilbakemelding at du har gått fra en datamaskin uten å låse den etc...

- Ja
- Nei
- Vet ikke

9. Hvor komfortabel er du med å fortelle en kollega dersom du ser noe som kan utgjøre en informasjonssikkerhetsrisiko?

- Veldig komfortabel
- Litt komfortabel
- Litt ukomfortabel
- Veldig ukomfortabel
- Sier ikke i fra
- Vet ikke

10. I hvilken grad mener du at bruk av følgende aktiviteter utgjør en risiko på jobb?

I svært liten grad / I ganske liten grad / I ganske stor grad / I svært stor grad / Vet ikke

- Epost
- Sosiale medier
- Smart Devices (Smarthøyttalere, chatbots etc..)
- Minnepinner/bærbare lagringsmedium
- Skytjenester

11. I hvilken grad mener du at bruk av følgende aktiviteter utgjør en risiko hjemme?

I svært liten grad / I ganske liten grad / I ganske stor grad / I svært stor grad / Vet ikke

- Epost
- Sosiale medier
- Smart Devices (Smarthøyttalere, chatbots etc..)
- Minnepinner/bærbare lagringsmedium
- Skytjenester
- Lånte passord

12. I hvilken grad mener du at følgene trusler utgjør en risiko for informasjonssikkerheten i din jobb?

Informasjonssikkerheten i jobbsammenheng

I svært liten grad / I ganske liten grad / I ganske stor grad / I svært stor grad / Vet ikke

- Phishing
- Vishing (svindel igjennom telefon eller telefonsvarer)
- Spear-phishing (direktørsvindel)
- Løsepengevirus
- Utpressningsvirus
- Utnyttelse av svakheter i software og hardware
- Komprimittert HelseID/Påloggingsinformasjon/BankID
- Angrep på eksterne tjenestetilbydere (eksempel: chatbots etc...)
- Utnyttelse av situasjon i samfunnet (eksempel: Covid-pandemien)
- Angrep på infrastruktur (strøm, vann, internett)

13. I hvilken grad mener du at følgene trusler utgjør en risiko for din egen informasjonssikkerhet?

Informasjonssikkerheten i privat sammenheng

I svært liten grad / I ganske liten grad / I ganske stor grad / I svært stor grad / Vet ikke

- Phishing
- Vishing (svindel igjennom telefon eller telefonsvarer)

- Spear-phishing (direktørsvindel)
- Løsepengevirus
- Utpressningsvirus
- Utnyttelse av svakheter i software og hardware
- Komprimittert HelseID/Påloggingsinformasjon/BankID
- Angrep på eksterne tjenestetilbydere (eksempel: chatbots etc...)
- Utnyttelse av situasjon i samfunnet (eksempel: Covid-pandemien)
- Angrep på infrastruktur (strøm, vann, internett)

Del 3 Syn på styring og kontroll på din arbeidsplass

14. Har du oversikt over reglene og retningslinjene som gjelder informasjonssikkerhet på din avdeling?

I svært liten grad / I ganske liten grad / I ganske stor grad / I svært stor grad / Vet ikke

15. I hvilken grad er disse reglene og retningslinjene til hinder for arbeidet ditt?

I svært liten grad / I ganske liten grad / I ganske stor grad / I svært stor grad / Vet ikke

16. Ønsker du å utdype på hvilken måte reglene og retningslinjene hindrer arbeidet ditt?

Kom gjerne med generelle eksempler, som at journalføring tar for lang tid etc...

17. I hvilken grad har fokuset på informasjonssikkerhet endret måten du jobber på?

I svært liten grad / I ganske liten grad / I ganske stor grad / I svært stor grad / Vet ikke

18. I hvilken grad...

I svært liten grad / I ganske liten grad / I ganske stor grad / I svært stor grad / Vet ikke

- kjenner du til prosedyrene ved mistanke om en digital sikkerhetshendelse?
- har din arbeidsgiver gitt klare retningslinjer i forhold til informasjonssikkerhet?
- setter ledelsen krav til deg i forhold til informasjonssikkerhet?
- kjenner du til konsekvensene av brudd på taushetsplikten i forhold til pasientdata?

19. Har det hendt at du bevisst har brutt retningslinjene din arbeidsgiver har pålagt deg i forhold til informasjonssikkerhet?

- Ja
- Nei
- Vet ikke

Del 4 - Adferd

20. På jobb - hva gjør du?

Ja, alltid / Ja, som regel / Ja, av og til / Nei, aldri / Vet ikke

- Undersøker du om en nettside er sikker før du bruker den?
- Undersøker du linker og vedlegg du mottar før du åpner dem?
- Undersøker du avsenderadressen i eposter du mottar?
- Låser du datamaskinen din / logger ut av HelseID din når du forlater enheten?
- Bruker du private enheter tilkoblet jobbnettverket?
- Rapportert en mistenkelig epost som spam/phishing?

21. Hjemme - hva gjør du?

Ja, alltid / Ja, som regel / Ja, av og til / Nei, aldri / Vet ikke

- Undersøker du om en nettside er sikker før du bruker den?
- Undersøker du linker og vedlegg du mottar før du åpner dem?
- Undersøker du avsenderadressen i eposter du mottar?
- Låser du datamaskinen din / logger ut av HelseID din når du forlater enheten?
- Bruker du private enheter tilkoblet jobbnettverket?
- Rapportert en mistenkelig epost som spam/phishing?

22. Har du gjort noen av følgene...?

Ja / Nei / Vet ikke

- Brukt samme passord hjemme som på jobb?
- Brukt epost for å sende pasientdata internt/eksternt?
- Kopiert pasientdata til ukrypterte enheter?
- Skrevet detaljer om jobben på sosiale medier?

Del 5 - Kunnskap og motivasjon

23. Hvor har du lært om informasjonssikkerhet?

Du må velge minst ett svaralternativ.

- Selvstudie
- Gjennom interne kurs/trening
- Gjennom eksterne kurs/trening
- Informasjon fra arbeidsgiver

24. Har du blitt tilbudt trening eller kurs innen informasjonssikkerhet de siste to årene?

- Ja, har deltatt
- Ja, men har ikke deltatt
- Nei

- Vet ikke

25. Hva mener du hadde vært gode hjelpemidler for å øke oppmerksomheten rundt informasjonssikkerhet?

E-læringskurs og kjappe beskjeder på intranett er gjerne standard i jobbsammenheng, men finnes det bedre alternativer for å øke oppmerksomheten?

Du må velge minst ett svaralternativ.

- Fagdager med eksperter
- Læring ved hjelp av spill (Gamification)
- Fysiske kurs tilpasset arbeidsområdet
- E-læringskurs tilpasset arbeidsområdet
- Filmer om temaet

26. Jeg ønsker mer kunnskap om

Du må velge minst ett svaralternativ.

- hvordan jeg kan ivareta informasjonssikkerheten på jobb
- hvordan jeg kan ivareta informasjonssikkerheten hjemme
- sikker bruk av epost
- hvordan behandle pasientdata på en sikker måte
- hvordan varsle om informasjonssikkerhetshendelser på jobb
- bruk av sky-tjenester
- kurs tilgjengelig

Del 6 - Avslutning

Tusen takk for din deltakelse i denne spørreundersøkelsen.

Dine svar på undersøkelsen er viktige for kartleggelsen av digital bevissthet og sikkerhetskultur blant helsepersonell.

Skulle du ha noen tilbakemelding til skjemaet, noe å tilføye til ditt svar eller har spørsmål angående masteroppgaven, ta gjerne kontakt med meg på epostadresse weronicn@stud.ntnu.no eller skriv det inn i svarfeltet under.

Alle henvendelser i nettskjema er anonyme.

Welcome to this survey on Digital Safety Culture in Health Care.

Who made the survey and what is it about?

My name is Weronica Nilsen, and I am a master's student at NTNU in Gjøvik where I study information security. My master's thesis is about digital awareness and safety culture within health care. Part of it is to map awareness of digital security in a job context and privately. Another section deals with mapping whether the policies and policies imposed on healthcare professionals affect work life.

Survey

The survey consists of 26 questions divided into 5 different categories and the survey itself will take just under 10 minutes to complete.

- Part 1 is background information, whether you're using digital health systems, work affiliation, and whether you've completed information security courses or training.
- Part 2 is about attitudes and risk perception.
- Part 3 is about perception of governance and control.
- Part 4 is about behavior related to the use of the internet at work and at home.
- Part 5 is about where the knowledge of information security comes from and about what methods motivate learning for you.

Anonymity and participation

The survey is completely anonymous, but all the questions are mandatory except for text responses that are completely voluntary to answer. Another important aspect is that since the survey is anonymous, it will be completely impossible to delete your responses after you submit. The submitted response will then be treated as consent for participation. You are completely free to cancel the survey at any time before it is submitted. Then all replies you have delivered will be deleted.

Contact

If you have any questions or comments regarding the task or would like to read the task after it is finished, please contact me by email weronicn@stud.ntnu.no. The task will be guided by Vasileios Gkioulos (vasileios.gkioulos@ntnu.no) and Gaute Wangen (gaute.wangen@ntnu.no).

Thank you very much for your help!

Part 1 - Background information

1. Do you use electronic patient records or other digital health systems?

- Yes
- No

Part 1 - Background information

2. Gender

- Woman
- Man
- Non-binary
- Do not want to respond

3. How old are you?

- Under 20s
- 20-29 years
- 30-39 years
- 40-49 years
- 50-59 years
- 60-69 years
- 70 - 00:00

4. In which health care do you work?

If you can't find the right health care, add it below another.

- Specialist health service
- Primary health care
- Social services
- Other

5. Have you undergone information safety training?

Information security training means internal or external activities in the form of strengthening information security under the auspices of the employer/contracting authority.

- Yes
- No

Part 2 - Attitudes and risk perceptions to digital security

6. How agree do you agree with the following claims?

These are your subjective attitudes to digitization and information security.

Totally disagree / Partially disagree / Partially agree / Totally enig / Do not *know*

- I am positive about new technology in the job context
- I am positive about new technology privately
- There is high risk associated with using the internet at work
- It is high risk associated with using the internet privately
- I've got good information about digital threats at work
- I have received good information about digital threats privately
- I'm anxious that my computer or ID can be connected to security incidents
- I have no problems with my employer monitoring online activities at work
- Employer has my full confidence when it comes to processing my personnel folder
- Electronic patient records are a safe way to process patient data
- I feel safe in the use of the electronic systems we have at work

7. Where is it most important to think about information security?

- Private
- At work
- It's just as important
- None of them are important
- Don't know

8. Have you experienced that colleagues have given you feedback that what you do poses a risk to information security?

It may be that you have received feedback that you have left a computer without locking it etc...

- Yes
- No
- Don't know

9. How comfortable are you to tell a colleague if you see something that could pose an information security risk?

- Very comfortable
- A little comfortable
- A little uncomfortable
- Very uncomfortable
- Don't let you know
- Don't know

10. To what extent do you believe that using the following activities poses a risk at work?

To a very small extent / To a fairly small extent / To a fairly *large extent* / To a very *large extent* / Do *not know*

- Email
- Social media
- Smart Devices (Smart Speakers, Chatbots, etc..)
- Flash drives/portable storage media
- Cloud services

11. To what extent do you think that using the following activities poses a risk at home?

To a very small extent / To a fairly small extent / To a fairly *large extent* / To a very *large extent* / Do *not know*

- Email
- Social media
- Smart Devices (Smart Speakers, Chatbots, etc..)
- Flash drives/portable storage media
- Cloud services
- Borrowed password

12. To what extent do you believe that the consequences of threats pose a risk to information security in your job?

Information security at work

To a very small extent / To a fairly small extent / To a fairly *large extent* / To a very *large extent* / Do *not know*

- Phishing
- Vishing (scam through phone or answering machine)
- Spear phishing (director scam)
- Ransomware
- Blackmail virus
- Exploitation of weaknesses in software and hardware
- Compatible HealthID/Login Information/BankID
- Attacks on external service providers (example: chatbots etc...)
- Exploitation of situation in society (example: Covid-pandemic)
- Attacks on infrastructure (electricity, water, internet)

13. To what extent do you believe that the consequences of threats pose a risk to your own information security?

Information security in a private context

To a very small extent / To a fairly small extent / To a fairly *large extent* / To a very *large extent* / Do *not know*

- Phishing
- Vishing (scam through phone or answering machine)
- Spear phishing (director scam)
- Ransomware
- Blackmail virus
- Exploitation of weaknesses in software and hardware
- Compatible HealthID/Login Information/BankID
- Attacks on external service providers (example: chatbots etc...)
- Exploitation of situation in society (example: Covid-pandemic)
- Attacks on infrastructure (electricity, water, internet)

Part 3 Views on management and control in your workplace

14. Do you have an overview of the rules and policies that apply to information security in your department?

To a very small extent / To a fairly small extent / To a fairly *large extent* / To a very *large extent* / Do *not know*

15. To what extent are these rules and policies hindering your work?

To a very small extent / To a fairly small extent / To a fairly large extent / To a very large extent / Do not know

16. Do you want to elaborate on the way the rules and policies hinder your work?

Feel free to provide general examples, such as journaling taking too long etc...

17. To what extent has your focus on information security changed the way you work?

To a very small extent / To a fairly small extent / To a fairly large extent / To a very large extent / Do not know

18. To what extent...

To a very small extent / To a fairly small extent / To a fairly *large extent* / To a very *large extent* / Do *not know*

- do you know the procedures in case of a digital security incident?
- has your employer given clear guidelines in relation to thesecurity of information?
- does management set requirements for you in relation to information security?
- do you know the consequences of breaches of confidentiality in relation to patient data?

19. Has it happened that you have deliberately violated the policies your employer has imposed on you in relation to information security?

- Yes
- No
- Don't know

Part 4 - Behavior

20. At work - what are you doing?

Yes, always / Yes, as a rule / Yes, occasionally / No, never / Do not *know*

- Do you check whether a website is secure before using it?
- Do you examine the links and attachments you receive before opening them?
- Do you examine the sender address in emails you receive?
- Do you lock your computer/log out of your Health ID when you leave your device?
- Are you using private devices connected to your work network?
- Reported a suspicious email asspam/phishing?

21. At home - what are you doing?

Yes, always / Yes, as a rule / Yes, occasionally / No, never / Do not *know*

- Do you check whether a website is secure before using it?
- Do you examine the links and attachments you receive before opening them?
- Do you examine the sender address in emails you receive?
- Do you lock your computer/log out of your Health ID when you leave your device?
- Are you using private devices connected to your work network?
- Reported a suspicious email asspam/phishing?

22. Have you done any of the consequences... ?

Yes / No / Do not know

- Used the same password at home as at work?
- Used email to send patient data internally/externally?
- Copied patient data to unencrypted devices?
- Written details of the job on social media?

Part 5 - Knowledge and Motivation

23. Where have you learned about information security?

You must select at least one answer option.

- Self-study

- Through internal courses/training
- Through external courses/training
- Information from the employer

24. Have you been offered training or information security courses in the last two years?

- Yes, have participated
- Yes, but have not participated
- No
- Don't know

25. What do you think would be good tools to raise awareness about information security?

E-learning courses and quick messages on the intranet are often standard in the job context, but are there better options for raising awareness?

You must select at least one answer option.

- Professional days with experts
- Learning using games (Gamification)
- Physical courses adapted to the workspace
- E-learning courses adapted to the workspace
- Movies on the subject

26. I would like more knowledge about

You must select at least one answer option.

- how I can ensure information security at work
- how I can ensure information security at home
- secure use of email
- how to safely process patient data
- how to notify about information security incidents at work
- use of cloud services
- courses available

Part 6 - Conclusion

Thank you very much for your participation in this survey.

Your responses to the survey are important for the mapping of digital awareness and safety culture among healthcare professionals.

Should you have any feedback to the form, something to add to your answer or have questions regarding the master thesis, feel free to contact me at the email address weronicn@stud.ntnu.no or enter it in the answer box below.

All inquiries in the online form are anonymous.

