UiA Universitetet i Agder

Teachers’ awareness, knowledge and practice of information security in school

Rune Vålandsmyr Olsen
Simen Tokerud

Supervisor
Associate Professor - Cathrine Edelhard Tømte

University of Agder, 2020
Faculty of social sciences
Department of Information systems

PREFACE

This master thesis is written by two students from the two-year Master-program of Information systems at the University of Agder.

The aim of this thesis was to figure out how teachers' awareness, knowledge and practice of information systems are, and develop suggestions of how to improve it.

We chose this topic because of our interest in and previous work on information security and crisis management. In addition to this, we have both been interested in the digitalization of the school system from a young age. We grew up during the transition from pen and paper to computers, and always preferred using the latter. Furthermore, the topic of information security in the school system is largely understudied, especially in Norway. As technology becomes a core part of education, so must information security, and that is why this topic is more relevant now than ever.

The work with the thesis has been challenging. Teachers have very busy schedules and it was hard for us to get interviews with them. Because of the Covid-19 situation, getting interviews became even harder and several of our planned interviews were cancelled. This resulted in less collected data than we had planned for, but we still consider our empirical basis for this thesis to be solid.

We would like to thank all our respondents for their contributions. We know that they have a very tight schedule, and we are grateful that they took time of their busy day to answer our questions. We would also like to thank ProDiG for providing us with a scholarship and allowing us to use their contact network to get in touch with the teachers. Lastly, we would like to thank associate professor Cathrine Edelhard Tømte for all the help and regular feedback she has given us through the process of writing this thesis.

Rune V.

ST

Rune Vålandsmyr Olsen

Simen Tokerud

SUMMARY

We found that the teachers in our respondent schools lacked formal training on topics of information security. Most of them did not know what phishing, backdoors and keyloggers are, and many reused passwords across multiple sites. The teachers were also concerned about lacking the knowledge to properly teach their students about information security and netiquette. The principals did not consider information security to be a primary concern and the IT-department employees had varying knowledge of information security. Meanwhile the municipality has been focused on procuring hardware and software for the teachers and students, and ensuring proper use of these digital teaching aids, while neglecting the information security aspect. Based on our findings and literature from the IS field, we have developed an overview of the 15 key problem areas we identified with improvement suggestions.

All our suggestions are concrete measures to transition towards a more information security friendly organizational culture. This change in culture must be encouraged by the municipality. We suggest arranging a yearly information security week and workshops, partnering up with already existing national incentives to increase teacher knowledge. We also suggest short weekly discussions on information security led by an information security champion to keep awareness levels high. Further standardization of the applications used in schools and the introduction of a password manager and more multi-factor authentication are also encouraged.

In this thesis we aimed to find out more about teachers' knowledge, awareness and practice of information security in school. With more and more technology being introduced in not only school, but in all areas of the society, it is important to have knowledge about potential risks that come with the new technology. Information security in school is a very understudied concept, especially in a Norwegian context. That is one of the reasons we found it interesting to find out more about this topic.

We did a qualitative approach where we interviewed four teachers, three IT-managers and two principals at primary and secondary schools in Kristiansand and Vennesla. During our research, we also realized that the municipality is responsible for many of the aspects of information security in the schools, so we interviewed one representative from the municipality as well. We wanted to find out how their knowledge, awareness and practice were about information security in a school context. Next, we would develop solutions for how to improve this knowledge, awareness and practice. We used the CIA-model from the information security literature, as well as the C3-Framework as our frameworks. The focus of the report is on information security and the CIA-model, with some knowledge gaps within cybersafety being pointed out as well. The 15 key problem areas were categorized in four categories; cybersafety, confidentiality, integrity and availability. The proposed suggestions were iteratively improved through discussions with teachers.

Our goal when writing this thesis is to produce a thesis that can be used to improve the information security knowledge, awareness and practice in Norwegian schools, and to contribute to the literature on information security in Norwegian schools. We have not been able to find any qualitative studies on this topic in Norway, and we therefore hope to encourage further research on an understudied, yet incredibly important topic.

INDEX

1. INTRODUCTION

Information security is an increasingly relevant topic. As technology plays a larger role in our society, more knowledge and awareness of information security issues and threats is required. We see this digitalization trend in schools as well, with more than 50% of all students having their own digital device in school all the way down to first grade (Fjørtoft, Thun, & Buvik, 2019). For many of these students this is the first time they are responsible for their own data in a digital society. Therefore, it is important that teachers can teach them about information security, so they are able to keep their data safe. If the teachers don't have enough knowledge of information security, the students will also struggle to protect their data.

In this master thesis, we aim to find out more about teachers' awareness, knowledge and practice in dealing with information security. We also want to find out more about how the situation can be improved. This is an understudied topic, especially in the Norwegian context.

The Norwegian Directorate for Education and Training (Utdanningsdirektoratet) has decided to renew all curriculums in primary, secondary and high school implemented from the fall of 2020. They describe five basic skills that are necessary for students to understand, learn and display their knowledge in all grades (Udir, 2020): Reading, writing, calculation, oral skills and digital skills. With the introduction of digital skills to the curriculum, it is important that teachers have the necessary competence on the topic.

The teachers have a framework for how to improve their own digital competence called the Professional Digital Competence Framework for Teachers (Kelentric, Helland, & Arstorp, 2017). The framework was first introduced in 2012 because they found the need to improve teachers' digital competence so that they could pass this knowledge on to their students. It is a joint effort based on national regulations, guidelines for teacher education programmes, the national curriculum, the Basic Skills Framework and the National Qualifications Framework.

The Professional Digital Competence Framework consists of seven competence areas. Ethics is the part that covers what teachers should know about information security, or data security as it is called in the framework. It states the following: "Teachers should be able to apply and teach the rules about copyright, privacy, data security, source criticism and right use of sources" (Kelentric, Helland, & Arstorp, 2017). It also states that the teachers should have knowledge about the laws, regulations and guidelines that concern intellectual property rights, and how to handle the personal data of pupils, guardians and colleagues.

There have been many examples of poor information security practices the Norwegian school system over the last few years. Some of them could have had potentially catastrophic consequences. One of the most known examples is the case where a 13-year old boy was able to find the unencrypted usernames and passwords of 35 000 people Bergen (Johansen, 2019). The file itself was unencrypted but hidden in a directory system. This means that everyone with access to the directory system had access to this file if they knew where to look. The boy warned the authorities about the security hole, but he was not heard until six months later when he sent out an email from the principal's email address. The municipality of Bergen was fined 1.6 million NOK from Datatilsynet for the breach on the new GDPR-regulations.

SINTEF, a Norwegian research institute, did a study on the digital state of Norwegian schools and kindergartens (Fjørtoft, Thun, & Buvik, 2019). This report was called Monitor 2019. They found that both schools and kindergartens have improved when it comes to using technology in education, but there is still need for further improvement. They need better routines for risk assessments of critical ICT-systems. About a third of the teachers asked stated that their school had good routines for registering, use, access, storing and deletion of sensitive data. This suggests that there is still potential for improvement, either in the shape of making existing guidelines known to everyone or making new ones.

There are many terms that are similar to information security: Data security, cyber security and digital safety are some of them. By information security we mean issues that are related to the confidentiality, integrity and availability of the data (Digitaliseringsdirektoratet, 2020). In this thesis we will also include the term cybersafety within information security. Furthermore, we will look at the knowledge, awareness and practice of information security in schools.

1.1 Research questions

This thesis is a continuation of the preliminary research we conducted during the autumn semester of 2019. During the preliminary research we conducted a systematic literature review on the topic of information security in the school context as well as four interviews. Two teachers, one principal and one IT-department employee were interviewed, all working in the same school. We wanted to expand this research to involve more schools, as well as the municipality and create suggestions that can be implemented to improve the situation.

Based on what we learned we have formulated the following research questions.

RQ1: How are teachers' awareness, knowledge and practice about information security in school?

RQ2: How can teachers improve their awareness, knowledge and practice about information security?

We decided to do a qualitative approach by doing interviews with teachers, IT-managers and principals at schools in two municipalities in Agder. In addition, we have interviewed a digitalization consultant at one of the municipalities who is responsible for IT-related issues in all the schools in the municipality.

1.2 THE STRUCTURE OF THE THESIS

The thesis is built up in six main chapters, with subchapters for each chapter. Chapter one is where we give you a quick introduction to what the purpose of this master thesis is.

In chapter 2.0, Background theory, we give a summary of our systematic literature review, define key terms used in our report and explain our chosen framework.

In chapter 3.0, Research approach and analysis, we explain our research approach, respondent selection, data collection and analysis. Validity and ethical concerns are also discussed here.

In chapter 4.0, Findings, we present the results from our data analysis. We have divided the chapter in four main parts; cybersafety, confidentiality, integrity and availability.

In chapter 5.0, Discussion, we discuss our findings and relate them up to previous research. We will also develop possible solutions to improve the knowledge, awareness and practice of information security in school.

In chapter 6.0, Conclusion, we conclude and present our findings from the study. In this chapter we answer our research questions. We also discuss the implications of our thesis as well as its weaknesses and propose topics for further research.

2. Background Theory

We will start off this chapter by looking at some key terms that will be used in this thesis. Then we will proceed to summarize a literature review that was conducted during our preliminary research the previous semester. Lastly, we will discuss the frameworks that we will use in our thesis.

2.1 Key terms

In this chapter we will the define key terms used in this thesis that people outside the IS-field may not be familiar with.

Digital footprint management: The act of managing your digital footprints. Digital footprints are the digital traces left when people go online. While some of this is deliberatively created, it also encompasses the passively recorded evidence of people's online activity (Buchanan, Southgate, & Smith, 2019).

Keylogger: A malicious piece of software that logs keystrokes on a computer and sends them off to an external source. Keyloggers are often used to steal passwords and other sensitive information. There are hardware keyloggers as well, but those require physical access to the computer and are outside of the scope of this thesis (Grebennikov, 2007).

Backdoor: A backdoor is a way to access a system without the owner knowing about it. The backdoor is planted by an attacker. Through this backdoor the attacker can get access to read, change or delete information. Other possibilities are logging keystrokes, spying on network traffic, running code on the system or further hacking of other computers connected to the network (Nätt, 2019).

