NTNU
Norwegian University of
Science and Technology

Information Security in Norwegian High Schools

A Case Study

Leif Olav Fjellingsdal

15-12-2016

Master's Thesis

Master of Science in Information Security

30 ECTS

Department of Computer Science and Media Technology

Norwegian University of Science and Technology, 2016

Supervisor: Professor Stewart Kowalski, NTNU

Abstract

In Norwegian high schools, the use of information technology has changed dramatically the last years. At the same time, challenges related to information security have grown. Several students are just curious and want to find out what resources are possible to reach, and some have even modified their own grades. Others are more destructive, and some have spoiled the exams for both their own school and the rest of the county. There have also been other types of incidents related to information security in the schools.

This master thesis is a case study, trying to identify the threats the schools are facing. One single school is examined in a qualitative study, which means that the finding are not necessarily representative.

The study use a socio-technical approach, i.e. a view where information systems are seen as much more than machines, electronics and software. The socio-technical view describes the information system as an interaction between humans and machines.

The analysis show that the school are relatively well prepared to handle certain types of security incidents, especially on technical level. On the other hand, the school also have some considerable challenges, especially on the social levels.

Sammendrag

I norske videregående skoler har broken av informasjonsteknologi endret seg dramatisk de siste årene. I den samme perioden har utfordringer knyttet til informasjonssikkerhet økt betraktelig. En del elever er nysgjerrige og ønsker å finne ut hva slags ressurser de klarer å nå, og noen har til og med klart å endre sine egne karakterer. Andre er mer destruktive, og noen har klart å ødelegge eksamen, ikke bare for egen skole, men for hele fylket. Det har også vært andre typer hendelser knyttet til informasjonssikkerhet i skolene.

Denne masteroppgaven er en case studie som forsøker å identifisere truslene som skolene står overfor. En enkelt skole er undersøkt i en kvalitativ undersøkelse, noe som betyr at funnene ikke nødvendigvis er representative.

Studien har en sosio-teknisk tilnærming, dvs. et syn der informasjonssystemet blir sett på som mye mer enn maskiner, elektronikk og programvare. Det sosio-tekniske tilnærmingen beskriver informasjonssystemet som en samhandling mellom mennesker og maskiner.

Analysen vise at skolen er relativt godt forberedt på sikkerhetshendelser, spesielt på teknisk nivå. På den annen side, skolen har også noen betydelige utfordringer, spesielt på de sosiale nivåene.

Preface

This master thesis represents the end of journey that started in 2013. I have worked with ICT for many years, and within this field, security has always interested me. When I became aware of the Master's program in Information Security in Gjøvik, I decided to apply almost immediately. This journey has indeed given me a large amount of new knowledge.

Now, at the end of the study, I have many people to thank for their help. First my supervisor, Professor Stewart Kowalski. He was lecturer in two of my previous subjects, and the reason for choosing this thesis. I will also thank all the participating informants, especially the principal and the two ICT informants. Thanks also to my employer for allowing me to spend time on exams and this thesis, and thanks for all help from to my colleagues and good friends. And finally, a special thanks to my dear family, you have been a fantastic support. A special little thank goes to my baby granddaughter Mia, you bring so much light to all of us.

Table of content

List of figures

List of tables

Abbreviations

BIOS	Basic Input/Output System
BYOD	Bring Your Own Device
CAD	Computer-Aided Design
CEO	Chief Executive Officer
DDoS	Distributed Denial of Service (Attack)
DMZ	Demilitarized Zone
EAP	Extensible Authentication Protocol
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IEEE	The Institute of Electrical and Electronics Engineers Standards Association
IP	Internet Protocol
IS	Information System
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
LMS	Learning Management System
NTNU	Norwegian University of Science and Technology
OS	Operating System
PEAP	Protected Extensible Authentication Protocol
SAS	School Administration Software
SBC	Security By Consensus
SCCM	System Center Configuration Manager

STS	Socio-Technical System
UPS	Uninterruptible Power-Supply
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

1 Introduction

Over the past years, the use of computers in Norwegian high schools has changed dramatically. The primary purpose of a high school is to educate students aged 16-19 years old. In Norway, 13 years of school attendance is a legal right, and almost all (98 %) 16 year old youths start in high school after completing junior high school, which is mandatory.

The first stand-alone, desktop computers arrived in the classrooms in the 1980's. During the next decade, computers were connected, both to each other in Local Area Networks (LAN), and to the Internet. The wired LANs have been replaced by wireless connections, and laptops, tablets, cell phones and other devices have replaced the desktop computers. In addition, BYOD (bring-your-own device) solutions have become usual in many schools today.

Before 2005, computer labs were dominating in the school system. These labs typically had a number of the school's own desktop computers wired together, and the institutions rarely offered a wireless network to teachers or students. The number of computers was usually far lower than the number of students, so these labs were dedicated to specific subjects or specific lectures. Some of the teachers did not use computers at all. To a certain extent, it was possible for a teacher to ignore Information technology and to do his teaching 'the old way', without the use of digital devices, both in the classroom and for carrying out administrative tasks, such as registering grades. All this could be done without the use of digital tools, if the teacher preferred. Some schools did put some pressure on the teachers to use digital technology, others did not.

The Norwegian educational reform 'Kunnskapsløftet' (the Knowledge Promotion Reform) in 2006 defined the use of digital tools as a fifth basic skill, in addition to the other four; reading, writing, calculating and oral and written expression.

Consequently, high school education soon became computer-based in all subjects and most lectures. To provide computer access also for homework, most schools owners offered individual laptops to all students. Others schools offered some subsides, so that the students could buy one themselves. The teachers also got laptops to use in the classroom. In contrast to previous wire-based computer labs, communication is now mainly wireless. Computers are also the main administrative tool, both at operation level in the classroom as well as for the school administration. Vital information on each student is gathered, processed, stored and distributed, all by the use of computers. Furthermore, written tests and external exams depend on Internet access.

Within this period, information security topics have also changed dramatically, and questions related to information security have become more and more complex. In addition to the technical challenges themselves, methods and routines have changed.

Mass media have reported several incidents that might be related to schools' possible poor information security. For instance, headlines showing Internet-based exams gone wrong because of DDoS attacks (Larsen 2015) and (Grønlie 2015). Or students improving their own grades by hacking into the school's database (Sandve 2016). Another example is sensitive student data in the hands of unauthorized or external individuals (Moss_Avis 2007).

Some of these incidents might be of a technical nature, others might be linked to social or cultural causes. There seems to be little research on the possible causes for such incidents.

1.1 Keywords

Information security, Education, High schools, Socio-technical System.

1.2 Background

In Norway, the main task of high schools is to educate 16-19 year old students, even if a number of students are older. In this thesis, the American term *High School* is used, the corresponding term in British English is Upper Secondary School.

Each institution offers one or more of the 13 study programs available in Norway. The largest schools have more than 2000 students and 350 employees, the smallest schools have less than 100 students. The smallest schools might offer only one vocational education program, the larger schools typically offer both an educational program for specialization in general studies, as well as several vocational education programs. In addition, many schools also provide a number of courses for adults, like language courses, or courses for higher education qualification.

Such variety in both size and activities may cause very different challenges related to information security. Small schools may not have personnel dedicated to ICT tasks in general, or to Information security in particular. With as few as 100 or fewer people in the school community, there might be closer social relationships between the different groups of people, and the school society might appear more like a big 'family'. Larger schools tend to have more ICT personnel in place, with the opportunity to solve more complex tasks, and the ICT personnel might be able to become more specialized, and therefore obtain a higher level of competence in their field, including Information security. At the same time, large schools

naturally might tend to be more impersonal, in the way that it is very difficult to get to know each individual in the school.

Most Norwegian high schools are owned and managed by the 19 counties[1]. There are also a number of private schools, and about 7 per cent of the students attend private schools (Sentralbyrå 2016). There is a large variation of how ICT services are organized in the different counties. Some counties have a centralized structure, with most ICT personnel and ICT competence gathered at one location, typically at the county's central administration. Other counties have a more distributed structure, with more ICT personnel located at each school.

1.3 Definitions and conventions

A large number or words and phrases differ between US English and British English. In this thesis, US English is chosen. Therefore, the American term *High School* is used instead of the British term *Upper secondary school*. In the same way, the American term *Principal* is used for the person in charge at each school, not the British term *Headmaster*. The term *Student* is used, even at pre-college education, the corresponding British term would be *Pupil.*

There are several definitions of Information security. This thesis will use the definition given by ISO – The International Organization for Standardization. According to ISO/IEC 27002, which refers to the definitions in ISO/IEC 27000, information security is defined as *Preservation of confidentiality, integrity and availability of information … In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.* (ISO/IEC 2016)

The term ICT (Information and Communication Technology) is used in this master thesis, instead of the term IT (Information Technology). In this context, discussing IT without the communication part would be almost meaningless, since most activities include communication in some way. Often the two terms can be regarded as synonyms, even if the term ICT explicitly includes the use of communication technology. Sallai (Sallai 2012) defines it thus*: Information and communication(s) technology (ICT) is considered an extended synonym for IT to emphasis the integration of the unified (tele)communications.* In addition, the term ICT is dominating in the Norwegian school system.

[1] An ongoing reform will reduce the number of counties, however, the future number of counties is not yet known.

1.4 Related Work

There are a few related works available in this field. Staurheim (Staurheim 2013) focuses in her master thesis on three different county administrations in Norway. She deals with the county organization in general, However, her work also includes security issues related to schools.

In a Norwegian master thesis, Leiknes (Leiknes 2011) deals with information security in schools. His work is based on interviews with ICT-leaders in Norwegian municipalities, and the results are related to primary schools and junior high schools. However, there are similarities to the security questions for high schools, which are examined in this master thesis.

Internationally there seems to be little available research on this field.

1.5 Problem description

Incidents like the ones mentioned previously in the introduction might seem to be a part of the educational institutions' daily life. The problems are very different from each other, and the reasons might also be very different. There might be several information security weaknesses causing the mentioned incidents. Some might be related to technical solutions, which might be caused by the methods, i.e. direct use of machines in some way, or related to the machines themselves. Moreover, some might be related to social aspects, and have institutional cultural or structural causes. This project has the intention of describing and classifying each threat. It is also an intention to suggest adequate measures related to the most serious threats.

1.6 Research Questions

Several possible research questions might be derived from the problem description. However, this thesis will focus on the following research questions:

- What types of information security threats are Norwegian high schools facing today related to confidentiality, integrity and availability?
- How are these threats handled?
- How can the institutions improve their information security?

1.7 Limitations

The findings in this master thesis are, of course, primarily limited to the examined school. However, some findings may also be relevant for other schools in Norway, both high schools, as well as for elementary and lower secondary school. This is because many factors are common for all these school types, for instance legal and organizational aspects. Technical solutions might also be similar in some cases.

2 Methodology

There are several possible methods to approach the research questions. The security issues in a school, like in other organizations are complex. In addition to technical aspects, there are many social aspects that need to be examined. In the Introduction, some security incidents caused by students, were described briefly. Unlike most other organization, schools have to keep even destructive persons inside the organization, allowing them access to both assets and data. To point out what security challenges the schools are facing, it is difficult to see how this can be measured quantitatively. Given the complexity of most large organization, how could e.g. a questionnaire point out what information security threats that exist, without giving the participants presumable alternatives? There is a strong possibility that threats would end up undiscovered because the researcher had not thought of it in advance. Open questions in a questionnaire might catch some of this, but the researcher would have no possibility to follow interesting leads included in the answers. Therefore, a qualitative approach seems better in an initial phase. This way, the informants will be able to elaborate their answers, and it will be possible to ask new questions, to get information that is more detailed. A case study examining one school is chosen, instead of examining several or many schools.

2.1 Case Study

Yin (Yin 1981) argues for considering empirical research strategies from a pluralistic perspective, not hierarchical. Each research strategy has its strengths and weaknesses. Therefore, the choice of research strategy depends on which set of conditions that are present, since each strategy is best suited for different situations.

The strength of the case study is primarily that it is able to cover both the contemporary phenomenon, as well as its context. A case study is suited when there is a need to examine a contemporary phenomenon in its real-life context, especially when the boundaries between the phenomenon and its context are not clear. (Yin 1981). In other words, the case study is relevant when a phenomenon is difficult to separate from its context. It is therefore well suited for studying knowledge utilization. The case study is primarily used to explain ‘How?’ or ‘Why?’.

On the other hand, when the context has been included in the study, the number of variables will logically exceed the number of data points, which in this case means the number of cases. This means that only a few, or maybe none, statistics are relevant for data analysis. (Yin 1981)

However, there are several definitions of the case study. Gerring (Gerring 2004) calls the case study a 'definitional morass' because different researchers have many things in mind when they refer to the case study as research strategy. Some of these distinguishes might be; a small number of investigated objects, participant-observation or otherwise 'in-the field', characterized by process-tracing, investigation of one single case, or investigation of the properties of one single case.

Gerring (Gerring 2004) defines the case study *as 'an intensive study of a single unit for the purpose of understanding a larger class of (similar) units'*

A case study is not linked to one specific way of collecting data. The case study might use either qualitative or quantitative evidence, or a combination. Or the evidence might come from observations, fieldwork, archival records, or combinations of two or more of these methods. (Yin 1981).

2.1.1 Single case vs. multi case

For explanatory purposes, there are two basic research designs, single case and multi case. Since a case study is defined as a study of one single case, it is relevant to compare with a study of two or more units, a cross-unit study. The cross-unit study offers conclusions based on investigation of a group of cases, at least two. This is relevant when a phenomenon might exist in several variations of situations. The case study, on the other hand, investigates one single case in depth. It can be used e.g. to theory testing, especially disconfirming (Yin 1981). Very often, the case study focuses on subjects, which there is previously little knowledge about. Typically, the case study is exploratory in order to generate theory, while the cross-unit study is confirmatory, in other words, it is used to test theories.

While the cross-unit study's type of interference is causal, the case study is descriptive (Gerring 2004).

Since there is little existing research related to information security in schools, a case study seems to be a relevant choice of research strategy in this thesis.

2.1.2 Alternative strategies

The case study represents a research strategy that can be compared to an experiment, a history or a simulation. Neither are associated with a single way of collecting data (Yin 1981). Given the research questions, could some of these alternative research strategies have been relevant?

In this case, it is hard to see how simulations or lab experiments could be possible. The schools are complex organizations, and so are the security aspects. Some security challenges might have been detected during a simulation or lab experiment, but there would be considerable limitations. Technical issues could have been analyzed. For instance, one could carry out a DDoS attack, and registered how this affects the organization. Or, one could educate a group of employees and/or students, and test how they respond to certain aspects, compared to a control group. Simulations are difficult; they would probably have to take place in the field, during ordinary operation. In addition, the researcher's ability to find possible threats would be a limitation in itself.

2.2 Qualitative vs. Quantitative approach

It should be well known that there are two dominating types of research designs; quantitative research and qualitative research. Aliga and Gunderson define quantitative research as *'Explaining phenomena by collecting numerical data that are analyzed using mathematically based methods (in particular statistics)'* (Muijs 2010). This approach is suitable for counting or measuring certain phenomena. Related to information security in a school, this could be for instance:

- counting DDoS attacks
- measuring uptime of a certain service
- counting the number of failed authentication attempts

However, this approach presumes knowledge about the fact, that the examined phenomenon already is present. Such knowledge is not available, so the purpose of this master thesis is to identify what information security-related phenomena that actually exist. In addition, what phenomena that must be considered as threats.

Therefore, a qualitative approach is preferred. Qualitative research means focusing on collecting and analyzing non-numerical data, such as

- observation in the field
- informants' stories e.g. via interviews

A mix of qualitative and quantitative is sometimes a relevant strategy. The combination might provide answers to questions that neither of the strategies could manage by themselves. However, in this master thesis, a qualitative strategy is chosen, in order to identify information security threats. A combined strategy could give extra information e.g. related to statistics, or the probability of a certain incident.

2.2.1 Interviews

There are several ways of conducting interviews with the participants. Each way has its pros and cons, and there are several aspects that need to be considered. Regardless of the format of the interviews, it is of highly importance that the researcher manages to establish trust relations with the informants. If some – or all – informants do not trust the researcher, it is likely that their answers might be biased, and that the answers lose their value. For instance, if an informant believes that the researcher cannot guarantee his anonymity, he might not want to expose certain security breaches, especially when he is involved in some way. Another example is that the manager or principal might restrain information if he thinks that the organization might be injured in some way.

One aspect related to the interviews is, how should the interviews be structured? One possible way is to have a *fully-structured interview*, with very specific questions with specific alternatives. One advantage is that coding will be easier, it will probably also more correct, since an *open interview* might include elements that are not easy to classify. There are also *semi-structured interviews*, which include both types of questions.

Should the interviews be one-to-one? Alternatively, should the informants participate in pairs? Alternatively, in smaller or larger groups? Each setting has its advantages and disadvantages. The one-to-one interview might cause the informants to speak more freely, since no other representative from the organization is present. This is obvious when it comes to personal routines or habits, especially activities that might be embarrassing to admit. On the other hand, group interviews might produce answers that would have been difficult to get by the use of individual interviews. For instance, a group of employees might be more distinct when it comes to blameworthy aspects, such as a lack of security training.