Table B.1: Measurment Objectives Questionnaire

Q. no	Topic	Targets	Measurement objective	Research Q.
1	Check	EPJ users	Sort out the ones that do not use electronic systems	-
2	Job title	All	Determine the categories	-
3	Job title	All	Other job titles not described in Q.3	-
4	Self-assessment	All	Received training (*ST)/ not received training(*WST)	-
5	Self-assessment	ST/WST	Attitudes towards digitation	3
6	Self-assessment	ST/WST	Determine their focus on information security	4
7	Routines	ST/WST	Feedback/reporting	3
8	Routines	ST/WST	Threshold for reporting	3
9	Risk awareness	ST/WST	Risk awareness work	2/3/4
10	Risk awareness	ST/WST	Risk awareness private	4
11	Threat awareness	ST/WST	Threat awareness work	2/3/4
12	Threat awareness	ST/WST	Threat awareness private	4
13	Policy	ST/WST	Policy awareness	3
14	Policy	ST/WST	Determine if policy complicates work	3
15	Policy	ST/WST	Elaborate what complicates work	3
16	Policy	ST/WST	Change in work habits	3
17	Policy	ST/WST	Policy awareness	3
18	Policy	ST/WST	Regarding of policy	3
19	Behaviour	ST/WST	Behaviour work	3/4
20	Behaviour	ST/WST	Behaviour private	4
21	Behaviour scenario	ST/WST	Creating security issues	3/4
22	Knowledge	ST/WST	Main source of training	3/4
23	Knowledge	ST/WST	Offered Training	1/3
24	Knowledge	ST/WST	Means for learning	3/4
25	Knowledge	ST/WST	Gaining knowledge	1/3/4
26	Feedback	All	Feedback on questionnaire/other	-

Appendix C

Information Letter to the Participants of the Interviews

Vil du delta i forskningsprosjektet

«Digital sikkerhetskultur innen helsevesenet»?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt som skal resultere i en masteroppgave hvor formålet er å kartlegge sikkerhetskultur blant helsepersonell med og uten sikkerhetstrening. Forskningsprosjektet vil også forsøke å kartlegge om det er noen forskjeller i hvordan helsepersonell behandler informasjon i jobbsammenheng og privat. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål
Formålet med denne masteroppgaven er å kartlegge sikkerhetskultur blant helsepersonell, enten de har gjennomgått sikkerhetstrening eller ikke. Det utarbeides en anonym spørreundersøkelse som skal distribueres til helsepersonell verd ulike helseforetak, med spørsmål om deres holdninger og risikooppfatning til informasjonssikkerhet, deres digitale adferd og hvor de har tilegnet seg kunnskap om informasjonssikkerhet

Masteroppgaven består av 4 ulike forskningsspørsmål:

1. Hvilke organiserte alternativer til sikkerhetstrening det finnes og blir disse metodene brukt av utvalgte virksomhetene?
2. Hvordan ser det digitale trusselbildet ut for helsevesenet i dag?
3. Hvordan påvirkes helsepersonell av sikkerhetstreningen i sitt daglige arbeid?
4. Hvordan behandler helsepersonell sin egen informasjon hjemme?

Informasjonen som blir innhentet vil bli behandlet, lagret og brukt kun i tidsrommet som oppgaven skrives, som er estimert vårsemesteret 2021.

Hvem er ansvarlig for forskningsprosjektet?
Norges teknisk-naturvitenskapelige universitet – NTNU – Institutt for informasjonssikkerhet og kommunikasjonsteknologi er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?
Masteroppgaven innebærer å innhente informasjon om trusselbildet som spesielt omfatter helsevesenet, og ved å innhente informasjon direkte fra de som jobber med å sikre helsevesenet mot slike trusler, vil informasjonen og resultatet av prosjektet blir mer presis. De som jobber med dette, vil også ha en god kunnskap om hvordan sikkerhetstreningen blir utført og ha kjennskap til hvilke metoder som blir brukt.

Hva innebærer det for deg å delta?
Din deltakelse i intervjuprosessen vil bidra til å øke forståelsen om trusselbildet norsk helsevesen er utsatt for i dagens samfunn, både for denne masteroppgaven og eventuelle videre arbeid i dette feltet.

Intervjuet vil bestå av 10 spørsmål med noen oppfølgingsspørsmål, anslått at intervjuet vil ta 45min. Spørsmålene vil være at den art ingen sensitiv informasjon vil innhentes, og det vil heller ikke bli spurt spørsmål angående drift eller infrastruktur. Spørsmålene vil i all hovedsak omhandle generelle metoder og rutiner som inngår i begrepet «sikkerhetskultur»

Hvis det du samtykker, vil lyden av intervjuet tas opp og lagres på en sikker måte ved NTNU. Dette samtykke kan når som helst trekkes tilbake.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg. Hvis du samtykker til lydopptak kan dette samtykket trekkes tilbake uten at det påvirker ditt bidrag til oppgaven hvis det fremdeles er et ønske om å bidra.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

Informasjonen vil bli lagret og bearbeidet på et kryptert lagringsområde hos NTNU.
Det vil verken bli nevnt navn på deltaker eller virksomhet i oppgaven om det ikke er ønskelig.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?
Opplysningene anonymiseres når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er innen utgangen av juni 2021. Etter at oppgaven blir godkjent, vil alle lydopptak slettes.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:
- innsyn i hvilke personopplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene,
- å få rettet personopplysninger om deg,
- å få slettet personopplysninger om deg, og
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra NTNU har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?
Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med NTNU – Institutt for informasjonssikkerhet og kommunikasjonsteknologi.

- Veiledere for masteroppgaven:
  Vasileios Gkioulos - vasileios.gkioulos@ntnu.no
  Gaute Wangen – gaute.wangen@ntnu.no

- Studentens navn: Weronica Nilsen – epost weronicn@stud.ntnu.no

- Vårt personvernombud: Thomas Helgesen – epost Thomas.helgesen@ntnu.no eller telefon 93079038

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:
- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 55 58 21 17.

Med vennlig hilsen

Prosjektansvarlig
(Forsker/veileder) (Student)

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *Digital sikkerhetskultur innen helsevesenet*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i intervju

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

---

(Signert av prosjektdeltaker, dato)

Do you want to participate in the research project

«Digital security culture in health care»?

This is a question for you to participate in a research project that will result in a master's thesis where the purpose is to map security culture and healthcare professionals with and without cyber security training. The research project will also try to determine whether there are any differences in how healthcare professionals process information in a job context and privately. In this writing, we provide you with information about the goals of the project and what participation will entail for you.

Purpose
The purpose of this master's thesis is to map security culture among healthcare professionals, whether they have undergone security training or not. An anonymous survey is being prepared to distribute to healthcare professional's worth different health trusts, with questions about their attitudes and risk perceptions of information security, their digital behavior and where they have acquired knowledge about information security

The master's thesis consists of 4 different research questions:

1. What organized alternatives to security training are available and are these methods used by selected businesses?
2. What does the digital threat picture look like for health care today?
3. How are healthcare professionals affected by the security training in their daily work?
4. How do healthcare professionals process their own information at home?

The information collected will be processed, stored, and used only during the period in which the assignment is written, which is estimated spring semester 2021.

Who is responsible for the research project?
The Norwegian University of Science and Technology – NTNU – The Department of Information Security and Communication Technology is responsible for the project.

Why are you asked to participate?
The master's thesis involves collecting information about the threat picture that specifically includes health care, and by collecting information directly from those working to secure health care against such threats, the information and results of the project will be more precise. Those working on this will also have a good knowledge of how the security training is carried out and have knowledge of what methods are being used.

What does it mean for you to participate?
Your participation in the interview process will help to increase your understanding of the threat picture the Norwegian health system is exposed to in today's society, both for this master's thesis and any further work in this field.

The interview will consist of 10 questions with some follow-up questions, estimated that the interview will take45min. The questions will be that the nature of any sensitive information will be collected, nor will questions be asked regarding operations or infrastructure. The questions will mainly deal with general methods and routines included in the term "security culture".

If you agree, the audio of the interview will be recorded and stored securely by NTNU. This consent can be withdrawn at any time.

It is voluntary to participate
It is voluntary to participate in the project. If you choose to participate, you may withdraw your consent at any time without giving any reason. All your personalinformation will thenbe deleted. It will have no negative consequences for you if you do not want to participate or later choose to withdraw. If you agree to audio recordings, this consent may be withdrawn without affecting your contribution to the task if there is still a desire to contribute.

Your privacy – how we store and use your information
We will only use your information for the purposes we have disclosed in this writing. We treat the data confidentially and in accordance with the Privacy Policy.

The information will be stored and processed on an encrypted storage area at NTNU.
There will be no mention of the name of the participant or business in the task if there is nowish.

What happens to your information when we finish the research **project?**
The information is anonymized when the project is completed/thesis is approved, which is scheduled to be by the end of June 2021. After the task is approved, all audio recordings will be deleted.

Your rights
As long as you can be identified in the data material, you are entitled to:
- information about you, and to provide a copy of the data,
- to have personal data rectified about you,
- to have personal information deleted about you, and
- to lodge a complaint with the Norwegian Data Protection Authority about the processing of your personal data.

What gives us the right to process personal data about you?
We process information about you based on your consent.

On behalf of NTNU, NSD – The Norwegian Centre for Research Data AS has assessed that the processing of personal data in this project is in accordance with the data protection regulations.

Where can I find more information?
If you have any questions about the study, or would like to use your rights, please contact NTNU – Department of Information Security and Communication Technology.

- Supervisors for the master's thesis:
  Vasileios Gkioulos - vasileios.gkioulos@ntnu.no
  Gaute Wangen – gaute.wangen@ntnu.no

- Student's name: Weronica Nilsen – email weronicn@stud.ntnu.no

- Our Data Protection Officer: Thomas Helgesen – email Thomas.helgesen@ntnu.no or phone 93079038

If you have any questions related to NSD's assessment of the project, please contact:
- NSD – Norwegian Centre for Research Data AS by e-mail (personverntjenester@nsd.no) or by phone: +47 55 58 21 17.

Yours sincerely

Project Manager
(Researcher/supervisor) (Student)

Consent Statement

I have received and understood information about the project *Digital security culture in health care* and have been given the opportunity to ask questions. I agree to:

- ☐ to participate in an interview

I agree that my information is processed until the project is completed

---
(Signed by project participant, date)

Appendix D

SPSS Data sheet

SPSS data sheet

Innhold

Part 1 - Attitude and risk perception to digital security

New Technology

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_ja_tech_jobb	Female	198	3.77	.498	.035	3.70	3.84	1	4
	Male	44	3.91	.362	.055	3.80	4.02	2	4
	Total	242	3.80	.478	.031	3.74	3.86	1	4
var_ja_tech_privat	Female	198	3.65	.567	.040	3.57	3.73	1	5
	Male	44	3.95	.211	.032	3.89	4.02	3	4
	Total	242	3.70	.533	.034	3.63	3.77	1	5
var_nei_tech_jobb	Female	108	3.68	.609	.059	3.56	3.79	1	4
	Male	30	3.53	.629	.115	3.30	3.77	2	4
	Total	138	3.64	.614	.052	3.54	3.75	1	4
var_nei_tech_privat	Female	108	3.56	.740	.071	3.42	3.71	1	5
	Male	30	3.57	.626	.114	3.33	3.80	2	4
	Total	138	3.57	.714	.061	3.44	3.69	1	5

Figure 1 Descriptives New Technology

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_ja_tech_jobb	Between Groups	.669	1	.669	2.953	.087
	Within Groups	54.409	240	.227		
	Total	55.079	241			
var_ja_tech_privat	Between Groups	3.417	1	3.417	12.585	.000
	Within Groups	65.162	240	.272		
	Total	68.579	241			
var_nei_tech_jobb	Between Groups	.477	1	.477	1.270	.262
	Within Groups	51.124	136	.376		
	Total	51.601	137			
var_nei_tech_privat	Between Groups	.000	1	.000	.000	.990
	Within Groups	69.913	136	.514		
	Total	69.913	137			

Figure 2 One-Way ANOVA New Technology

Correlations

		var_ja_tech_jobb	var_ja_tech_privat	var_nei_tech_jobb	var_nei_tech_privat
var_ja_tech_jobb	Pearson Correlation	1	.576**	.b	.b
	Sig. (2-tailed)		.000	.	.
	N	242	242	0	0
var_ja_tech_privat	Pearson Correlation	.576**	1	.b	.b
	Sig. (2-tailed)	.000		.	.
	N	242	242	0	0
var_nei_tech_jobb	Pearson Correlation	.b	.b	1	.711**
	Sig. (2-tailed)	.	.		.000
	N	0	0	138	138
var_nei_tech_privat	Pearson Correlation	.b	.b	.711**	1
	Sig. (2-tailed)	.	.	.000	
	N	0	0	138	138

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

b. Cannot be computed because at least one of the variables is constant.

Figure 3 Correlations New Technology

Risks and Threats

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_nei_risiko_jobb	Female	108	2.64	1.072	.103	2.43	2.84	1	5
	Male	30	2.27	.691	.126	2.01	2.52	1	3
	Total	138	2.56	1.011	.086	2.39	2.73	1	5
var_nei_risiko_privat	Female	108	2.59	.996	.096	2.40	2.78	1	5
	Male	30	2.57	.858	.157	2.25	2.89	1	4
	Total	138	2.59	.965	.082	2.42	2.75	1	5
var_nei_trusler_jobb	Female	108	2.02	1.032	.099	1.82	2.22	1	5
	Male	30	2.10	.923	.168	1.76	2.44	1	4
	Total	138	2.04	1.007	.086	1.87	2.21	1	5
var_nei_trusler_privat	Female	108	2.57	.978	.094	2.39	2.76	1	4
	Male	30	2.97	.809	.148	2.66	3.27	1	4
	Total	138	2.66	.955	.081	2.50	2.82	1	4
var_ja_risiko_jobb	Female	198	2.73	.899	.064	2.60	2.85	1	5
	Male	44	2.32	.740	.112	2.09	2.54	1	4
	Total	242	2.65	.885	.057	2.54	2.76	1	5
var_ja_risiko_privat	Female	198	2.83	.848	.060	2.71	2.95	1	5
	Male	44	2.43	.789	.119	2.19	2.67	1	4
	Total	242	2.76	.850	.055	2.65	2.87	1	5
var_ja_trusler_jobb	Female	198	2.98	1.042	.074	2.83	3.13	1	4
	Male	44	2.93	.846	.128	2.67	3.19	1	4
	Total	242	2.97	1.008	.065	2.84	3.10	1	4
var_ja_trusler_privat	Female	198	3.07	.873	.062	2.94	3.19	1	4
	Male	44	3.09	.858	.129	2.83	3.35	1	4
	Total	242	3.07	.869	.056	2.96	3.18	1	4

Figure 4 Descriptives Risk&Threats

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_nei_risiko_jobb	Between Groups	3.253	1	3.253	3.234	.074
	Within Groups	136.783	136	1.006		
	Total	140.036	137			
var_nei_risiko_privat	Between Groups	.016	1	.016	.017	.897
	Within Groups	127.441	136	.937		
	Total	127.457	137			
var_nei_trusler_jobb	Between Groups	.156	1	.156	.153	.696
	Within Groups	138.663	136	1.020		
	Total	138.819	137			
var_nei_trusler_privat	Between Groups	3.619	1	3.619	4.055	.046
	Within Groups	121.374	136	.892		
	Total	124.993	137			
var_ja_risiko_jobb	Between Groups	6.025	1	6.025	7.909	.005
	Within Groups	182.818	240	.762		
	Total	188.843	241			
var_ja_risiko_privat	Between Groups	5.804	1	5.804	8.276	.004
	Within Groups	168.295	240	.701		
	Total	174.099	241			
var_ja_trusler_jobb	Between Groups	.083	1	.083	.081	.776
	Within Groups	244.715	240	1.020		
	Total	244.798	241			
var_ja_trusler_privat	Between Groups	.023	1	.023	.030	.862
	Within Groups	181.783	240	.757		
	Total	181.806	241			

Figure 5 One-Way ANOVA Risk&Threats

Figure 6 Correlation risk&threats

Correlations

		var_ja_risiko_jobb	var_ja_risiko_privat	var_ja_trusler_jobb	var_ja_trusler_privat	var_nei_risiko_jobb	var_nei_risiko_privat	var_nei_trusler_jobb	var_nei_trusler_privat
var_ja_risiko_jobb	Pearson Correlation	1	.694**	-.021	.059	.b	.b	.b	.b
	Sig. (2-tailed)		.000	.750	.362	.	.	.	.
	N	242	242	242	242	0	0	0	0
var_ja_risiko_privat	Pearson Correlation	.694**	1	-.071	-.011	.b	.b	.b	.b
	Sig. (2-tailed)	.000		.271	.867	.	.	.	.
	N	242	242	242	242	0	0	0	0
var_ja_trusler_jobb	Pearson Correlation	-.021	-.071	1	.491**	.b	.b	.b	.b
	Sig. (2-tailed)	.750	.271		.000	.	.	.	.
	N	242	242	242	242	0	0	0	0
var_ja_trusler_privat	Pearson Correlation	.059	-.011	.491**	1	.b	.b	.b	.b
	Sig. (2-tailed)	.362	.867	.000		.	.	.	.
	N	242	242	242	242	0	0	0	0
var_nei_risiko_jobb	Pearson Correlation	.b	.b	.b	.b	1	.695**	-.178*	-.127
	Sig. (2-tailed)	.	.	.	.		.000	.037	.138
	N	0	0	0	0	138	138	138	138
var_nei_risiko_privat	Pearson Correlation	.b	.b	.b	.b	.695**	1	-.037	.005
	Sig. (2-tailed)	.	.	.	.	.000		.666	.957
	N	0	0	0	0	138	138	138	138
var_nei_trusler_jobb	Pearson Correlation	.b	.b	.b	.b	-.178*	-.037	1	.453**
	Sig. (2-tailed)	.	.	.	.	.037	.666		.000
	N	0	0	0	0	138	138	138	138
var_nei_trusler_privat	Pearson Correlation	.b	.b	.b	.b	-.127	.005	.453**	1
	Sig. (2-tailed)	.	.	.	.	.138	.957	.000	
	N	0	0	0	0	138	138	138	138

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

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

b. Cannot be computed because at least one of the variables is constant.