Phishing: Phishing is a social engineering tactic designed to trick users into divulging sensitive personal information, such as one's social security or bank account numbers, through impersonation of a trustworthy third party (Lawson, Pearson, Crowson, & Mayhorn, 2020). These attacks usually happen via email, but it is also possible to perform such attacks via phone or even face-to-face.

Password Manager: A password manager is a piece of software that generates strong and unique passwords for all services that require an account. Most password managers are also capable of auto-filling passwords and automatically updating passwords regularly. Password managers usually work across multiple devices and store the user's passwords securely, either in the cloud or locally, depending on the user's needs (LastPass, 2020).

Multi-factor authentication: Multi-factor authentication requires the user to present multiple pieces of evidence to an authentication mechanism (Lujan, 2019). The five most used authentication factors are:
Something you know – Often a password or passphrase.

Something you have – A code from a physical authenticator or authenticator app on your phone.

Something you do – A gesture to a camera or drawing a specific pattern on your screen.

Something you are – Biometric data such as fingerprint and iris scans.

Somewhere you are – Your physical location. Usually the local network you are connected to.

GDPR: The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The main goals of GDPR are to take a firm stance on data privacy and security, and to give users more control of their data (GDPR.EU, 2020).

Practice is the actual application or use of an idea, belief, or method, as opposed to theories relating to it (Oxford University, 2020).

Knowledge is facts, information, and skills acquired through experience or education; the theoretical or practical understanding of a subject (Oxford University, 2020).

Awareness is knowledge or perception of a situation or fact (Oxford University, 2020).

2.2 LITERATURE REVIEW

We conducted a systematic literature review on teachers' knowledge and awareness of information security in school during our previous semester. The literature review followed the guidelines outlined by Kitchenham and Charters in 2007 (Kitchenham & Charters, 2007). This section of the master thesis is a summarized version of that literature review (Vålandsmyr Olsen & Tokerud, 2019).

We found that teacher knowledge and awareness levels tended to be moderate or high on topics of cyberethics and cybersafety, but low on matters of cybersecurity. The amount of literature we found on each of the three topics also reflected this, resulting in the most knowledge gaps within cybersecurity. The topic is largely understudied and finding relevant literature proved to be a difficult task.

Our literature review revealed that studies on information security in schools focused on the following areas: Passwords, backdoors, keyloggers, phishing, cybersafety, information security awareness and knowledge, the digital divide, ethics, cyberbullying, netiquette and privacy. We found the most articles on cyberbullying, ethics, the digital divide and cybersafety. Only two out of 20 articles were Norwegian, once again suggesting that the topic is understudied in Norway.

Below we will summarize the categories with findings that are most relevant for our research questions: Passwords, phishing, backdoors, cybersafety and information security awareness and knowledge. These categories coincide very well with the knowledge gaps identified in our literature review, with some categories having as few as a single article mentioning them.

Passwords

Tomczyk lists creating secure logins and passwords as one of the key components of digital literacy (Tomczyk, 2019). According to Monitor 2019, 84.3% of teachers stated that they use their Feide username and password for logging in to most of the systems and digital learning resources that they use. This suggests to us that most teachers use the same password for multiple services. 12.2% of the teachers also stated that logging in to teaching services is difficult because they have many different usernames and passwords (Fjørtoft, Thun, & Buvik, 2019). According to Pusey and Sadera, password strength is something the teachers in their American study were rather confident in teaching (Pusey & Sadera, 2012). The results seem to indicate that although teachers are confident in generating strong passwords, they tend to either use the same password for multiple services or they struggle remembering them all.

Backdoors, keyloggers and phishing

We only found a single article exploring teacher knowledge on backdoors, keyloggers and phishing: An American study of preservice teacher knowledge about information security. A Likert scale from one to four was used, where one means that the respondent had never heard anything about the topic and four meant that they know about it and could model and teach it to others. The article states that teacher knowledge about phishing was rather low, scoring a mean value of 1.88 (Pusey & Sadera, 2012). In the same study, teachers also reported a low score of 1.58 when asked about Keyloggers, meaning very few teachers had even heard of the term. Backdoors are a similar story with a score of 1.49. These are only three of countless digital threats to information security that teachers should ideally know more about.

Cybersafety

Digital footprint management falls under the cybersafety category. More studies have been conducted on cybersafety topics compared to information security topics, and we would therefore like to highlight the findings of one Australian article on digital footprint management and one African study on cybersafety, as well as the American study mentioned above. An Australian article on digital footprint management found that both parents and teachers were concerned about controlling the digital footprints of the students (Buchanan, Southgate, & Smith, 2019). The article went on to state that this topic is becoming increasingly more important in our digital society, especially now that many services are free and rely on collecting the users' personal information as their main income. An African study on cultivating a cybersafety culture among school learners in South Africa stated that 76% of their respondents had posted pictures of other people online, while only 27% asked for permission beforehand (Kritzinger, 2017). The American study on preservice teacher knowledge found that several topics within cybersafety such as identity theft, internet predators, online identities and cyberbullying scored from 2.62-2.9, meaning the teachers knew about the topics, but were unable to model and teach them to others.

Information security knowledge and awareness

We found two studies exploring information security knowledge and awareness in general: The American study mentioned above and a Turkish study on teachers' knowledge levels about virtual information security. In the American study, a total of four C3 topics received high means greater than 3.5, meaning the teachers felt prepared to teach them: Cell phones, text messaging, attachments and plagiarism. At the other end of the spectrum there were nine C3 topics that the participants in the study rated with a mean less than 1.5. A total of 31 C3 topics were rated between 1.5 and 2.5 with another 31 topics between 2.5 and 3.5. Most of the highly rated topics are within the domains of cyberethics or cybersafety, while the cybersecurity topics are often given low ratings. Furthermore, a Turkish study of teachers' knowledge levels about virtual information security found that 46.7% of their respondents did not know how to prevent spyware from installing on their computers, and 43.7% stated they could not notice if their computers were infected (Karabatak & Karabatak, 2018). In Monitor 2019 it was uncovered that 17.4% of teachers don't have good routines for registering, using, accessing, storage and deletion of personal information, with 50.6% stating that the routines were neither good nor bad (Fjørtoft, Thun, & Buvik, 2019).

2.3 The C3 Framework

We have chosen to base this thesis on the C3 framework. The C3 framework consists of three overlapping knowledge areas: Cyberethics, Cybersafety and Cybersecurity. Cyberethics is the moral choices individuals make when using Internet-capable technologies and digital media. Copyright, online etiquette, hacking and online addictions fall into this category. Cybersafety consists of the actions individuals take to minimize the dangers they could encounter when using internet-capable technology. Online predators, unwanted communications, viruses and spyware fall into this category. Cybersecurity involves technical interventions that protect data, identity information and hardware from unauthorized access or harm. Antivirus software, internet content filters, firewalls and password protection fall into this category (Pusey & Sadera, 2012). Cybersecurity is also a part of information security, which is the focus of this thesis. Due to the emphasis teachers put on cybersafety we have decided to include that knowledge area in our thesis as well.

2.4 Information Security

Information security is the practice of protecting information by mitigating information risks. At the heart of information security are three principles described by the CIA triad: Confidentiality, Integrity and Availability (Fruhlinger, 2020). Confidentiality means that information should never be disclosed to unauthorized individuals. Integrity means that the data should be accurate and complete during its entire lifecycle. Availability means that the data should be readily available to authorized individuals when they need it. These principles conflict with each other and a balance between them must be struck to ensure good information security practices. This balance varies based on how sensitive the information is. In this article, the term Information Security will be used to refer to both Cybersafety and Cybersecurity.

Schools deal with a lot of sensitive information such as grades, personal information, employee records and incident reports. It is important that this information is handled in a responsible way, which requires adequate knowledge, awareness and practices regarding information security. Few people before us have studied this topic and we were unable to find any qualitative studies to describe the current situation in Norway. We would therefore like to study this topic.

3. RESEARCH APPROACH AND ANALYSIS

In this chapter, we will discuss our research approach, our design decisions, data collection, respondent selection process, data analysis, validity and ethical concerns. Limitations will be discussed in chapter 6.0.

3.1 RESEARCH APPROACH

The aim of the thesis is to explore teachers' knowledge, awareness and practice around information security in school. This is a rather understudied topic judging by our literature review the previous semester. The knowledge gaps were largest in cybersecurity, which is where we aim to make our contribution to the literature. We did find some quantitative data in monitor 2019, but this data alone does not adequately describe the situation. To our knowledge, no qualitative studies have been carried out on this topic in Norway. We therefore decided to do a qualitative study to dive deeper into the current situation.

Interviews are great at dealing with topics in depth and detail (Oates, 2012) and using semi-structured interviews allows us to adjust our line of inquiry if we discover something of interest during the interview. We have also noticed that the response percentage of surveys sent out to teachers is low, making interviews a less risky method of data collection compared to surveys. Due to this, we decided to gather our data through semi-structured interviews.

3.2 RESEARCH DESIGN

In our previous semester, we did some preliminary research on this topic. In order to get a complete overview of the situation and include the most relevant perspectives, we decided to interview three groups: Teachers, principals and IT-department employees. Principals offer a more administrative perspective, while IT-department members offer a technical perspective.

The first version of our interview guide was developed during this preliminary research. The guide itself was based on common information security topics in existing literature and the findings of monitor 2019. We went through three iterations with feedback from our supervisor after each iteration over the course of two months. The result is an interview guide with two sections: One general information security section and one section tailored specifically towards each respondent group.

During our preliminary research in the previous semester, we had only included the teacher, IT-department employee and principal respondent groups. After conducting some interviews, we realized that the municipality is largely responsible for a lot of the decisions related to information security, which is why we decided to add them as the fourth respondent group. We developed a new interview guide tailored towards the municipality employee respondent group and refined our other interview guides based on our experiences from the preliminary interviews. The final interview guides can be found in appendices 8.1 and 8.2.

3.3 Data collection and respondents

Our respondents are from two municipalities in Agder. We chose to interview respondents locally so that we would get the chance to talk with them face-to-face and see the schools that they work in first-hand. We have interviewed teachers, IT-managers and principals at primary schools and secondary schools. We have also interviewed a digitalization consultant who works in at one of the municipalities and is responsible for the IT in the public schools within the municipality.