Another aspect related to the interview situation is the form of the interview. Should the interviews be made face-to-face? Voice or video recording? Stenography? Alternatively, should

the researcher choose a remote solution, such as telephone or video conference? Alternatively, e-mail? Due to e-mail security level, it can be challenging to guarantee anonymity to the participants, even if both questions and answers are encrypted. For instance, the fact that an employee has sent e-mail to the researcher might be exposing.

2.2.2 Alternative Methods

There are several other methods for approaching the research questions. For instance, the researcher can do observations inside the organization. Related to information security, there might be many interesting locations and situations. Are critical components secured in a proper way? Is there an electronic access control to servers and critical network components? What procedures exist for allowing visitors, e.g. craftsmen access? How are confidential printouts handled? All these things might be registered by observation. However, many aspects would be very difficult to observe. For instance, an individual's considerations when handling personal, confidential information; Should this information be reported to e.g. the principal or the police, or should the actual person's integrity have priority.

Another method could be to examine an information security incident, and do a root cause analysis. This mean removing the factor that is considered as the root cause to the problem. However, this results in a kind of experiment, and might be challenging to do at a school, it depends on the type of incident, and the type of factor.

Even if the chosen strategy is qualitative, questionnaires might be another possible method. This might offer a larger group of informants, but there is more difficult to follow interesting clues given in the answers.

2.3 Analytical Methods

2.3.1 Socio-Technical Systems

The term Socio-Technical Systems (STS) refers to a view that technical systems are note only technical, they also interact with humans, organizations and other social structures. STS also include actions within the system as a whole. This broader view means that e.g. modifying laws and regulations directly influence on Information Systems. In addition, cultural or organizational differences might have great impact on how information security issues are handled. For instance, two organizations with almost the same technical infrastructure, operating systems and applications – almost the same in every way at technical level - will use

Information Systems very differently because of other factors. These factors might for instance be

- Branch or business sector; A software developing company vs. a car manufacturer
- Public/Private sector; A municipality administration vs. a bank administration
- Geographical; Laws and regulations in different countries or regions
- Organizational structure; is the ICT department, or alternatively Information Security Officer, placed close to the Chief Executive (CEO) in the organization, or further down in the organizational hierarchy

The different organizations have different needs for their Information Systems, and the need for security solutions reflects this. An improvement in one part of the STS might cause other, surprising - and even unwanted - changes in other parts of the system. For instance, introducing a stricter password policy in an organization, might lead to the use of post-it notes with passwords written on them, just because the users are not capable of remembering the complex passwords, in combination with frequently forced password change. Another example is centralizing the printing service, from a larger number of local printers placed close to the end-users, to fewer but more centrally placed printer devices. This might be more cost-effective, and the centralized printers might be located in secure areas, so that e.g. visitors have no physical access to them. However, this solution might also lead to 'batch printing'. If there is a long walk to collect the printouts, the users might print several documents at a time, and collect them later. If the documents are confidential, the user cannot be sure if others have seen them, or the documents might be mixed with other users' documents.

Kowalski (Kowalski 1994) describes an STS as a system that includes different social and technical components and the interactions between these components. The system consists of a technical part that includes machines and methods; and a social part, that includes structure and culture. This is shown at a general level in Figure 1 Socio-Technical System (Kowalski 1994).

The different parts of the STS interchange and the system itself will try to find an equilibrium. A change in one component will therefore always cause influence the other parts of the system. One single change will cause a disequilibrium, and the STS as a system will find another balancing point. If the connection between some of the four entities are disturbed or broken, the system's security will become compromised.

The consequences in other parts do not necessary have to be negative, but they have to be discovered through analysis and taken into consideration. For instance, implementing an

information security education in an organization *might* lead to better Information security in several fields, due to improved awareness about the subject.

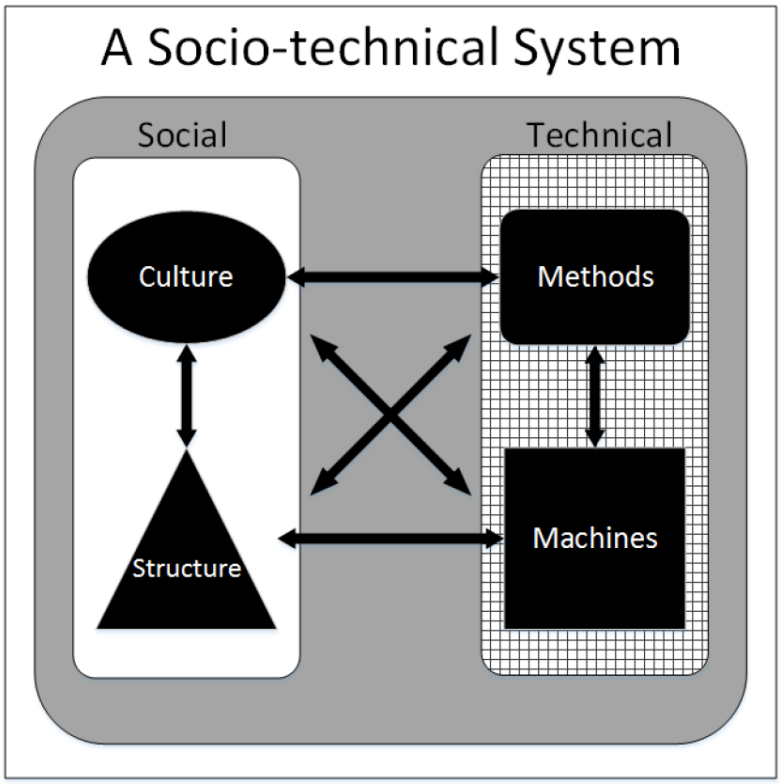

Figure 1 Socio-Technical System (Kowalski 1994)

2.3.2 Socio-Technical Systems and security

All four entities of the STS model are closely related to Information security. All security aspects will therefore have both social and technical elements. Kowalski (Kowalski 1994) introduces a framework for how to chart the different types of Information security issues. This framework is named *the Security by Consensus* (SBC) model.

The SBC model consists of two different parts – one technical category and one social. These two parts are then divided into several layers. This is illustrated in Figure 2 SBC - Security By Consensus (Kowalski 1994), and the layers are:

Social

- Ethical/Cultural
- Legal/Political/Contractual
- Administrational/Managerial
- Operational/Procedural

Technical

- Mechanical/electronical

- Information/Data

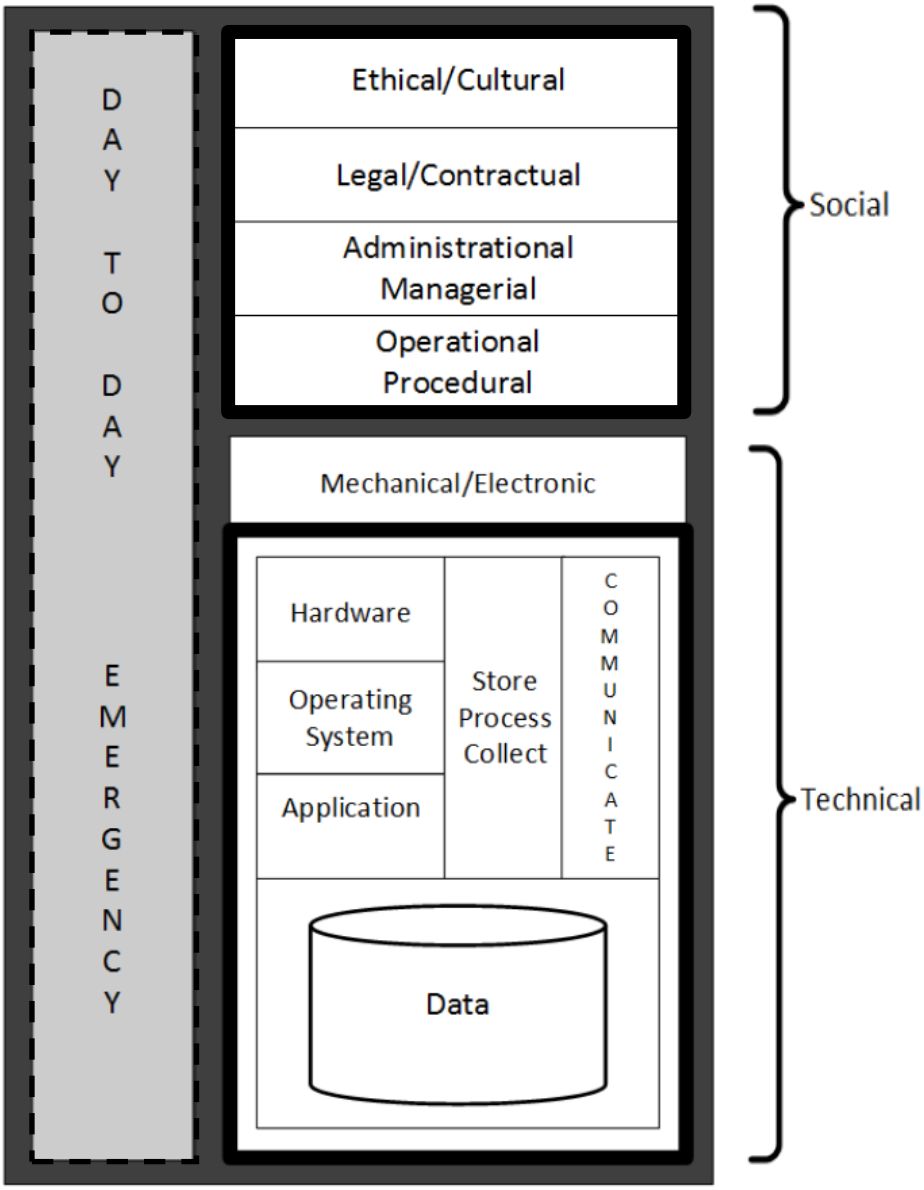

Figure 2 SBC - Security By Consensus (Kowalski 1994)

One of the purposes of the SBC model is to be a tool for analyzing a systems interchanges with other systems. Every other system can also be viewed as an STS. Such a system might e.g. be at national or international level. A change in, for instance a certain law or regulation at national level, will affect other systems that depends on this. Introducing certain requirements related to storing specific information, might lead to a change of e.g. hardware, operating system,

applications, or even physical or procedural changes. The types of change that are needed will depend on what type of new requirements that are introduced.

The SBC model can also be used for examining internal flow in the system. A new organizational structure or moving a department into new physical areas, might cause changes in the other entities. This is shown in Figure 3 SBC model combined with social and technical changes (Kowalski 1994).

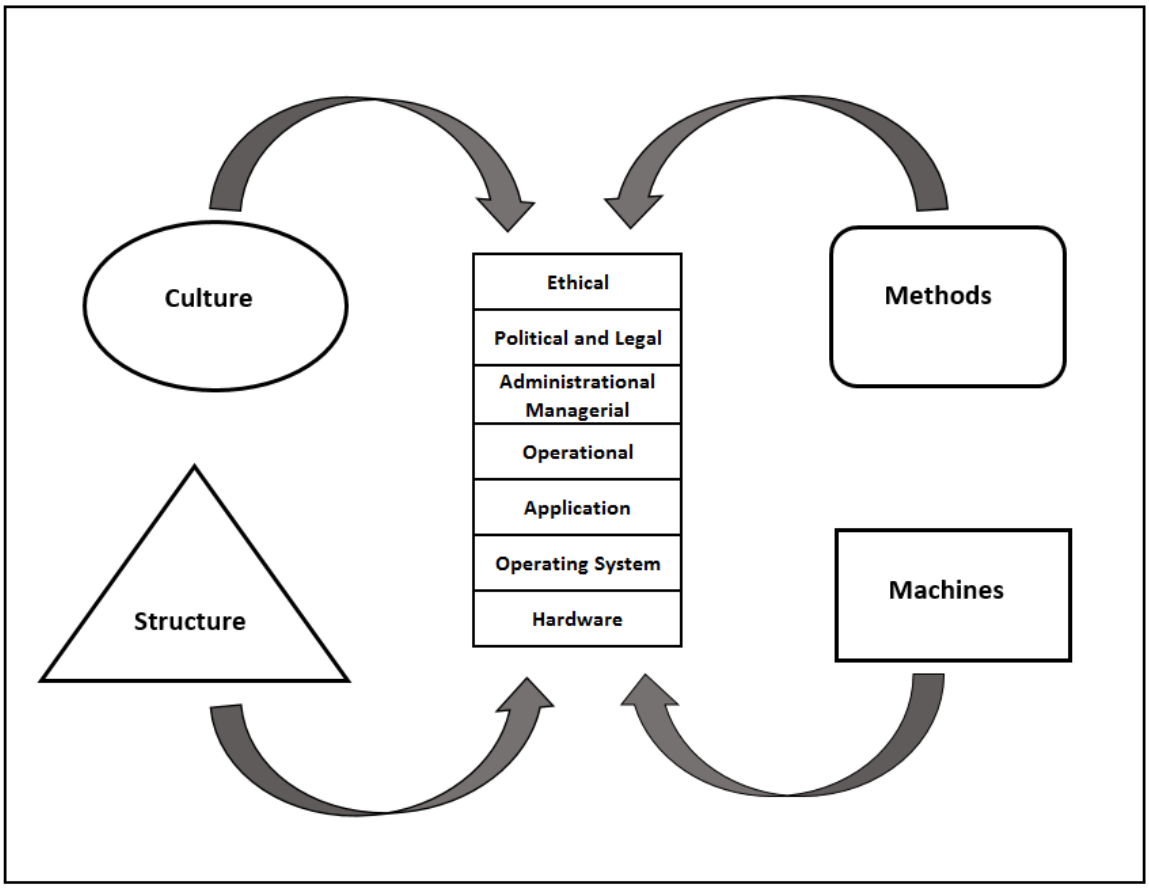

Figure 3 SBC model combined with social and technical changes (Kowalski 1994)

2.4 Reproducibility

Other researchers might deal with some of the same Information security aspects or research questions. Therefore, the interview questions are available in both English and Norwegian as appendixes. The interviews are semi-structured. This means that there is a core of questions, with the possibility to follow up interesting leads. This is to make corresponding studies in other

schools and organizations easier. In addition, repeating studies in other organizations will be more comparable.

2.4.1 Reliability and Validity

Reliability means that it should be possible for other researchers (and others) to examine methods, procedures and choices, as well as decisions made during the research project. This is done by describing the different factors as detailed as possible, including the interviews themselves. Such descriptive transparency is important in general, to show others how and why conclusions were stated. In addition, transparency is important in order to avoid or minimize that the researcher's possible personal interests or view might influence the study (Denscombe 2014).

Data collected in the study might be validated and corrected by presenting the data to the respondents. In this thesis, this means involving the respondents by giving them the opportunity to read transcriptions of their own interview. In this way, the informants were given the chance to correct and clarify in case they had been misunderstood. In addition, the respondents would be given the chance to add things they forgot to mention during the interview.

At the end of the interview, each informant was asked if he or she wanted the transcription sent. Only four participants answered that they wanted this.

2.5 Ethical aspects

As far as possible, this thesis follows the ethical recommendations published by The Norwegian National Research Ethics Committees - De nasjonale forskningsetiske komiteene - (Commitees 2016).

This includes informing the participants about the purpose of the study and which institution the researcher represents. In addition, every informant is guaranteed full anonymity. Each participant is also informed that he or she contributes on voluntarily basis. This also means that the informants are given the chance to withdraw from the study at any time, and that they would not have to give a reason for a possible withdrawal. Since the interviews were audio recorded, the participants were informed about this fact prior to the interview. The interviews took place in a room with closed door and with no other persons present. Audio recordings were done by the use of a relatively large and fully visible table-microphone connected to the researcher's laptop.

Prior to the interview, each participating informant signed a form, saying that they were aware of, and agreed to the above-mentioned aspects. No participant wanted to withdraw during the interviewing process.

3 Application of Research Method

3.1 Samples selection

There are several aspects to consider when choosing one specific school to investigate. Some information security issues might not be relevant for the smallest schools; therefore, a larger school was more of interest. In addition, some issues might not be relevant for all study programs, so a school with a broad specter of study programs was wanted. In fact, the school had to have both education program for specialization in general studies as well as a broad specter of vocational education program. A list of Norwegian high schools grouped by the number of students is shown in Table 1 Norwegian high schools grouped

Norwegian high schools grouped by number of students	
> 800	74
400-800	134
< 400	186

Table 1 Norwegian high schools grouped

The list is not official, but this is considered not very important (Wikipedia 2015). The purpose is to find a typical Norwegian high school.

3.2 Interview Questions

Questions are developed to be related to the different layers in the SBC model. It was a goal to interview as many stakeholder as possible to get information from different parts and levels of the organization. There is no single answer to how many informants that should be used. According to (Marshall, Cardon et al. 2013), case studies are among the most difficult types of qualitative research to classify. They refer to that Yin argues for at least 6 informants, but other researchers argues for 4-5 informants. In this case a larger number is chosen. The different

stakeholders have very different roles in the school system, and all groups brought new elements in the interviews.