At work

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_ja_engstelig	Female	198	2.60	1.060	.075	2.45	2.75	1	5
	Male	44	2.14	.878	.132	1.87	2.40	1	4
	Total	242	2.52	1.044	.067	2.38	2.65	1	5
var_ja_overvaakining	Female	198	3.38	.892	.063	3.26	3.51	1	5
	Male	44	2.93	1.087	.164	2.60	3.26	1	4
	Total	242	3.30	.944	.061	3.18	3.42	1	5
var_ja_tilitt	Female	198	3.48	.779	.055	3.38	3.59	1	5
	Male	44	3.32	.829	.125	3.07	3.57	1	4
	Total	242	3.45	.789	.051	3.35	3.55	1	5
var_ja_epj_trygg	Female	198	3.61	.687	.049	3.51	3.71	1	5
	Male	44	3.59	.622	.094	3.40	3.78	2	5
	Total	242	3.61	.675	.043	3.52	3.69	1	5
var_ja_trygg_bruk	Female	198	3.66	.580	.041	3.58	3.74	1	5
	Male	44	3.59	.622	.094	3.40	3.78	2	4
	Total	242	3.65	.587	.038	3.57	3.72	1	5

Figure 7 Descriptives At work – with training

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_ja_engstelig	Between Groups	7.772	1	7.772	7.325	.007
	Within Groups	254.662	240	1.061		
	Total	262.434	241			
var_ja_overvaakining	Between Groups	7.356	1	7.356	8.503	.004
	Within Groups	207.624	240	.865		
	Total	214.979	241			
var_ja_tilitt	Between Groups	1.000	1	1.000	1.611	.206
	Within Groups	149.000	240	.621		
	Total	150.000	241			
var_ja_epj_trygg	Between Groups	.015	1	.015	.032	.858
	Within Groups	109.692	240	.457		
	Total	109.707	241			
var_ja_trygg_bruk	Between Groups	.180	1	.180	.521	.471
	Within Groups	82.965	240	.346		
	Total	83.145	241			

Figure 8 One-Way ANOVA at work - with training

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_nei_engstelig	Female	108	2.72	1.296	.125	2.48	2.97	1	5
	Male	30	2.40	.932	.170	2.05	2.75	1	4
	Total	138	2.65	1.230	.105	2.45	2.86	1	5
var_nei_overvaakning	Female	108	3.03	1.131	.109	2.81	3.24	1	5
	Male	30	2.57	1.135	.207	2.14	2.99	1	4
	Total	138	2.93	1.144	.097	2.73	3.12	1	5
var_nei_tillit	Female	108	3.37	.923	.089	3.19	3.55	1	5
	Male	30	3.07	1.081	.197	2.66	3.47	1	5
	Total	138	3.30	.964	.082	3.14	3.47	1	5
var_nei_epj_trygg	Female	108	3.52	.704	.068	3.38	3.65	1	5
	Male	30	3.50	.731	.133	3.23	3.77	2	5
	Total	138	3.51	.707	.060	3.40	3.63	1	5
var_nei_trygg_bruk	Female	108	3.57	.644	.062	3.45	3.70	1	5
	Male	30	3.40	.770	.141	3.11	3.69	1	4
	Total	138	3.54	.674	.057	3.42	3.65	1	5

Figure 9 Descriptives at work- no training

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_nei_engstelig	Between Groups	2.438	1	2.438	1.618	.206
	Within Groups	204.867	136	1.506		
	Total	207.304	137			
var_nei_overvaakning	Between Groups	4.992	1	4.992	3.895	.050
	Within Groups	174.283	136	1.281		
	Total	179.275	137			
var_nei_tillit	Between Groups	2.166	1	2.166	2.355	.127
	Within Groups	125.052	136	.919		
	Total	127.217	137			
var_nei_epj_trygg	Between Groups	.008	1	.008	.016	.900
	Within Groups	68.463	136	.503		
	Total	68.471	137			
var_nei_trygg_bruk	Between Groups	.711	1	.711	1.571	.212
	Within Groups	61.607	136	.453		
	Total	62.319	137			

Figure 10 One-Way ANOVA at work - no training

Correlations

		var_ja_engstelig	var_ja_overvaakining	var_ja_tilitt	var_ja_epj_trygg	var_ja_trygg_bruk	var_nei_engstelig	var_nei_overvaakning	var_nei_tillit	var_nei_epj_trygg	var_nei_trygg_bruk
var_ja_engstelig	Pearson Correlation	1	.102	-.034	.006	-.217**	.b	.b	.b	.b	.b
	Sig. (2-tailed)		.113	.595	.922	.001	.	.	.	.	.
	N	242	242	242	242	242	0	0	0	0	0
var_ja_overvaakining	Pearson Correlation	.102	1	.406**	.108	.080	.b	.b	.b	.b	.b
	Sig. (2-tailed)	.113		.000	.092	.217	.	.	.	.	.
	N	242	242	242	242	242	0	0	0	0	0
var_ja_tilitt	Pearson Correlation	-.034	.406**	1	.383**	.256**	.b	.b	.b	.b	.b
	Sig. (2-tailed)	.595	.000		.000	.000	.	.	.	.	.
	N	242	242	242	242	242	0	0	0	0	0
var_ja_epj_trygg	Pearson Correlation	.006	.108	.383**	1	.499**	.b	.b	.b	.b	.b
	Sig. (2-tailed)	.922	.092	.000		.000	.	.	.	.	.
	N	242	242	242	242	242	0	0	0	0	0
var_ja_trygg_bruk	Pearson Correlation	-.217**	.080	.256**	.499**	1	.b	.b	.b	.b	.b
	Sig. (2-tailed)	.001	.217	.000	.000		.	.	.	.	.
	N	242	242	242	242	242	0	0	0	0	0
var_nei_engstelig	Pearson Correlation	.b	.b	.b	.b	.b	1	-.096	-.199*	-.086	-.099
	Sig. (2-tailed)	.	.	.	.	.		.263	.019	.313	.248
	N	0	0	0	0	0	138	138	138	138	138
var_nei_overvaakning	Pearson Correlation	.b	.b	.b	.b	.b	-.096	1	.351**	-.008	.107
	Sig. (2-tailed)	.	.	.	.	.	.263		.000	.928	.209
	N	0	0	0	0	0	138	138	138	138	138
var_nei_tillit	Pearson Correlation	.b	.b	.b	.b	.b	-.199*	.351**	1	.304**	.354**
	Sig. (2-tailed)	.	.	.	.	.	.019	.000		.000	.000
	N	0	0	0	0	0	138	138	138	138	138
var_nei_epj_trygg	Pearson Correlation	.b	.b	.b	.b	.b	-.086	-.008	.304**	1	.458**
	Sig. (2-tailed)	.	.	.	.	.	.313	.928	.000		.000
	N	0	0	0	0	0	138	138	138	138	138
var_nei_trygg_bruk	Pearson Correlation	.b	.b	.b	.b	.b	-.099	.107	.354**	.458**	1
	Sig. (2-tailed)	.	.	.	.	.	.248	.209	.000	.000	
	N	0	0	0	0	0	138	138	138	138	138

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

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

b. Cannot be computed because at least one of the variables is constant.

Where is infosec most important?

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_ja_hvor	Female	198	2.68	.510	.036	2.61	2.75	1	3
	Male	44	2.70	.553	.083	2.54	2.87	1	3
	Total	242	2.68	.517	.033	2.62	2.75	1	3
var_nei_hvor	Female	108	2.78	.439	.042	2.69	2.86	1	3
	Male	30	2.67	.606	.111	2.44	2.89	1	3
	Total	138	2.75	.480	.041	2.67	2.83	1	3

Figure 12 Descriptives most important

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_ja_hvor	Between Groups	.028	1	.028	.103	.748
	Within Groups	64.472	240	.269		
	Total	64.500	241			
var_nei_hvor	Between Groups	.290	1	.290	1.258	.264
	Within Groups	31.333	136	.230		
	Total	31.623	137			

Figure 13 One-Way ANOVA most important

Feedback

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_nei_tilbakemelding	Female	108	1.98	.273	.026	1.93	2.03	1	3
	Male	30	1.97	.183	.033	1.90	2.03	1	2
	Total	138	1.98	.255	.022	1.94	2.02	1	3
var_ja_tilbakemeld	Female	198	1.90	.302	.021	1.86	1.94	1	2
	Male	44	1.84	.370	.056	1.73	1.95	1	2
	Total	242	1.89	.315	.020	1.85	1.93	1	2

Figure 14 Description feedback from colleagues

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_nei_tilbakemelding	Between Groups	.005	1	.005	.078	.780
	Within Groups	8.930	136	.066		
	Total	8.935	137			
var_ja_tilbakemeld	Between Groups	.121	1	.121	1.221	.270
	Within Groups	23.866	240	.099		
	Total	23.988	241			

Figure 15 One-Way ANOVA feedback from colleagues

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_nei_gibeskjed	Female	108	2.30	1.355	.130	2.04	2.55	1	6
	Male	30	1.93	.868	.159	1.61	2.26	1	4
	Total	138	2.22	1.271	.108	2.00	2.43	1	6
var_ja_gibeskjed	Female	198	1.94	1.040	.074	1.79	2.09	1	6
	Male	44	1.77	1.031	.155	1.46	2.09	1	6
	Total	242	1.91	1.039	.067	1.78	2.04	1	6

Figure 16 Descriptives comfort level

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_nei_gibeskjed	Between Groups	3.093	1	3.093	1.926	.167
	Within Groups	218.385	136	1.606		
	Total	221.478	137			
var_ja_gibeskjed	Between Groups	1.000	1	1.000	.927	.337
	Within Groups	259.000	240	1.079		
	Total	260.000	241			

Figure 17 One-Way ANOVA comfort level

Correlations

		var_ja_tilbakemeld	var_ja_gibeskjed	var_nei_tilbakemelding	var_nei_gibeskjed
var_ja_tilbakemeld	Pearson Correlation	1	.096	.[a]	.[a]
	Sig. (2-tailed)		.138	.	.
	N	242	242	0	0
var_ja_gibeskjed	Pearson Correlation	.096	1	.[a]	.[a]
	Sig. (2-tailed)	.138		.	.
	N	242	242	0	0
var_nei_tilbakemelding	Pearson Correlation	.[a]	.[a]	1	.105
	Sig. (2-tailed)	.	.		.222
	N	0	0	138	138
var_nei_gibeskjed	Pearson Correlation	.[a]	.[a]	.105	1
	Sig. (2-tailed)	.	.	.222	
	N	0	0	138	138

a. Cannot be computed because at least one of the variables is constant.

Figure 18 Correlations feedback

Online activities and consequences - Risk

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_ja_jobb_epost	Female	198	2.41	.872	.062	2.29	2.53	1	5
	Male	44	2.43	.846	.128	2.17	2.69	1	4
	Total	242	2.41	.866	.056	2.30	2.52	1	5
var_ja_jobb_some	Female	198	3.05	1.105	.079	2.89	3.20	1	5
	Male	44	2.84	.939	.142	2.56	3.13	1	5
	Total	242	3.01	1.078	.069	2.87	3.14	1	5
var_ja_jobb_smart	Female	198	3.20	1.517	.108	2.98	3.41	1	5
	Male	44	2.93	1.388	.209	2.51	3.35	1	5
	Total	242	3.15	1.495	.096	2.96	3.34	1	5
var_ja_jobb_lagring	Female	198	2.89	1.227	.087	2.72	3.07	1	5
	Male	44	2.86	.905	.136	2.59	3.14	1	5
	Total	242	2.89	1.174	.075	2.74	3.04	1	5
var_ja_jobb_sky	Female	198	3.17	1.332	.095	2.98	3.35	1	5
	Male	44	2.89	1.017	.153	2.58	3.20	1	5
	Total	242	3.12	1.283	.082	2.95	3.28	1	5
var_ja_jobb_passord	Female	198	3.55	.980	.070	3.41	3.68	1	5
	Male	44	3.68	.800	.121	3.44	3.93	2	5
	Total	242	3.57	.950	.061	3.45	3.69	1	5

Figure 19 Descriptives Risk work - with training

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_ja_jobb_epost	Between Groups	.019	1	.019	.025	.875
	Within Groups	180.659	240	.753		
	Total	180.678	241			
var_ja_jobb_some	Between Groups	1.506	1	1.506	1.298	.256
	Within Groups	278.477	240	1.160		
	Total	279.983	241			
var_ja_jobb_smart	Between Groups	2.531	1	2.531	1.133	.288
	Within Groups	536.114	240	2.234		
	Total	538.645	241			
var_ja_jobb_lagring	Between Groups	.033	1	.033	.024	.877
	Within Groups	331.955	240	1.383		
	Total	331.988	241			
var_ja_jobb_sky	Between Groups	2.829	1	2.829	1.723	.191
	Within Groups	393.932	240	1.641		
	Total	396.760	241			
var_ja_jobb_passord	Between Groups	.669	1	.669	.742	.390
	Within Groups	216.636	240	.903		
	Total	217.306	241			

Figure 20n One-Way ANOVA Risk work - with training

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_ja_privat_epost	Female	198	2.45	.875	.062	2.33	2.57	1	5
	Male	44	2.23	.937	.141	1.94	2.51	1	4
	Total	242	2.41	.889	.057	2.30	2.52	1	5
var_ja_privat_some	Female	198	2.80	.912	.065	2.67	2.93	1	5
	Male	44	2.57	.974	.147	2.27	2.86	1	4
	Total	242	2.76	.926	.060	2.64	2.87	1	5
var_ja_privat_smart	Female	198	3.08	1.492	.106	2.87	3.29	1	5
	Male	44	2.68	1.290	.194	2.29	3.07	1	5
	Total	242	3.01	1.463	.094	2.82	3.19	1	5
var_ja_privat_lagring	Female	198	2.47	1.237	.088	2.30	2.64	1	5
	Male	44	2.11	.841	.127	1.86	2.37	1	4
	Total	242	2.40	1.181	.076	2.26	2.55	1	5
var_ja_privat_sky	Female	198	2.82	1.281	.091	2.64	3.00	1	5
	Male	44	2.66	1.055	.159	2.34	2.98	1	5
	Total	242	2.79	1.243	.080	2.63	2.95	1	5
var_ja_privat_passord	Female	198	3.34	1.095	.078	3.18	3.49	1	5
	Male	44	3.16	1.119	.169	2.82	3.50	1	5
	Total	242	3.31	1.100	.071	3.17	3.45	1	5

Figure 21 Descriptives Risk home - with training

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_ja_privat_epost	Between Groups	1.778	1	1.778	2.261	.134
	Within Groups	188.722	240	.786		
	Total	190.500	241			
var_ja_privat_some	Between Groups	1.901	1	1.901	2.229	.137
	Within Groups	204.715	240	.853		
	Total	206.616	241			
var_ja_privat_smart	Between Groups	5.731	1	5.731	2.696	.102
	Within Groups	510.253	240	2.126		
	Total	515.983	241			
var_ja_privat_lagring	Between Groups	4.564	1	4.564	3.302	.070
	Within Groups	331.750	240	1.382		
	Total	336.314	241			
var_ja_privat_sky	Between Groups	.911	1	.911	.589	.444
	Within Groups	371.341	240	1.547		
	Total	372.252	241			
var_ja_privat_passord	Between Groups	1.157	1	1.157	.957	.329
	Within Groups	290.215	240	1.209		
	Total	291.372	241			