We sent our requests for interviews via email to all schools in Vennesla and Kristiansand municipalities in December 2019. Follow-up requests were sent in early January 2020. Due to the low response rate we proceeded to contact seven schools in Kristiansand and five schools in Vennesla via phone. A total of four schools agreed to participate in interviews. Due to the corona situation, several of our planned interviews for March were cancelled. We did, however, manage to interview respondents from all the roles and have been diligent in comparing our empirical data to existing theory.

We have done a total of ten interviews. This includes four teachers, three IT-managers, two principals and one employee from the municipality. The data collected is anonymous according to the privacy rules set by NSD (Norsk Senter for Forskningsdata (Norwegian Centre for Research Data)). It is not possible to recognize people based on the data we have collected. Their rights were either emailed to them in advance or have been read aloud before commencing the interview. They have all expressed informed consent orally on tape. The interviews were recorded using a dictaphone with no internet access and the audio files were stored on UiA's secure servers. We chose to anonymise all the respondents because of their right to privacy and to minimize the danger of the respondents giving us "the correct answers" instead of what they would normally do and think.

The interviews were all done in Norwegian. However, we have chosen to translate our quotes to English to better accommodate our English-speaking readers. This means that some nuances could potentially have been lost in translation. We were aware of this and made every effort to make the translations as accurate as possible.

In the following table (Table 1) we present our respondents along with some demographic data such as age, experience and what level of school they work on. We also state whether the interview was done during the preliminary research or not.

Table 1: Respondent overview

Position	Age	Experience in teaching (years)	Primary/ Secondary school	Preliminary research
Teacher	35	10 years	Secondary school	Yes
Teacher	47	18 years	Secondary school	Yes
Teacher	34	10 years	Secondary school	No
Teacher	43	20 years	Primary school	No
IT-Manager	63	20 years as teacher 11 years as consultant	Secondary school	Yes
IT-Manager	44	15 years	Primary school	No
Secretary/ IT-Manager	60	Never taught	Primary school	No
Principal	41	10 years as teacher 9 years as assistant principal and principal	Secondary school	Yes
Principal	53	25 years as teacher 1 year as principal	Primary school	No
Digitalization Consultant	35		Municipality	No

The data was collected in the period from November 2019 to March 2020. We have included the interviews we did in our preliminary research during the fall of 2019. Some of our questions in our interview guide were yet to be included at that time, so the results from those interviews are a little more limited compared to the ones we did in February and March this year.

3.4 Analysis

We transcribed and anonymized the interviews within five days of the interview. Once all the interviews were transcribed, we coded the data using a thematic analysis table. In our first version of the thematic analysis table, the data was coded deductively based on relevant topics within information security and cybersafety based on our literature review and interview guide. We then proceeded to inductively add more categories based on the interview data that we collected (Jacobsen, 2015). Furthermore, we divided them into either knowledge, awareness or practice to better answer our research questions.

The thematic analysis table allowed us to easily spot themes across all our interviews and compare answers from different respondent groups (Oates, 2012). It is one of the most used methods of analysis in qualitative studies and allows us to pinpoint which areas of information security that the teachers can improve in. With the added administrative and technical perspectives from the other respondent groups we can also say something about the reason why the situation is as described.

Once the thematic analysis table was completed, we discussed our results in an online meeting. During the discussion we identified 15 key problem areas and developed potential solutions. The solutions were based on our own knowledge of organization management from prior university courses and relevant literature from the IS field.

Once we had developed our potential solutions, we worked together with two teachers to make iterative improvements. During the first iteration, the full list of solutions was sent to an anonymous teacher and we had an online meeting to discuss them a few days later. During this meeting we discussed what the teacher thought of our solutions, how realistic they would be to implement and if the teacher had any other ideas. This feedback was when incorporated in our list of solutions. For the second iteration we received written feedback from a second teacher via email. We proceeded to incorporate this feedback into our solutions as well. After the second iteration, we considered our suggestions to be realistic and effective.

3.5 VALIDITY AND ETHICAL CONSIDERATIONS

To achieve validity in our findings, we have looked for themes that occur across multiple interviews and compared these themes to existing literature. Unless we explicitly state otherwise, all the findings in chapter 4.0 are themes that have been expressed through multiple interviews with literature to back it up. Due to time constraints, it was not possible for us to send copies of the interview transcripts back to the interviewee for checking. This issue, and the issue of reliability are both discussed further in chapter 6.1.

Our main ethical consideration was to ensure that all the respondents received all the information they needed to make an informed consent before starting the interview. We wrote an information document with help from NSD for this purpose. During our preliminary interview, this document was read aloud before asking for consent and a card with all the necessary contact details was provided to each respondent. This semester we instead opted to email the information document to the respondents in advance, including all our contact details in the email.

Making sure all the privacy of all our respondents is protected is also a key concern. We have chosen to anonymize all our respondents and deliberately refrain from mentioning which specific schools we have visited in order to protect our respondents' privacy. All the teachers, IT-department employees and principals have been assigned a number and will only be referred to by their role and assigned number.

4. FINDINGS

In this chapter, we will present the results of the data analysis. We have divided the results into four main parts, based on the C3-framework and the CIA-model. Some of the problem areas we have identified impact more than one category and will therefore be brought up multiple times.

For the purposes of anonymization, all our cited respondents will be given a letter corresponding to their role and a number: T for teachers, I for IT-department employees, S for secretary/IT-department employees, P for principals and M for municipality employees.

4.1 CYBERSAFETY

The respondents themselves often brought up Cybersafety during our interviews when asked about other topics within information security that they considered important:

> I put a lot of emphasis on teaching my students to be critical of where they post their personal information online, especially when posting images. It is easy for most people to access this information, and for this generation that has grown up with social media, it is extra important to be critical in every way. (T2, 2019)

This is because it relates more closely to the schools' primary task of education when compared to information security.

Training and management support

Most respondents were concerned their own and their colleagues' knowledge levels on the topic and stated that they had received no formal training: "We have not received formal training in information security. We have been told to watch what we publish on the internet and not to leave our computers unattended while logged in, but that is all" (T2, 2019). All the respondents reported that they had a high focus on making sure that they log out of their computers before leaving them unattended, and that they instructed their students to do the same.

Furthermore, they expressed a need for more engagement from the principal and the municipality:

> Management has the responsibility to ensure that teachers are given the necessary competence to teach matters of cybersafety to their students. Not all teachers are equally motivated to learn about cybersafety, so the matter may need to be forced upon some teachers (T3, 2019).

One of the principals stated the following as a response to why the knowledge and awareness of information security and cybersafety was lacking:

> Information security is not our primary concern. From our perspective this is a matter of time. We do not have enough time to learn more about it since our focus is

> directed at our students. We have not invested a lot of time into it because we do not have to. We do things when we must, but not before. (P2, 2020)

Our teacher respondents stated that the responsibility for teaching their students good cybersafety practice was shared between the schools and the parents: “The schools must take responsibility for teaching their students about cybersafety together with the parents. This requires that the teachers themselves know enough about cybersafety” (T3, 2019).

Teaching the students about cybersafety

Most of the respondents reported that they brought up the following topics within cybersafety to their students: Publishing images and other personal information online (Digital footprint management), creation of strong passwords, sharing of passwords and critical thinking. There was no specific mention of viruses or anti-virus programs.

One of the schools we visited decided to outsource the teaching of cybersafety to an external company in cooperation with the municipality:

> I think making students aware of cybersafety is important. Don’t store passwords carelessly for example. This is something we are working on now. Privacy is important to us. We have not allocated hours for it in our schedule for the semester, but last year the municipality arranged for an external company to hold four-day courses for our students on cybersafety. (T1, 2019)

The other respondent schools did not have external coursing for their students.

Software usage

When asked about what software the teachers used during their education one of the respondents stated the following:

> I use what I am told to use by the IT-department, but sometimes I use other services and programs outside of what the IT-department recommends. I follow recommendations from other teachers, but I do not check whether the software is safe to use beyond that. I never use software where the students must register themselves. (T3, 2019)

We found that most of the respondents relied upon recommendations from other teachers and performed very few safety checks themselves when using software not directly recommended by the IT-department or municipality. This does not necessarily compromise the students’ cybersafety if no registration is required to use the program. The respondents in this thesis did not use any software that required the students to register outside of what was recommended by the IT-department.

We also asked the municipality about their digitalization strategy in terms of cybersafety. The respondent stated the following:

> The goals in our digitalization strategy change with the times. Back in 2008 the most important goal was to obtain digital equipment, not how to use it. This strategy changed over time and in 2018 the focus had shifted to educational use of digital equipment, resulting in the acquisition of tablets for use in the classrooms. Our new goals going forward have shifted towards information security. This is quite typical for the municipality: We move swiftly forward and make some experiences, and then we take a few steps back and learn from our mistakes. (M1, 2020)

They also stated that they have a heavy focus on standardization to make all the schools offer the same experience for their students, while making it easier to ensure that apps and software that is being used is safe.

4.2 INFORMATION SECURITY

We have divided our results relating to information security into three categories based on the three principles of information security: Confidentiality, Integrity and availability.

4.2.1 Confidentiality

Confidentiality is incredibly important in the school context. We have seen numerous incidents in the media recently where information confidentiality has been broken. The schools are responsible for a lot of sensitive information, and good information security practices are therefore a must. In this subchapter we look at our findings regarding information confidentiality in the school context.

The Term “Information security”

It is important to establish what the teachers, IT-managers and principals think of when they hear the term “information security”. Only one of the respondents stated that information security is about confidentiality, integrity and availability of the data. This was one of the IT-managers: “Three things: That no unauthorized person shall get access to my data. That the data is correct and that we should have access to our data.” (I2, 2020) The answers from the other respondents were a little more mixed, but most of them defined it as protecting their own and their students’ data. This includes password-protection, a secure network, firewall and routines for digital archiving. Some of them also talked about the importance of privacy, and that they have a lot of sensitive information that needs to be protected.