- Principal
- ICT leader
- Social worker
- Teachers
- Students
- Politician, leader of the schools board
- Parent
- ICT consultant at County's central ICT department

The number of interviewed teachers was 3 (one of them is also a union leader), the number of students was 4. In other words, this is a large number. The teachers were not picked at random; this was also the case when choosing students. Since this is a case study, with qualitative approach, it is more important to have voices from different parts of the school. It was also a goal to have both sexes and different ages represented the group of participants. No other criteria for selection was used. One teacher (the union leader) was suggested by the principal. The others by were chosen by visiting their department and simply ask the first to show up. The departments are located in different buildings. Again, the goal was not to pick them at random.

Not all informants were asked the same questions. For instance, the technical questions were only asked the ICT personnel.

3.3 Implementation

3.3.1 Case Study Implementation

The interviews were done in voice form, and all interviews were audio recorded. All informants participated voluntarily, and each signed a paper to confirm this. This confirmation also included information about the master thesis, and the fact that the interview was recorded, and that they could leave the interview at any time, if they wanted. Each participant was also offered the transcription sent by e- mail later. Since e-mail is considered an unsecure channel, the text file would have to be encrypted and password secured. The informants would then have the password sent by SMS. Four of the informants wanted the transcription of their interview.

None of the asked persons refused to participate. In fact, all informants were very glad to participate. However, one teacher said that he did not have time, because he was to have lectures all the specific day.

3.3.2 Interview Implementation

To secure the quality of the questions, a pilot study was done in advance. Some of the interview forms were tested at other schools to see if some of the questions needed to be changed. These forms were:

- Principal
- ICT leader
- Teacher

A couple of questions were modified, some due to feedback, and some because the informants had problems with understanding the meaning of the question. No questions were skipped, but a couple of follow-ups were added.

4 Findings

4.1 Technical levels

Interview questions about technical solutions, servers and network devices were asked the school's ICT leader and the consultant at the county administration's central ICT department. This is natural, since the schools infrastructure and technical solutions are a part of the county's technical solutions. The two informants have specific knowledge about 'their' part of the technical solutions the school is using. Other informants do assumingly not have knowledge about the infrastructure and technical solutions, an assumption that was confirmed by the two relevant informants.

An important issue related to technical level is investments technical equipment. According to the two relevant informants, equipment is bought via purchase contracts. Such contracts are made after a competing call for bids, where the county chooses the best tender. This is according to Norwegian regulations in this field.

4.1.1 Machine level

Network

All the high schools in the county are connected to the Internet via the county's central network infrastructure, located at the county administration. The connection between each school and the county administration is fiber-based. It is a switched, layer 2 connection, and the fibers are offered by the ISP (Internet Service Provider). There is only one connection to each school, and therefore no alternative solutions if this line gets unavailable. This is also the case with the common Internet access from the county administration. However, an ongoing project will better this rather soon. An extra data center will be available for both the county administration as well as for the schools. The extra data center is located in another city, and the two data centers will be duplicates. Each school will have a connection to both data centers to ensure redundancy, and each data center will provide Internet access to the schools.

A few downtime instances of short duration have been registered, both for the Internet connection and for connection between the school and the county administration. However, more serious and long-lasting incidents have been avoided. Until 2014-2015, there were a number of DDoS attacks. Both the school's ICT leader and the consultant at the county administration relate these attacks to exams periods, or to major student test periods. This might indicate that students have caused or ordered the attacks, but this is very difficult to investigate.

However, in cooperation with the ISP, the problem seems to be solved, by implementing devices to detect unwanted traffic and drop packages before they reach the ISP.

Based on purchase contracts, the county has chosen Cisco as standard for network infrastructure devices for all organizational units, both at the schools and at the county administration. This includes switches and routers, as well as access points and WLAN controllers. Cisco network devices provide a secure separation of networks, so-called VLANs (Virtual LANs). The schools and county administration use this utility to separate traffic, e.g. all student traffic are separated from employee traffic. Confidential information about both students and employees is separated in a secure zone via a dedicated VLAN. VLAN is considered secure, and it is approved by Datatilsynet - The Norwegian Data Protection Authority (Datatilsynet 2011). However, the VLAN security level depends on correct configuration.

Firewall

A redundant firewall solution is located at the county administration. These two firewalls serve all schools and the county administration, and they are mirrored in a HA (High availability) solution, which means that if one of them gets unavailable, the other one takes over and handles all traffic.

Servers

At the county administration, there are 10-12 physical servers in a cluster. The physical servers serve as hosts for about 250 virtual servers. VMWare is chosen as the virtualization platform. The VMWare installation is configured with both load balancing and HA, so if one host becomes unavailable, all its servers will automatically be moved to other hosts.

At the school, there are 5 physical servers, which serve as hosts for about 20 virtual servers. HA is not implemented, the virtual servers have to be moved manually or, if a host fails, restored from backup or reinstalled.

At both locations, in addition to the virtual machines, there is a small number of physical servers. These servers have specific roles, such as firewalls or deployment servers. These machines must have certain specifications in order to; for instance, handle large amounts of I/O data.

Windows is standard operating systems on servers at both locations. Several versions are used, but at the moment, Windows Server 2012R2 is most commonly used. Windows Server 2016 is in-house for testing and will soon be implemented. Windows Server versions not supported by

Microsoft are not in use. The windows servers are automatically updated with the latest Windows updates, via SCCM.

A small number of Linux servers are also present. These servers use well-known, stable Linux distributions, and they have very specific roles, e.g. mail transfer agent in a DMZ (demilitarized zone). There is not a focus on having latest updates on these servers, due to little Internet exposure.

Physical security

Critical components are in general physically secured.

At the county administration location, the data center is physically locked, with electronic access control. Only a small number of employees have access, Every attempt to enter the data center is logged, both date and time, and which card being used. The data center also have video surveillance, so it is recorded whoever enters the room. The video recordings are stored in another location than the county administration. In addition, there is an intrusion alarm. The data center is equipped with an argon fire extinguishing system.

All critical components are secured by two UPS's (uninterruptable power supply). The UPS's have two major functions; by the use of batteries, they are supposed to provide power of good quality to the actual devices in case of a power outage. In addition, they are supposed to protect the devices from spikes, caused for instance by lightning. Today, the UPS's offer power to critical components for at least two hours in case of power shortage. There is no power generator present, but there is an ongoing process to get one. A power generator will, if no problems occur, produce electrical power as long as it has fuel available.

The school has a small data center, and like the county administration's data center, it is protected with electronic access control. The school's servers and other critical components are protected with one UPS. The server hard disks are configured as RAID10, but are not encrypted. Equipment for fire extinguishing is present.

Edge switches are placed in lockers.

Logical security

The most critical components at the county administration, such as firewalls, are only accessible for a small group of authorized personnel. As an extra security, the firewalls are only accessible from the data center, or via a dedicated management VLAN. The firewalls' management system is proprietary, but there is no two-factor authentication. A two-factor authentication has

been suggested, but due to the mentioned steps, the firewalls' security is considered good enough. All attempts to get access to the firewalls are logged, both successful and unsuccessful attempts. Updates are handled automatically.

For both the school and the county administration, Windows servers that are members of a domain use the domain's user credentials (username and password) to log on. Authorized personnel have special administrator accounts to do server-related work, in addition to their ordinary accounts.

Other servers offer use of local users accounts to get access.

Remote access for vendors, technical consultants and others who need access to resources inside the firewalls, is offered via a two-factor, VPN (Virtual Private Network) solution.

In addition, the county provides many services to the schools, and some of the servers are common for all schools in the county.

The school's wireless network is encrypted with WPA-2 Enterprise (Wi-Fi Protected Access.

Workstations

Most workstations are laptops, both for students and employees, even if a small number of desktops are present. Desktops are mostly for administrative work, not in classrooms, or for specialized use, such as CAD (Computer-aided design). Local disks in all workstations are encrypted with Bitlocker, and BIOS is password protected. The workstations are configured not to boot from USB devices. This is to protect workstation's disk from being read if stolen.

The organization endeavors to have the latest versions of operating systems on both servers and workstations; this is for the schools as well as for the county administration. For workstations, this is Windows 10. Users do not have administrator privileges. However, most employees can, without applying for approval, create a local user with administrative privileges. This localadmin user account is not able to access network resources, but might be used to install software on the workstation. In fact, this is the purpose of the localadmin account; it is used e.g. by teachers to explore alternative pedagogical software.

Critical applications

The consultant at the county administration refers to a survey a few years ago, where employees were asked which applications they could not manage without. Surprisingly for the ICT department, e-mail was on top of that list. However, the interviews give a more balanced impression. All employees focus on the administrative applications related to classroom

activity. This means access to pedagogical Internet resources in general, and the Learning Management System (LMS) and the School Administration Software (SAS) in particular. The LMS is used for administering pedagogical resources, e.g. distributing subject matters and organizing tests. The SAS provides a web interface connected to the student- and employee database, and is used for registering students' absence as well as registering their grades. A teacher's registering in SAS is directly written into the database. However, a teacher's write access to the database is limited to registering grades and absence for his own student in the subjects and classes he is responsible for.

In addition, administrative personnel focus on administrative applications, such as student and employees databases, and journal systems. Some of the administrative applications are used to handle confidential information. Such information might e.g. be related to health, reading- and writing difficulties, or if a student has secret address or telephone number. Other administrative applications are systems for handling accounting and other economical aspects.

The school's and the county's only telephone solution is Skype for Business, which includes a Voice over IP service. None of the informants emphasizes telephony as a critical application. A switchboard is located in the schools expedition, but a cell phone is used as a backup for incoming calls in case of loss of Internet connection.

Security in critical applications

Both e-mail, the LMS and the SAS use one-level authentication, i.e. username and password. The username and password is common for all three services, and the same credentials are used for logging on to the school's LAN. LMS and the SAS are Internet-based services, while e-mail is provided by the county. E-mail is also available via the Internet, through a web access interface. There are no restrictions against accessing these services from any device connected to the Internet, as long as it has a browser. Neither there are no other restrictions, e.g. time for logging on to these services.

Administrative systems, such as student- and employee databases have other, proprietary solutions, with their own set of user credentials. However, there are no systems in the school using two-factor authentication, nor other types of authentication, such as fingerprints.

4.1.2 Mechanical and electronic level

The descriptions directly related to critical infra structure are described in the previous section, *4.1.1.Machine level*, such as securing the data centers. As mentioned, the data centers are

protected physically, with both electronic access control and alarms, as well as UPS and fire extinguishing equipment.

However, many others measures are related to the mechanical and electronical level. Among these factors is how buildings are designed and used when it comes to handling confidential information. One of the informants, the social worker, points at the fact that she and her colleagues have offices designed and furnished in a way so that the screens might be seen from the corridor. The social workers are located together in a specific part of the school, shielded from other activities at the school. However, both students and others have meetings and errands there. Windows make it possible to view a computer screen while passing an office. In addition, the offices are narrow, so today's office desks can not be turned into another direction.

The social workers have asked the school management to improve this, and this will be done. It is not decided how the problem will be solved. One solution is mounting shields on each computer screen, anotther possible solution is buying new furniture that can be turned more correctly related to Information security.

4.2 Social levels

Interview questions related to social levels in the SBC model were asked all informants. However, not all questions are relevant for all participants. For instance, the students are not asked questions about what juridical aspects are the most important in their profession.

4.2.1 Ethical

Questions related to ethics level in the SBC model were asked all participants, not only employees at the school, but also students, the politician and the consultant at the county administration. Ethics is, simplified, about choosing and performing right versus wrong actions, separating good from evil, and prioritizing between different measures related to this. However, ethics is not a neutral, time- and location independent measure. Ethics has changed through history, and there are also considerable country- and region variations.

STSs are complex systems, and humans and technology tend to be connected in a positive feedback loop. This means that changing one part of the system will lead to a larger change in other part of the system, and vice versa. Without regulation, the system will become unstable. For instance, the organization introduces a new procedure, with improved security but more inconvenient for the users. This might lead some users to create shortcuts or in other ways damage the intensions of the new procedure. This might in turn lead to new and stricter

procedures, and so on. However, the result might very well be information security at a lower level, not higher.

Having in mind that many users in the school organization handles sensitive information on regularly or daily basis, it is important to avoid Information security evolving to a lower level.

Employees in general seem to be aware that they handle confidential information. On a scale from 1-5, where 5 is the highest, all respondents were asked to estimate how aware employees in general are to their ethical responsibility when handling confidential information.

All participating employees estimate that employees in general are medium or more than medium aware of their ethical responsibility. Except for the ICT leader, all participating employees at the school grade this general awareness as 3 or 4. The ICT leader estimates it as 5, the same does the politician. All students grades this as 4 or 5. As a follow-up question, they were asked if they thought the awareness is reflected in the employee's behavioral.

In addition, each participating employee were asked to estimate his or her own awareness to the same subject. Here it is possible to find a difference among the answers. The principal, the ICT leader and the social worker were extremely focused on this matter. In their job, they handle sensitive information on daily basis, and it seems that as a group they are very aware of this. Each of them estimates their own awareness related to ethical aspects when handling confidential information as 5.

The other group of employees consist of teachers. They seem to be less aware than the other employees are, and they consider themselves approximately equal to other employees in this question.

Participating employees were asked if employees in general are aware that the school and the county register several types of hidden data, such as system- and network logs and position information, e.g. where at the school area they are when they log on. There seems to be very little awareness of this. Only one informant estimates this as 3, all the others have answered 1 or 2. One respondent suggests that younger employees are more concerned about issues related to personal privacy and surveillance.

The same question, but related to students' awareness, was asked all participants. A larger variation in answers are seen here. In general, there seem to be little awareness among the students as well. The students themselves estimate this in an interval between 1 and 3. However, most participating employees emphasize that there is a large variation among the students.

According to the employees' answers, several students both are interested in, and have knowledge about the subject, but most students do not seem to care.

All informants were asked if they had experienced any ethical dilemmas related to Information security. All non-teaching employees answered Yes to this. They were also asked to give examples, and one example was about reporting a user to the police. Other examples were related to when it is right to use information collected confidentially in a job situation for e.g. helping another person.

4.2.2 Political and legal

Questions about political and juridical issues were asked all participating employees, as well as the consultant at the county administration and the politician.

As a public service provider, the school has few corporate or organizational secrecies. All the relevant informants are very clear that protecting confidential information about individuals is the most important thing. Student information is mentioned first and emphasized by all participants, but each informant also mention protecting confidential information about employees.

The same informants were also asked if there are any political guidelines or instructions related to possible use of other communication channels than the official, when communicating with non-employees, such as students, parents, and media. Unofficial communication channels, such as social medias, might possible be used in reputation building or marketing. It is well known that most young people use social medias daily, and this could very well be an arena for marketing the school to its target group. Even if there have not been a risk analysis, social medias are considered to represent a possible security risk (Dinerman 2011), and the purpose of this question is to find out if decisions or guidelines from politicians creates a backdoor to the schools Information Systems.

However, none of the relevant informants had heard of this, neither employees nor the politician.

4.2.3 Administrative and managerial

Organization of the ICT service

The school's ICT department provides ICT services to the whole school. It consists of the ICT leader and two other permanently employed. In addition, there are two trainees, on temporarily basis. The ICT reports directly to the principal.

Since the school is an organizational unit of the county, and since the school's LAN is connected to the county's network, there is a natural daily, continuous cooperation with the ICT department at the county administration. The latter counts 11 permanently employed, as well as two trainees.

The school very seldom uses external consultant, and no services are outsourced, except pc repairs. However, at county administration, sometimes buys consultative services from vendors with whom they have contracts.

Both the ICT leader and the consultant at the county administration describe a situation where the organization tries to duplicate competence. During a busy working day this can be challenging, but there is a focus on the issue. There is also a focus on documentation. Both informants describe that most systems are well documented. Both documentation and competence duplication are important information security issues, since if one ICT employee quits or get sick – or dies- the organization must have others to do this person's job.

Cloud-based services are not used, except for the LMS. In addition, both e-mail and one part of the SAS have web interface, and can be accessed from the Internet, even if data is stored on local servers.

Security Education

In October the last two years, an Information security education program has been offered all employees at the school, as well as for the rest of the county. The program consists of a number of micro sized self-study lectures, so-called Nano-learning. Each lecture takes only a few minutes, and each users can decide when to take it. Each lecture has a certain amount of information in it, and each lecture ends with a set of control questions to ensure that the user has absorbed the knowledge. All employees are encouraged to participate, but the courses are not mandatory. One of the lectures in this year's course had focus on malicious links in e.g. e-mail and social medias. Still, only two weeks after the course, the organization was exposed to several phishing attacks. Such attacks try to deceive users to give their user credentials to the attacker, typically by clicking on a link. Shortly after taking course two users had been deceived, and both had participated in the course. However, it was not clear in the interview which organizational unit these two belong.

In addition to the user-level Nano-learning lectures, security-related courses are offered ICT personnel.

Written procedures

There seems to be a tendency that security related procedures exist, but they are not written. Both at the school and at the county administration personnel have been employed for many years. They seem to 'know' what to do, based on several years of experience. For instance, controlling system logs is a task that is done regularly, but there is no written procedure for when to do it and what to look for, or how to follow up possible unwanted findings.

4.2.4 Operational

Due to both information security challenges and the job situation in general, this section is divided in two parts. Teachers spend much of their time in the classroom, among the students. In addition, they have an office. Many teachers share office with one or more colleagues, for instance in an open-plan office. All teachers at the school use the LMS regularly, as well as the SAS, where the students' grades and absence is registered. In addition, several teachers deals with socio-pedagogical issues, such as if a student has dyslexia.