Figure 22 One-Way ANOVA Risk home - with training

Figure 23Correlation Risk - with training

Correlations

		var_ja_jobb_epost	var_ja_jobb_some	var_ja_jobb_smart	var_ja_jobb_lagring	var_ja_jobb_sky	var_ja_jobb_passord	var_ja_privat_epost	var_ja_privat_some	var_ja_privat_smart	var_ja_privat_lagring	var_ja_privat_sky	var_ja_privat_passord
var_ja_jobb_epost	Pearson Correlation	1	.312**	.119	.221**	.136*	.091	.507**	.302**	.099	.181**	.201**	.080
	Sig. (2-tailed)		.000	.065	.001	.034	.159	.000	.000	.125	.005	.002	.213
	N	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_jobb_some	Pearson Correlation	.312**	1	.349**	.378**	.350**	.340**	.256**	.360**	.239**	.186**	.187**	.246**
	Sig. (2-tailed)	.000		.000	.000	.000	.000	.000	.000	.000	.004	.003	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_jobb_smart	Pearson Correlation	.119	.349**	1	.395**	.437**	.156*	.148*	.209**	.625**	.269**	.312**	.139*
	Sig. (2-tailed)	.065	.000		.000	.000	.015	.022	.001	.000	.000	.000	.031
	N	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_jobb_lagring	Pearson Correlation	.221**	.378**	.395**	1	.491**	.288**	.167**	.181**	.232**	.431**	.291**	.191**
	Sig. (2-tailed)	.001	.000	.000		.000	.000	.009	.005	.000	.000	.000	.003
	N	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_jobb_sky	Pearson Correlation	.136*	.350**	.437**	.491**	1	.218**	.177**	.268**	.364**	.289**	.434**	.160*
	Sig. (2-tailed)	.034	.000	.000	.000		.001	.006	.000	.000	.000	.000	.013
	N	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_jobb_passord	Pearson Correlation	.091	.340**	.156*	.288**	.218**	1	.037	.060	.050	.111	.007	.607**
	Sig. (2-tailed)	.159	.000	.015	.000	.001		.566	.355	.436	.084	.910	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_privat_epost	Pearson Correlation	.507**	.256**	.148*	.167**	.177**	.037	1	.606**	.262**	.411**	.270**	.164*
	Sig. (2-tailed)	.000	.000	.022	.009	.006	.566		.000	.000	.000	.000	.010
	N	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_privat_some	Pearson Correlation	.302**	.360**	.209**	.181**	.268**	.060	.606**	1	.341**	.387**	.388**	.241**
	Sig. (2-tailed)	.000	.000	.001	.005	.000	.355	.000		.000	.000	.000	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_privat_smart	Pearson Correlation	.099	.239**	.625**	.232**	.364**	.050	.262**	.341**	1	.380**	.380**	.063
	Sig. (2-tailed)	.125	.000	.000	.000	.000	.436	.000	.000		.000	.000	.330
	N	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_privat_lagring	Pearson Correlation	.181**	.186**	.269**	.431**	.289**	.111	.411**	.387**	.380**	1	.400**	.265**
	Sig. (2-tailed)	.005	.004	.000	.000	.000	.084	.000	.000	.000		.000	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_privat_sky	Pearson Correlation	.201**	.187**	.312**	.291**	.434**	.007	.270**	.388**	.380**	.400**	1	.093
	Sig. (2-tailed)	.002	.003	.000	.000	.000	.910	.000	.000	.000	.000		.150
	N	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_privat_passord	Pearson Correlation	.080	.246**	.139*	.191**	.160*	.607**	.164*	.241**	.063	.265**	.093	1
	Sig. (2-tailed)	.213	.000	.031	.003	.013	.000	.010	.000	.330	.000	.150	
	N	242	242	242	242	242	242	242	242	242	242	242	242

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

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

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_nei_jobb_epost	Female	108	2.31	1.072	.103	2.10	2.51	1	5
	Male	30	2.33	.661	.121	2.09	2.58	1	3
	Total	138	2.31	.995	.085	2.14	2.48	1	5
var_nei_jobb_some	Female	108	2.80	1.092	.105	2.59	3.00	1	5
	Male	30	2.67	.922	.168	2.32	3.01	1	5
	Total	138	2.77	1.055	.090	2.59	2.95	1	5
var_nei_jobb_smart	Female	108	3.40	1.540	.148	3.10	3.69	1	5
	Male	30	2.73	1.202	.219	2.28	3.18	1	5
	Total	138	3.25	1.495	.127	3.00	3.51	1	5
var_nei_jobb_lagring	Female	108	2.81	1.341	.129	2.56	3.07	1	5
	Male	30	2.80	1.031	.188	2.42	3.18	1	5
	Total	138	2.81	1.276	.109	2.60	3.03	1	5
var_nei_jobb_sky	Female	108	3.14	1.488	.143	2.86	3.42	1	5
	Male	30	2.73	1.230	.225	2.27	3.19	1	5
	Total	138	3.05	1.441	.123	2.81	3.29	1	5
var_nei_jobb_passord	Female	108	3.34	1.153	.111	3.12	3.56	1	5
	Male	30	3.60	.675	.123	3.35	3.85	2	5
	Total	138	3.40	1.071	.091	3.22	3.58	1	5

Figure 24 Descriptive Risk Work - no training

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_nei_jobb_epost	Between Groups	.018	1	.018	.018	.893
	Within Groups	135.583	136	.997		
	Total	135.601	137			
var_nei_jobb_some	Between Groups	.395	1	.395	.353	.554
	Within Groups	152.185	136	1.119		
	Total	152.580	137			
var_nei_jobb_smart	Between Groups	10.377	1	10.377	4.772	.031
	Within Groups	295.746	136	2.175		
	Total	306.123	137			
var_nei_jobb_lagring	Between Groups	.005	1	.005	.003	.955
	Within Groups	223.096	136	1.640		
	Total	223.101	137			
var_nei_jobb_sky	Between Groups	3.862	1	3.862	1.870	.174
	Within Groups	280.783	136	2.065		
	Total	284.645	137			
var_nei_jobb_passord	Between Groups	1.556	1	1.556	1.360	.246
	Within Groups	155.524	136	1.144		
	Total	157.080	137			

Figure 25 One-Way ANOVA Risk work - No training

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_nei_privat_epost	Female	108	2.35	.950	.091	2.17	2.53	1	5
	Male	30	2.50	1.009	.184	2.12	2.88	1	4
	Total	138	2.38	.961	.082	2.22	2.55	1	5
var_nei_privat_some	Female	108	2.65	.998	.096	2.46	2.84	1	5
	Male	30	2.63	1.033	.189	2.25	3.02	1	5
	Total	138	2.64	1.002	.085	2.48	2.81	1	5
var_nei_privat_smart	Female	108	3.19	1.480	.142	2.90	3.47	1	5
	Male	30	2.47	1.008	.184	2.09	2.84	1	5
	Total	138	3.03	1.419	.121	2.79	3.27	1	5
var_nei_privat_lagring	Female	108	2.51	1.398	.134	2.24	2.78	1	5
	Male	30	2.13	.973	.178	1.77	2.50	1	5
	Total	138	2.43	1.323	.113	2.20	2.65	1	5
var_nei_privat_sky	Female	108	2.90	1.394	.134	2.63	3.16	1	5
	Male	30	2.33	.922	.168	1.99	2.68	1	5
	Total	138	2.78	1.324	.113	2.55	3.00	1	5
var_nei_privat_passord	Female	108	3.15	1.281	.123	2.90	3.39	1	5
	Male	30	3.37	1.159	.212	2.93	3.80	1	5
	Total	138	3.20	1.255	.107	2.98	3.41	1	5

Figure 26Descriptives Risk home - no training

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_nei_privat_epost	Between Groups	.515	1	.515	.556	.457
	Within Groups	126.130	136	.927		
	Total	126.645	137			
var_nei_privat_some	Between Groups	.005	1	.005	.005	.943
	Within Groups	137.596	136	1.012		
	Total	137.601	137			
var_nei_privat_smart	Between Groups	12.121	1	12.121	6.250	.014
	Within Groups	263.763	136	1.939		
	Total	275.884	137			
var_nei_privat_lagring	Between Groups	3.318	1	3.318	1.908	.169
	Within Groups	236.457	136	1.739		
	Total	239.775	137			
var_nei_privat_sky	Between Groups	7.490	1	7.490	4.380	.038
	Within Groups	232.546	136	1.710		
	Total	240.036	137			
var_nei_privat_passord	Between Groups	1.121	1	1.121	.710	.401
	Within Groups	214.596	136	1.578		
	Total	215.717	137			

Figure 27 One-Way ANOVA Risk home - no training

Figure 28 Correlation Risk - no training

Correlations

		var_nei_jobb_epost	var_nei_jobb_some	var_nei_jobb_smart	var_nei_jobb_lagring	var_nei_jobb_sky	var_nei_jobb_passord	var_nei_privat_epost	var_nei_privat_some	var_nei_privat_smart	var_nei_privat_lagring	var_nei_privat_sky	var_nei_privat_passord
var_nei_jobb_epost	Pearson Correlation	1	.410**	.148	.271**	.182*	.177*	.477**	.287**	.045	.209*	.142	.074
	Sig. (2-tailed)		.000	.084	.001	.032	.038	.000	.001	.598	.014	.096	.391
	N	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_jobb_some	Pearson Correlation	.410**	1	.463**	.309**	.368**	.315**	.319**	.356**	.365**	.192*	.234**	.183*
	Sig. (2-tailed)	.000		.000	.000	.000	.000	.000	.000	.000	.024	.006	.031
	N	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_jobb_smart	Pearson Correlation	.148	.463**	1	.465**	.448**	.260**	.257**	.290**	.716**	.318**	.435**	.195*
	Sig. (2-tailed)	.084	.000		.000	.000	.002	.002	.001	.000	.000	.000	.022
	N	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_jobb_lagring	Pearson Correlation	.271**	.309**	.465**	1	.501**	.290**	.327**	.290**	.398**	.584**	.385**	.187*
	Sig. (2-tailed)	.001	.000	.000		.000	.001	.000	.001	.000	.000	.000	.028
	N	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_jobb_sky	Pearson Correlation	.182*	.368**	.448**	.501**	1	.237**	.244**	.275**	.392**	.325**	.668**	.136
	Sig. (2-tailed)	.032	.000	.000	.000		.005	.004	.001	.000	.000	.000	.112
	N	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_jobb_passord	Pearson Correlation	.177*	.315**	.260**	.290**	.237**	1	.240**	.187*	.117	.193*	.182*	.458**
	Sig. (2-tailed)	.038	.000	.002	.001	.005		.005	.028	.171	.023	.033	.000
	N	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_privat_epost	Pearson Correlation	.477**	.319**	.257**	.327**	.244**	.240**	1	.643**	.275**	.300**	.286**	.264**
	Sig. (2-tailed)	.000	.000	.002	.000	.004	.005		.000	.001	.000	.001	.002
	N	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_privat_some	Pearson Correlation	.287**	.356**	.290**	.290**	.275**	.187*	.643**	1	.454**	.396**	.468**	.352**
	Sig. (2-tailed)	.001	.000	.001	.001	.001	.028	.000		.000	.000	.000	.000
	N	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_privat_smart	Pearson Correlation	.045	.365**	.716**	.398**	.392**	.117	.275**	.454**	1	.495**	.563**	.230**
	Sig. (2-tailed)	.598	.000	.000	.000	.000	.171	.001	.000		.000	.000	.007
	N	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_privat_lagring	Pearson Correlation	.209*	.192*	.318**	.584**	.325**	.193*	.300**	.396**	.495**	1	.614**	.363**
	Sig. (2-tailed)	.014	.024	.000	.000	.000	.023	.000	.000	.000		.000	.000
	N	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_privat_sky	Pearson Correlation	.142	.234**	.435**	.385**	.668**	.182*	.286**	.468**	.563**	.614**	1	.361**
	Sig. (2-tailed)	.096	.006	.000	.000	.000	.033	.001	.000	.000	.000		.000
	N	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_privat_passord	Pearson Correlation	.074	.183*	.195*	.187*	.136	.458**	.264**	.352**	.230**	.363**	.361**	1
	Sig. (2-tailed)	.391	.031	.022	.028	.112	.000	.002	.000	.007	.000	.000	
	N	138	138	138	138	138	138	138	138	138	138	138	138

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

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

Online activities and consequences – Threats

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_ja_jobb_phishing	Female	103	2.44	.925	.091	2.26	2.62	1	4
	Male	37	2.62	.924	.152	2.31	2.93	1	4
	Total	140	2.49	.925	.078	2.33	2.64	1	4
var_ja_jobb_vishing	Female	155	1.94	.902	.072	1.79	2.08	1	4
	Male	41	1.93	.905	.141	1.64	2.21	1	4
	Total	196	1.93	.901	.064	1.81	2.06	1	4
var_ja_jobb_spearphising	Female	103	2.02	.960	.095	1.83	2.21	1	4
	Male	32	1.91	.963	.170	1.56	2.25	1	4
	Total	135	1.99	.958	.082	1.83	2.16	1	4
var_ja_jobb_losepenge	Female	136	1.96	.969	.083	1.80	2.13	1	4
	Male	42	2.21	1.048	.162	1.89	2.54	1	4
	Total	178	2.02	.991	.074	1.88	2.17	1	4
var_ja_jobb_utpressing	Female	140	1.96	.992	.084	1.80	2.13	1	4
	Male	42	2.19	.969	.149	1.89	2.49	1	4
	Total	182	2.02	.989	.073	1.87	2.16	1	4
var_ja_jobb_exploit	Female	136	2.68	.942	.081	2.52	2.84	1	4
	Male	41	2.54	.977	.153	2.23	2.85	1	4
	Total	177	2.64	.949	.071	2.50	2.78	1	4
var_ja_jobb_ID	Female	151	2.28	1.014	.083	2.12	2.44	1	4
	Male	43	2.12	.823	.125	1.86	2.37	1	4
	Total	194	2.24	.975	.070	2.10	2.38	1	4
var_ja_jobb_supplychain	Female	103	2.31	.919	.091	2.13	2.49	1	4
	Male	37	2.30	.812	.133	2.03	2.57	1	4
	Total	140	2.31	.889	.075	2.16	2.46	1	4
var_ja_jobb_samfunn	Female	141	2.77	.867	.073	2.62	2.91	1	4
	Male	40	2.25	.840	.133	1.98	2.52	1	4
	Total	181	2.65	.885	.066	2.52	2.78	1	4
var_ja_jobb_infrastruktur	Female	154	2.53	1.049	.085	2.36	2.69	1	4
	Male	41	2.34	.855	.133	2.07	2.61	1	4
	Total	195	2.49	1.012	.072	2.34	2.63	1	4

Figure 29 Descriptives Threat work - with training

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_ja_jobb_phishing	Between Groups	.929	1	.929	1.086	.299
	Within Groups	118.043	138	.855		
	Total	118.971	139			
var_ja_jobb_vishing	Between Groups	.002	1	.002	.003	.957
	Within Groups	158.135	194	.815		
	Total	158.138	195			
var_ja_jobb_spearphising	Between Groups	.313	1	.313	.339	.561
	Within Groups	122.680	133	.922		
	Total	122.993	134			
var_ja_jobb_losepenge	Between Groups	2.023	1	2.023	2.071	.152
	Within Groups	171.888	176	.977		
	Total	173.910	177			
var_ja_jobb_utpressing	Between Groups	1.653	1	1.653	1.697	.194
	Within Groups	175.298	180	.974		
	Total	176.951	181			
var_ja_jobb_exploit	Between Groups	.616	1	.616	.683	.410
	Within Groups	157.960	175	.903		
	Total	158.576	176			
var_ja_jobb_ID	Between Groups	.877	1	.877	.921	.338
	Within Groups	182.736	192	.952		
	Total	183.613	193			
var_ja_jobb_supplychain	Between Groups	.005	1	.005	.006	.938
	Within Groups	109.788	138	.796		
	Total	109.793	139			
var_ja_jobb_samfunn	Between Groups	8.295	1	8.295	11.183	.001
	Within Groups	132.777	179	.742		
	Total	141.072	180			
var_ja_jobb_infrastruktur	Between Groups	1.102	1	1.102	1.077	.301
	Within Groups	197.616	193	1.024		
	Total	198.718	194			