Some of our respondents defined the term as safety online and that they should be aware of their digital footprints and have routines to avoid exposing themselves too much online. This definition is more related to the cybersafety aspect of information security.

Sensitive information

We asked our respondents how they would define sensitive information. All respondents stated that it was related to personal information and how important it is to keep it confidential. Some stated it was documents that should be kept internally and not shared with others, such as student files, personal information, documentation and grades for example. “If I need to talk to the child protection service, I have to keep in mind how sensitive the information I give them is. We have guidelines for what we can share with a colleague via email.” (I2, 2020) They were also saying it could depend from case to case what is regarded as sensitive information. “It is a consideration from case to case. It is hard to answer in general, I would rather consider it in each individual case.” (I2, 2020)

CIA – Model

None of the respondents knew the CIA-model by name. However, one of the IT-managers had already mentioned the components of the model when we asked them to define the term “information security”.

Passwords and Password Strength

We asked our respondents how long their passwords generally are, if they use any numbers, a mix of lower- and uppercase letters or special characters such as exclamation marks or question marks. The respondents stated that their password length is 8-12 characters. Everyone used numbers and lower- and uppercase letters. Most of them also used special characters. On most of the systems they have minimum requirements and guidelines for what the passwords should contain. The respondents also get notifications from the municipality when it is time to change their passwords. Most of the respondents stated that they do not change their password until they get notified. At home they very rarely change their passwords, partly because they do not get regular reminders to do so. Our respondents stated that their work-related passwords are stronger than the ones they use privately. They also stated that they found it hard to remember passwords on multiple systems. Therefore, some of them reused their passwords.

Some of the respondents stated that the municipality’s password requirements and guidelines were getting stricter. They can no longer alternate between two passwords and every password must be strong, unique and secure. They found that to be a good thing. However, some of them stated that a secure and complex password is important, but user-friendliness must be considered as well.

Multi-factor authentication

We asked our respondents if they used multi-factor authentication on any of their systems. Not everyone knew what we meant by multi-factor authentication at first, but all of them stated that had used it and knew how it worked when we explained it to them. Some of the systems at the school requires multi-factor authentication to log in already, but most do not. The principals and IT-department employees stated that they were working towards implementing multi-factor authentication for more of their systems.

Our respondent from the municipality stated that they would like to have more multi-factor authentication. They had prior experiences with some students pretending to be someone else and logging into their accounts. With multi-factor authentication this would be more difficult to accomplish.

There were mixed responses to introducing more multi-factor authentication, but the respondents agreed that it was important, especially in the systems that contain sensitive information. When they talked about sensitive data, they were not only talking about names, addresses and so on, but also student evaluations:

> Especially in the school context where we work with children's lives. We have a lot of sensitive information like grades, class lists and other personal information that no unauthorized people should have access to. It sounds very reasonable to have two checks to go through before being allowed to log in. It could be too insecure with just one. (T4, 2020)

Email and Attachments

Approximately 50% of all communication happens through email according to our respondents. They are sending and receiving emails daily. This means it is important to have good information security practices and routines for dealing with emails. They have routines for not sending sensitive information through email and instead use a secure archival system for that purpose. If they are referring to specific students, they use initials or other codewords to avoid transmitting personal information via email.

More and more of the communication between the teachers is happening through Microsoft Teams and the learning management system they have at the school. This transition away from email is encouraged by the municipality as a part of their new digitalization strategy that focuses on information security.

We asked our respondents if they ever opened attachments from unknown senders. None of the respondents stated that they do. They make sure to look at the name, email address, if the language seems suspicious and the context. Some of them stated that they sent a reply to the email, called the sender or asked them in person whether it was safe to open the attachment. If they were uncertain, they would ask the IT-department.

We also asked them if they had routines to make sure attachments are safe before they open them regardless if they are from a known sender or not. Most of the respondents seem to trust the filter from the municipality which filters out most of the spam, phishing attempts and viruses. They do not do any virus scans, but some look at the email address the email was sent from to make sure it is safe to open.

Phishing and Social Engineering

When we asked our respondents if they had experienced a phishing attempt, not everyone was sure what we meant by that term. Most of the respondents had heard about the concept when we explained it to them. None of them except one had experienced it personally as far as they knew. The one teacher that had experienced it was suspicious about an email they had received. It was from someone they did not have regular have contact with. One hour later they received an email that warned that this was a phishing attempt. Most of the phishing attempts targeting schools are blocked by a filter or firewall provided by the municipality.

Some our respondents stated that they knew someone who had fallen for a phishing attempt. They stated that some of their colleagues would click on everything without making sure the content in the email was safe. However, they stated that they trust the filtering system from the municipality, and that not many malicious emails slip through. If a malicious email should slip through the filter, the municipality is usually quick to send out an email warning everyone about the email in question.

When we asked about social engineering, none of the respondents had heard the term before.

Preventative measures

We asked the IT-managers and principals if they had any preventative measures. They stated that they do a risk and vulnerability analysis to map potential threats and have solutions for dealing with them, including threats regarding information security. They pick a team from different positions at the school, and they make a report. This report is later shared with the teachers. In addition to this, they also get regulations and guidelines from the municipality that they must follow.

When asked about how they perceive the focus on information security at their school, one of the principals stated the following:

> We still have potential for improvement. We did a risk and vulnerability analysis on our systems last year. Right now, we are focusing heavily on logging off the computer before leaving the classroom. The focus is there, but we need constant reminders to keep focus high. (P1, 2019)

4.2.2 Integrity

Integrity is about always keeping the information up to date and correct. A big part of integrity is to reduce information duplication, since having multiple copies of the same information makes it much harder to keep them all updated. Having good storage practices and a unified platform to store information will benefit information integrity greatly. In this subchapter we will discuss our findings related to information integrity.

The Term "Information Security"

Only one of the IT-mangers mentioned integrity specifically when we asked them to define information security. Some of the others mentioned digitally archiving as an important aspect. This be considered a matter of integrity.

We also asked them how they perceive the focus on information security at their school. Most of them were satisfied with the current level of focus on information security. They feel that the focus is increasing every year as the school gets more and more digital. They used to have student files in a physical archive, but now everything is stored digitally. There are more regulations to follow regarding sensitive information, especially GDPR. At the same time the municipality is focusing on standardization, which will help maintain information integrity.

Sensitive information

When we interviewed the representative from the municipality, they stated that there had been some issues regarding integrity and sensitive information. Whenever there is an incident involving bullying, the teacher who discovers it must write a 9A-case. The schools we interviewed had a special system for handling these 9A-cases called Compilo. However, the teachers sometimes write these incident reports in Office documents and save them to their One Drives instead:

> We have 9A-cases related to bullying of students. We hear about teachers who for example write 9A-cases in an Office document. This is an example of insecure storage, and we want them to use the system that already is place, Compilo. Whenever teachers write 9A-cases in Office documents, they are told to report them in Compilo instead. (M1, 2020)

Leaving computer logged in and lending it to students

None of the teachers we interviewed lent their computer or iPad to students if they had forgotten theirs at home. If a student forgets their iPad, they must use pen and paper or take turns using a fellow student's iPad. Some schools have spare iPads for the purpose of lending it to students who forgot theirs at home. A few of our respondents admitted to previously having lent a student their computer, but that never happens anymore.

We also asked if they ever left their iPads or computers without logging off. They stated that this never happens. Some stated that it might have happened before, but not anymore. This was an issue that was recently taken up in a meeting at one of the schools. "No, we do not leave the classroom without logging of. We use tablets a lot more now, but we make sure to lock it whenever we leave it unattended. This is something we have discussed lately." (T1, 2019)

Keyloggers and Backdoors

We asked our respondents if they have heard of either keyloggers or backdoors. None of our respondents had heard of these terms except one of the principals who had heard of backdoors. The principal stated it was a term they had heard, but they were not entirely sure what it meant. They went on to state that they had experienced that someone had opened a malicious email attachment before the municipality had time to issue a warning.

Memory sticks

Memory sticks are not used frequently anymore. It was more common in the past, and the teachers were weary of using memory sticks. This is no longer an issue:

> Memory sticks are rarely being used anymore. In the past students would use memory sticks for transferring their PowerPoint presentations to the classroom computer. Nowadays with Apple and everything, they can store it in the cloud and show it that way. (T4, 2020)

Most of the use cases for memory sticks have been taken over by the cloud, but some teachers stated still using memory sticks for backups of old assignments or presentations and transferring their own files between computers.

4.2.3 Availability

Availability of information is essential for the teachers to be able to do their jobs properly. Overall, there seems to have been a high focus on availability, with the municipality being responsible for the applications that are used for storing and sending information. The municipality states that their primary focus right now is standardization:

> Before we implemented 1:1 coverage there were huge differences between the schools. Now we are standardizing and minimizing these differences. We are also removing programs that we do not have adequate control over and entering data processing agreements (M1, 2020).

Software and hardware

Our respondents stated that the software they are using works most of the time, but there are occasional issues resulting in a loss of availability:

> There have been issues with our applications not working. Especially after we got our tablets. Usually the applications do not open at all or do not work properly. Recently I had to reinstall Word because it refused to open on my tablet and computer. It is a bit silly when the municipality tells us to use different software since we are an Office 365 municipality and then the applications do not work. You expect them to work properly since you have been told by the municipality to use them, but that is not always the case. (T2, 2019)

Some respondents also reported hardware issues:

> We teachers use a combination of computers and iPads, while all the students have iPads. Usually the software works fine, but the hardware can often be a problem. The tablets are much more limited in terms of software compared to our computers. I have not experienced any issues related to instability and downtime yet (T2, 2019).

Information Security practices

Although all our respondents acknowledged the importance of having strong passwords, many of them stated having trouble remembering them all: “As long as I can remember them all, I’m happy!” (S1, 2020). “There are incredibly many passwords for all the different places where I have to log in.” (I2, 2020). “I use the same password in multiple places. I know that this is not smart, but I need to be able to have an overview of all my passwords so I can remember them.” (P2, 2020).