The other group of employees consists of non-teaching personnel, i.e. the principal, section managers, social counsellors and secretaries. Common for this group is that the members typically are dealing with sensitive personal information. In addition, they typically have an office at their own disposal.

According to the interviews, there have been several incidents where sensitive information has been sent via e-mail. This counts for both groups. In one case, the intention was to send a mail to one colleague, but by mistake it was sent to a group called *All Employees*.

Administrative personnel and social counsellors

Based on the interviews, sensitive information seems to relatively safe when handled *correctly*. The most highly graded sensitive information can only be accessed inside a secured zone. This includes a VLAN that separates the traffic from all other network traffic. Only predefined users and computers can access the secured zone, and authentication is via a specific user database through a VPN connection. Printouts from secured zone are only available from one specified printer located relatively securely.

However, the secured zone is available both via the school's wired and wireless network. In addition, the secured zone is available via internet, but still limited to authorized users and computers. The reason for this VPN-based remote access is that many employees claim that they need to work from home or when they travel.

Teachers

The teaching situation in the classroom generates very specific challenges. Some students might have interest in accessing the teacher's files, e-mail or LMS- or SAS resources. The motivation for this is obvious, as described in the Introduction section. If a student gets such access, he might modify his own grades, or get access to tomorrow's test or exam text.

According to the interviews, many teachers are aware that the teaching situation generates specific challenges. They lock their computer when they leave it in the classroom, e.g. to help a student. In addition, they do not let students watch while they type their password, and they bring the computer with them when leaving the classroom.

However, not all teachers are that careful. The participating teachers claim to be careful themselves, but two of the employees have witnessed colleagues leave the classroom with their computer unlocked. The participating students have not witnessed this. In addition, one employee has witnessed a student borrowing the teacher's computer.

Passwords

All main systems at the school use one-factor authentication, i.e. username and password. Since this is the systems' only protection, it is interesting to see how good protected the systems are, related to the users' password praxis.

All informants except the politician were asked some questions about their own passwords, as well as their observations at the school. Table 2 Passwords findings gives a compact view of both questions and answers. The full text of the questions are to be found in the interview section in the appendixes. The answers are separated in an employee- and a student part, but the order is not the same as the chronological interview order listed in the appendix.

Some participating employees use more than one system, with different user credentials. However, it was specified to each informant that the questions were dealing with user accounts for accessing the school's network. The same user credentials are used for accessing both the LMS and the SAS.

There was no measure of password length or password strength. Two of the employees claimed that they have their own 'secure' password system. However, *none of the informants had any strategy for changing passwords.* Several users had passwords that were many years old. Some informants had never changed passwords, and two participants –one employee and one student- did not know how to change their password. One participating employee said: *'Have never changed password. I am satisfied with the password I got'*.

One employee uses the same password for services outside the school. Two out of four students do the same, and the third claims that he/she used to do it. The students give the impression that this is rather common among the students.

The users were also asked if they believed that others might know their password, but all informants answered – in some variations- No to this.

The informants were also asked if they knew at least one other user's password. All employees answered No to this. For the students, this question were separated:

- Do you know another student's password?
- Do you know an employee's password?

No students knew the password of any employee, but one student implied that other students had such information. One other participating student said that *'The teachers are good at keeping password secret.'*

However, the students seem to share passwords with each other, i.e. with their friends.

	Same password LAN/ external services	Last password change?	Know other users' passwords?	Others know your password?
Employee	No	Since time immorial. Don't know how to change	No	No
Employee	No	2008, I am satisfied with the password I got	No	No, then I would have changed it
Employee	No, have my own system	Very long time ago	No	No
Employee	No, have my own system	6 months ago	No	No
Employee	No	6 months ago	No	Don't think so
Employee	Yes	Between 1-2 years ago	No	No
Employee	No but others propably do	When I got a new laptop, 1 year ago	No	No
Student	Yes, that is rather usual	2 years ago	Other students' passwords. Share passwords with friends	Don't think so
Student	No, but used to	Have never changed	No	No
Student	Yes, that is rather usual	A couple of months ago	No, but others might have such info, also about teachers' passwords	Don't think so
Student	No	Have never changed, don't know how	No. Teachers are god at keeping passwords secretly	No

Table 2 Passwords findings

5 Analysis and modelling

5.1 Introduction

A fundamental characteristic of all research is that the researcher is sincere with his methods, and thereby let others examine the work with critical eyes. Qualitative research has sometimes been criticized for not being transparent enough, and this applies in particular the data analysis phase (Flick 2009) . Making analysis transparent and well documented is therefore an important issue in qualitative research.

One of the main advantages in applying qualitative research is that it might generate brand new and sometimes unexpected knowledge. This knowledge might in turn generate new research statements. Qualitative analysis often involves that the researcher has to interpret the empirical data. In this thesis, empirical data mainly consist of the interviews. The researcher has no possibility to make onsite observations over time, so the informants act as the researchers 'eyes'.

Unlike a survey in quantitative research, analysis will often be in in progress during data collection. In this thesis however, most interviews had to be conducted in a short period, due to travel challenges. All interviews at the school took place in two days, included the interview with the politician. The consultant at the county administration was interviewed four days later.

5.2 SBC Model Result

In the Methodology section, a level-based model for describing information security was presented. One of the main tasks of this analysis is to adapt the findings described in the Findings section to the SBC model, and to generate a security profile for the examined school, showing which levels might be most vulnerable, related to information security. This is similar to the work presented by (Nohlberg, Kowalski et al. 2008).

Based on the interviews and impressions from the interviews, the answers are rated on a scale from 0-10, where 10 indicates the best influence on security.

Ethical (7):

There seems to be some awareness of ethical issues. Both employees and students think that employees are aware their ethical responsibility when handling confidential information, this is also reflected in employees' behavior. It seems that employees who handle the highest graded

confidential information, such as principal, ICT leader and social counsellor, are much more aware than the teachers are. The three non-teaching employees have also experienced and reflected on ethical dilemmas; only one teacher had experienced this. On the other hand, there seems to be little knowledge and awareness to 'hidden' information collecting, among both employees and students, even if *all* respondents think the school should inform them.

Political/Legal (3):

All employees, as well as the politician and the consultant at the county administration, are familiar with the laws and juridical regulations their positions involve. However, there seems to be little knowledge and awareness of political influence related to information security. The politician had little knowledge about information security issues at the school, even if he accentuated the importance of information security in general terms.

Administrational/Managerial (6):

The ICT service seems to be organized relatively well, when it comes to both organizational level, as well as documentation and competence duplication. However, there is a lack of written procedures. Some IS education is offered for employees, but it is not mandatory, and. There is no requirements related to knowledge related to information security.

Operational (4):

Sensitive personal information is technically secured, but security incidents might occur in case the user is only a little careless. Considerable variation in how teachers handle IS in the classroom. Very little awareness related to passwords.

Technical (9):

This part describes the school and the county administration together.

IS has been focused for years, and the infrastructure reflects this, both at the school and the county administration. Critical devices are protected and partly duplicated. Ongoing projects will improve this, e.g. by having two data centers, with each school having connections to both. However, lack of redundancy internet connection lowers the rating.

The different ratings are shown in Figure 4. SBC Implementation

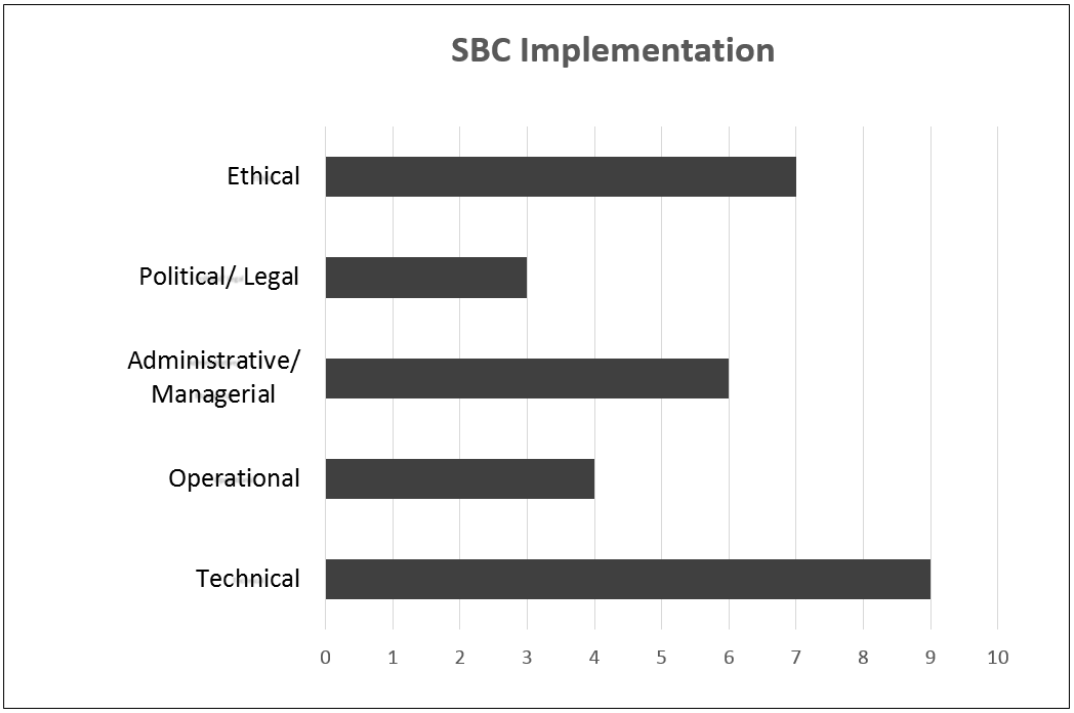

Figure 1 SBC Implemetation

5.3 Socio-technical analysis model

When communicating socio-technical threats with non-technical personnel, it might be necessary to have models they are able to understand. Alsabbagh and Kowalski have developed a such a model (Alsabbagh and Kowalski 2011). This visual model consists of a coordinate system that can be used to show the relationship between threats from the surroundings and the security posture of the orqanization. The x-axis represents the threat level (right) and the posture level (left). The y-axis represent social complexity (up) and technical complexity (down) .

The findings in this case study might be adopted to the Socio-technical analysis model .

In general, the threat level of a Norwegian high school is concidered low (level 1). There is no big money, or political or important infrastructure involved. The only actual ‘enemy’ are the students. The attack vectors are concidered medium (Level 2), both in social- and technical complexity. This Is visualized by the red rectangle in Figure 2 Socio-technical analysis model

On the left side of the same figure, the blue rectangle shows that the school has a low posture level (Level 2) . However, the organization’s capability to handle social threats is considered to be lower than technical orientde threats.

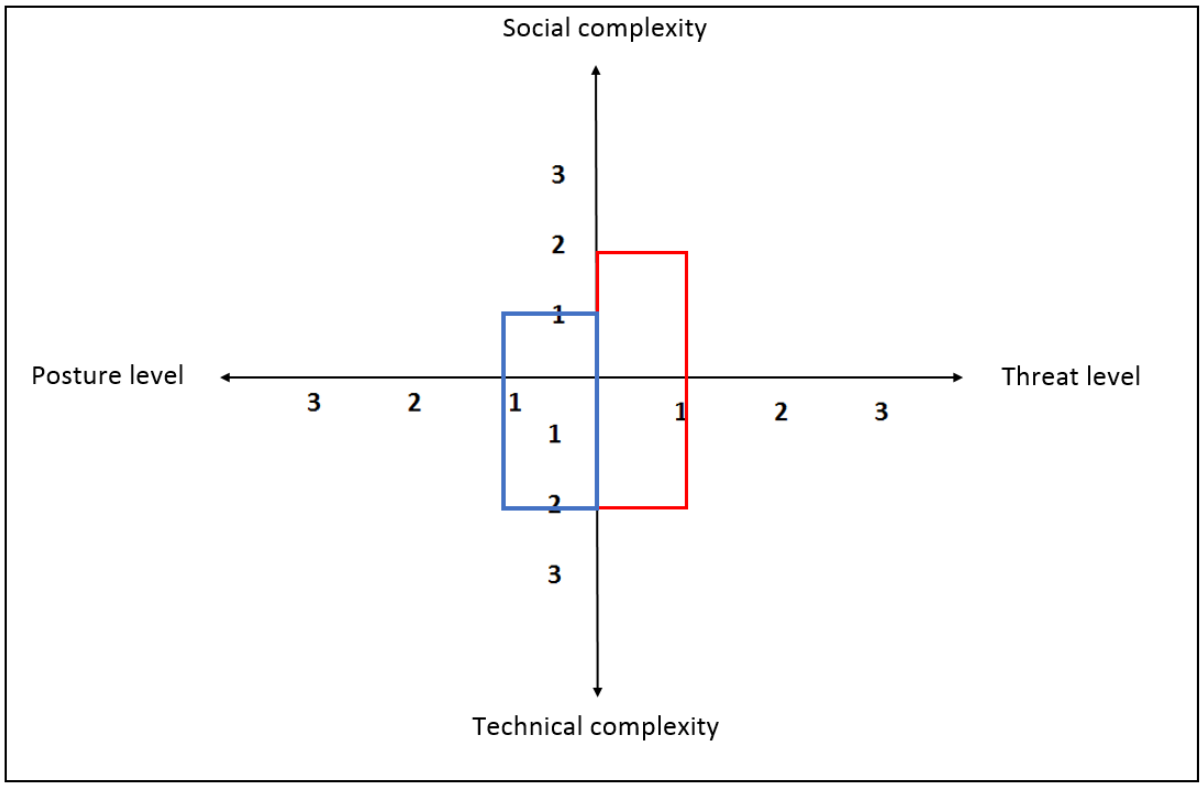

Figure 2 Socio-technical analysis model

6 Conclusions and discussion

6.1 Conclusion

Referring to the research questions, the goal of this thesis is first to identify the information security threats that Norwegian high schools are facing, related to confidentiality, integrity and availability. The SBC model has been used to view the properties of the examined school's information system, in order to find which levels are strong and which level are weak.

In the introduction section, three incidents were mentioned, each primarily representing the three pillars of information security.

- Sensitive printouts falling into the wrong hands is typically an incident related to confidentiality
- Students modifying their own grades is typically an incident related to integrity
- DDoS attacks destroying an exam is typically an incident related to availability

The analysis section shows that the school is relatively well prepared to face some types of threats, but relatively unprepared to face other types.

DDoS attacks were successful 2-3 years ago. Investing in protecting equipment has been relatively successful in preventing such attacks. Other types of attacks against parts of the infrastructure will also be challenging. Bot at the school and at the county administration critical components are protected and redundant. However, the school has only one internet connection.

Sensitive information can still fall into the wrong hands. However, considerable efforts have been done to prevent this. The highest graded confidential information is relatively well protected, as long the users follow the procedures correctly. Information is technically secured, and printouts are for exceptional use. However, users are able to access this information from home or other location with internet connection, where non-employees might watch the screen.

None of the informants has heard of students modifying their grades at this specific school, but this might very well happen. In the classroom, teachers and students are relatively close, and it is easy for a student to observe – or film- the teacher typing his password. This fact can be combined with the findings in this thesis; many employees never change their password. There is no other protection than username and password. Mandatory password change might improve this a little, but two-factor authentication is far better. Datatilsynet - The Norwegian Data Protection Authority – also recommends two-factor authentication in this case (Datatilsynet 2014).

6.2 Discussion

The analysis part show that the school's risk level is relatively low. However, this might change in the future. First, students might get a higher information security competence level. Therefore this might change, even if no such considerable risks were found in this study. In addition, other things might happen, such as a major social conflict.

Unlike quantitative research, qualitative research has no intention of being representative. In qualitative research a case or a phenomenon is examined, and it is more important to explore this case or phenomenon in depth. A case study represents an adequate research method when there is little knowledge about the subject, like in this case. The case must be studied from several views, which in this case means through the interviewed stakeholders' eyes. A qualitative study is not relevant if the goal is to find out the amount of something, or the frequency. However, the qualitative study might e.g. generate new information about a subject, or identify categories of problems and perhaps strategies for solving them. In this case challenges related to information security was categorized by connecting them to the different layers in the SBC model.

Both before and during the research process, and after a conclusion is made, it is important for the researcher to have a humble approach to his work. No matter how rigid and accurate every phase of the process has been, there is always a possibility that the researcher e.g. has overlooked something, or specific information have not been available.

There are many possible pitfalls. One is that the researcher has specific presumptions. He might have a hope or an interest in achieving a specific result. Alternatively, the informants might know the researcher in advance, and therefore the informants might have specific presumptions.

In this study the interviews were audio recorded. Perhaps a video recording would have been better. Video recordings register e.g. an informant hesitating, rolling his eyes or clenching his fist. By using audio recordings, such details are challenging to catch. In addition, the transcription process might lose some important details. In this case all interviews were conducted in Norwegian. Later they were translated into English, and some details might be lost in the translation process.

6.3 Future studies

This study has identified some of the major threats the Norwegian high schools are facing today. It should be clear that the threats are of socio-technical nature. Therefore a deeper socio-technical analysis should be next step .