Figure 30 One-Way ANOVA Threats work - with training

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_ja_privat_phishing	Female	119	2.29	1.011	.093	2.11	2.48	1	4
	Male	38	2.37	.883	.143	2.08	2.66	1	4
	Total	157	2.31	.980	.078	2.16	2.47	1	4
var_ja_privat_vishing	Female	168	2.24	1.041	.080	2.09	2.40	1	4
	Male	42	1.95	.936	.144	1.66	2.24	1	4
	Total	210	2.19	1.025	.071	2.05	2.33	1	4
var_ja_privat_spearphishing	Female	120	1.68	.881	.080	1.52	1.83	1	4
	Male	34	1.53	.706	.121	1.28	1.78	1	3
	Total	154	1.64	.845	.068	1.51	1.78	1	4
var_ja_privat_losepenge	Female	151	1.90	.978	.080	1.74	2.06	1	4
	Male	42	1.95	.854	.132	1.69	2.22	1	4
	Total	193	1.91	.951	.068	1.78	2.05	1	4
var_ja_privat_utpressing	Female	151	1.88	.959	.078	1.73	2.03	1	4
	Male	42	1.86	.872	.134	1.59	2.13	1	4
	Total	193	1.88	.938	.068	1.74	2.01	1	4
var_ja_privat_exploit	Female	155	2.54	.969	.078	2.38	2.69	1	4
	Male	41	2.61	.919	.143	2.32	2.90	1	4
	Total	196	2.55	.957	.068	2.42	2.69	1	4
var_ja_privat_ID	Female	163	2.20	.957	.075	2.05	2.35	1	4
	Male	43	1.86	.804	.123	1.61	2.11	1	4
	Total	206	2.13	.936	.065	2.00	2.26	1	4
var_ja_privat_supplychain	Female	115	2.07	.943	.088	1.90	2.24	1	4
	Male	38	2.08	.941	.153	1.77	2.39	1	4
	Total	153	2.07	.940	.076	1.92	2.22	1	4
var_ja_privat_samfunn	Female	153	2.37	.978	.079	2.21	2.52	1	4
	Male	42	1.81	.773	.119	1.57	2.05	1	4
	Total	195	2.25	.964	.069	2.11	2.38	1	4
var_ja_privat_infrastruktur	Female	150	2.35	.970	.079	2.20	2.51	1	4
	Male	41	2.10	.944	.147	1.80	2.40	1	4
	Total	191	2.30	.968	.070	2.16	2.44	1	4

Figure 31 Descriptives Threats home - with training

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_ja_privat_phishing	Between Groups	.159	1	.159	.165	.685
	Within Groups	149.548	155	.965		
	Total	149.707	156			
var_ja_privat_vishing	Between Groups	2.858	1	2.858	2.741	.099
	Within Groups	216.899	208	1.043		
	Total	219.757	209			
var_ja_privat_spearphishing	Between Groups	.562	1	.562	.785	.377
	Within Groups	108.796	152	.716		
	Total	109.357	153			
var_ja_privat_losepenge	Between Groups	.088	1	.088	.097	.756
	Within Groups	173.415	191	.908		
	Total	173.503	192			
var_ja_privat_utpressing	Between Groups	.018	1	.018	.021	.886
	Within Groups	168.997	191	.885		
	Total	169.016	192			
var_ja_privat_exploit	Between Groups	.179	1	.179	.195	.660
	Within Groups	178.311	194	.919		
	Total	178.490	195			
var_ja_privat_ID	Between Groups	3.979	1	3.979	4.626	.033
	Within Groups	175.482	204	.860		
	Total	179.461	205			
var_ja_privat_supplychain	Between Groups	.003	1	.003	.003	.958
	Within Groups	134.207	151	.889		
	Total	134.209	152			
var_ja_privat_samfunn	Between Groups	10.205	1	10.205	11.587	.001
	Within Groups	169.979	193	.881		
	Total	180.185	194			
var_ja_privat_infrastruktur	Between Groups	2.106	1	2.106	2.264	.134
	Within Groups	175.883	189	.931		
	Total	177.990	190			

Figure 32 One-Way ANOVA Threats home - with training

Figure 33 Correlation Threats - with training

Correlations

		var_nei_jobb_phishing	var_nei_jobb_vishing	var_nei_jobb_spearphishing	var_nei_jobb_losepenge	var_nei_jobb_utpressing	var_nei_jobb_exploit	var_nei_jobb_ID	var_nei_jobb_supplychain	var_nei_jobb_samfunn	var_nei_jobb_infrastruktur	var_nei_privat_phishing	var_nei_privat_vishing	var_nei_privat_spearphishing	var_nei_privat_losepenge	var_nei_privat_utpressing	var_nei_privat_exploit	var_nei_privat_ID	var_nei_privat_supplychain	var_nei_privat_samfunn	var_nei_privat_infrastruktur
var_nei_jobb_phishing	Pearson Correlation	1	.428**	.424**	.338**	.365**	.562**	.435**	.460**	.329**	.433**	.610**	.420**	.367**	.371**	.382**	.362**	.307**	.416**	.260**	.400**
	Sig. (2-tailed)		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.002	.000
	N	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_jobb_vishing	Pearson Correlation	.428**	1	.499**	.532**	.535**	.501**	.492**	.463**	.419**	.502**	.401**	.536**	.389**	.485**	.467**	.429**	.363**	.532**	.398**	.398**
	Sig. (2-tailed)	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_jobb_spearphishing	Pearson Correlation	.424**	.499**	1	.651**	.659**	.536**	.445**	.637**	.433**	.457**	.477**	.439**	.691**	.504**	.524**	.403**	.355**	.629**	.380**	.404**
	Sig. (2-tailed)	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_jobb_losepenge	Pearson Correlation	.338**	.532**	.651**	1	.915**	.600**	.503**	.670**	.434**	.484**	.361**	.362**	.459**	.536**	.539**	.352**	.379**	.572**	.350**	.296**
	Sig. (2-tailed)	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_jobb_utpressing	Pearson Correlation	.365**	.535**	.659**	.915**	1	.613**	.494**	.674**	.489**	.500**	.399**	.380**	.466**	.516**	.542**	.344**	.399**	.611**	.382**	.307**
	Sig. (2-tailed)	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_jobb_exploit	Pearson Correlation	.562**	.501**	.536**	.600**	.613**	1	.669**	.645**	.485**	.559**	.438**	.521**	.382**	.423**	.440**	.548**	.453**	.482**	.395**	.417**
	Sig. (2-tailed)	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_jobb_ID	Pearson Correlation	.435**	.492**	.445**	.503**	.494**	.669**	1	.543**	.586**	.585**	.308**	.382**	.319**	.400**	.422**	.512**	.556**	.386**	.446**	.434**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_jobb_supplychain	Pearson Correlation	.460**	.463**	.637**	.670**	.674**	.645**	.543**	1	.516**	.603**	.428**	.400**	.521**	.449**	.450**	.466**	.361**	.716**	.434**	.452**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_jobb_samfunn	Pearson Correlation	.329**	.419**	.433**	.434**	.489**	.485**	.586**	.516**	1	.687**	.333**	.390**	.342**	.398**	.410**	.420**	.437**	.465**	.675**	.534**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_jobb_infrastruktur	Pearson Correlation	.433**	.502**	.457**	.484**	.500**	.559**	.585**	.603**	.687**	1	.328**	.455**	.296**	.378**	.394**	.489**	.497**	.547**	.560**	.680**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_privat_phishing	Pearson Correlation	.610**	.401**	.477**	.361**	.399**	.438**	.308**	.428**	.333**	.328**	1	.645**	.618**	.595**	.604**	.595**	.530**	.577**	.496**	.471**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_privat_vishing	Pearson Correlation	.420**	.536**	.439**	.362**	.380**	.521**	.382**	.400**	.390**	.455**	.645**	1	.666**	.675**	.675**	.654**	.537**	.543**	.598**	.522**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000
	N	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_privat_spearphishing	Pearson Correlation	.367**	.389**	.691**	.459**	.466**	.382**	.319**	.521**	.342**	.296**	.618**	.666**	1	.734**	.739**	.571**	.469**	.625**	.512**	.390**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000
	N	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_privat_losepenge	Pearson Correlation	.371**	.485**	.504**	.536**	.516**	.423**	.400**	.449**	.398**	.378**	.595**	.675**	.734**	1	.976**	.681**	.616**	.606**	.553**	.514**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000
	N	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_privat_utpressing	Pearson Correlation	.382**	.467**	.524**	.539**	.542**	.440**	.422**	.450**	.410**	.394**	.604**	.675**	.739**	.976**	1	.704**	.645**	.622**	.562**	.519**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000
	N	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_privat_exploit	Pearson Correlation	.362**	.429**	.403**	.352**	.344**	.548**	.512**	.466**	.420**	.489**	.595**	.654**	.571**	.681**	.704**	1	.713**	.660**	.697**	.635**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000
	N	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_privat_ID	Pearson Correlation	.307**	.363**	.355**	.379**	.399**	.453**	.556**	.361**	.437**	.497**	.530**	.537**	.469**	.616**	.645**	.713**	1	.538**	.620**	.570**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000
	N	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_privat_supplychain	Pearson Correlation	.416**	.532**	.629**	.572**	.611**	.482**	.386**	.716**	.465**	.547**	.577**	.543**	.625**	.606**	.622**	.660**	.538**	1	.588**	.580**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000
	N	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_privat_samfunn	Pearson Correlation	.260**	.398**	.380**	.350**	.382**	.395**	.446**	.434**	.675**	.560**	.496**	.598**	.512**	.553**	.562**	.697**	.620**	.588**	1	.705**
	Sig. (2-tailed)	.002	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000
	N	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_privat_infrastruktur	Pearson Correlation	.400**	.398**	.404**	.296**	.307**	.417**	.434**	.452**	.534**	.680**	.471**	.522**	.390**	.514**	.519**	.635**	.570**	.580**	.705**	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	
	N	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138	138

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

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_nei_jobb_phishing	Female	46	2.30	1.008	.149	2.00	2.60	1	4
	Male	22	2.50	.859	.183	2.12	2.88	1	4
	Total	68	2.37	.960	.116	2.14	2.60	1	4
var_nei_jobb_vishing	Female	80	1.74	.853	.095	1.55	1.93	1	4
	Male	25	1.48	.653	.131	1.21	1.75	1	3
	Total	105	1.68	.814	.079	1.52	1.83	1	4
var_nei_jobb_spearphishing	Female	51	1.73	.918	.129	1.47	1.98	1	4
	Male	17	1.65	.702	.170	1.29	2.01	1	3
	Total	68	1.71	.865	.105	1.50	1.92	1	4
var_nei_jobb_losepenge	Female	65	1.86	.982	.122	1.62	2.10	1	4
	Male	23	1.96	.878	.183	1.58	2.34	1	4
	Total	88	1.89	.952	.101	1.68	2.09	1	4
var_nei_jobb_utpressing	Female	64	1.88	.984	.123	1.63	2.12	1	4
	Male	22	1.95	.999	.213	1.51	2.40	1	4
	Total	86	1.90	.983	.106	1.68	2.11	1	4
var_nei_jobb_exploit	Female	69	2.45	.978	.118	2.21	2.68	1	4
	Male	24	2.46	.932	.190	2.06	2.85	1	4
	Total	93	2.45	.961	.100	2.25	2.65	1	4
var_nei_jobb_ID	Female	78	2.06	.888	.101	1.86	2.26	1	4
	Male	26	2.35	1.018	.200	1.94	2.76	1	4
	Total	104	2.13	.925	.091	1.95	2.31	1	4
var_nei_jobb_supplychain	Female	53	2.21	.948	.130	1.95	2.47	1	4
	Male	19	2.11	.994	.228	1.63	2.58	1	4
	Total	72	2.18	.954	.112	1.96	2.40	1	4
var_nei_jobb_samfunn	Female	74	2.50	.983	.114	2.27	2.73	1	4
	Male	27	2.56	.974	.187	2.17	2.94	1	4
	Total	101	2.51	.976	.097	2.32	2.71	1	4
var_nei_jobb_infrastruktur	Female	74	2.27	.941	.109	2.05	2.49	1	4
	Male	26	2.35	.936	.183	1.97	2.72	1	4
	Total	100	2.29	.935	.094	2.10	2.48	1	4

Figure 34Descriptives Threats work - no training

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_nei_jobb_phishing	Between Groups	.570	1	.570	.614	.436
	Within Groups	61.239	66	.928		
	Total	61.809	67			
var_nei_jobb_vishing	Between Groups	1.263	1	1.263	1.921	.169
	Within Groups	67.728	103	.658		
	Total	68.990	104			
var_nei_jobb_spearphishing	Between Groups	.078	1	.078	.103	.749
	Within Groups	50.039	66	.758		
	Total	50.118	67			
var_nei_jobb_losepenge	Between Groups	.153	1	.153	.167	.683
	Within Groups	78.710	86	.915		
	Total	78.864	87			
var_nei_jobb_utpressing	Between Groups	.104	1	.104	.106	.745
	Within Groups	81.955	84	.976		
	Total	82.058	85			
var_nei_jobb_exploit	Between Groups	.001	1	.001	.002	.969
	Within Groups	85.031	91	.934		
	Total	85.032	92			
var_nei_jobb_ID	Between Groups	1.551	1	1.551	1.828	.179
	Within Groups	86.564	102	.849		
	Total	88.115	103			
var_nei_jobb_supplychain	Between Groups	.146	1	.146	.159	.691
	Within Groups	64.506	70	.922		
	Total	64.653	71			
var_nei_jobb_samfunn	Between Groups	.061	1	.061	.064	.802
	Within Groups	95.167	99	.961		
	Total	95.228	100			
var_nei_jobb_infrastruktur	Between Groups	.111	1	.111	.126	.724
	Within Groups	86.479	98	.882		
	Total	86.590	99			

Figure 35 One-Way ANOVA Threats work - no training

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_nei_privat_phishing	Female	60	2.17	1.028	.133	1.90	2.43	1	4
	Male	24	2.38	.824	.168	2.03	2.72	1	4
	Total	84	2.23	.974	.106	2.01	2.44	1	4
var_nei_privat_vishing	Female	85	2.11	1.012	.110	1.89	2.32	1	4
	Male	28	1.71	.763	.144	1.42	2.01	1	4
	Total	113	2.01	.968	.091	1.83	2.19	1	4
var_nei_privat_spearphishing	Female	58	1.66	1.001	.131	1.39	1.92	1	4
	Male	22	1.59	.796	.170	1.24	1.94	1	4
	Total	80	1.64	.945	.106	1.43	1.85	1	4
var_nei_privat_losepenge	Female	71	1.80	1.037	.123	1.56	2.05	1	4
	Male	28	1.89	.832	.157	1.57	2.22	1	4
	Total	99	1.83	.980	.098	1.63	2.02	1	4
var_nei_privat_utpressing	Female	70	1.79	1.034	.124	1.54	2.03	1	4
	Male	28	1.96	.838	.158	1.64	2.29	1	4
	Total	98	1.84	.981	.099	1.64	2.03	1	4
var_nei_privat_exploit	Female	80	2.53	.993	.111	2.30	2.75	1	4
	Male	27	2.56	.934	.180	2.19	2.92	1	4
	Total	107	2.53	.974	.094	2.35	2.72	1	4
var_nei_privat_ID	Female	81	2.25	.956	.106	2.04	2.46	1	4
	Male	30	2.47	.900	.164	2.13	2.80	1	4
	Total	111	2.31	.942	.089	2.13	2.48	1	4
var_nei_privat_supplychain	Female	57	2.05	1.042	.138	1.78	2.33	1	4
	Male	21	2.33	.913	.199	1.92	2.75	1	4
	Total	78	2.13	1.011	.114	1.90	2.36	1	4
var_nei_privat_samfunn	Female	78	2.23	1.056	.120	1.99	2.47	1	4
	Male	27	2.15	.818	.157	1.82	2.47	1	4
	Total	105	2.21	.997	.097	2.02	2.40	1	4
var_nei_privat_infrastruktur	Female	74	2.16	.980	.114	1.94	2.39	1	4
	Male	29	2.31	.967	.180	1.94	2.68	1	4
	Total	103	2.20	.974	.096	2.01	2.39	1	4

Figure 36 Descriptives Threats home - no training

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_nei_privat_phishing	Between Groups	.744	1	.744	.783	.379
	Within Groups	77.958	82	.951		
	Total	78.702	83			
var_nei_privat_vishing	Between Groups	3.230	1	3.230	3.523	.063
	Within Groups	101.761	111	.917		
	Total	104.991	112			
var_nei_privat_spearphishing	Between Groups	.066	1	.066	.073	.788
	Within Groups	70.422	78	.903		
	Total	70.487	79			
var_nei_privat_losepenge	Between Groups	.163	1	.163	.168	.683
	Within Groups	93.918	97	.968		
	Total	94.081	98			
var_nei_privat_utpressing	Between Groups	.638	1	.638	.660	.419
	Within Groups	92.750	96	.966		
	Total	93.388	97			
var_nei_privat_exploit	Between Groups	.019	1	.019	.020	.889
	Within Groups	100.617	105	.958		
	Total	100.636	106			
var_nei_privat_ID	Between Groups	1.057	1	1.057	1.194	.277
	Within Groups	96.528	109	.886		
	Total	97.586	110			
var_nei_privat_supplychain	Between Groups	1.209	1	1.209	1.186	.280
	Within Groups	77.509	76	1.020		
	Total	78.718	77			
var_nei_privat_samfunn	Between Groups	.137	1	.137	.137	.712
	Within Groups	103.254	103	1.002		
	Total	103.390	104			
var_nei_privat_infrastruktur	Between Groups	.457	1	.457	.480	.490
	Within Groups	96.261	101	.953		
	Total	96.718	102			