When asked to change their passwords regularly, the problem grows even bigger, especially after the summer holidays. One of the teachers in our interviews stated the following: “Every year after the summer holidays it is complete chaos. It is a tradition that people arrive at work with a locked computer on the first day." (T1, 2019). The IT-department employees we interviewed also brought this issue up:

> The reminder to change passwords is often sent right before the summer holidays. This is incredibly bad timing. It is very common that people forget the password during the holidays, but most municipalities have a password portal where the teachers can log on and reset their passwords without involving us. (I2, 2020)

All the schools we interviewed reported this being a problem.

The introduction of more multi-factor authentication was also met with mixed responses from the respondents: "Oh, no. I have more than enough stuff to remember already!" (S1, 2020). "Absolutely! I think it is very important that it is difficult for potential attackers to access our systems. It needs to be easy and convenient for us to use, though." (T4, 2020). Overall, the respondents were positive if the solution being implemented was easy and convenient for them to use.

One of our respondents reported that teachers sharing their accounts to have access to more software is a big issue at their school:

> Now our focus is directed towards people sharing their usernames and passwords. It is more common than you would think that a teacher without access to a specific program borrows another teacher's account to get access. We are actively cleaning up our digital licenses and purchasing more to give more teachers access. (I2, 2020)

Email

Email is still the main form of communication between teachers according to our respondents. That is about to change with the move towards other solutions such as Microsoft Teams and Office 365. This has the added benefit of multiple users being able to edit and access the same document at the same time, increasing availability: "A lot of our information has already been digitalized, and now we have focused on improving our digitalization. We have shifted towards using online documents instead of sharing PDF-files via email for example" (I2, 2020).

Communicating via email also often results in information being lost when a principal quits the job for example: "We are trying to move away from email and towards Microsoft Teams. This also reduces the loss of information if a principal should quit and reduces the risk of sending an email to the wrong recipient" (M1, 2020). Teams handles the transition between principals and other key personnel better and prevents loss of information.

Incidents leading to a loss of information

In 2019, one of the schools we interviewed suffered a big loss of information. Both teachers and students lost all the data that was stored locally on their tablets. This was due to a system update from the operating system provider, which wiped all local storage for all the apps installed on the tablet:

> It did not impact me personally since I had a backup on my computer, but a lot of my students lost a lot of the work they had done on their tablets. The students were very upset when they realized that there was no way to recover the work they had lost. This should not happen. I find it strange that there is no safety net in the IT-department that catches these things. I thought they rolled out updates gradually instead of updating everything at once. I was lucky to have everything on my tablet saved in the cloud. It remains to be seen how secure the cloud is, though. (T2, 2019)

The teachers stated that they had received an email from the municipality with concrete measures to prevent this data loss from reoccurring, but they did not have the time to read it properly: "We have received an explanation, but I haven't had the time to look into it thoroughly." (T1, 2019). Meanwhile the IT-department stated that the municipality would be responsible for the measures:

> The municipality assumes responsibility. They have notified the supplier of the software and assured us that it should not repeat itself. That is all I know. I do not think they can guarantee anything. I am also unsure if all apps can save data to the cloud, so we may need to investigate other storage services. This is incredibly inconvenient. (I1, 2019)

4.3 KEY PROBLEM AREAS

We identified a total of 15 key problem areas in our findings. All these problem areas are summarized in the table below (Table 2):

Table 2: Key problem areas

Problem	Category
Lack of formal training	Cybersafety, Confidentiality, Integrity, Availability
Lack of management support	Cybersafety, Confidentiality, Integrity, Availability
Little skepticism towards software	Cybersafety, Confidentiality
Low focus on information security from the municipality	Cybersafety, Confidentiality, Integrity, Availability
Lack of time and resources	Cybersafety, Confidentiality, Integrity, Availability
Varying password strength	Confidentiality, Integrity, Availability
Low use of multi-factor authentication	Confidentiality, Availability
Low knowledge and awareness of information security	Cybersafety, Confidentiality, Integrity, Availability
Software issues	Availability
Hardware issues	Availability
Reuse of passwords	Cybersafety, Confidentiality, Availability
Forgotten passwords	Availability
Account sharing	Confidentiality, Integrity, Availability
Lost emails	Availability
Insufficient backup routines	Availability

From looking at the key problem areas we have identified, we can see that there are numerous problem areas caused by a low priority of and lack of focus on information security in schools coupled with a digitalization strategy from the municipality that focused on 1:1 coverage and introducing more digital teaching aids in the schools. Most of the problem areas span across multiple categories within information security.

5. Discussion

We identified 15 key problem areas in terms of information security in our findings section. In this discussion chapter we will discuss these problems and develop suggestions for how to improve the situation. All these suggestions are concrete measures to transition towards a more information security friendly organizational culture. The discussion will be divided into the same categories that we used for the results.

5.1 Cybersafety

The first issue related to cybersafety that we uncovered was lack of formal training. The Professional Digital Competence Framework for Teachers from 2017 states that teachers should be able to contribute to the students' development of digital judgement (Kelentric, Helland, & Arstorp, 2017). However, the teachers stated that they did not possess the necessary knowledge and awareness to teach their students about cybersafety. These findings align with the American study on preservice teacher knowledge mentioned chapter 2.0, where the teachers stated knowing about most topics within cybersafety but being unable to model or teach it to others (Pusey & Sadera, 2012).

The teachers also stated that they wanted to see more engagement from the management, while the principals often did not consider information security and cybersafety to be a primary concern. We think that a change in the organizational culture is necessary to remedy these issues, and that the municipality needs to encourage this change. A heightened focus on cybersafety and information security from the top management is a good place to start. We recommend that the municipality arranges information security and cybersafety courses and workshops to give all the principals a better understanding of information security and cybersafety. If the management's attitude towards information security is changed, the rest of the employees will most likely follow. We have seen examples of this from the Business Process Management literature, where top management support is frequently listed as one of the most important critical success factors to achieve change (Syed, Bandara, French, & Stewart, 2018). As soon as top management is on board, they are more likely to implement further changes to improve information security in their school.

The teachers often state that they do not have the time to learn about information security. We realize that the teachers have very hectic workdays and finding additional time to learn about information security may not be possible. It may therefore be necessary to give information security a higher priority at the expense of a different topic. For this to work, both the principal of the school and the municipality need to acknowledge the importance of information security topics. It is beyond the scope of this thesis to discuss exactly how the municipality and schools prioritize different topics, but we recommend giving information security a higher priority than it has today. We think that the Norwegian Directorate for Education and Training has taken a step in the right direction by adding digital skills to the curriculum, but this needs to be followed up by the municipalities and schools.

While the school transitions into a more information security friendly organizational culture, the students must still be taught about cybersafety and information security. We recommend arranging an “Information security week” like one of the schools in our thesis: Invite an external company or experts to do courses for the students and the teachers about information security and cybersafety related topics. Norway already has national initiatives such as privacy day and netiquette day. Extending these national initiatives to be more comprehensive and cover more topics related to information security is one potential way to create this information security week. This will help boost the knowledge and awareness levels of the teachers, while also ensuring that the students get the necessary knowledge to be safe online. Follow up with further courses and formal training for the teachers throughout the year to build up their competence.

In the past, the teachers have received information and individual tests via email from the municipality. These tests were sent out every year or every other year, depending on who we interviewed. We would recommend arranging yearly workshops where all the teachers can discuss information security topics and receive correct, updated information instead of these email tests. These workshops could be combined with our previous suggestion of arranging an information security week. Reading through some information in an email and completing a multiple-choice test is often perceived as tedious by the teachers. They wanted more opportunities for discussion and cooperation while learning about information security and arranging workshops will give them that. It also allows them to ask questions if they have any. As mentioned earlier, the municipality will have to prioritize differently for the teachers to have time to attend these workshops.

Teacher knowledge and awareness will also have to be maintained throughout the year. One of the principals brought up the need for constant reminders in our findings. We suggest spending five minutes or more every week during a lunch break discussing information security. We recommend talking about what went wrong and what to specifically watch out for based on recent incidents. This way everyone stays up to date and the awareness levels are maintained over time. It also encourages learning from past mistakes. Sharing this information with other schools and learning from each other’s mistakes is also highly encouraged. We realize that not everyone may be present every time but having regular discussions about information security topics is important to maintain awareness over time.

If the school has a teacher who is particularly passionate about information security, we would recommend appointing him or her as the information security champion of the school. We also recommend that this information security champion leads the weekly discussions about information security to create a stronger sense of ownership amongst the teachers. Having a passionate project champion is yet another of the most important critical success factors from the IS literature, and will help maintain awareness over time (Akkermans & van Helden, 2002).

We also found that many teachers use software that is not explicitly recommended by the IT-department. They perform few checks to make sure it is safe for use, and instead rely on recommendations from other teachers. We think that guidelines should be put in place when using such software. The Professional Digital Competence Framework for Teachers states that teachers should be able to do the following:

Can locate, critically evaluate, choose, and integrate digital teaching materials and digital learning resources based on pedagogical, subject didactic, and professional criteria, and adapt their use to the subject's content and methods (Kelentric, Helland, & Arstorp, 2017).

We would like to see an information security aspect of this critical evaluation as well. Avoiding the use of any software that requires the students to register an account is a very good starting point, and many teachers already do this. However, more checks should be made to make sure the company providing the software can be trusted, and that it is safe for educational use. The IT-department could be involved in this.

5.2 CONFIDENTIALITY

Passwords and password strength are one of the most essential and often the first step to good information security (Tomczyk, 2019). The teachers have multiple passwords on different systems and multi-factor authentication is used on a few of them. It can be very difficult to remember passwords when you must log on to so many different systems, which is one of the reasons teachers reuse their passwords. The reuse of passwords is not good information security practice and seems to be quite common amongst teachers based on our findings. None of the other studies that we found asked teachers if they reused their passwords. To mitigate this issue and strengthen information confidentiality, we recommend that teachers use a password manager for generating unique and strong passwords for every service they use. This password manager should be compatible with different systems such as iPads, laptops and phones. There are information availability benefits to this suggestion as well, which we will get back to in chapter 5.4.

We would also recommend using multi-factor authentication for the systems that have that as an option. It is particularly important to use multi-factor authentication on the password manager if this has been implemented. This will be an extra safety barrier to ensure that their data stay confidential. One of the factors could be geographical, and the other could be a notification on the phone that they must click to confirm. With the password manager auto-filling passwords, the login process overall should be more convenient than manually typing in a password and not using multi-factor authentication.