In addition, quantifying some of the finding could be very interesting. For instance, doing a survey where a large number of employees and students participate. In this thesis, none of the informants had any strategy for password change, even if they might have good and strong password phrases- that was not examined. An interesting question is; is this representative for the school? For all schools? For other organizations? Moreover, the media headlines about students modifying their grades, how common I that?

6.4 Ethical aspects

The participants are fully anonymized, both the identity of the persons and the name of the school. In principle, it is not possible to conjecture who has given a specific answer. However, all participants know that *their* school is examined. Therefore, the anonymity itself has specific limits, not formally, but in praxis. For instance, the principal knows who is the ICT leader at his school, and vice versa. In the same way, they both know who the social counsellor is. Therefore, if an employee – or a student – reveals compromising details, it might have negative impact on this informant. Due to this, as few details as possible might be connected to each person. However, some subjects are challenging to describe without referring to who in the small group is the informant. For instance, specific technical details might come from the ICT leader only. Having the transcriptions in the appendix part will therefore not be chosen in this thesis. Both audio recordings and transcriptions will be securely stored by the researcher for archival purposes.

Some studies might lead to negative consequences for some informants, such as delayed injury, or the informant regretting that he did participate. For this thesis, the researcher has evaluated the issue, and there should be minimal risk.

Bibliography

Alsabbagh, B. and S. Kowalski (2011). A cultural adaption model for global cyber security warning systems. 5th International Conference on Communications, Networking and Information Technology Dubai, UAE.

Commitees, T. N. N. R. E. (2016). "Guidelines for Research Ethics." Retrieved october, 2016, from https://www.etikkom.no/en/.

Datatilsynet. (2011). "Veileder i sikkerhetsarkitektur." Retrieved october, 2016

Datatilsynet. (2014). "Personvern i skole og barnehage." Retrieved november, 2016, from https://www.datatilsynet.no/globalassets/global/04_planer_rapporter/skoleprosjektet_samlerapport.pdf.

Denscombe, M. (2014). The good research guide: for small-scale social research projects, McGraw-Hill Education (UK).

Dinerman, B. (2011). "Social networking and security risks." GFI White Paper: 1-7.

Flick, U. (2009). An introduction to qualitative research, Sage.

Gerring, J. (2004). "What is a case study and what is it good for?" American political science review **98**(02): 341-354.

Grønlie, R. L., Heidi. (2015). "Hackere stoppet eksamen i hele fylket." Retrieved october, 2016, from http://www.nordlys.no/hackere-stoppet-eksamen-i-hele-fylket/s/5-34-159451.

ISO/IEC (2016). ISO/IEC 27000:2016(E). Terms and definitions**:** 2-14.

Kowalski, S. (1994). IT insecurity: a multi-disciplinary inquiry, Univ.

Larsen, P. W. S., Sigurd. (2015). "Nordland fylkeskommune rammet av hackerangrep." Retrieved october, 2016, from https://www.nrk.no/nordland/nordland-fylkeskommune-rammet-av-hackerangrep-1.12370373.

Leiknes, E. J. (2011). "Informasjonssikkerhet i komplekse systemer."

Marshall, B., P. Cardon, A. Poddar and R. Fontenot (2013). "Does sample size matter in qualitative research?: A review of qualitative interviews in IS research." Journal of Computer Information Systems **54**(1): 11-22.

Moss_Avis. (2007). "Elevinfo på avveie Protokoll trolig stjålet under innbrudd på skole." Retrieved october, 2016, from http://www.moss-avis.no/nyheter/elevinfo-pa-avveie-protokoll-trolig-stjalet-under-innbrudd-pa-skole/s/2-2.2643-1.4346855.

Muijs, D. (2010). Doing quantitative research in education with SPSS, Sage.

Nohlberg, M., S. Kowalski and K. Karlsson (2008). Ask and you shall know: using interviews and the SBC model for social-engineering penetration testing. International Multi-Conference on Engineering and Technological Innovation, IMETI 2008, 29 June-2 July 2008, Orlando, FL, USA.

Sallai, G. (2012). "Defining infocommunications and related terms." Acta Polytechnica Hungarica **9**(6): 5-15.

Sandve, E. S., Yngve; Damdsgaard, Eirik. (2016). "-Elever hacker lærernes PCer for å endre karakterer." from vg.no.

Sentralbyrå, S. (2016). "Videregående opplæring og annen videregående utdanning, 2015." Retrieved october, 2015, from https://www.ssb.no/utdanning/statistikker/vgu.

Staurheim, A. M. (2013). "Hvordan oppleves IKT sikkerhet og beredskapsarbeid i tre av landets fylkeskommuner?".

Wikipedia. (2015). "Liste over norske videregående skoler." Retrieved dec, 2016, from https://no.wikipedia.org/wiki/Liste_over_norske_videreg%C3%A5ende_skoler.

Yin, R. K. (1981). "The case study as a serious research strategy." Science communication **3**(1): 97-114.

A Overview over interviews

Interview Number	Role	Sex	Date	Duration (minutes)
1	ICT leader	M	23.nov	37
2	Teacher	M	23.nov	28
3	Student	F	23.nov	21
4	Teacher (union leader)	F	23.nov	21
5	Student	M	23.nov	17
6	Student	M	23.nov	18
7	Social counsellor	F	23.nov	42
8	Lærer	M	24.nov	25
9	Student	M	24.nov	16
10	Principal	M	24.nov	39
12	Politician	M	24.nov	16
13	Concultant county administration	M	28.nov	112

B STATEMENT OF COMPLIANCE

B.1 STATEMENT OF COMPLIANCE

Statement of participating to master thesis at NTNU

'Information security in Norwegian high schools – a Case study' /

'Informasjonssikkerhet ved norske videregående skoler - en Case studie'

I have received information about the project, and I confirm that I am willing to participate as an informant to the master thesis of Leif Olav Fjellingsdal.

My contribution is an interview that will be audio recorded and later transcribed. I have been offered a copy of the transcription and given the opportunity to make corrections. I am aware that all information related to the interview will be handled confidentially. I addition, I have been informed that I can withdraw from the interview at any time

Place and date:……
……..

Signature informant:……
……

B.2 SAMTYKKEERKLÆRING

Erklæring om deltakelse i arbeidet med masteroppgave ved NTNU

'Information security in Norwegian high schools – a Case study' /

'Informasjonssikkerhet ved norske videregående skoler - en Case studie'

Jeg har mottatt informasjon om prosjektet og bekrefter at jeg er villig til å delta som informant i masteroppgaven til Leif Olav Fjellingsdal.

Mitt bidrag skjer i form av et intervju som blir tatt opp og deretter transskribert. Jeg har fått tilbud om å få tilsendt en kopi av transskripsjonen og eventuelt komme med korrigeringer. Jeg er kjent med at all informasjon i forbindelse med intervjuet blir behandlet konfidensielt. Jeg er dessuten kjent med at jeg kan trekke meg fra undersøkelsen på et hvilket som helst tidspunkt.

Sted og dato:……
……..

Signatur informant:……
……

C Interviews in English

C.1 Interview, principal

Ethical level (about what is seen as right and wrong in society):

- How aware are employees in general of their responsibility related to handle sensitive personal information? And possible consequences for other persons integrity/dignity?
    - Scale 1-5 (low-high)
    - Is such awareness reflected in their behavior?
- How aware are *you* of your responsibility related to handle sensitive personal information? And possible consequences for other persons integrity/dignity?
    - Scale 1-5 (low-high)
- How aware are employees in general to the fact that 'hidden information about them is collected and stored? 'Hidden' means system logs, net logs, positioning information
    - Scale 1-5 (low-high)
- Should they be informed about this?
- How aware are students in general to the fact that 'hidden information about them is collected and stored? 'Hidden' means system logs, net logs, positioning information
    - Scale 1-5 (low-high)
- Should they be informed about this?
- Have you experienced ethical dilemmas related to information security?
    - For instance, getting hold of information that should be reported, but might compromise a person's integrity/dignity?
- Have there been incidents where a student or employee has got his/her integrity/dignity compromised because of poor routines related to information security?
    - Explain. Examples

Political and legal level (about laws and regulation sin society and how they are implemented):

- What are the most important legal topics you need to handle, related to information security?
    - Personal protection laws? Professional secrecy?
- Are there political influence to use social media in communication with non-employees, e.g. students, parents, external actors?
    - Reputation building. Marketing.

Administrative and managerial level (about managing and controlling operational tasks):

- How is ICT handled in your organization?
    - Internal services? External? Outsourcing? Other?
- How is ICT organized at the school?

    - What organization level? Number of employees.
- Is there some education for employees, related to information security?
    - Who, specific groups? New employees? Education for ICT personnel?
    - What type of education? Mandatory?
    - When? Regularly? When specific events occur?
    - Who is responsible for this type of education?
- Who in the organization deal(s) with sensitive or confidential information?
    - Groups? Teachers? Social counsellors? Administrative personnel?
- How is sensitive and confidential information secured?
    - Physical? Buildings or sections apart from other activity?
    - Routines, e.g. locking office while not present
    - Logical? Authentication. Passwords? Two-factor authentication? Other?
- How are unwanted security incidents reported?
    - Written procedures? Examples?
- Are there examples where the organization have improved information security because of security incidents?
    - Learned from previous events?
- Who is responsible for authenticity, accuracy and integrity of sensitive information?
    - Student data, employee data. Written procedures? Access logs?
- Have there been incidents where sensitive or confidential information has been stolen or by mistake come into wrong hands?
    - Examples? Describe the incident(s). Consequences? Personal. For the organization? For possible 'victim'?
- Which communication channels do you use to communicate with students and parents?
    - Phone. SMS. E-mail. LMS. Social media?
- How are social medias used in the organization in general?
    - Ethical guidelines available? Information about security threats through social media available? Written guidelines?
    - Do all employees have access to social media at work? Which social medias?
- Is a risk analysis performed every year?
    - If no, how often? Which organizational level? For the school? County?
- What procedures exist for discovering unwanted security incidents today?
    - Written procedures? Are system and security logs regularly checked?
- Irregular activity? Examples?
- How are unwanted security incidents handled today?
    - Types of incidents. Reactions, technical, personal penalty?
- *(Showing the informant Figure 2 SBC model)* Imagine that you have a budget dedicated to information security. In per cent, how would you divide the budget between the levels; Ethical, Political/Legal, Administrational/Managerial, Operational/Procedural, Technical?

Operational level (about directly security execution) :

- Have you *witnessed* one or more unwanted incidents related to information security?

    - Explain. What? When? How? Consequences?
- Have you *caused* one or more unwanted incidents related to information security?
    - Explain. What? When? How? Consequences?
- Personal question: The school use one-level authentication (username and password) for access to all main systems. This question is related to your access to the school's network. Do you use the same password for other, external services?
    - Do you know if other users do this?
    - When did you change password last time?
- Do you think any other person know your password?
- Do you know any other user's password?
    - Do you know if others have this type of information?

Other:

Do you have other things you want to add, related to information security? Questions that have not been asked?

C.2 Interview questions, ICT-leader

Technical level:

- Describe technical infrastructure.
    - Overview. Detail. Servers. Network. Wired/Wireless. What components are critical?
- How are critical components secured?
    - Physical? Logical? Other?
- What OS versions are used?
    - Server and workstations? Tablets? Other devices? Own devices vs private and other devices.
- What critical applications do you have in your organization?
- How are updates handled?
    - OS. Applications. Network devices.

Ethical level (about what is seen as right and wrong in society):

- How aware are employees in general of their responsibility related to handle sensitive personal information? And possible consequences for other persons integrity/dignity?
    - Scale 1-5 (low-high)
    - Is such awareness reflected in their behavior?
- How aware are *you* of your responsibility related to handle sensitive personal information? And possible consequences for other persons integrity/dignity?
    - Scale 1-5 (low-high)
- How aware are employees in general to the fact that 'hidden information about them is collected and stored? 'Hidden' means system logs, net logs, positioning information
    - Scale 1-5 (low-high)
- Should they be informed about this?
- How aware are students in general to the fact that 'hidden information about them is collected and stored? 'Hidden' means system logs, net logs, positioning information
    - Scale 1-5 (low-high)
- Should they be informed about this?
- Have you experienced ethical dilemmas related to information security?
    - For instance, getting hold of information that should be reported, but might compromise a person's integrity/dignity?
- Have there been incidents where a student or employee has got his/her integrity/dignity compromised because of poor routines related to information security?
    - Explain. Examples

Political and legal level (about laws and regulation sin society and how they are implemented):

- What are the most important legal topics you need to handle, related to information security?
    - Personal protection laws? Professional secrecy?
- Are there political influence to use social media in communication with non-employees, e.g. students, parents, external actors?
    - Reputation building. Marketing.

Administrative and managerial level (about managing and controlling operational tasks):

- How is ICT handled in your organization?
    - Internal services? External? Outsourcing? Other?
- How is ICT organized at the school?
    - What organization level? Number of employees.
- Is there some education for employees, related to information security?
    - Who, specific groups? New employees? Education for ICT personnel?
    - What type of education? Mandatory?
    - When? Regularly? When specific events occur?
    - Who is responsible for this type of education?
- Who in the organization deal(s) with sensitive or confidential information?
    - Groups? Teachers? Social counsellors? Administrative personnel?
- How is sensitive and confidential information secured?
    - Physical? Buildings or sections apart from other activity?
    - Routines, e.g. locking office while not present
    - Logical? Authentication. Passwords? Two-factor authentication? Other?
- How are unwanted security incidents reported?
    - Written procedures? Examples?
- Are there examples where the organization have improved information security because of security incidents?
    - Learned from previous events?
- Who is responsible for authenticity, accuracy and integrity of sensitive information?
    - Student data, employee data. Written procedures? Access logs?
- Have there been incidents where sensitive or confidential information has been stolen or by mistake come into wrong hands?
    - Examples? Describe the incident(s). Consequences? Personal. For the organization? For possible ‘victim’?
- Which communication channels do you use to communicate with students and parents?
    - Phone. SMS. E-mail. LMS. Social media?
- How are social medias used in the organization in general?
    - Ethical guidelines available? Information about security threats through social media available? Written guidelines?
    - Do all employees have access to social media at work? Which social medias?

- Is a risk analysis performed every year?
    - If no, how often? Which organizational level? For the school? County?
- What procedures exist for discovering unwanted security incidents today?
    - Written procedures? Are system and security logs regularly checked?
- Irregular activity? Examples?
- How are unwanted security incidents handled today?
    - Types of incidents. Reactions, technical, personal penalty?
- *(Showing the informant Figure 2 SBC model)* Imagine that you have a budget dedicated to information security. In per cent, how would you divide the budget between the levels; Ethical, Political/Legal, Administrational/Managerial, Operational/Procedural, Technical?

Operational level (about directly security execution) :

- Have you *witnessed* one or more unwanted incidents related to information security?
    - Explain. What? When? How? Consequences?
- Have you *caused* one or more unwanted incidents related to information security?
    - Explain. What? When? How? Consequences?
- Personal question: The school use one-level authentication (username and password) for access to all main systems. This question is related to your access to the school's network. Do you use the same password for other, external services?
    - Do you know if other users do this?
    - When did you change password last time?
- Do you think any other person know your password?
- Do you know any other user's password?
    - Do you know if others have this type of information?

Other:

Do you have other things you want to add, related to information security? Questions that have not been asked?

C.3 Interview questions, Social counsellor

Ethical level (about what is seen as right and wrong in society):

- How aware are employees in general of their responsibility related to handle sensitive personal information? And possible consequences for other persons integrity/dignity?
    - Scale 1-5 (low-high)
    - Is such awareness reflected in their behavior?
- How aware are *you* of your responsibility related to handle sensitive personal information? And possible consequences for other persons integrity/dignity?
    - Scale 1-5 (low-high)
- How aware are employees in general to the fact that 'hidden information about them is collected and stored? 'Hidden' means system logs, net logs, positioning information
    - Scale 1-5 (low-high)
- Should they be informed about this?
- How aware are students in general to the fact that 'hidden information about them is collected and stored? 'Hidden' means system logs, net logs, positioning information
    - Scale 1-5 (low-high)
- Should they be informed about this?
- Have you experienced ethical dilemmas related to information security?
    - For instance, getting hold of information that should be reported, but might compromise a person's integrity/dignity?
- Have there been incidents where a student or employee has got his/her integrity/dignity compromised because of poor routines related to information security?
    - Explain. Examples

Political and legal level (about laws and regulation sin society and how they are implemented):

- What are the most important legal topics you need to handle, related to information security?
    - Personal protection laws? Professional secrecy?
- Are there political influence to use social media in communication with non-employees, e.g. students, parents, external actors?
    - Reputation building. Marketing.

Administrative and managerial level (about managing and controlling operational tasks):

- Is there some education for employees, related to information security?
    - Who, specific groups? New employees? Education for ICT personnel?
    - What type of education? Mandatory?
    - When? Regularly? When specific events occur?
    - Who is responsible for this type of education?