Figure 37One-Way ANOVA Threats home - no training

Figure 38 Correlation Threats - no training

Correlations

		var_ja_privat_phishing	var_ja_privat_vishing	var_ja_privat_spearphishing	var_ja_privat_losepenge	var_ja_privat_utpressing	var_ja_privat_exploit	var_ja_privat_ID	var_ja_privat_supplychain	var_ja_privat_samfunn	var_ja_privat_infrastruktur	var_ja_jobb_phishing	var_ja_jobb_vishing	var_ja_jobb_spearphising	var_ja_jobb_losepenge	var_ja_jobb_utpressing	var_ja_jobb_exploit	var_ja_jobb_ID	var_ja_jobb_supplychain	var_ja_jobb_samfunn	var_ja_jobb_infrastruktur
var_ja_privat_phishing	Pearson Correlation	1	.551**	.570**	.495**	.511**	.528**	.408**	.569**	.479**	.356**	.674**	.447**	.499**	.458**	.513**	.336**	.253**	.508**	.392**	.266**
	Sig. (2-tailed)		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_privat_vishing	Pearson Correlation	.551**	1	.546**	.595**	.613**	.509**	.525**	.470**	.566**	.401**	.343**	.466**	.318**	.350**	.386**	.240**	.309**	.264**	.323**	.347**
	Sig. (2-tailed)	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_privat_spearphishing	Pearson Correlation	.570**	.546**	1	.676**	.670**	.547**	.443**	.530**	.462**	.424**	.449**	.481**	.612**	.544**	.539**	.388**	.322**	.400**	.343**	.345**
	Sig. (2-tailed)	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_privat_losepenge	Pearson Correlation	.495**	.595**	.676**	1	.934**	.614**	.528**	.494**	.577**	.501**	.359**	.459**	.392**	.645**	.651**	.433**	.403**	.350**	.387**	.420**
	Sig. (2-tailed)	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_privat_utpressing	Pearson Correlation	.511**	.613**	.670**	.934**	1	.627**	.540**	.482**	.578**	.513**	.353**	.456**	.395**	.595**	.645**	.413**	.398**	.332**	.389**	.418**
	Sig. (2-tailed)	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_privat_exploit	Pearson Correlation	.528**	.509**	.547**	.614**	.627**	1	.616**	.642**	.602**	.594**	.400**	.369**	.410**	.383**	.413**	.507**	.454**	.409**	.493**	.436**
	Sig. (2-tailed)	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_privat_ID	Pearson Correlation	.408**	.525**	.443**	.528**	.540**	.616**	1	.512**	.589**	.625**	.318**	.278**	.266**	.340**	.382**	.371**	.632**	.304**	.416**	.415**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_privat_supplychain	Pearson Correlation	.569**	.470**	.530**	.494**	.482**	.642**	.512**	1	.551**	.554**	.458**	.403**	.426**	.399**	.432**	.384**	.392**	.644**	.460**	.441**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_privat_samfunn	Pearson Correlation	.479**	.566**	.462**	.577**	.578**	.602**	.589**	.551**	1	.635**	.317**	.386**	.345**	.378**	.441**	.368**	.436**	.350**	.595**	.523**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_privat_infrastruktur	Pearson Correlation	.356**	.401**	.424**	.501**	.513**	.594**	.625**	.554**	.635**	1	.296**	.293**	.235**	.331**	.379**	.374**	.444**	.385**	.546**	.617**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_jobb_phishing	Pearson Correlation	.674**	.343**	.449**	.359**	.353**	.400**	.318**	.458**	.317**	.296**	1	.475**	.586**	.517**	.520**	.451**	.328**	.548**	.398**	.307**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_jobb_vishing	Pearson Correlation	.447**	.466**	.481**	.459**	.456**	.369**	.278**	.403**	.386**	.293**	.475**	1	.518**	.580**	.598**	.415**	.334**	.455**	.332**	.416**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_jobb_spearphising	Pearson Correlation	.499**	.318**	.612**	.392**	.395**	.410**	.266**	.426**	.345**	.235**	.586**	.518**	1	.610**	.601**	.500**	.362**	.534**	.423**	.371**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_jobb_losepenge	Pearson Correlation	.458**	.350**	.544**	.645**	.595**	.383**	.340**	.399**	.378**	.331**	.517**	.580**	.610**	1	.918**	.550**	.432**	.474**	.418**	.487**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_jobb_utpressing	Pearson Correlation	.513**	.386**	.539**	.651**	.645**	.413**	.382**	.432**	.441**	.379**	.520**	.598**	.601**	.918**	1	.571**	.453**	.509**	.446**	.472**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_jobb_exploit	Pearson Correlation	.336**	.240**	.388**	.433**	.413**	.507**	.371**	.384**	.368**	.374**	.451**	.415**	.500**	.550**	.571**	1	.546**	.527**	.515**	.401**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_jobb_ID	Pearson Correlation	.253**	.309**	.322**	.403**	.398**	.454**	.632**	.392**	.436**	.444**	.328**	.334**	.362**	.432**	.453**	.546**	1	.452**	.482**	.529**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_jobb_supplychain	Pearson Correlation	.508**	.264**	.400**	.350**	.332**	.409**	.304**	.644**	.350**	.385**	.548**	.455**	.534**	.474**	.509**	.527**	.452**	1	.537**	.473**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_jobb_samfunn	Pearson Correlation	.392**	.323**	.343**	.387**	.389**	.493**	.416**	.460**	.595**	.546**	.398**	.332**	.423**	.418**	.446**	.515**	.482**	.537**	1	.563**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000
	N	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_jobb_infrastruktur	Pearson Correlation	.266**	.347**	.345**	.420**	.418**	.436**	.415**	.441**	.523**	.617**	.307**	.416**	.371**	.487**	.472**	.401**	.529**	.473**	.563**	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	
	N	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242	242

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

Part 2 - Views on management and control in the workplace

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_ja_oversikt	Female	198	3.21	.680	.048	3.12	3.31	1	5
	Male	44	2.95	.608	.092	2.77	3.14	2	4
	Total	242	3.17	.674	.043	3.08	3.25	1	5
var_ja_hinder	Female	198	1.68	.840	.060	1.56	1.80	1	5
	Male	44	1.98	.821	.124	1.73	2.23	1	5
	Total	242	1.74	.843	.054	1.63	1.84	1	5
var_ja_forandret_fokus	Female	198	2.30	.981	.070	2.16	2.44	1	5
	Male	44	2.16	.834	.126	1.91	2.41	1	4
	Total	242	2.27	.955	.061	2.15	2.39	1	5
var_ja_prosedyre	Female	198	2.55	1.138	.081	2.39	2.71	1	5
	Male	44	2.23	.937	.141	1.94	2.51	1	4
	Total	242	2.49	1.109	.071	2.35	2.63	1	5
var_ja_retningslinjer	Female	198	3.03	.958	.068	2.89	3.16	1	5
	Male	44	2.84	.939	.142	2.56	3.13	1	5
	Total	242	2.99	.955	.061	2.87	3.11	1	5
var_ja_krav	Female	198	3.28	.848	.060	3.16	3.40	1	5
	Male	44	2.91	.960	.145	2.62	3.20	1	5
	Total	242	3.21	.879	.057	3.10	3.32	1	5
var_ja_konsekvens	Female	198	3.67	.628	.045	3.58	3.76	1	5
	Male	44	3.48	.698	.105	3.26	3.69	2	4
	Total	242	3.64	.644	.041	3.55	3.72	1	5

Figure 39 Descriptives views on management and control at work – with training

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_ja_oversikt	Between Groups	2.388	1	2.388	5.357	.021
	Within Groups	107.000	240	.446		
	Total	109.388	241			
var_ja_hinder	Between Groups	3.143	1	3.143	4.491	.035
	Within Groups	167.932	240	.700		
	Total	171.074	241			
var_ja_forandret_fokus	Between Groups	.694	1	.694	.760	.384
	Within Groups	219.306	240	.914		
	Total	220.000	241			
var_ja_prosedyre	Between Groups	3.761	1	3.761	3.084	.080
	Within Groups	292.722	240	1.220		
	Total	296.483	241			
var_ja_retningslinjer	Between Groups	1.223	1	1.223	1.342	.248
	Within Groups	218.760	240	.912		
	Total	219.983	241			
var_ja_krav	Between Groups	4.893	1	4.893	6.476	.012
	Within Groups	181.359	240	.756		
	Total	186.252	241			
var_ja_konsekvens	Between Groups	1.361	1	1.361	3.312	.070
	Within Groups	98.639	240	.411		
	Total	100.000	241			

Figure 40 One-Way ANOVA views on control and management at work – with training

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_nei_oversikt	Female	108	2.55	.990	.095	2.36	2.74	1	5
	Male	30	2.57	.728	.133	2.29	2.84	1	4
	Total	138	2.55	.936	.080	2.39	2.71	1	5
var_nei_hinder	Female	108	2.17	1.411	.136	1.90	2.44	1	5
	Male	30	1.90	1.094	.200	1.49	2.31	1	5
	Total	138	2.11	1.349	.115	1.88	2.34	1	5
var_nei_forandret_fokus	Female	108	2.25	1.128	.109	2.03	2.47	1	5
	Male	30	2.23	1.135	.207	1.81	2.66	1	5
	Total	138	2.25	1.126	.096	2.06	2.44	1	5
var_nei_prosedyre	Female	108	1.84	1.034	.099	1.65	2.04	1	5
	Male	30	1.87	.937	.171	1.52	2.22	1	5
	Total	138	1.85	1.010	.086	1.68	2.02	1	5
var_nei_retningslinjer	Female	108	2.53	1.315	.126	2.28	2.78	1	5
	Male	30	2.23	1.194	.218	1.79	2.68	1	5
	Total	138	2.46	1.291	.110	2.25	2.68	1	5
var_nei_krav	Female	108	2.67	1.085	.104	2.46	2.87	1	5
	Male	30	2.23	1.006	.184	1.86	2.61	1	5
	Total	138	2.57	1.080	.092	2.39	2.75	1	5
var_nei_konsekvens	Female	108	3.51	.755	.073	3.37	3.65	1	4
	Male	30	3.67	.758	.138	3.38	3.95	1	4
	Total	138	3.54	.756	.064	3.42	3.67	1	4

Figure 41 Descriptives views on management and control at work - no training

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_nei_oversikt	Between Groups	.010	1	.010	.011	.917
	Within Groups	120.135	136	.883		
	Total	120.145	137			
var_nei_hinder	Between Groups	1.670	1	1.670	.917	.340
	Within Groups	247.700	136	1.821		
	Total	249.370	137			
var_nei_forandret_fokus	Between Groups	.007	1	.007	.005	.943
	Within Groups	173.617	136	1.277		
	Total	173.623	137			
var_nei_prosedyre	Between Groups	.014	1	.014	.013	.909
	Within Groups	139.791	136	1.028		
	Total	139.804	137			
var_nei_retningslinjer	Between Groups	2.036	1	2.036	1.223	.271
	Within Groups	226.283	136	1.664		
	Total	228.319	137			
var_nei_krav	Between Groups	4.409	1	4.409	3.859	.052
	Within Groups	155.367	136	1.142		
	Total	159.775	137			
var_nei_konsekvens	Between Groups	.582	1	.582	1.019	.315
	Within Groups	77.657	136	.571		
	Total	78.239	137			

Figure 42 One-Way Anova views on management and control at work - no training

Descriptives

var_ja_bevisst_brudd

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Female	198	2.01	.363	.026	1.96	2.06	1	3
Male	44	1.77	.476	.072	1.63	1.92	1	3
Total	242	1.97	.396	.025	1.92	2.02	1	3

Figure 43 Descriptives knowingly broken protocol - with training

ANOVA

var_ja_bevisst_brudd

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	2.028	1	2.028	13.634	.000
Within Groups	35.707	240	.149		
Total	37.736	241			

Figure 44 One-Way ANOVA knowingly broken protocol - with training

Correlations

		var_ja_oversikt	var_ja_hinder	var_ja_forandret_fokus	var_ja_prosedyre	var_ja_retningslinjer	var_ja_krav	var_ja_konsekvens	var_ja_bevisst_brudd
var_ja_oversikt	Pearson Correlation	1	-.157*	.020	.346**	.453**	.375**	.263**	-.026
	Sig. (2-tailed)		.015	.758	.000	.000	.000	.000	.686
	N	242	242	242	242	242	242	242	242
var_ja_hinder	Pearson Correlation	-.157*	1	.085	-.051	-.126*	-.093	-.040	-.089
	Sig. (2-tailed)	.015		.189	.428	.049	.151	.533	.170
	N	242	242	242	242	242	242	242	242
var_ja_forandret_fokus	Pearson Correlation	.020	.085	1	.304**	.062	.134*	.088	.046
	Sig. (2-tailed)	.758	.189		.000	.340	.037	.174	.477
	N	242	242	242	242	242	242	242	242
var_ja_prosedyre	Pearson Correlation	.346**	-.051	.304**	1	.497**	.344**	.222**	.113
	Sig. (2-tailed)	.000	.428	.000		.000	.000	.000	.080
	N	242	242	242	242	242	242	242	242
var_ja_retningslinjer	Pearson Correlation	.453**	-.126*	.062	.497**	1	.615**	.184**	-.001
	Sig. (2-tailed)	.000	.049	.340	.000		.000	.004	.991
	N	242	242	242	242	242	242	242	242
var_ja_krav	Pearson Correlation	.375**	-.093	.134*	.344**	.615**	1	.143*	.020
	Sig. (2-tailed)	.000	.151	.037	.000	.000		.026	.756
	N	242	242	242	242	242	242	242	242
var_ja_konsekvens	Pearson Correlation	.263**	-.040	.088	.222**	.184**	.143*	1	-.015
	Sig. (2-tailed)	.000	.533	.174	.000	.004	.026		.819
	N	242	242	242	242	242	242	242	242
var_ja_bevisst_brudd	Pearson Correlation	-.026	-.089	.046	.113	-.001	.020	-.015	1
	Sig. (2-tailed)	.686	.170	.477	.080	.991	.756	.819	
	N	242	242	242	242	242	242	242	242

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

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

Figure 45 correlation management, control and protocol - with training

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_nei_oversikt	Female	108	2.55	.990	.095	2.36	2.74	1	5
	Male	30	2.57	.728	.133	2.29	2.84	1	4
	Total	138	2.55	.936	.080	2.39	2.71	1	5
var_nei_hinder	Female	108	2.17	1.411	.136	1.90	2.44	1	5
	Male	30	1.90	1.094	.200	1.49	2.31	1	5
	Total	138	2.11	1.349	.115	1.88	2.34	1	5
var_nei_forandret_fokus	Female	108	2.25	1.128	.109	2.03	2.47	1	5
	Male	30	2.23	1.135	.207	1.81	2.66	1	5
	Total	138	2.25	1.126	.096	2.06	2.44	1	5
var_nei_prosedyre	Female	108	1.84	1.034	.099	1.65	2.04	1	5
	Male	30	1.87	.937	.171	1.52	2.22	1	5
	Total	138	1.85	1.010	.086	1.68	2.02	1	5
var_nei_retningslinjer	Female	108	2.53	1.315	.126	2.28	2.78	1	5
	Male	30	2.23	1.194	.218	1.79	2.68	1	5
	Total	138	2.46	1.291	.110	2.25	2.68	1	5
var_nei_krav	Female	108	2.67	1.085	.104	2.46	2.87	1	5
	Male	30	2.23	1.006	.184	1.86	2.61	1	5
	Total	138	2.57	1.080	.092	2.39	2.75	1	5
var_nei_konsekvens	Female	108	3.51	.755	.073	3.37	3.65	1	4
	Male	30	3.67	.758	.138	3.38	3.95	1	4
	Total	138	3.54	.756	.064	3.42	3.67	1	4

Figure 46 Descriptives Views on management and control at work - no training

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_nei_oversikt	Between Groups	.010	1	.010	.011	.917
	Within Groups	120.135	136	.883		
	Total	120.145	137			
var_nei_hinder	Between Groups	1.670	1	1.670	.917	.340
	Within Groups	247.700	136	1.821		
	Total	249.370	137			
var_nei_forandret_fokus	Between Groups	.007	1	.007	.005	.943
	Within Groups	173.617	136	1.277		
	Total	173.623	137			
var_nei_prosedyre	Between Groups	.014	1	.014	.013	.909
	Within Groups	139.791	136	1.028		
	Total	139.804	137			
var_nei_retningslinjer	Between Groups	2.036	1	2.036	1.223	.271
	Within Groups	226.283	136	1.664		
	Total	228.319	137			
var_nei_krav	Between Groups	4.409	1	4.409	3.859	.052
	Within Groups	155.367	136	1.142		
	Total	159.775	137			
var_nei_konsekvens	Between Groups	.582	1	.582	1.019	.315
	Within Groups	77.657	136	.571		
	Total	78.239	137			