A big part of the communication between teachers happens through email, with our findings suggesting as much as 40-50%. Teachers do not open attachments from unknown senders, but many of them do if they know the sender. It is not uncommon for email accounts to be compromised, meaning that attachments from known senders may not always be safe. The firewall and filters from the municipality block most of the malicious emails targeting teachers, but some emails still get through on occasion. Therefore, we would recommend that teachers are more critical of attachments, even if they know the sender. They should be aware of the current context and why this person is sending an attachment. We also recommend that they check the senders address and see if it looks legitimate. They should also look at the language in the email to see if it looks grammatically correct, and that it is not just a hastily translated text using a translation program such as Google Translate. Additionally, we would recommend that they perform a virus scan of the attachment before opening it to ensure that it is safe to open or download.

We would also recommend that the teachers use systems such as Microsoft Teams to communicate with each other rather than using email. There is more of a limit to who you can send information to in Teams. By communicating with email, it is easier to send it to the wrong person, which could result in a breach of information confidentiality. As the municipality carries out its plans of standardizing the applications used throughout all the schools, every teacher, principal and IT-department employee should be able to communicate via Teams or similar software. Email will still be necessary when communicating with people outside the school system but the risk of internal communication being sent to an external party is gone.

Another important recommendation in terms of confidentiality is to utilize the knowledge of students who find ways to access confidential information. Ask the students that are particularly skilled in circumventing your school's security measures to explain how they do it and let them work together with the IT-department to patch the vulnerabilities.

5.3 INTEGRITY

The teachers read, store and share information on multiple different platforms regularly. Some of the information is sensitive, which means that there are separate guidelines for storage and sharing. The information is stored differently, with some of it being stored locally and some on a separate server or in the cloud. Sometimes there are also multiple copies of the same information stored in multiple places, which is a threat to information integrity. We would recommend that the teachers use one platform for storing information, instead of multiple different ones. If necessary, a secure area within this platform can be created for handling sensitive information, or an integration with the current secure archival system can be made. This will prevent conflicting information and outdated copies, while also making it easier to share and access information. The most prominent example of such integrated systems from the IS literature is ERP-systems (Enterprise Resource Planning), which have improved information flow across functional units in an organization since the 1990s (Jacobs & Weston Jr., 2007).

When it comes to lending computers, iPads, Chromebooks and such to their students, the teachers had good routines. They stated that they do not lend away their own hardware. If they did, a student could potentially enter the school's systems and change their own grades or other information about other students. The teachers seem to be aware of the potential problems this could cause. Even though none of the teachers we interviewed stated that they lend their hardware to students anymore, monitor 2019 found that between 18.7 and

21.8% of students had used their teacher’s computer (Fjørtoft, Thun, & Buvik, 2019). There are several possible explanations: The teachers may have given us more “correct” answers due to our background as information systems students, we may have interviewed teachers with above average interest in information security or there may have been an increased focus on this particular practice recently. The teachers also have good routines for not leaving their computer or iPad logged in when they are not in the room. It is important that this focus and awareness is maintained over time and having regular discussions about it during the lunch break as mentioned above is one possible solution to maintain this awareness.

All of our respondents were unaware of what keyloggers and backdoors are, which corresponds well with the American study mentioned in chapter 2.0, where teachers scored 1.58 and 1.49 on these topics respectively (Pusey & Sadera, 2012). These two threats pose a significant risk to information confidentiality and integrity. It is therefore important that the teachers know about these threats and how to identify and avoid them. As mentioned earlier in the discussion about cybersafety, we recommend that yearly workshops and an information security week is arranged to give teachers the necessary knowledge about these topics.

Memory sticks are as mentioned in chapter 4.0 not commonly used anymore. Regardless, the teachers should be careful when using memory sticks given to them by someone else and should exercise the same caution as when opening an email attachment. Ideally, memory sticks should be phased out entirely and be replaced by cloud solutions.

5.4 AVAILABILITY

The municipality is actively working on standardizing the applications used by all the schools, which we think is a good idea to ensure data availability. It is easier to communicate and share information in safe ways with municipality-approved and standardized software. At the same time, this does lead to some issues: Teachers keep using the old ways of communication and store information in the wrong places, making it harder to find later down the line and potentially resulting in a loss of information when those services are phased out completely. It is therefore important to make sure teachers receive adequate training in the use of these new standardized applications and that they perceive the new applications as useful. The Technology Acceptance Model (TAM) states that a user’s intention to use technology is based on the perceived ease of use and perceived usefulness of the technology (Chuttur, 2009). Proper training will result in an increased perceived ease of use.

Both the software and hardware are expensive and difficult to replace, so our only recommendation here would be to ensure proper training when introducing new software/hardware and to do thorough research on reliability, stability and security before procuring new software or hardware.

A lot of the teachers, principals and IT-department employees stated that they had very many different passwords and remembering them all was difficult. Many also stated that they used the same password in multiple places. The respondents would often forget their passwords when asked to change them right before the summer holidays, resulting in many people showing up with a locked PC on the first day. We would recommend using a password manager to remedy these issues. Using a password manager would result in the respondents only needing to remember one password: The one required to log in to their password manager, resulting in improved availability.

Once the teachers are logged into their password manager, it will take care of logging in anywhere else. Many teachers today use Feide to log in to most of the services they need during a normal workday (Fjørtoft, Thun, & Buvik, 2019). However, it is not possible to use Feide to log in to everything. A password manager will solve this issue by being compatible with Feide login as well as every other service that is not supported by Feide login. The password manager will conveniently auto fill passwords for any applications and update the passwords when prompted, saving the respondents time. In other words, the password manager will replace Feide login with a solution that supports every service a teacher needs across all his or her devices. We would highly recommend using multi-factor authentication when logging in to the password manager, along with a strong password. As mentioned earlier in this chapter, it is also very important that the teachers receive adequate training in the use of password managers before they are introduced.

Despite the mixed responses from our respondents, we recommend more use of multi-factor authentication, especially when dealing with sensitive information. With the convenience of a password manager and no longer having to remember several passwords, we think that most people would be open to using more multi-factor authentication. We recommend using location (Only being able to log in to certain services from the school's internal network, with a Virtual Private Network (VPN) alternative for home office) and a code from a physical authenticator or an authenticator app on a phone or tablet. Try implementing solutions where an authenticator key is only required when logging on from a new computer, or once a day/week to balance availability and confidentiality. The most important prerequisite for this change to work is once again an organizational culture that emphasized information security and cybersafety, while making sure the perceived ease of use is high so that the technology gets accepted by the teachers (Chuttur, 2009).

Having implemented a password manager and more multi-factor authentication will also discourage the sharing of accounts to access specific software. Most people would be more hesitant to give someone else full access to all their passwords and accounts, while the multi-factor authentication forces both parties to go through an additional step when sharing accounts. However, perceived ease of use is once again a significant factor here according to the TAM (Chuttur, 2009). Therefore, our main recommendation to remedy this issue is to keep acquiring more digital licenses so that all employees can use all the software they need.

We think that the municipality is doing a good job of standardizing applications and moving the communication away from email, towards other communication platforms such as teams. The increased use of document co-authoring is also a good change, both in terms of convenience and availability in general. However, we recommend making sure all the employees receive adequate training in the use of this software. Inadequate training will result in reduced availability and potential problems as users will attempt to circumvent the new standardized software. Somers and Nelson list user training and education as a critical success factor when implementing ERP-systems and this would apply to other system implementations or standardization projects as well (Somers & Nelson, 2001).

In terms of incidents that cause a loss of data, our recommendation would be to introduce a more robust backup system. Select a trustworthy cloud storage company to handle the backup. Save everything both locally and to the cloud. Make sure that updated are rolled out to a select few devices first and fix any problems that occur before rolling them out to everyone. For schools with a particularly tech-savvy IT-department, they could consider doing local backups as well, such as a local grandfather-father-son backup system (Sathiyanantham, 2019). We still recommend having a cloud-based backup system even when doing local backups.

5.4 Key problem areas with suggestions

Below is a version of our results summary table with added suggestions for each identified problem area (Table 3).

Table 3:Key problem areas with suggestions

Problem	Category	Suggestion
Lack of formal training	Cybersafety, Confidentiality, Integrity, Availability	Courses and workshops for the teachers and students held by experts or external companies.
Lack of management support	Cybersafety, Confidentiality, Integrity, Availability	Change in culture encouraged by the municipality, information security workshops for principals.
Little skepticism towards software	Cybersafety, Confidentiality	Higher awareness and knowledge levels with regular discussions about security.
Low focus on information security from the municipality	Cybersafety, Confidentiality, Integrity, Availability	Change of focus towards information security.
Lack of time and resources	Cybersafety, Confidentiality, Integrity, Availability	The municipality should prioritize information security higher.

Varying password strength	Confidentiality, Integrity, Availability	Introduce password manager.
Low use of multi-factor authentication	Confidentiality, Availability	More use of multi-factor authentication.
Low Knowledge and awareness of information security	Cybersafety, Confidentiality, Integrity, Availability	More formal training on information security terms and information security in general. Appoint a project champion to lead regular discussions and initiatives.
Software issues	Availability	A thorough research process before software procurement, more focus on training in software use.
Hardware issues	Availability	Regular hardware updates, more focus on taking good care of the hardware.
Reuse of passwords	Cybersafety, Confidentiality, Availability	Introduce a password manager.
Forgotten passwords	Availability	Introduce a password manager.
Account sharing	Confidentiality, Integrity, Availability	More use of multi-factor authentication. Ensure everyone has the digital licenses they need.
Lost emails	Availability	Move away from email towards other solutions such as MS Teams.
Insufficient backup routines	Availability	Team up with cloud backup providers, consider local backups. Improve backup routines.

As the table shows, most of our suggestions for improving the situation rely on a change in the priority of information security from the municipality and principals. We would also like to stress the importance of changing the organizational culture to be more focused on information security. These changes will take time to implement, and top management support is essential for the changes to occur (Syed, Bandara, French, & Stewart, 2018).