- Who in the organization deal(s) with sensitive or confidential information?
    - Groups? Teachers? Social counsellors? Administrative personnel?
- How is sensitive and confidential information secured?
    - Physical? Buildings or sections apart from other activity?
    - Routines, e.g. locking office while not present
    - Logical? Authentication. Passwords? Two-factor authentication? Other?
- How are unwanted security incidents reported?
    - Written procedures? Examples?
- Are there examples where the organization have improved information security because of security incidents?
    - Learned from previous events?
- Who is responsible for authenticity, accuracy and integrity of sensitive information?
    - Student data, employee data. Written procedures? Access logs?
- Have there been incidents where sensitive or confidential information has been stolen or by mistake come into wrong hands?
    - Examples? Describe the incident(s). Consequences? Personal. For the organization? For possible 'victim'?
- Which communication channels do you use to communicate with students and parents?
    - Phone. SMS. E-mail. LMS. Social media?
- How are social medias used in the organization in general?
    - Ethical guidelines available? Information about security threats through social media available? Written guidelines?
    - Do all employees have access to social media at work? Which social medias?
- *(Showing the informant Figure 2 SBC model)* Imagine that you have a budget dedicated to information security. In per cent, how would you divide the budget between the levels; Ethical, Political/Legal, Administrational/Managerial, Operational/Procedural, Technical?

Operational level (about directly security execution) :

- Have you *witnessed* one or more unwanted incidents related to information security?
    - Explain. What? When? How? Consequences?
- Have you *caused* one or more unwanted incidents related to information security?
    - Explain. What? When? How? Consequences?
- Personal question: The school use one-level authentication (username and password) for access to all main systems. This question is related to your access to the school's network. Do you use the same password for other, external services?
    - Do you know if other users do this?
    - When did you change password last time?
- Do you think any other person know your password?
- Do you know any other user's password?
    - Do you know if others have this type of information?

Other:

Do you have other things you want to add, related to information security? Questions that have not been asked?

C.4 Interview questions, Teachers

Ethical level (about what is seen as right and wrong in society):

- How aware are employees in general of their responsibility related to handle sensitive personal information? And possible consequences for other persons integrity/dignity?
    - Scale 1-5 (low-high)
    - Is such awareness reflected in their behavior?
- How aware are *you* of your responsibility related to handle sensitive personal information? And possible consequences for other persons integrity/dignity?
    - Scale 1-5 (low-high)
- How aware are employees in general to the fact that 'hidden information about them is collected and stored? 'Hidden' means system logs, net logs, positioning information
    - Scale 1-5 (low-high)
- Should they be informed about this?
- How aware are students in general to the fact that 'hidden information about them is collected and stored? 'Hidden' means system logs, net logs, positioning information
    - Scale 1-5 (low-high)
- Should they be informed about this?
- Have you experienced ethical dilemmas related to information security?
    - For instance, getting hold of information that should be reported, but might compromise a person's integrity/dignity?
- Have there been incidents where a student or employee has got his/her integrity/dignity compromised because of poor routines related to information security?
    - Explain. Examples

Political and legal level (about laws and regulation sin society and how they are implemented):

- What are the most important legal topics you need to handle, related to information security?
    - Personal protection laws? Professional secrecy?
- Are there political influence to use social media in communication with non-employees, e.g. students, parents, external actors?
    - Reputation building. Marketing.

Administrative and managerial level (about managing and controlling operational tasks):

- Is there some education for employees, related to information security?
    - Who, specific groups? New employees? Education for ICT personnel?
    - What type of education? Mandatory?
    - When? Regularly? When specific events occur?
    - Who is responsible for this type of education?

- Who in the organization deal(s) with sensitive or confidential information?
    - Groups? Teachers? Social counsellors? Administrative personnel?
- How is sensitive and confidential information secured?
    - Physical? Buildings or sections apart from other activity?
    - Routines, e.g. locking office while not present
    - Logical? Authentication. Passwords? Two-factor authentication? Other?
- How are unwanted security incidents reported?
    - Written procedures? Examples?
- Are there examples where the organization have improved information security because of security incidents?
    - Learned from previous events?
- Who is responsible for authenticity, accuracy and integrity of sensitive information?
    - Student data, employee data. Written procedures? Access logs?
- Have there been incidents where sensitive or confidential information has been stolen or by mistake come into wrong hands?
    - Examples? Describe the incident(s). Consequences? Personal. For the organization? For possible 'victim'?
- Which communication channels do you use to communicate with students and parents?
    - Phone. SMS. E-mail. LMS. Social media?
- How are social medias used in the organization in general?
    - Ethical guidelines available? Information about security threats through social media available? Written guidelines?
    - Do all employees have access to social media at work? Which social medias?
- *(Showing the informant Figure 2 SBC model)* Imagine that you have a budget dedicated to information security. In per cent, how would you divide the budget between the levels; Ethical, Political/Legal, Administrational/Managerial, Operational/Procedural, Technical?

Operational level (about directly security execution) :

- Have you *witnessed* one or more unwanted incidents related to information security?
    - Explain. What? When? How? Consequences?
- Have you *caused* one or more unwanted incidents related to information security?
    - Explain. What? When? How? Consequences?
- Personal question: The school use one-level authentication (username and password) for access to all main systems. This question is related to your access to the school's network. Do you use the same password for other, external services?
    - Do you know if other users do this?
    - When did you change password last time?
- Do you think any other person know your password?
- Do you know any other user's password?
    - Do you know if others have this type of information?

Other:

Do you have other things you want to add, related to information security? Questions that have not been asked?

C.5 Interview questions, Students

Ethical level (about what is seen as right and wrong in society):

- How aware are employees in general of their responsibility related to handle sensitive personal information? And possible consequences for other persons integrity/dignity?
    - Scale 1-5 (low-high)
    - Is such awareness reflected in their behavior?
- How aware are students in general to the fact that 'hidden information about them is collected and stored? 'Hidden' means system logs, net logs, positioning information
    - Scale 1-5 (low-high)
- Should they be informed about this?
- Have you experienced ethical dilemmas related to information security?
    - For instance, getting hold of information that should be reported, but might compromise a person's integrity/dignity?
- Have there been incidents where a student or employee has got his/her integrity/dignity compromised because of poor routines related to information security?
    - Explain. Examples

Administrative and managerial level (about managing and controlling operational tasks):

- Is there some education for students, related to information security?
    - Who? Specific groups? New students?
    - What type of education? Mandatory?
    - When? Regularly? When specific events occur?
    - Who is responsible for this type of education?
- How are unwanted security incidents discovered by students reported?
    - Written procedures? Examples?
- Have there been incidents where sensitive or confidential information has been stolen or by mistake come into wrong hands?
    - Examples? Describe the incident(s). Consequences? Personal. For the organization? For possible 'victim'?
- Which communication channels do you use to communicate with students and parents?
    - Phone. SMS. E-mail. LMS. Social media?
- How are social medias used in the organization in general?
    - Ethical guidelines available? Information about security threats through social media available? Written guidelines?
    - Do all students have access to social media at work? Which social medias?
- *(Showing the informant Figure 2 SBC model)* Imagine that you have a budget dedicated to information security. In per cent, how would you divide the budget between the levels; Ethical, Political/Legal, Administrational/Managerial, Operational/Procedural, Technical?

Operational level (about directly security execution) :

- Have you *witnessed* one or more unwanted incidents related to information security?
    - Explain. What? When? How? Consequences?
- Have you *caused* one or more unwanted incidents related to information security?
    - Explain. What? When? How? Consequences?
- Personal question: The school use one-level authentication (username and password) for access to all main systems. This question is related to your access to the school's network. Do you use the same password for other, external services?
    - Do you know if other users do this? Is this common among students?
    - When did you change password last time?
- Do you think any other person know your password?
- Do you know any other student's password?
    - If so, how did you get it?
    - Do you know if other students have this type of information?
- Do you know any employee's password?
    - If so, how did you get it?
    - Do you know if other students have this type of information?

Other:

Do you have other things you want to add, related to information security? Questions that have not been asked?

C.6 Interview questions, ICT consultant at county administration

Technical level:

- Describe technical infrastructure.
    - Overview. Detail. Servers. Network. Wired/Wireless. What components are critical?
- How are critical components secured?
    - Physical? Logical? Other?
- What OS versions are used?
    - Server and workstations? Tablets? Other devices? Own devices vs private and other devices.
- What critical applications do you have in your organization?
- How are updates handled?
    - OS. Applications. Network devices.

Ethical level (about what is seen as right and wrong in society):

- How aware are employees in general of their responsibility related to handle sensitive personal information? And possible consequences for other persons integrity/dignity?
    - Scale 1-5 (low-high)
    - Is such awareness reflected in their behavior?
- How aware are *you* of your responsibility related to handle sensitive personal information? And possible consequences for other persons integrity/dignity?
    - Scale 1-5 (low-high)
- How aware are employees in general to the fact that 'hidden information about them is collected and stored? 'Hidden' means system logs, net logs, positioning information
    - Scale 1-5 (low-high)
- Should they be informed about this?
- How aware are students in general to the fact that 'hidden information about them is collected and stored? 'Hidden' means system logs, net logs, positioning information
    - Scale 1-5 (low-high)
- Should they be informed about this?
- Have you experienced ethical dilemmas related to information security?
    - For instance, getting hold of information that should be reported, but might compromise a person's integrity/dignity?
- Have there been incidents where a student or employee has got his/her integrity/dignity compromised because of poor routines related to information security?
    - Explain. Examples

Political and legal level (about laws and regulation sin society and how they are implemented):

- What are the most important legal topics you need to handle, related to information security?
    - Personal protection laws? Professional secrecy?
- Are there political influence to use social media in communication with non-employees, e.g. students, parents, external actors?
    - Reputation building. Marketing.

Administrative and managerial level (about managing and controlling operational tasks):

- How is ICT handled in your organization?
    - Internal services? External? Outsourcing? Other?
- How is ICT organized at the school?
    - What organization level? Number of employees.
- Is there some education for employees, related to information security?
    - Who, specific groups? New employees? Education for ICT personnel?
    - What type of education? Mandatory?
    - When? Regularly? When specific events occur?
    - Who is responsible for this type of education?
- Who in the organization deal(s) with sensitive or confidential information?
    - Groups? Teachers? Social counsellors? Administrative personnel?
- How is sensitive and confidential information secured?
    - Physical? Buildings or sections apart from other activity?
    - Routines, e.g. locking office while not present
    - Logical? Authentication. Passwords? Two-factor authentication? Other?
- How are unwanted security incidents reported?
    - Written procedures? Examples?
- Are there examples where the organization have improved information security because of security incidents?
    - Learned from previous events?
- Who is responsible for authenticity, accuracy and integrity of sensitive information?
    - Student data, employee data. Written procedures? Access logs?
- Have there been incidents where sensitive or confidential information has been stolen or by mistake come into wrong hands?
    - Examples? Describe the incident(s). Consequences? Personal. For the organization? For possible 'victim'?
- Which communication channels do you use to communicate with students and parents?
    - Phone. SMS. E-mail. LMS. Social media?
- How are social medias used in the organization in general?
    - Ethical guidelines available? Information about security threats through social media available? Written guidelines?
    - Do all employees have access to social media at work? Which social medias?
- Is a risk analysis performed every year?
    - If no, how often? Which organizational level? For the school? County?
- What procedures exist for discovering unwanted security incidents today?

    - Written procedures? Are system and security logs regularly checked?
- Irregular activity? Examples?
- How are unwanted security incidents handled today?
    - Types of incidents. Reactions, technical, personal penalty?
- *(Showing the informant Figure 2 SBC model)* Imagine that you have a budget dedicated to information security. In per cent, how would you divide the budget between the levels; Ethical, Political/Legal, Administrational/Managerial, Operational/Procedural, Technical?

Operational level (about directly security execution) :

- Have you *witnessed* one or more unwanted incidents related to information security?
    - Explain. What? When? How? Consequences?
- Have you *caused* one or more unwanted incidents related to information security?
    - Explain. What? When? How? Consequences?
- Personal question: The school use one-level authentication (username and password) for access to all main systems. This question is related to your access to the school's network. Do you use the same password for other, external services?
    - Do you know if other users do this?
    - When did you change password last time?
- Do you think any other person know your password?
- Do you know any other user's password?
    - Do you know if others have this type of information?

Other:

Do you have other things you want to add, related to information security? Questions that have not been asked?

C.7 Interview questions, Politician

Ethical level (about what is seen as right and wrong in society):

- How aware are employees in general of their responsibility related to handle sensitive personal information? And possible consequences for other persons integrity/dignity?
    - Scale 1-5 (low-high)
    - Is such awareness reflected in their behavior?
- How aware are *you* of your responsibility related to handle sensitive personal information? And possible consequences for other persons integrity/dignity?
    - Scale 1-5 (low-high)
- How aware are employees in general to the fact that 'hidden information about them is collected and stored? 'Hidden' means system logs, net logs, positioning information
    - Scale 1-5 (low-high)
- Should they be informed about this?
- How aware are students in general to the fact that 'hidden information about them is collected and stored? 'Hidden' means system logs, net logs, positioning information
    - Scale 1-5 (low-high)
- Should they be informed about this?
- Have you experienced ethical dilemmas related to information security?
    - For instance, getting hold of information that should be reported, but might compromise a person's integrity/dignity?
- Have there been incidents where a student or employee has got his/her integrity/dignity compromised because of poor routines related to information security?
    - Explain. Examples

Political and legal level (about laws and regulation sin society and how they are implemented):

- What are the most important legal topics you need to handle, related to information security?
    - Personal protection laws? Professional secrecy?
- Are there political influence to use social media in communication with non-employees, e.g. students, parents, external actors?
    - Reputation building. Marketing.

Administrative and managerial level (about managing and controlling operational tasks):

- Is there some education for employees, related to information security?
    - Who, specific groups? New employees?
    - What type of education? Mandatory?
    - When? Regularly? When specific events occur?
    - Who is responsible for this type of education?

- Who in the organization deal(s) with sensitive or confidential information?
    - Groups? Teachers? Social counsellors? Administrative personnel?
- Are there examples where the organization have improved information security because of security incidents?
    - Learned from previous events?
- Have there been incidents where sensitive or confidential information has been stolen or by mistake come into wrong hands?
    - Examples? Describe the incident(s). Consequences? Personal. For the organization? For possible 'victim'?
- Which communication channels do you use to communicate with students and parents?
    - Phone. SMS. E-mail. LMS. Social media?
- How are social medias used in the organization in general?
    - Ethical guidelines available? Information about security threats through social media available? Written guidelines?
    - Do all employees have access to social media at work? Which social medias?
- *(Showing the informant Figure 2 SBC model)* Imagine that you have a budget dedicated to information security. In per cent, how would you divide the budget between the levels; Ethical, Political/Legal, Administrational/Managerial, Operational/Procedural, Technical?

Operational level (about directly security execution) :

- Have you *witnessed* one or more unwanted incidents related to information security?
    - Explain. What? When? How? Consequences?
- Have you *caused* one or more unwanted incidents related to information security?
    - Explain. What? When? How? Consequences?
- Do you know any user's password (employee or student)?
    - Do you know if others have this type of information?

Other:

Do you have other things you want to add, related to information security? Questions that have not been asked?

D Intervjuer på norsk

D.1 Intervju, rektor

Ethical level (about what is seen as right and wrong in society):

- Hvor bevisst er ansatte generelt sitt etiske ansvar, med tanke på å behandle sensitive persondata? Samt mulige konsekvenser for andre personers integritet integritet/selvrespekt/verdighet?
    - Grader på en skala fra 1-5 (lav-høy)
    - Reflekteres dette i adferden deres?
- Hvor bevisst er *du selv* på ditt etiske ansvar, med tanke på å behandle sensitive persondata? Samt mulige konsekvenser for andre personers integritet/selvrespekt/verdighet?
    - Grader på en skala fra 1-5 (lav-høy)
- I hvor stor grad vet ansatte generelt hvilken 'skjult' informasjon som blir samlet om dem og lagret? Hvor bevisste er ansatte omkring slike ting? Skjult betyr her systemlogger, nettverkslogger, informasjon om posisjon og lignende.
    - Grader på en skala fra 1-5 (lav-høy)
- Burde ansatte bli informert om slike ting?
- Vet elevene generelt hvilken 'skjult' informasjon som blir samlet om dem og lagret? Hvor bevisste er ansatte omkring slike ting? Skjult betyr her systemlogger, nettverkslogger, informasjon om posisjon og lignende.
    - Grader på en skala fra 1-5 (lav-høy)
- Burde elevene bli informert om slike ting?
- Har du opplevd etiske dilemmaer knyttet til informasjonssikkerhet?
    - For eksempel å få informasjon som burde blitt rapportert, men som i så fall kunne skadet en persons integritet/verdighet/omdømme? Eller: Innsamlede data blir brukt i en annen sammenheng enn det som var hensikten, uten at 'offeret' har kjennskap til det?
- Har det forekommet hendelser der elever eller ansatte har fått skadet verdighet/omdømme pga for dårlige prosedyrer knyttet til informasjonssikkerhet?
    - Forklar. Eksempler

Political and legal level (about laws and regulation sin society and how they are implemented) :

- Hva er de viktigste juridiske aspektene du er nødt til å håndtere, med tanke på informasjonssikkerhet?
    - Personopplysningsloven? Taushetsplikt?