Figure 47 One-Way ANOVA views on management and control at work - no training

Descriptives

var_nei_bevisst_brudd

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Female	108	2.00	.362	.035	1.93	2.07	1	3
Male	30	2.13	.507	.093	1.94	2.32	1	3
Total	138	2.03	.400	.034	1.96	2.10	1	3

Figure 48 Descriptives knowingly broken protocol - no training

ANOVA

var_nei_bevisst_brudd

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	.417	1	.417	2.644	.106
Within Groups	21.467	136	.158		
Total	21.884	137			

Figure 49 One-way ANOVA knowingly broken protocol - no training

Correlations

		var_nei_oversikt	var_nei_hinder	var_nei_forandret_fokus	var_nei_prosedyre	var_nei_retningslinjer	var_nei_krav	var_nei_konsekvens	var_nei_bevisst_brudd
var_nei_oversikt	Pearson Correlation	1	-.157	-.012	.213*	.155	.184*	.152	.094
	Sig. (2-tailed)		.065	.889	.012	.069	.031	.076	.275
	N	138	138	138	138	138	138	138	138
var_nei_hinder	Pearson Correlation	-.157	1	.381**	-.031	-.021	.092	-.151	.075
	Sig. (2-tailed)	.065		.000	.721	.809	.282	.076	.380
	N	138	138	138	138	138	138	138	138
var_nei_forandret_fokus	Pearson Correlation	-.012	.381**	1	.168*	-.064	.201*	.004	-.065
	Sig. (2-tailed)	.889	.000		.049	.455	.018	.958	.451
	N	138	138	138	138	138	138	138	138
var_nei_prosedyre	Pearson Correlation	.213*	-.031	.168*	1	.256**	.261**	.243**	.011
	Sig. (2-tailed)	.012	.721	.049		.002	.002	.004	.898
	N	138	138	138	138	138	138	138	138
var_nei_retningslinjer	Pearson Correlation	.155	-.021	-.064	.256**	1	.473**	.196*	.044
	Sig. (2-tailed)	.069	.809	.455	.002		.000	.021	.604
	N	138	138	138	138	138	138	138	138
var_nei_krav	Pearson Correlation	.184*	.092	.201*	.261**	.473**	1	.171*	-.106
	Sig. (2-tailed)	.031	.282	.018	.002	.000		.046	.214
	N	138	138	138	138	138	138	138	138
var_nei_konsekvens	Pearson Correlation	.152	-.151	.004	.243**	.196*	.171*	1	-.077
	Sig. (2-tailed)	.076	.076	.958	.004	.021	.046		.371
	N	138	138	138	138	138	138	138	138
var_nei_bevisst_brudd	Pearson Correlation	.094	.075	-.065	.011	.044	-.106	-.077	1
	Sig. (2-tailed)	.275	.380	.451	.898	.604	.214	.371	
	N	138	138	138	138	138	138	138	138

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

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

Figure 50 correlation management, control and protocol - no training

Part 3 - Behaviour

Online behaviour with training

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_ja__jobb_nettside	Female	198	2.43	1.014	.072	2.29	2.58	1	5
	Male	44	2.80	1.069	.161	2.47	3.12	1	5
	Total	242	2.50	1.032	.066	2.37	2.63	1	5
var_ja_jobb_linker	Female	198	1.88	.935	.066	1.75	2.01	1	5
	Male	44	1.98	1.023	.154	1.67	2.29	1	4
	Total	242	1.90	.950	.061	1.78	2.02	1	5
var_ja_jobb_avsender	Female	198	1.79	.926	.066	1.66	1.92	1	4
	Male	44	1.98	1.067	.161	1.65	2.30	1	4
	Total	242	1.82	.954	.061	1.70	1.94	1	4
var_ja_jobb_laaser_loggerut	Female	198	1.48	.602	.043	1.40	1.57	1	3
	Male	44	1.70	.904	.136	1.43	1.98	1	4
	Total	242	1.52	.671	.043	1.44	1.61	1	4
var_ja_jobb_private_enheter	Female	198	3.45	.815	.058	3.34	3.56	1	5
	Male	44	3.18	.995	.150	2.88	3.48	1	4
	Total	242	3.40	.855	.055	3.29	3.51	1	5
var_ja_jobb_rapport	Female	198	2.70	1.317	.094	2.51	2.88	1	5
	Male	44	2.77	1.292	.195	2.38	3.17	1	5
	Total	242	2.71	1.310	.084	2.54	2.88	1	5

Figure 51 Descriptives Behaviour at work - with training

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_ja__jobb_nettside	Between Groups	4.694	1	4.694	4.474	.035
	Within Groups	251.806	240	1.049		
	Total	256.500	241			
var_ja_jobb_linker	Between Groups	.314	1	.314	.347	.556
	Within Groups	217.306	240	.905		
	Total	217.620	241			
var_ja_jobb_avsender	Between Groups	1.291	1	1.291	1.421	.234
	Within Groups	218.068	240	.909		
	Total	219.360	241			
var_ja_jobb_laaser_loggerut	Between Groups	1.738	1	1.738	3.912	.049
	Within Groups	106.614	240	.444		
	Total	108.351	241			
var_ja_jobb_private_enheter	Between Groups	2.579	1	2.579	3.567	.060
	Within Groups	173.540	240	.723		
	Total	176.120	241			
var_ja_jobb_rapport	Between Groups	.207	1	.207	.120	.729
	Within Groups	413.545	240	1.723		
	Total	413.752	241			

Figure 52 One-Way ANOVA behaviour at work - with training

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_ja_privat_nettside	Female	198	2.17	.949	.067	2.03	2.30	1	5
	Male	44	2.36	.917	.138	2.08	2.64	1	4
	Total	242	2.20	.945	.061	2.08	2.32	1	5
var_ja_privat_linker	Female	198	1.61	.771	.055	1.50	1.72	1	5
	Male	44	1.82	.922	.139	1.54	2.10	1	4
	Total	242	1.65	.802	.052	1.55	1.75	1	5
var_ja_privat_avsender	Female	198	1.69	.827	.059	1.57	1.80	1	5
	Male	44	1.95	.939	.142	1.67	2.24	1	4
	Total	242	1.74	.852	.055	1.63	1.84	1	5
var_ja_privat_laaser_log gerut	Female	198	2.45	1.059	.075	2.31	2.60	1	5
	Male	44	2.61	1.083	.163	2.28	2.94	1	4
	Total	242	2.48	1.063	.068	2.35	2.62	1	5
var_ja_privat_jobb_enhet er	Female	198	3.38	.839	.060	3.26	3.50	1	4
	Male	44	3.02	1.067	.161	2.70	3.35	1	4
	Total	242	3.31	.893	.057	3.20	3.43	1	4
var_ja_privat_rapport	Female	198	2.40	1.134	.081	2.24	2.56	1	5
	Male	44	2.45	1.130	.170	2.11	2.80	1	4
	Total	242	2.41	1.131	.073	2.27	2.55	1	5

Figure 53 Descriptives Behaviour at home - with training

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_ja_privat_nettside	Between Groups	1.397	1	1.397	1.569	.212
	Within Groups	213.682	240	.890		
	Total	215.079	241			
var_ja_privat_linker	Between Groups	1.544	1	1.544	2.412	.122
	Within Groups	153.601	240	.640		
	Total	155.145	241			
var_ja_privat_avsender	Between Groups	2.579	1	2.579	3.589	.059
	Within Groups	172.495	240	.719		
	Total	175.074	241			
var_ja_privat_laaser_log gerut	Between Groups	.911	1	.911	.805	.370
	Within Groups	271.523	240	1.131		
	Total	272.434	241			
var_ja_privat_jobb_enhet er	Between Groups	4.564	1	4.564	5.840	.016
	Within Groups	187.568	240	.782		
	Total	192.132	241			
var_ja_privat_rapport	Between Groups	.111	1	.111	.086	.769
	Within Groups	308.389	240	1.285		
	Total	308.500	241			

Figure 54 One-Way ANOVA Behaviour at home - with training

Figure 55 Correlations work and home

Correlations

		var_ja__jobb_nettside	var_ja_jobb_linker	var_ja_jobb_avsender	var_ja_jobb_laaser_loggerut	var_ja_jobb_private_enheter	var_ja_jobb_rapport	var_ja_privat_nettside	var_ja_privat_linker	var_ja_privat_avsender	var_ja_privat_laaser_loggerut	var_ja_privat_jobb_enheter	var_ja_privat_rapport
var_ja__jobb_nettside	Pearson Correlation	1	.499**	.390**	.135*	-.007	.236**	.581**	.363**	.335**	.206**	-.054	.307**
	Sig. (2-tailed)		.000	.000	.036	.913	.000	.000	.000	.000	.001	.403	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_jobb_linker	Pearson Correlation	.499**	1	.580**	.186**	.029	.267**	.429**	.634**	.459**	.138*	-.061	.331**
	Sig. (2-tailed)	.000		.000	.004	.657	.000	.000	.000	.000	.032	.345	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_jobb_avsender	Pearson Correlation	.390**	.580**	1	.231**	-.004	.214**	.473**	.574**	.743**	.232**	-.129*	.260**
	Sig. (2-tailed)	.000	.000		.000	.952	.001	.000	.000	.000	.000	.045	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_jobb_laaser_loggerut	Pearson Correlation	.135*	.186**	.231**	1	-.101	.202**	.192**	.244**	.215**	.312**	.070	.219**
	Sig. (2-tailed)	.036	.004	.000		.118	.002	.003	.000	.001	.000	.277	.001
	N	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_jobb_private_enheter	Pearson Correlation	-.007	.029	-.004	-.101	1	.037	-.008	-.048	-.065	-.027	.144*	.044
	Sig. (2-tailed)	.913	.657	.952	.118		.564	.896	.458	.317	.677	.025	.493
	N	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_jobb_rapport	Pearson Correlation	.236**	.267**	.214**	.202**	.037	1	.208**	.270**	.266**	.217**	.117	.511**
	Sig. (2-tailed)	.000	.000	.001	.002	.564		.001	.000	.000	.001	.069	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_privat_nettside	Pearson Correlation	.581**	.429**	.473**	.192**	-.008	.208**	1	.576**	.556**	.241**	-.100	.330**
	Sig. (2-tailed)	.000	.000	.000	.003	.896	.001		.000	.000	.000	.120	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_privat_linker	Pearson Correlation	.363**	.634**	.574**	.244**	-.048	.270**	.576**	1	.737**	.224**	-.048	.323**
	Sig. (2-tailed)	.000	.000	.000	.000	.458	.000	.000		.000	.000	.456	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_privat_avsender	Pearson Correlation	.335**	.459**	.743**	.215**	-.065	.266**	.556**	.737**	1	.274**	-.032	.259**
	Sig. (2-tailed)	.000	.000	.000	.001	.317	.000	.000	.000		.000	.618	.000
	N	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_privat_laaser_loggerut	Pearson Correlation	.206**	.138*	.232**	.312**	-.027	.217**	.241**	.224**	.274**	1	.102	.180**
	Sig. (2-tailed)	.001	.032	.000	.000	.677	.001	.000	.000	.000		.115	.005
	N	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_privat_jobb_enheter	Pearson Correlation	-.054	-.061	-.129*	.070	.144*	.117	-.100	-.048	-.032	.102	1	.041
	Sig. (2-tailed)	.403	.345	.045	.277	.025	.069	.120	.456	.618	.115		.529
	N	242	242	242	242	242	242	242	242	242	242	242	242
var_ja_privat_rapport	Pearson Correlation	.307**	.331**	.260**	.219**	.044	.511**	.330**	.323**	.259**	.180**	.041	1
	Sig. (2-tailed)	.000	.000	.000	.001	.493	.000	.000	.000	.000	.005	.529	
	N	242	242	242	242	242	242	242	242	242	242	242	242

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

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

Online behaviour no training

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_nei_jobb_nettside	Female	108	2.63	1.124	.108	2.42	2.84	1	5
	Male	30	2.67	1.028	.188	2.28	3.05	1	5
	Total	138	2.64	1.100	.094	2.45	2.82	1	5
var_nei_jobb_linker	Female	108	2.12	1.150	.111	1.90	2.34	1	5
	Male	30	2.13	1.167	.213	1.70	2.57	1	5
	Total	138	2.12	1.149	.098	1.93	2.32	1	5
var_nei_jobb_avsender	Female	108	1.91	.991	.095	1.72	2.10	1	5
	Male	30	1.90	1.094	.200	1.49	2.31	1	5
	Total	138	1.91	1.010	.086	1.74	2.08	1	5
var_nei_jobb_laaser_log gerut	Female	108	1.61	.759	.073	1.47	1.76	1	4
	Male	30	1.67	1.028	.188	1.28	2.05	1	5
	Total	138	1.62	.821	.070	1.48	1.76	1	5
var_nei_jobb_private_en heter	Female	108	3.38	.924	.089	3.20	3.56	1	4
	Male	30	3.57	.858	.157	3.25	3.89	1	5
	Total	138	3.42	.911	.078	3.27	3.57	1	5
var_nei_jobb_mistenkeli g	Female	108	2.93	1.477	.142	2.64	3.21	1	5
	Male	30	3.13	1.332	.243	2.64	3.63	1	5
	Total	138	2.97	1.445	.123	2.73	3.21	1	5

Figure 56 Descriptives behaviour work - no training

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_nei_jobb_nettside	Between Groups	.032	1	.032	.026	.871
	Within Groups	165.852	136	1.219		
	Total	165.884	137			
var_nei_jobb_linker	Between Groups	.004	1	.004	.003	.957
	Within Groups	180.902	136	1.330		
	Total	180.906	137			
var_nei_jobb_avsender	Between Groups	.001	1	.001	.001	.972
	Within Groups	139.774	136	1.028		
	Total	139.775	137			
var_nei_jobb_laaser_log gerut	Between Groups	.072	1	.072	.107	.744
	Within Groups	92.333	136	.679		
	Total	92.406	137			
var_nei_jobb_private_en heter	Between Groups	.821	1	.821	.990	.321
	Within Groups	112.802	136	.829		
	Total	113.623	137			
var_nei_jobb_mistenkeli g	Between Groups	1.010	1	1.010	.482	.489
	Within Groups	284.874	136	2.095		
	Total	285.884	137			

Figure 57 One-Way ANOVA behaviour at work - no training

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_nei_privat_nettside	Female	108	2.30	1.016	.098	2.10	2.49	1	4
	Male	30	2.23	.858	.157	1.91	2.55	1	4
	Total	138	2.28	.982	.084	2.12	2.45	1	4
var_nei_privat_linker	Female	108	1.69	.837	.081	1.53	1.85	1	4
	Male	30	1.67	.922	.168	1.32	2.01	1	4
	Total	138	1.69	.853	.073	1.54	1.83	1	4
var_nei_privat_avsender	Female	108	1.68	.874	.084	1.51	1.84	1	4
	Male	30	1.77	.858	.157	1.45	2.09	1	4
	Total	138	1.70	.868	.074	1.55	1.84	1	4
var_nei_privat_laaser_loggerut	Female	108	2.50	1.115	.107	2.29	2.71	1	5
	Male	30	2.53	1.008	.184	2.16	2.91	1	4
	Total	138	2.51	1.089	.093	2.32	2.69	1	5
var_nei_privat_jobb_enheter	Female	108	3.60	.710	.068	3.47	3.74	1	5
	Male	30	3.50	.777	.142	3.21	3.79	1	4
	Total	138	3.58	.723	.062	3.46	3.70	1	5
var_nei_privat_mistenkelig	Female	108	2.50	1.384	.133	2.24	2.76	1	5
	Male	30	2.83	1.392	.254	2.31	3.35	1	5
	Total	138	2.57	1.388	.118	2.34	2.81	1	5

Figure 58 Descriptives behaviour at home - no training

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_nei_privat_nettside	Between Groups	.093	1	.093	.096	.757
	Within Groups	131.885	136	.970		
	Total	131.978	137			
var_nei_privat_linker	Between Groups	.018	1	.018	.025	.875
	Within Groups	99.583	136	.732		
	Total	99.601	137			
var_nei_privat_avsender	Between Groups	.193	1	.193	.255	.614
	Within Groups	103.024	136	.758		
	Total	103.217	137			
var_nei_privat_laaser_loggerut	Between Groups	.026	1	.026	.022	.883
	Within Groups	162.467	136	1.195		
	Total	162.493	137			
var_nei_privat_jobb_enheter	Between Groups	.244	1	.244	.464	.497
	Within Groups	71.380	136	.525		
	Total	71.623	137			
var_nei_privat_mistenkelig	Between Groups	2.609	1	2.609	1.358	.246
	Within Groups	261.167	136	1.920		
	Total	263.775	137			