6. CONCLUSION

In this chapter we answer our research questions and summarize our findings. We will also present limitations for our thesis, as well as possible future research related to our findings. Our research questions are as follows:

RQ1: How are teachers' awareness, knowledge and practice about information security in school?

RQ2: How can teachers improve their awareness, knowledge and practice about information security?

With this thesis we were aiming to figure out how teachers' knowledge, awareness and practice of information security were in school. We found out that some of the areas we examined in this thesis were good, but there were also room for improvements in several areas. We have identified 15 key problem areas and developed suggestions detailing how the situation can be improved. The main change that needs to happen is a change in organizational culture to be more information security friendly, and our suggestions are concrete measures to achieve that. We found several problem areas regarding passwords, and we recommend that they use a password manager and multi-factor authentication where this is possible. In general, we see that there is a lack of training in information security. Some common terms about information security are unknown for many of the teachers in this thesis. According to the Professional Digital Competence Framework, teachers should have more knowledge and better practices than what we found out in this thesis. The teachers have a very busy schedule and have very little time to spare for formal training. The municipality should prioritize information security higher than they are doing today and allow the teachers more time to learn about information security. With more and more integration of technologies in schools, it is important that the users of the technology have adequate knowledge about it. It is important that teachers have knowledge of potential risks and how to minimize them. We would like to see more proactive risk management going forward. Teachers need to receive adequate training and knowledge about the technology prior to implementation, not the other way around. That is why we find it important that the municipality have information security as a priority.

There must be a change towards a more information security friendly culture in the schools. The teachers should be encouraged and supported by the municipality and principals to build a strong information security culture. This is not done overnight but needs time to be implemented. It is important to understand that every individual in the school system has their own responsibility for maintaining the information security. By building a strong information security culture, everyone will be aware that they are responsible for information security in school in some way or another and proactively prevent incidents from happening. We think that our suggestions will contribute to achieving this cultural change.

6.1 LIMITATIONS

In this chapter we will discuss the limitations of our thesis. Both the methods used in this thesis and the sample we picked introduces limitations. Lastly, we will discuss what we did to limit the impact of these limitations and assure the reliability of our results.

Due to time and resource constraints, we were unable to send interview transcripts back to the interviewees for checking. This could potentially mean that we have misinterpreted or misquoted what the interviewees meant or stated. We consider this to be a minimal risk since our recording quality was clear, and we asked for clarification whenever we were unsure of what the respondent meant.

Another potential limitation of our thesis is the impact the interviewers can have on the interviewee. The effect of the researcher and the context mean that consistency and objectivity are hard to achieve. The interviews can also potentially be misleading due to us relying on what the interviewees say they do, rather than what might really be the case (Oates, 2012). This issue is particularly relevant in our case: Two master students in information systems from the University of Agder visiting a school to conduct and interview about information security, a topic many teachers may be uncomfortable with, may impact the results. The data gathered can also be artificial since the interviewees know they are speaking for the record, so false impressions may be given (Oates, 2012).

We have tried to reduce the impacts of these limitations by comparing our data to data gathered from larger quantitative and qualitative studies in various countries and looking for patterns. All the respondents have also been anonymized to reduce the chances of them providing us with “the correct answer” instead of what they would normally do. We have also presented our findings to teachers and other people who are familiar with the context we studied in form of oral presentations. The feedback we received on those presentations was that we described the situation accurately, and they can relate to the issues that we bring up.

It is also hard to generalize our findings to a larger population due to conducting a limited number of interviews in a geographically limited area. We know that some municipalities have progressed further in the digitalization process and changed their focus to information security earlier. The municipality we interviewed stated that they cooperated with a municipality that was ahead of them in terms of digitalization and tried to learn from their mistakes. We have taken this into consideration and interviewed teachers from two different municipalities in different stages of the digitalization progress. Although the teachers in the more advanced municipality had slightly higher knowledge and awareness levels, the same key problem areas were still present in both municipalities. Most of the schools we interviewed were from the less advanced municipality.

6.2 Implications

We think this thesis has both theoretical and practical implications. Furthermore, we think that the thesis could be of use in both the educational field and the information systems field.

Theoretical implications

This thesis is to our knowledge the first qualitative deep dive into the information security situation in Norwegian schools. We have mapped out the information security situation in Agder and developed potential solutions to key problem areas within information security in schools. This thesis can be used as a basis for further studies on information security topics in schools and is therefore contribution to the very limited literature on the topic of information security in Norwegian schools.

Practical Implications

The thesis also has practical implications. Our goal from the start was to be able to give something back to the teachers, principals and IT-department employees who spent some of their very limited time answering our interview questions. We therefore came up with 15 concrete suggestions for how the schools can improve in the key problem areas that we discovered. We hope that the schools find these suggestions useful and would love to see some or all of them being implemented in the future!

6.3 Further Research

In this chapter we will discuss opportunities for further research. We would like to highlight three different potential directions: Further studies on this topic, a study on students' knowledge, awareness and practice in information security and a case study on implementing our suggestions in a school.

Further studies on this topic

Our thesis focused mainly on cybersecurity and cybersafety in schools in Agder. A further development of this thesis could be to include cyberethics and try to make the findings more generalizable. We would suggest starting out with a quantitative approach to map out the situation in a more generalizable way. You could then proceed to do a qualitative study to dive deeper into the findings of the quantitative study. Using the whole C3 framework also allows you to explore topics such as copyright online etiquette, hacking and online addictions, and how teachers deal with these topics.

A study on students' knowledge, awareness and practice in information security

Our thesis does not map the students' knowledge, awareness and practice in information security. This would be an interesting topic for further research, especially in primary school. Grades 11-13 have had 1:1 coverage with laptops for a long while and primary schools are now doing the same. Do the students in primary school have adequate knowledge and awareness on the topic? Where do they gain this knowledge from? Are the parents and teachers the main sources of information or are the students self-taught?

A case study on implementing our suggestions

We have identified 15 key problem areas and developed suggestions for how to improve in these areas. A case study of a school trying to implement these suggestions would be very interesting. A combination of qualitative methods such as interviews and observation could be used to explore the effects of implementing our suggestions and potential problems. These experiences would be very useful for other schools attempting to improve their information security knowledge, awareness and practices.

7. REFERENCES

Akkermans, H., & van Helden, K. (2002). Vicious and virtuous cycles in ERP implementation: a case study of interrelations between critical success factors. *European Journal of Information Systems*.

Buchanan, R., Southgate, E., & Smith, S. (2019). 'The whole world's watching really': Parental and educator perspectives on managing children's digital lives. *Global studies of childhood*.

Chuttur, M. (2009). Overview of the Technology Acceptance Model: Origins, Developments and Future Directions. *Sprouts*.

Digitaliseringsdirektoratet. (2020). *Begrepsliste: Informasjonssikkerhet*. Hentet fra Difi: https://internkontroll-infosikkerhet.difi.no/begrepsliste-informasjonssikkerhet

Fjørtoft, S. O., Thun, S., & Buvik, M. P. (2019). *Monitor 2019.* Trondheim: SINTEF.

Fruhlinger, J. (2020, February 10). *The CIA triad: Definition, components and examples*. Hentet fra CSO: https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html

GDPR.EU. (2020, May 31). *What is GDPR, the EU's new data protection law?* Hentet fra GDPR.EU: https://gdpr.eu/what-is-gdpr/

Grebennikov, N. (2007, March 29). *Keyloggers: How they work and how to detect them (Part 1)*. Hentet fra Securelist: https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/

Jacobs, R., & Weston Jr., T. (2007). Enterprise resource planning (ERP) - A brief history. *Journal of Operations Management*.

Jacobsen, D. (2015). *Hvordan gjennomføre undersøkelser?* Cappelen Damm Akademisk.

Johansen, E. N. (2019, January 25). *Nektar å godta historisk millionbot frå Datatilsynet*. Hentet fra NRK: https://www.nrk.no/hordaland/bergen-kommune-meiner-millionbot-fra-datatilsynet-er-for-hog-1.14394292

Karabatak, S., & Karabatak, M. (2018). Teachers' Knowledge Levels About Virtual Information Security. *IEEE*.

Kelentric, M., Helland, K., & Arstorp, A.-T. (2017). *Professional Digital Competence for Teachers.* The Norwegian Center for ICT in Education.

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing Systematic Literature Reviews in Software Engineering.* Keele University & Durham University.

Kritzinger, E. (2017). Cultivating a cyber-safety culture among school learners in South Africa. *Africa Education Review*.

LastPass. (2020, May 31). *What is a password manager?* Hentet fra LastPass: https://www.lastpass.com/password-manager

Lawson, P., Pearson, C., Crowson, A., & Mayhorn, C. (2020). Email phishing and signal detection: How persuation principles and personality influence response patterns and accuracy. *Applied Ergonomics*.

Lujan, V. (2019, October 18). *What is Multi-Factor Authentication*. Hentet fra Security Boulevard: https://securityboulevard.com/2019/10/what-is-multi-factor-authentication-mfa/

M1. (2020, March 4). Knowledge, Awareness and Practice on Information Security in School. (R. Vålandsmyr Olsen, & S. Tokerud, Intervjuere)

Nätt, T. (2019, November 22). *Bakdør (Backdoor)*. Hentet fra Store Norske Leksikon (Big Norwegian Lexicon): https://snl.no/bakd%C3%B8r

Oates, B. (2012). *Researching Information Systems and Computing.* Coydon: SAGE.

Oxford University. (2020, May 11). *Awareness*. Hentet fra Lexico: https://www.lexico.com/definition/awareness

Oxford University. (2020, May 10). *Knowledge*. Hentet fra Lexico: https://www.lexico.com/definition/knowledge

Oxford University. (2020, May 11). *Practice*. Hentet fra Lexico: https://www.lexico.com/definition/practice

Pusey, P., & Sadera, W. (2012). Cyberethics, Cybersafety and Cybersecurity: Preservice Teacher Knowledge, Preparedness, and the Need for Teacher Education to Make a Difference. *Journal of Digital Learning in Teacher Education*.