- Foreligger det noen politiske føringer for å bruke sosiale medier i kommunikasjon med ikke-ansatte, for eksempel elever, foresatte eller eksterne aktører?
    - Omdømmebygging. Markedsføring

Administrative and managerial level (about managing and controlling operational tasks):

- Hvordan håndteres IT I din organisasjon?
    - Interne tjenester? Eksterne? Outsourcing? Annet?
- Hvordan er IT-tjenesten organisert ved skolen?
    - Nivå i organisasjonen. Antall ansatte
- Eksisterer det noen opplæring knyttet for ansatte, knyttet til informasjonssikkerhet?
    - Hvem? Bestemte grupper? Nyansatte? IKT-ansatte?
    - Hva slags opplæring? Obligatorisk?
    - Når? Regelmessig? Ved bestemte hendelser?
    - Hvem er ansvarlig for slik opplæring?
- Hvem I organisasjonen håndterer sensitive eller konfidensiell informasjon?
    - Grupper? Lærere? Rådgivere, PPT? Administrativt personell?
- Hvordan er sensitiv og konfidensiell informasjon sikret?
    - Fysisk? Bygninger eller avdelinger/seksjoner atskilt fra annen aktivitet?
    - Rutiner, for eksempel låsing av kontor når man ikke er tilstede?
    - Logisk? Autentisering? Passord? Tofaktorautentisering? Annet?
- Hvordan blir uønskede hendelser knyttet til informasjonssikkerhet rapportert?
    - Skrevne prosedyrer? Eksempler?
- Finnes det eksempler der organisasjonen har forbedret informasjonssikkerheten pga sikkerhetshendelser?
    - Har man lært av tidligere hendelser?
- Hvem er ansvarlig for tilganger til sensitiv informasjon, samt at informasjonen er korrekt?
    - Opplysninger om elever og ansatte. Skrevne prosedyrer? Tilgangslogger?
- Hard et forekommet uønskede hendelser der sensitiv eller konfidensiell informasjon har blitt stjålet eller kommet i gale hender ved feiltakelse?
    - Eksempler? Beskriv hendelsen(e). Konsekvenser. Personlige konsekvenser? For organisasjonen? For mulig ‘offer’?
- Hvilke kommunikasjonskanaler bruker skolen for å kommunisere med elever og foreldre?
    - Telefon. SMS. E-post. LMS. Sosiale medier?
- Hvordan bruke sosiale medier I organisasjonen generelt?
    - Finnes det etiske retningslinjer for bruken? Er det tilgjengelig informasjon om sikkerhetstrusler gjennom sosiale medier? Skriftlig informasjon og retningslinjer?
    - Har alle ansatte tilgang til sosiale medier på arbeid? Hvilke (typer) sosiale medier?

- Foretas det en risikoanalyse hvert år?
- Hvis ikke, hvor ofte? På hvilket organisasjonsnivå? For skolen? For fylket som helhet? Hvilke prosedyrer eksisterer for å oppdage sikkerhetshendelser I dag?
    - Skrevne prosedyrer? Blir system- og sikkerhetslogger jevnlig sjekket?
    - Unormal aktivitet? Eksempler?
- Hvordan blir sikkerhetshendelser håndtert I dag?
    - Ulike typer uønskede hendelser. Reaksjoner, teknisk, personlige konsekvenser?
    -
- *(Viser informanten Figure 2 SBC model*) Forestill deg at du har et budsjett som er øremerket informasjonssikkerhet. Hvor mange prosent vil du bruke på hvert av de følgende nivåene: Etisk, politisk/juridisk, administrativt, operativt, teknisk?

Operational level (about directly security execution) :

- Har du vært *vitne til* en eller flere uønskede hendelser relater til informasjonssikkerhet?
    - Forklar. Hva? Når? Hvordan? Konsekvenser?
- Har du selv *forårsaket* en eller flere uønskede hendelser relater til informasjonssikkerhet?
    - Forklar. Hva? Når? Hvordan? Konsekvenser?
- Personlig spørsmål: Skolen bruker ettnivå/enfaktor autentisering (brukernavn og password) for tilgang til alle sentrale systemer. Dette spørsmålet gjelder tilgang til skolens nettverk. Bruker du samme passord til en eller flere andre, eksterne tjenester?
    - Kjenner du til om andre gjør det?
    - Når byttet du sist passord?
- Kjenner du passordet til en eller flere andre brukere?

Other:

Har du andre ting du ønsker å tilføye, knyttet til informasjonssikkerhet. Spørsmål som ikke har stilt?

D.2 Intervju, IKT-leder

Technical level:

- Beskriv teknisk infrastruktur
    - Oversikt. Detalj. Servere. Nettverk. Tråd/Trådløst. Hvilke komponenter er kritiske?
- Hvordan er kritiske komponenter sikret?
    - Fysisk? Logisk? Annet?
- Hvilke OS versjoner er i bruk?
    - Servere og arbeidsstasjoner? Nettbrett? Andre enheter? Skolens enheter vs private?
- Hvilke kritiske applikasjoner finnes I organisasjonen?
- Hvordan håndteres oppdateringer?
    - OS. Applikasjoner. Nettverksutstyr.

Ethical level (about what is seen as right and wrong in society):

- Er ansatte generelt bevisst sitt etiske ansvar, med tanke på å behandle sensitive persondata? Samt mulige konsekvenser for andre personers integritet/selvrespekt/verdighet?
    - Grader på en skala fra 1-5 (lav-høy)
    - Reflekteres dette i adferden deres?
- Hvor bevisst er *du selv* på ditt etiske ansvar, med tanke på å behandle sensitive persondata? Samt mulige konsekvenser for andre personers integritet/selvrespekt/verdighet?
    - Grader på en skala fra 1-5 (lav-høy)
- Vet ansatte generelt hvilken 'skjult' informasjon som blir samlet om dem og lagret? Hvor bevisste er ansatte omkring slike ting? Skjult betyr her systemlogger, nettverkslogger, informasjon om posisjon og lignende.
    - Grader på en skala fra 1-5 (lav-høy)
- Burde ansatte bli informert om slike ting?
- Vet elevene generelt hvilken 'skjult' informasjon som blir samlet om dem og lagret? Hvor bevisste er ansatte omkring slike ting? Skjult betyr her systemlogger, nettverkslogger, informasjon om posisjon og lignende.
    - Grader på en skala fra 1-5 (lav-høy)
- Burde elevene bli informert om slike ting?
- Har du opplevd etiske dilemmaer knyttet til informasjonssikkerhet?
    - For eksempel å få informasjon som burde blitt rapportert, men som i så fall kunne skadet en persons verdighet/omdømme? Eller: Innsamlede data blir brukt i en annen sammenheng enn det som var hensikten, uten at 'offeret' har

kjennskap til det?

- Har det forekommet uønskede hendelser der elever eller ansatte har fått skadet verdighet/omdømme pga for dårlige prosedyrer knyttet til informasjonssikkerhet?
    - Forklar. Eksempler

Political and legal level (about laws and regulation sin society and how they are implemented) :

- Hva er de viktigste juridiske aspektene du er nødt til å håndtere, med tanke på informasjonssikkerhet?
    - Personopplysningsloven. Taushetsplikt
- Foreligger det noen politiske føringer for å bruke sosiale medier i kommunikasjon med ikke-ansatte, for eksempel elever, foresatte eller eksterne aktører?
    - Omdømmebygging. Markedsføring

Administrative and managerial level (about managing and controlling operational tasks):

- Hvordan håndteres IT I din organisasjon?
    - Interne tjenester? Eksterne? Outsourcing? Annet?
- Hvordan er IT-tjenesten organisert ved skolen?
    - Nivå i organisasjonen. Antall ansatte
- Eksisterer det noen opplæring knyttet for ansatte, knyttet til informasjonssikkerhet?
    - Hvem? Bestemte grupper? Nyansatte? IKT-ansatte?
    - Hva slags opplæring? Obligatorisk?
    - Når? Regelmessig? Ved bestemte hendelser?
    - Hvem er ansvarlig for slik opplæring?
- Hvem I organisasjonen håndterer sensitive eller konfidensiell informasjon?
    - Grupper? Lærere? Rådgivere, PPT? Administrativt personell?
- Hvordan er sensitiv og konfidensiell informasjon sikret?
    - Fysisk? Bygninger eller avdelinger/seksjoner atskilt fra annen aktivitet?
    - Rutiner, for eksempel låsing av kontor når man ikke er tilstede?
    - Logisk? Autentisering? Passord? Tofaktorautentisering? Annet?
- Hvordan blir uønskede hendelser knyttet til informasjonssikkerhet rapportert?
    - Skrevne prosedyrer? Eksempler?
- Finnes det eksempler der organisasjonen har forbedret informasjonssikkerheten pga sikkerhethendelser?
    - Har man lært av tidligere hendelser?
- Hvem er ansvarlig for tilganger til sensitiv informasjon, samt at informasjonen er

korrekt?
    - Opplysninger om elever og ansatte. Skrevne prosedyrer? Tilgangslogger?
- Hard et forekommet uønskede hendelser der sensitiv eller konfidensiell informasjon har blitt stjålet eller kommet i gale hender ved feiltakelse?
    - Eksempler? Beskriv hendelsen(e). Konsekvenser. Personlige konsekvenser? For organisasjonen? For mulig 'offer'?
- Hvilke kommunikasjonskanaler brukes for å kommunisere med elever og foreldre?
    - Telefon. SMS. E-post. LMS. Sosiale medier
- Hvordan brukes sosiale medier I organisasjonen generelt?
    - Finnes det etiske retningslinjer for bruken? Er det tilgjengelig informasjon om sikkerhetstrusler gjennom sosiale medier? Skriftlig informasjon og retningslinjer?
    - Har alle ansatte tilgang til sosiale medier på arbeid? Hvilke (typer) sosiale medier?
- Foretas det en risikoanalyse hvert år?
    - Hvis ikke, hvor ofte? På hvilket organisasjonsnivå? For skolen? For fylket som helhet?
- Forestill deg at du har et budsjett som er øremerket informasjonssikkerhet. Hvor mange prosent vil du bruke på hvert av de følgende nivåene: Etisk, politisk/juridisk, administrativt, operativt, teknisk?

Operational level (about directly security execution) :

- Hvilke prosedyrer eksisterer for å oppdage sikkerhetshendelser I dag?
    - Skrevne prosedyrer? Blir system- og sikkerhetslogger jevnlig sjekket?
    - Unormal aktivitet? Eksempler?
- Hvordan blir sikkerhetshendelser håndtert I dag?
    - Ulike typer hendelser. Reaksjoner, teknisk, personlige konsekvenser?
- Har du vært vitne til en eller flere uønskede hendelser relater til informasjonssikkerhet?
    - Forklar. Hva? Når? Hvordan? Konsekvenser?
- Har du selv forårsaket en eller flere uønskede hendelser relater til informasjonssikkerhet?
    - Forklar. Hva? Når? Hvordan? Konsekvenser?
- Personlig spørsmål: Skolen bruker ettnivå/enfaktor autentisering (brukernavn og password) for tilgang til alle sentrale systemer. Dette spørsmålet gjelder tilgang til skolens nettverk. Bruker du samme passord til en eller flere andre, eksterne tjenester?
    - Kjenner du til om andre gjør det?
    - Når byttet du sist passord?
- Kjenner du passordet til en eller flere andre brukere?

Other:

Har du andre ting du ønsker å tilføye, som det ikke har blitt spurt om?

D.3 Intervju, Spes.ped rådgiver

Ethical level (about what is seen as right and wrong in society):

- Er ansatte generelt bevisst sitt etiske ansvar, med tanke på å behandle sensitive persondata? Samt mulige konsekvenser for andre personers integritet/selvrespekt/verdighet?
    - Grader på en skala fra 1-5 (lav-høy)
    - Reflekteres dette i adferden deres?
- Hvor bevisst er *du selv* på ditt etiske ansvar, med tanke på å behandle sensitive persondata? Samt mulige konsekvenser for andre personers integritet/selvrespekt/verdighet?
    - Grader på en skala fra 1-5 (lav-høy)
- Vet ansatte generelt hvilken 'skjult' informasjon som blir samlet om dem og lagret? Hvor bevisste er ansatte omkring slike ting? Skjult betyr her systemlogger, nettverkslogger, informasjon om posisjon og lignende.
    - Grader på en skala fra 1-5 (lav-høy)
- Burde ansatte bli informert om slike ting?
- Vet elevene generelt hvilken 'skjult' informasjon som blir samlet om dem og lagret? Hvor bevisste er ansatte omkring slike ting? Skjult betyr her systemlogger, nettverkslogger, informasjon om posisjon og lignende.
    - Grader på en skala fra 1-5 (lav-høy)
- Burde elevene bli informert om slike ting?
- Har du opplevd etiske dilemmaer knyttet til informasjonssikkerhet?
    - For eksempel å få informasjon som burde blitt rapportert, men som i så fall kunne skadet en persons verdighet/omdømme? Eller: Innsamlede data blir brukt i en annen sammenheng enn det som var hensikten, uten at 'offeret' har kjennskap til det?
- Har det forekommet uønskede hendelser der elever eller ansatte har fått skadet integritet/verdighet/omdømme pga for dårlige prosedyrer knyttet til informasjonssikkerhet?
    - Forklar. Eksempler

Political and legal level (about laws and regulation sin society and how they are implemented) :

- Hva er de viktigste juridiske aspektene du er nødt til å håndtere, med tanke på informasjonssikkerhet?
    - Personopplysningsloven. Taushetsplikt
- Foreligger det noen politiske føringer for å bruke sosiale medier i kommunikasjon med ikke-ansatte, for eksempel elever, foresatte eller eksterne aktører?
    - Omdømmebygging. Markedsføring

Administrative and managerial level (about managing and controlling operational tasks):

- Eksisterer det noen opplæring knyttet for ansatte, knyttet til informasjonssikkerhet?
    - Hvem? Bestemte grupper? Nyansatte? IKT-ansatte?
    - Hva slags opplæring? Obligatorisk?
    - Når? Regelmessig? Ved bestemte hendelser?
    - Hvem er ansvarlig for slik opplæring?
- Hvem I organisasjonen håndterer sensitive eller konfidensiell informasjon?
    - Grupper? Lærere? Rådgivere, PPT? Administrativt personell?
- Hvordan er sensitiv og konfidensiell informasjon sikret?
    - Fysisk? Bygninger eller avdelinger/seksjoner atskilt fra annen aktivitet?
    - Rutiner, for eksempel låsing av kontor når man ikke er tilstede?
    - Logisk? Autentisering? Passord? Tofaktorautentisering? Annet?
- Hvordan blir uønskede hendelser knyttet til informasjonssikkerhet rapportert?
    - Skrevne prosedyrer? Eksempler?
- Finnes det eksempler der organisasjonen har forbedret informasjonssikkerheten pga sikkerhethendelser?
    - Har man lært av tidligere hendelser?
- Hvem er ansvarlig for tilganger til sensitiv informasjon, samt at informasjonen er korrekt?
    - Opplysninger om elever og ansatte. Skrevne prosedyrer? Tilgangslogger?
- Hard et forekommet uønskede hendelser der sensitiv eller konfidensiell informasjon har blitt stjålet eller kommet i gale hender ved feiltakelse?
    - Eksempler? Beskriv hendelsen(e). Konsekvenser. Personlige konsekvenser? For organisasjonen? For mulig ‘offer’?
- Hvilke kommunikasjonskanaler brukes for å kommunisere med elever og foreldre?
    - Telefon. SMS. E-post. LMS. Sosiale medier
- Hvordan brukes sosiale medier I organisasjonen generelt?
    - Finnes det etiske retningslinjer for bruken? Er det tilgjengelig informasjon om sikkerhetstrusler gjennom sosiale medier? Skriftlig informasjon og retningslinjer?
    - Har alle ansatte tilgang til sosiale medier på arbeid? Hvilke (typer) sosiale medier?
- Forestill deg at du har et budsjett som er øremerket informasjonssikkerhet. Hvor mange prosent vil du bruke på hvert av de følgende nivåene: Etisk, politisk/juridisk, administrativt, operativt, teknisk?

Operational level (about directly security execution) :

- Har du vært vitne til en eller flere uønskede hendelser relater til informasjonssikkerhet?
    - Forklar. Hva? Når? Hvordan? Konsekvenser?
- Har du selv forårsaket en eller flere uønskede hendelser relater til informasjonssikkerhet?
    - Forklar. Hva? Når? Hvordan? Konsekvenser?

- Personlig spørsmål: Skolen bruker ettnivå/enfaktor autentisering (brukernavn og password) for tilgang til alle sentrale systemer. Dette spørsmålet gjelder tilgang til skolens nettverk. Bruker du samme passord til en eller flere andre, eksterne tjenester?
    - Kjenner du til om andre gjør det?
    - Når byttet du sist passord?
- Kjenner du passordet til en eller flere andre brukere?

Other:

Har du andre ting du ønsker å tilføye, som det ikke har blitt spurt om?