Figure 59 One-Way ANOVA behaviour at home - no training

Figure 60 Correlation behaviour - no training

Correlations

		var_nei_jobb_nettside	var_nei_jobb_linker	var_nei_jobb_avsender	var_nei_jobb_laaser_loggerut	var_nei_jobb_private_enheter	var_nei_jobb_mistenkelig	var_nei_privat_nettside	var_nei_privat_linker	var_nei_privat_avsender	var_nei_privat_laaser_loggerut	var_nei_privat_jobb_enheter	var_nei_privat_mistenkelig
var_nei_jobb_nettside	Pearson Correlation	1	.445**	.468**	.147	.000	.260**	.501**	.314**	.258**	.118	.037	.232**
	Sig. (2-tailed)		.000	.000	.086	.999	.002	.000	.000	.002	.168	.670	.006
	N	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_jobb_linker	Pearson Correlation	.445**	1	.601**	.065	.138	.138	.493**	.531**	.316**	.113	-.025	.171*
	Sig. (2-tailed)	.000		.000	.449	.105	.105	.000	.000	.000	.187	.770	.045
	N	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_jobb_avsender	Pearson Correlation	.468**	.601**	1	.045	.139	.238**	.351**	.364**	.608**	.044	.045	.252**
	Sig. (2-tailed)	.000	.000		.601	.105	.005	.000	.000	.000	.610	.597	.003
	N	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_jobb_laaser_loggerut	Pearson Correlation	.147	.065	.045	1	.067	.052	.206*	.102	.135	.419**	.051	.171*
	Sig. (2-tailed)	.086	.449	.601		.436	.543	.016	.233	.115	.000	.553	.044
	N	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_jobb_private_enheter	Pearson Correlation	.000	.138	.139	.067	1	-.030	.168*	.066	.145	.034	.037	.109
	Sig. (2-tailed)	.999	.105	.105	.436		.731	.048	.438	.091	.695	.663	.205
	N	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_jobb_mistenkelig	Pearson Correlation	.260**	.138	.238**	.052	-.030	1	.093	.028	.063	.102	.100	.347**
	Sig. (2-tailed)	.002	.105	.005	.543	.731		.276	.743	.465	.233	.243	.000
	N	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_privat_nettside	Pearson Correlation	.501**	.493**	.351**	.206*	.168*	.093	1	.594**	.444**	.152	-.027	.213*
	Sig. (2-tailed)	.000	.000	.000	.016	.048	.276		.000	.000	.076	.755	.012
	N	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_privat_linker	Pearson Correlation	.314**	.531**	.364**	.102	.066	.028	.594**	1	.650**	.156	-.178*	.177*
	Sig. (2-tailed)	.000	.000	.000	.233	.438	.743	.000		.000	.068	.036	.038
	N	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_privat_avsender	Pearson Correlation	.258**	.316**	.608**	.135	.145	.063	.444**	.650**	1	.010	-.031	.261**
	Sig. (2-tailed)	.002	.000	.000	.115	.091	.465	.000	.000		.907	.719	.002
	N	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_privat_laaser_loggerut	Pearson Correlation	.118	.113	.044	.419**	.034	.102	.152	.156	.010	1	.022	.135
	Sig. (2-tailed)	.168	.187	.610	.000	.695	.233	.076	.068	.907		.794	.115
	N	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_privat_jobb_enheter	Pearson Correlation	.037	-.025	.045	.051	.037	.100	-.027	-.178*	-.031	.022	1	.009
	Sig. (2-tailed)	.670	.770	.597	.553	.663	.243	.755	.036	.719	.794		.919
	N	138	138	138	138	138	138	138	138	138	138	138	138
var_nei_privat_mistenkelig	Pearson Correlation	.232**	.171*	.252**	.171*	.109	.347**	.213*	.177*	.261**	.135	.009	1
	Sig. (2-tailed)	.006	.045	.003	.044	.205	.000	.012	.038	.002	.115	.919	
	N	138	138	138	138	138	138	138	138	138	138	138	138

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

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

Risk-posing actions

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_ja_passord_hjemme	Female	198	1.66	.485	.034	1.59	1.73	1	3
	Male	44	1.80	.462	.070	1.66	1.94	1	3
	Total	242	1.69	.483	.031	1.62	1.75	1	3
var_ja_pasientdata_epost	Female	198	1.93	.320	.023	1.89	1.98	1	3
	Male	44	1.91	.291	.044	1.82	2.00	1	2
	Total	242	1.93	.314	.020	1.89	1.97	1	3
var_ja_kopiert_data	Female	198	2.02	.159	.011	1.99	2.04	1	3
	Male	44	1.95	.211	.032	1.89	2.02	1	2
	Total	242	2.00	.170	.011	1.98	2.03	1	3
var_ja_detaljer_some	Female	198	1.98	.141	.010	1.96	2.00	1	2
	Male	44	2.00	.000	.000	2.00	2.00	2	2
	Total	242	1.98	.128	.008	1.97	2.00	1	2

Figure 61 Descriptives actions - with training

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_ja_passord_hjemme	Between Groups	.645	1	.645	2.789	.096
	Within Groups	55.487	240	.231		
	Total	56.132	241			
var_ja_pasientdata_epost	Between Groups	.023	1	.023	.232	.631
	Within Groups	23.783	240	.099		
	Total	23.806	241			
var_ja_kopiert_data	Between Groups	.132	1	.132	4.624	.033
	Within Groups	6.864	240	.029		
	Total	6.996	241			
var_ja_detaljer_some	Between Groups	.015	1	.015	.900	.344
	Within Groups	3.919	240	.016		
	Total	3.934	241			

Figure 62 One-Way ANOVA actions - with training

Descriptives

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
var_nei_passord_hjemme	Female	108	1.58	.495	.048	1.49	1.68	1	2
	Male	30	1.63	.490	.089	1.45	1.82	1	2
	Total	138	1.59	.493	.042	1.51	1.68	1	2
var_nei_pasientdata_epost	Female	108	1.91	.291	.028	1.85	1.96	1	2
	Male	30	1.93	.365	.067	1.80	2.07	1	3
	Total	138	1.91	.308	.026	1.86	1.96	1	3
var_nei_data	Female	108	2.04	.190	.018	2.00	2.07	2	3
	Male	30	2.00	.263	.048	1.90	2.10	1	3
	Total	138	2.03	.207	.018	1.99	2.06	1	3
var_nei_detaljer_some	Female	108	2.01	.096	.009	1.99	2.03	2	3
	Male	30	2.00	.000	.000	2.00	2.00	2	2
	Total	138	2.01	.085	.007	1.99	2.02	2	3

Figure 63 Descriptives actions - no training

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
var_nei_passord_hjemme	Between Groups	.059	1	.059	.240	.625
	Within Groups	33.217	136	.244		
	Total	33.275	137			
var_nei_pasientdata_epost	Between Groups	.016	1	.016	.166	.684
	Within Groups	12.941	136	.095		
	Total	12.957	137			
var_nei_data	Between Groups	.032	1	.032	.748	.388
	Within Groups	5.852	136	.043		
	Total	5.884	137			
var_nei_detaljer_some	Between Groups	.002	1	.002	.276	.600
	Within Groups	.991	136	.007		
	Total	.993	137			

Figure 64 One-Way ANOVA actions - no training

Correlations

		var_nei_passord_hjemme	var_nei_pasientdata_epost	var_nei_data	var_nei_detaljer_some	var_ja_passord_hjemme	var_ja_pasientdata_epost	var_ja_kopiert_data	var_ja_detaljer_some
var_nei_passord_hjemme	Pearson Correlation	1	.054	-.170*	.071	.b	.b	.b	.b
	Sig. (2-tailed)		.526	.046	.411	.	.	.	.
	N	138	138	138	138	0	0	0	0
var_nei_pasientdata_epost	Pearson Correlation	.054	1	-.189*	.024	.b	.b	.b	.b
	Sig. (2-tailed)	.526		.026	.778	.	.	.	.
	N	138	138	138	138	0	0	0	0
var_nei_data	Pearson Correlation	-.170*	-.189*	1	-.012	.b	.b	.b	.b
	Sig. (2-tailed)	.046	.026		.889	.	.	.	.
	N	138	138	138	138	0	0	0	0
var_nei_detaljer_some	Pearson Correlation	.071	.024	-.012	1	.b	.b	.b	.b
	Sig. (2-tailed)	.411	.778	.889		.	.	.	.
	N	138	138	138	138	0	0	0	0
var_ja_passord_hjemme	Pearson Correlation	.b	.b	.b	.b	1	.073	.016	.185**
	Sig. (2-tailed)	.	.	.	.		.259	.806	.004
	N	0	0	0	0	242	242	242	242
var_ja_pasientdata_epost	Pearson Correlation	.b	.b	.b	.b	.073	1	.005	.178**
	Sig. (2-tailed)	.	.	.	.	.259		.933	.006
	N	0	0	0	0	242	242	242	242
var_ja_kopiert_data	Pearson Correlation	.b	.b	.b	.b	.016	.005	1	-.187**
	Sig. (2-tailed)	.	.	.	.	.806	.933		.003
	N	0	0	0	0	242	242	242	242
var_ja_detaljer_some	Pearson Correlation	.b	.b	.b	.b	.185**	.178**	-.187**	1
	Sig. (2-tailed)	.	.	.	.	.004	.006	.003	
	N	0	0	0	0	242	242	242	242

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

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

b. Cannot be computed because at least one of the variables is constant.

Figure 65 Pearson correlation actions

Part 4 - Knowledge and motivation

With training

Training

Frequencies Where have you learned about information security?

		Responses N	Responses Percent	Percent of Cases
Where[a]	Self-Study	85	20.2%	35.1%
	Internal courses	149	35.5%	61.6%
	External courses	25	6.0%	10.3%
	Information from employer	161	38.3%	66.5%
Total		420	100.0%	173.6%

a. Group

Figure 66 Frequencies "Where have you learned about information security?

Training offered

kurs

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes, I have participated	135	34.4	55.8	55.8
	Yes, but I have not participated	8	2.0	3.3	59.1
	No	85	21.7	35.1	94.2
	Do not know	14	3.6	5.8	100.0
	Total	242	61.7	100.0	
Missing	System	150	38.3		
Total		392	100.0		

Figure 67 Frequencies courses the last two years

Tools to raise awareness.

Tools Frequencies

		Responses N	Responses Percent	Percent of Cases
Tools[a]	Coursing with experts	108	22.8%	44.6%
	Gamification	39	8.2%	16.1%
	Customized physical courses	72	15.2%	29.8%
	Customized e-learning courses	184	38.9%	76.0%
	Films	70	14.8%	28.9%
Total		473	100.0%	195.5%

a. Group

Figure 68 Frequencies What learning tools would you prefer?

Want to learn more about

More knowledge Frequencies

		Responses N	Responses Percent	Percent of Cases
More knowledge[a]	Infosec at work	147	23.4%	61.0%
	Infosec at home	117	18.6%	48.5%
	Secure e-mail	81	12.9%	33.6%
	Report Infosec incident	111	17.6%	46.1%
	Cloud services	96	15.3%	39.8%
	Courses available	77	12.2%	32.0%
Total		629	100.0%	261.0%

a. Group

Figure 69 Frequencies want more knowledge

No training

Training

Where have you learned about informatio security
Frequencies

		Responses		Percent of Cases
		N	Percent	
Where[a]	Self-Study	87	50.6%	63.0%
	Internal courses	14	8.1%	10.1%
	External courses	8	4.7%	5.8%
	Information from employer	63	36.6%	45.7%
Total		172	100.0%	124.6%

a. Group

Figure 70 Frequencies learned about information security

Training offered

Courses the last two years

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes, I have participated	7	1.8	5.1	5.1
	Yes, but I have not participated	5	1.3	3.6	8.7
	No	113	28.8	81.9	90.6
	Do not know	13	3.3	9.4	100.0
	Total	138	35.2	100.0	
Missing	System	254	64.8		
Total		392	100.0		

Figure 71 Frequencies coursed the last two years

Tools to raise awareness

Tools Frequencies

		Responses		Percent of Cases
		N	Percent	
Tools[a]	Coursing with experts	68	29.8%	49.3%
	Gamification	6	2.6%	4.3%
	Customized physical courses	55	24.1%	39.9%
	Customized e-learning courses	75	32.9%	54.3%
	Films	24	10.5%	17.4%
Total		228	100.0%	165.2%

a. Group

Figure 72 Frequencies What learning tools would you prefer?

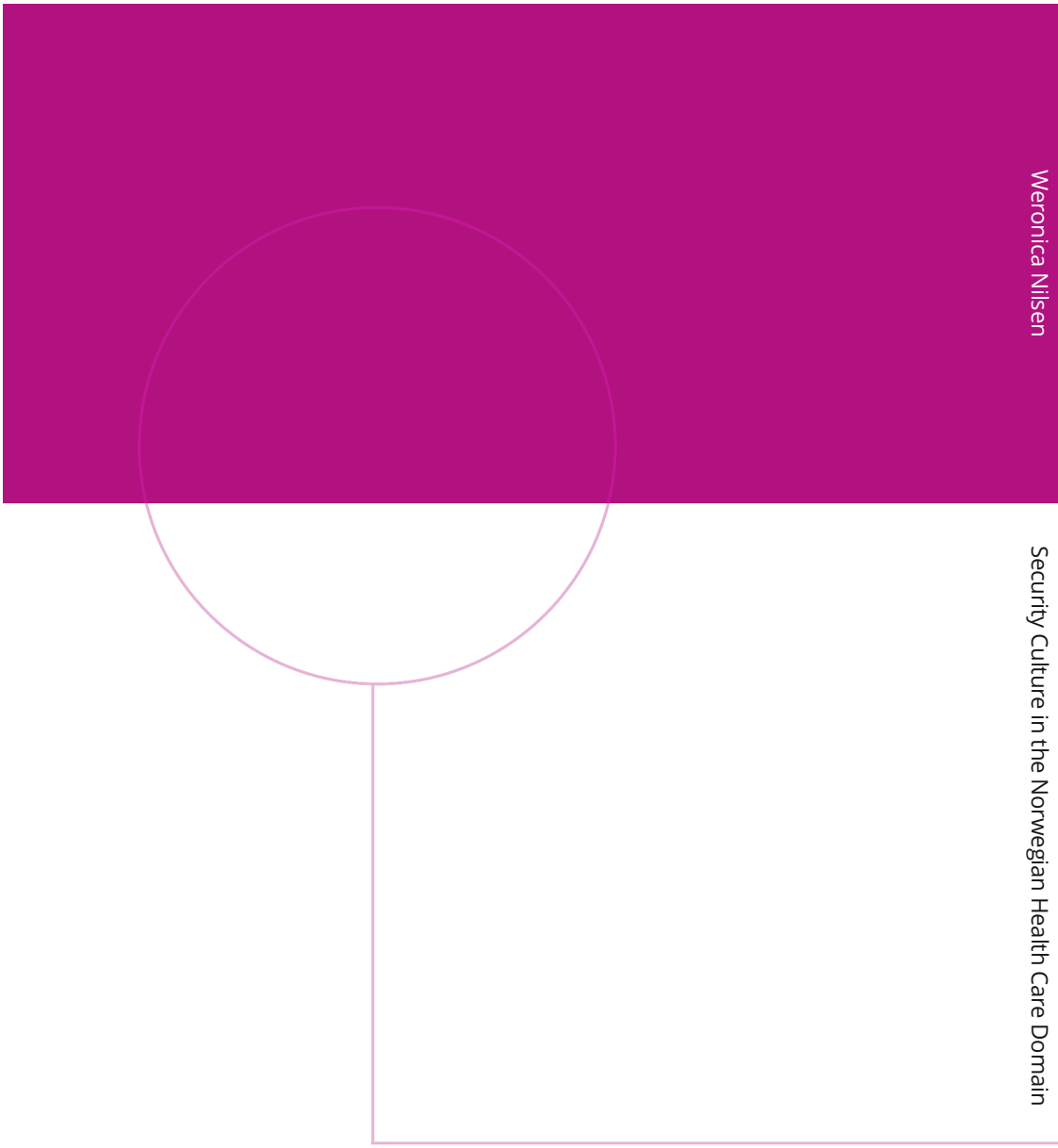
Want to learn more about?

More knowledge Frequencies

		Responses		Percent of Cases
		N	Percent	
More knowledge[a]	Infosec at work	96	21.9%	69.6%
	Inforsec at home	63	14.4%	45.7%
	Secure use of e-mail	47	10.7%	34.1%
	Securely treat patient data	61	13.9%	44.2%
	Report inforsec incidents	59	13.5%	42.8%
	Cloud services	53	12.1%	38.4%
	Courses available	59	13.5%	42.8%
Total		438	100.0%	317.4%

a. Group

Figure 73 Frequencies learn more about



Weronica Nilsen

Security Culture in the Norwegian Health Care Domain

NTNU
Norwegian University of
Science and Technology