S1. (2020, February 20). Knowledge, Awareness and Practice on Information Security in School. (R. Vålandsmyr Olsen, & S. Tokerud, Intervjuere)

Sathiyanantham, V. (2019, September 19). *Grandfather-Father-Son Backup Retention*. Hentet fra Medium: https://medium.com/@as.vignesh/grandfather-father-son-backup-retention-509110f8d692

Somers, T., & Nelson, K. (2001). The Impact of Critical Success Factors across the Stages of Enterprise Resource Planning Implementations. *Proceedings of the 34th Hawaii International Conference on System Sciences.* Hawaii: IEEE.

Syed, R., Bandara, W., French, E., & Stewart, G. (2018). Getting it right! Critical Success Factors of BPM in the Public Sector: A Systematic Literature Review. *Australasian Journal of Information Systems*.

Tomczyk, Ł. (2019). Skills in the area of digital safety as a key component of digital literacy among teachers. *Education and Information Technologies*.

Udir. (2020). *Kompetanse i fagene*. Hentet fra Udir.no: https://www.udir.no/lk20/overordnet-del/prinsipper-for-laring-utvikling-og-danning/kompetanse-i-fagene/

Vålandsmyr Olsen, R., & Tokerud, S. (2019). *A Literature Review on Teachers' Awareness and Knowledge of Information Security in School.* Kristiansand: Universitetet i Agder.

8. APPENDICES

8.1 INTERVIEW GUIDE FOR TEACHERS, IT-DEPARTMENT EMPLOYEES AND PRINCIPALS NORWEGIAN

Demografisk

Alder?

Klassetrinn? (Hvis relevant)

Fag?

Hvor lenge har du undervist?

Hvor lenge har du brukt digitale hjelpemidler i undervisningen?

Bruker du mye IT på fritiden?

Kunnskap og bevissthet rundt informasjonssikkerhet

Hva legger du i begrepet "Informasjonssikkerhet"? **(Kunnskap og bevissthet)**

Har du hørt om CIA-modellen for informasjonssikkerhet? **(Kunnskap, bevissthet)**

Hvordan oppfatter du fokuset på informasjonssikkerhet ved skolen? **(Bevissthet)**

Får dere noen form for formell opplæring angående informasjonssikkerhet? **(Kunnskap)**

Hvordan holder du deg oppdatert? (retningslinjer, initiativer fra skolen) **(Bevissthet og Praksis)**

Hvordan vil du selv beskrive ditt kunnskaps- og bevissthetsnivå om informasjonssikkerhet? **(Kunnskap og bevissthet)**

Hvor stor del av kommunikasjonen mellom deg og andre ansatte går via epost? **(Praksis)**

Hva legger du i begrepet sensitiv "informasjon"? **(Bevissthet, Kunnskap)**

Har det skjedd at du sender sensitiv informasjon (f.eks. Personopplysninger, interne dokumenter osv.) via epost? **(Bevissthet og Praksis)**

Hva legger du i begrepene “phishing” og “social engineering”? **(Kunnskap, bevissthet)**

Har du hørt om bakdører og keyloggere? Hva innebærer disse begrepene? **(Kunnskap, bevissthet)**

Har det skjedd at du har blitt utsatt for phishing (Social engineering, bedrageri) forsøk? **(Kunnskap og Bevissthet)**

Hender det at du åpner vedlegg fra ukjente epostadresser? **(Bevissthet og Praksis)**

Hvordan forsikrer du deg om at vedlegg du mottar via epost er trygge før du åpner dem? **(Praksis, Kunnskap)**

Har du hørt om de fem autentiseringsfaktorene? Kan du nevne noen? **(Kunnskap)**

Hvor viktig mener to to- eller flerfaktorautentisering (to- eller flertrinns-verifisering) er? **(Bevissthet)**

Hvor viktig mener du passordstyrke er? **(Bevissthet)**

Hva er din definisjon på et sikkert passord? **(Kunnskap)**

Passord **(Praksis)**
Passordlengde (antall tegn totalt)

Tall

Små/store bokstaver

Spesialtegn (f.eks. !”#¤%)

Hvor ofte bytter du passord?**(Praksis)**

Hender det at du bytter passord uoppfordret? **(Praksis)**

Lærere

Hvordan går du frem for å rapportere avvik? Har dere rutiner som dere følger? **(Praksis)**

Hvor stor tillit har du til programvare du blir bedt om å bruke av IT-avdelingen? **(Bevissthet)**

Hvor ofte bruker du annen programvare enn den du har blitt bedt om å bruke av IT-avdelingen i jobbsammenheng? **(Bevissthet og Praksis)**

Hva gjør du for å forsikre deg om at et program som ikke er direkte anbefalt av IT-avdelingen er sikkert før bruk? (Se på omdømme, sikkerhetshull etc.) **(Bevissthet)**

Hvor ofte forlater du klasserommet uten å logge ut av PC-en? **(Bevissthet og Praksis)**

Hender det at du låner bort din egen PC hvis en elev har glemt sin? Bærbar eller stasjonær? **(Bevissthet og Praksis)**

Hvordan håndterer du minnepinner du får fra elever eller kollegaer? Sjekker du om de er trygge før bruk? **(Bevissthet, kunnskap)**

IT-ansvarlig

Har dere en digitaliseringsstrategi? Hvis ja, forklar litt om målsettinger, tiltak etc. **(Kunnskap og bevissthet)**

Hvilke tiltak innebærer denne strategien for å bedre informasjonssikkerhet i skolen? **(Kunnskap og bevissthet)**

Har dere en handlingsplan for informasjonssikkerhet eller en handlingsplan for digitalisering som omfatter informasjonssikkerhet? **(Bevissthet)**

Hvilke initiativer har dere for å holde lærerne oppdatert? **(Bevissthet og Praksis)**

Hvilke forebyggende tiltak har dere? **(Kunnskap og bevissthet)**

Hvordan velger dere ut software som skal brukes av ansatte? (Kriterier osv.) **(Kunnskap og Praksis)**

Står lærerne fritt til å bruke annen software enn den dere anbefaler? (Hvis ja, hva mener dere om det?) **(Bevissthet)**

Rektor/ledelse

Har dere en digitaliseringsstrategi? Hvis ja, forklar litt om målsettinger, tiltak etc. **(Kunnskap og bevissthet)**

Hvilke tiltak innebærer denne strategien for å bedre informasjonssikkerhet i skolen? **(Kunnskap og bevissthet)**

Har dere en handlingsplan for informasjonssikkerhet eller en handlingsplan for digitalisering som omfatter informasjonssikkerhet? **(Bevissthet)**

Hvilke initiativer har dere for å holde lærerne oppdatert? **(Bevissthet og Praksis)**

Hvilke forebyggende tiltak har dere? **(Kunnskap og bevissthet)**

Har dere rutiner for rapportering av avvik? **(Praksis)**

Avsluttende spørsmål

Hvem har ansvaret for informasjonssikkerheten i skolen? **(Kunnskap, bevissthet)**

Har du flere tema innen informasjonssikkerhet som mener er viktige? **(Kunnskap og bevissthet og praksis)**

8.2 INTERVIEW GUIDE FOR MUNICIPALITIES NORWEGIAN

Kunnskap og bevissthet rundt informasjonssikkerhet

Hva legger du i begrepet “Informasjonssikkerhet”? **(Kunnskap og bevissthet)**

Hørt om CIA-modellen? **(Kunnskap)**

Hvordan oppfatter du fokuset på informasjonssikkerhet i kommunen? **(Bevissthet)**

Får dere noen form for formell opplæring angående informasjonssikkerhet? **(Kunnskap)**

Hvordan holder du deg oppdatert? (retningslinjer, initiativer fra skolen) **(Bevissthet og Praksis)**

Hvordan vil du selv beskrive ditt kunnskaps- og bevissthetsnivå om informasjonssikkerhet? **(Kunnskap og bevissthet)**

Hva legger du i begrepet sensitiv “informasjon”? **(Bevissthet, Kunnskap)**

Hva legger du i begrepene “phishing” og “social engineering”? **(Kunnskap)**

Har det skjedd at du har blitt utsatt for phishing (Social engineering, bedrageri) forsøk? **(Kunnskap og Bevissthet)**

Har dere rutiner for å blokkere farlige eposter som sendes til skolene? **(Praksis)**

Har du hørt om de fem autentiseringsfaktorene? Kan du nevne noen? **(Kunnskap)**

Hvor viktig mener to to- eller flerfaktorautentisering (to- eller flertrinns-verifisering) er? **(Bevissthet)**

Hvor viktig mener du passordstyrke er? **(Bevissthet)**

Hva er din definisjon på et sikkert passord? **(Kunnskap)**

Retningslinjer for passord/2FA ved bruk av kommunale ressurser? **(Praksis)**
Passordlengde (antall tegn totalt)

Tall

Små/store bokstaver

Spesialtegn (f.eks. !”#¤%)

Hvor ofte må ansatte i skolen bytte passord?**(Praksis)**

Har dere en digitaliseringsstrategi? Hvis ja, forklar litt om målsettinger, tiltak etc. **(Kunnskap og bevissthet)**

Har dere en handlingsplan for informasjonssikkerhet eller en handlingsplan for digitalisering som omfatter informasjonssikkerhet? **(Bevissthet)**

Hvilke initiativer har dere for å holde skolene oppdatert? **(Bevissthet og Praksis)**

Hvordan jobber dere for å øke kunnskap og bevissthet rundt informasjonssikkerhet i skolen? **(Kunnskap og bevissthet)**

Holder dere kurs for skolene? (Kan vi eventuelt få innsyn i kursmaterialet?) **(Kunnskap, bevissthet)**

Hvilke forebyggende tiltak har dere? **(Kunnskap og bevissthet)**

Hvordan velger dere ut software som skal brukes av skolene? (Kriterier, bakgrunnssjekk osv.) **(Kunnskap og Praksis)**

Står skolene fritt til å bruke annen software enn den dere anbefaler? (Hvis ja, hva mener dere om det?) **(Bevissthet)**

Hvilke rutiner har dere for håndtering av avvik relatert til informasjonssikkerhet? **(Praksis)**

Hvem har ansvaret for informasjonssikkerheten i skolen? **(Kunnskap, bevissthet)**

Har du flere tema innen informasjonssikkerhet som mener er viktige? **(Kunnskap og bevissthet og praksis)**