D.4 Intervju, lærere

Ethical level (about what is seen as right and wrong in society):

- Er ansatte generelt bevisst sitt etiske ansvar, med tanke på å behandle sensitive persondata? Samt mulige konsekvenser for andre personers integritet/selvrespekt/verdighet?
    - Grader på en skala fra 1-5 (lav-høy)
    - Reflekteres dette i adferden deres?
- Hvor bevisst er *du selv* på ditt etiske ansvar, med tanke på å behandle sensitive persondata? Samt mulige konsekvenser for andre personers integritet/selvrespekt/verdighet?
    - Grader på en skala fra 1-5 (lav-høy)
- Vet ansatte generelt hvilken 'skjult' informasjon som blir samlet om dem og lagret? Hvor bevisste er ansatte omkring slike ting? Skjult betyr her systemlogger, nettverkslogger, informasjon om posisjon og lignende.
    - Grader på en skala fra 1-5 (lav-høy)
- Burde ansatte bli informert om slike ting?
- Vet elevene generelt hvilken 'skjult' informasjon som blir samlet om dem og lagret? Hvor bevisste er ansatte omkring slike ting? Skjult betyr her systemlogger, nettverkslogger, informasjon om posisjon og lignende.
    - Grader på en skala fra 1-5 (lav-høy)
- Burde elevene bli informert om slike ting?
- Har du opplevd etiske dilemmaer knyttet til informasjonssikkerhet?
    - For eksempel å få informasjon som burde blitt rapportert, men som i så fall kunne skadet en persons verdighet/omdømme? Eller: Innsamlede data blir brukt i en annen sammenheng enn det som var hensikten, uten at 'offeret' har kjennskap til det?
- Har det forekommet uønskede hendelser der elever eller ansatte har fått skadet integritet/verdighet/omdømme pga for dårlige prosedyrer knyttet til informasjonssikkerhet?
    - Forklar. Eksempler

Political and legal level (about laws and regulation sin society and how they are implemented) :

- Hva er de viktigste juridiske aspektene du er nødt til å håndtere, med tanke på informasjonssikkerhet?
    - Personopplysningsloven. Taushetsplikt
- Foreligger det noen politiske føringer for å bruke sosiale medier i kommunikasjon med ikke-ansatte, for eksempel elever, foresatte eller eksterne aktører?
    - Omdømmebygging. Markedsføring

Administrative and managerial level (about managing and controlling operational tasks):

- Eksisterer det noen opplæring knyttet for ansatte, knyttet til informasjonssikkerhet?
    - Hvem? Bestemte grupper? Nyansatte? IKT-ansatte?
    - Hva slags opplæring? Obligatorisk?
    - Når? Regelmessig? Ved bestemte hendelser?
    - Hvem er ansvarlig for slik opplæring?
- Hvem I organisasjonen håndterer sensitive eller konfidensiell informasjon?
    - Grupper? Lærere? Rådgivere, PPT? Administrativt personell?
- Hvordan er sensitiv og konfidensiell informasjon sikret?
    - Fysisk? Bygninger eller avdelinger/seksjoner atskilt fra annen aktivitet?
    - Rutiner, for eksempel låsing av kontor når man ikke er tilstede?
    - Logisk? Autentisering? Passord? Tofaktorautentisering? Annet?
- Hvordan blir uønskede hendelser knyttet til informasjonssikkerhet rapportert?
    - Skrevne prosedyrer? Eksempler?
- Finnes det eksempler der organisasjonen har forbedret informasjonssikkerheten pga sikkerhethendelser?
    - Har man lært av tidligere hendelser?
- Hvem er ansvarlig for tilganger til sensitiv informasjon, samt at informasjonen er korrekt?
    - Opplysninger om elever og ansatte. Skrevne prosedyrer? Tilgangslogger?
- Hard et forekommet uønskede hendelser der sensitiv eller konfidensiell informasjon har blitt stjålet eller kommet i gale hender ved feiltakelse?
    - Eksempler? Beskriv hendelsen(e). Konsekvenser. Personlige konsekvenser? For organisasjonen? For mulig ‘offer’?
- Hvilke kommunikasjonskanaler brukes for å kommunisere med elever og foreldre?
    - Telefon. SMS. E-post. LMS. Sosiale medier
- Hvordan brukes sosiale medier I organisasjonen generelt?
    - Finnes det etiske retningslinjer for bruken? Er det tilgjengelig informasjon om sikkerhetstrusler gjennom sosiale medier? Skriftlig informasjon og retningslinjer?
    - Har alle ansatte tilgang til sosiale medier på arbeid? Hvilke (typer) sosiale medier?
- Forestill deg at du har et budsjett som er øremerket informasjonssikkerhet. Hvor mange prosent vil du bruke på hvert av de følgende nivåene: Etisk, politisk/juridisk, administrativt, operativt, teknisk?

Operational level (about directly security execution) :

- Har du vært vitne til en eller flere uønskede hendelser relater til informasjonssikkerhet?
    - Forklar. Hva? Når? Hvordan? Konsekvenser?
- Har du selv forårsaket en eller flere uønskede hendelser relater til informasjonssikkerhet?
    - Forklar. Hva? Når? Hvordan? Konsekvenser?

- Personlig spørsmål: Skolen bruker ettnivå/enfaktor autentisering (brukernavn og password) for tilgang til alle sentrale systemer. Dette spørsmålet gjelder tilgang til skolens nettverk. Bruker du samme passord til en eller flere andre, eksterne tjenester?
    - Kjenner du til om andre gjør det?
    - Når byttet du sist passord?
- Kjenner du passordet til en eller flere andre brukere?

Other:

Har du andre ting du ønsker å tilføye, som det ikke har blitt spurt om?

D.5 Intervju, elever

Ethical level (about what is seen as right and wrong in society):

- Er ansatte generelt bevisst sitt etiske ansvar, med tanke på å behandle sensitive persondata? Samt mulige konsekvenser for andre personers integritet integritet/selvrespekt/verdighet?
    - Grader på en skala fra 1-5 (lav-høy)
- Vet elevene generelt hvilken 'skjult' informasjon som blir samlet om dem og lagret? Hvor bevisste er ansatte omkring slike ting? Skjult betyr her systemlogger, nettverkslogger, informasjon om posisjon og lignende.
    - Grader på en skala fra 1-5 (lav-høy)
- Burde elevene bli informert om slike ting?
- Har du opplevd etiske dilemmaer knyttet til informasjonssikkerhet?
    - For eksempel å få informasjon som burde blitt rapportert, men som i så fall kunne skadet en persons integritet/verdighet/omdømme? Eller: Innsamlede data blir brukt i en annen sammenheng enn det som var hensikten, uten at 'offeret' har kjennskap til det?
- Har det forekommet uønskede hendelser der elever eller ansatte har fått skadet verdighet/omdømme pga for dårlige prosedyrer knyttet til informasjonssikkerhet?
    - Forklar. Eksempler

Administrative and managerial level (about managing and controlling operational tasks):

- Eksisterer det noen opplæring for elever, knyttet til informasjonssikkerhet?
    - Hvem? Bestemte grupper? Nye elever?
    - Hva slags opplæring? Obligatorisk?
    - Når? Regelmessig? Ved bestemte hendelser?
    - Hvem er ansvarlig for slik opplæring?
- Hvordan blir uønskede hendelser oppdaget av elever knyttet til informasjonssikkerhet rapportert?
    - Skrevne prosedyrer? Eksempler?
- Hard et forekommet uønskede hendelser der sensitiv eller konfidensiell informasjon har blitt stjålet eller kommet i gale hender ved feiltakelse?
    - Eksempler? Beskriv hendelsen(e). Konsekvenser. Personlige konsekvenser? For organisasjonen? For mulig 'offer'?
- Hvilke kommunikasjonskanaler brukes for å kommunisere med elever og foreldre?
    - Telefon. SMS. E-post. LMS. Sosiale medier
- Hvordan brukes sosiale medier I organisasjonen generelt?
    - Finnes det etiske retningslinjer for bruken? Er det tilgjengelig informasjon om sikkerhetstrusler gjennom sosiale medier? Skriftlig informasjon og retningslinjer?
    - Har alle elever tilgang til sosiale medier i skoletida? Hvilke (typer) sosiale

medier?

- Forestill deg at du har et budsjett som er øremerket informasjonssikkerhet. Hvor mange prosent vil du bruke på hvert av de følgende nivåene: Etisk, politisk/juridisk, administrativt, operativt, teknisk?

Operational level (about directly security execution) :

- Har du vært vitne til en eller flere uønskede hendelser relater til informasjonssikkerhet?
    - Forklar. Hva? Når? Hvordan? Konsekvenser?
- Har du selv forårsaket en eller flere uønskede hendelser relater til informasjonssikkerhet?
    - Forklar. Hva? Når? Hvordan? Konsekvenser?
- Personlig spørsmål: Skolen bruker ettnivå/enfaktor autentisering (brukernavn og password) for tilgang til alle sentrale systemer. Dette spørsmålet gjelder tilgang til skolens nettverk. Bruker du samme passord til en eller flere andre, eksterne tjenester?
    - Kjenner du til om andre gjør det? Er det vanlig blant elever?
    - Når byttet du sist passord?
- Kjenner du passordet til en annen elev? Evt flere?
    - Hvis ja, hvordan fikk du tak i det?
    - Vet du om andre elever innehar slik informasjon? Hvordan fikk de tak i det?
- Kjenner du passordet til en ansatt? Evt flere?
    - Hvis ja, hvordan fikk du tak i det?
    - Vet du om andre elever innehar slik informasjon? Hvordan fikk de tak i det?

Other:

Har du andre ting du ønsker å tilføye, som det ikke har blitt spurt om?

D.6 Intervju, IKT-konsulent ved fylkeskommunens administrasjon

Technical level:

- Beskriv teknisk infrastruktur
    - Oversikt. Detalj. Servere. Nettverk. Tråd/Trådløst. Hvilke komponenter er kritiske?
- Hvordan er kritiske komponenter sikret?
    - Fysisk? Logisk? Annet?
- Hvilke OS versjoner er i bruk?
    - Servere og arbeidsstasjoner? Nettbrett? Andre enheter? Skolens enheter vs private?
- Hvilke kritiske applikasjoner finnes I organisasjonen?
- Hvordan håndteres oppdateringer?
    - OS. Applikasjoner. Nettverksutstyr.

Ethical level (about what is seen as right and wrong in society):

- Er ansatte generelt bevisst sitt etiske ansvar, med tanke på å behandle sensitive persondata? Samt mulige konsekvenser for andre personers integritet/selvrespekt/verdighet?
    - Grader på en skala fra 1-5 (lav-høy)
    - Reflekteres dette i adferden deres?
- Hvor bevisst er *du selv* på ditt etiske ansvar, med tanke på å behandle sensitive persondata? Samt mulige konsekvenser for andre personers integritet/selvrespekt/verdighet?
    - Grader på en skala fra 1-5 (lav-høy)
- Vet ansatte generelt hvilken 'skjult' informasjon som blir samlet om dem og lagret? Hvor bevisste er ansatte omkring slike ting? Skjult betyr her systemlogger, nettverkslogger, informasjon om posisjon og lignende.
    - Grader på en skala fra 1-5 (lav-høy)
- Burde ansatte bli informert om slike ting?
- Vet elevene generelt hvilken 'skjult' informasjon som blir samlet om dem og lagret? Hvor bevisste er ansatte omkring slike ting? Skjult betyr her systemlogger, nettverkslogger, informasjon om posisjon og lignende.
    - Grader på en skala fra 1-5 (lav-høy)
- Burde elevene bli informert om slike ting?
- Har du opplevd etiske dilemmaer knyttet til informasjonssikkerhet?
    - For eksempel å få informasjon som burde blitt rapportert, men som i så fall kunne skadet en persons verdighet/omdømme? Eller: Innsamlede data blir brukt

i en annen sammenheng enn det som var hensikten, uten at 'offeret' har kjennskap til det?

- Har det forekommet uønskede hendelser der elever eller ansatte har fått skadet verdighet/omdømme pga for dårlige prosedyrer knyttet til informasjonssikkerhet?
    - Forklar. Eksempler

Political and legal level (about laws and regulation sin society and how they are implemented) :

- Hva er de viktigste juridiske aspektene du er nødt til å håndtere, med tanke på informasjonssikkerhet?
    - Personopplysningsloven. Taushetsplikt
- Foreligger det noen politiske føringer for å bruke sosiale medier i kommunikasjon med ikke-ansatte, for eksempel elever, foresatte eller eksterne aktører?
    - Omdømmebygging. Markedsføring

Administrative and managerial level (about managing and controlling operational tasks):

- Hvordan håndteres IT I din organisasjon?
    - Interne tjenester? Eksterne? Outsourcing? Annet?
- Hvordan er IT-tjenesten organisert ved skolen?
    - Nivå i organisasjonen. Antall ansatte
- Eksisterer det noen opplæring knyttet for ansatte, knyttet til informasjonssikkerhet?
    - Hvem? Bestemte grupper? Nyansatte? IKT-ansatte?
    - Hva slags opplæring? Obligatorisk?
    - Når? Regelmessig? Ved bestemte hendelser?
    - Hvem er ansvarlig for slik opplæring?
- Hvem I organisasjonen håndterer sensitive eller konfidensiell informasjon?
    - Grupper? Lærere? Rådgivere, PPT? Administrativt personell?
- Hvordan er sensitiv og konfidensiell informasjon sikret?
    - Fysisk? Bygninger eller avdelinger/seksjoner atskilt fra annen aktivitet?
    - Rutiner, for eksempel låsing av kontor når man ikke er tilstede?
    - Logisk? Autentisering? Passord? Tofaktorautentisering? Annet?
- Hvordan blir uønskede hendelser knyttet til informasjonssikkerhet rapportert?
    - Skrevne prosedyrer? Eksempler?
- Finnes det eksempler der organisasjonen har forbedret informasjonssikkerheten pga sikkerhethendelser?
    - Har man lært av tidligere hendelser?

- Hvem er ansvarlig for tilganger til sensitiv informasjon, samt at informasjonen er korrekt?
    - Opplysninger om elever og ansatte. Skrevne prosedyrer? Tilgangslogger?
- Hard et forekommet uønskede hendelser der sensitiv eller konfidensiell informasjon har blitt stjålet eller kommet i gale hender ved feiltakelse?
    - Eksempler? Beskriv hendelsen(e). Konsekvenser. Personlige konsekvenser? For organisasjonen? For mulig 'offer'?
- Hvilke kommunikasjonskanaler brukes for å kommunisere med elever og foreldre?
    - Telefon. SMS. E-post. LMS. Sosiale medier
- Hvordan brukes sosiale medier I organisasjonen generelt?
    - Finnes det etiske retningslinjer for bruken? Er det tilgjengelig informasjon om sikkerhetstrusler gjennom sosiale medier? Skriftlig informasjon og retningslinjer?
    - Har alle ansatte tilgang til sosiale medier på arbeid? Hvilke (typer) sosiale medier?
- Foretas det en risikoanalyse hvert år?
    - Hvis ikke, hvor ofte? På hvilket organisasjonsnivå? For skolen? For fylket som helhet?
- Forestill deg at du har et budsjett som er øremerket informasjonssikkerhet. Hvor mange prosent vil du bruke på hvert av de følgende nivåene: Etisk, politisk/juridisk, administrativt, operativt, teknisk?

Operational level (about directly security execution) :

- Hvilke prosedyrer eksisterer for å oppdage sikkerhetshendelser I dag?
    - Skrevne prosedyrer? Blir system- og sikkerhetslogger jevnlig sjekket?
    - Unormal aktivitet? Eksempler?
- Hvordan blir sikkerhetshendelser håndtert I dag?
    - Ulike typer hendelser. Reaksjoner, teknisk, personlige konsekvenser?
- Har du vært vitne til en eller flere uønskede hendelser relater til informasjonssikkerhet?
    - Forklar. Hva? Når? Hvordan? Konsekvenser?
- Har du selv forårsaket en eller flere uønskede hendelser relater til informasjonssikkerhet?
    - Forklar. Hva? Når? Hvordan? Konsekvenser?
- Personlig spørsmål: Skolen bruker ettnivå/enfaktor autentisering (brukernavn og password) for tilgang til alle sentrale systemer. Dette spørsmålet gjelder tilgang til skolens nettverk. Bruker du samme passord til en eller flere andre, eksterne tjenester?
    - Kjenner du til om andre gjør det?
    - Når byttet du sist passord?
- Kjenner du passordet til en eller flere andre brukere?

Other:

Har du andre ting du ønsker å tilføye, som det ikke har blitt spurt om?

D.7 Intervju, politiker

Ethical level (about what is seen as right and wrong in society):

- Er ansatte generelt bevisst sitt etiske ansvar, med tanke på å behandle sensitive persondata? Samt mulige konsekvenser for andre personers integritet/selvrespekt/verdighet?
    - Grader på en skala fra 1-5 (lav-høy)
    - Reflekteres dette i adferden deres?
- Hvor bevisst er *du selv* på ditt etiske ansvar, med tanke på å behandle sensitive persondata? Samt mulige konsekvenser for andre personers integritet/selvrespekt/verdighet?
    - Grader på en skala fra 1-5 (lav-høy)
- Vet ansatte generelt hvilken 'skjult' informasjon som blir samlet om dem og lagret? Hvor bevisste er ansatte omkring slike ting? Skjult betyr her systemlogger, nettverkslogger, informasjon om posisjon og lignende.
    - Grader på en skala fra 1-5 (lav-høy)
- Burde ansatte bli informert om slike ting?
- Vet elevene generelt hvilken 'skjult' informasjon som blir samlet om dem og lagret? Hvor bevisste er ansatte omkring slike ting? Skjult betyr her systemlogger, nettverkslogger, informasjon om posisjon og lignende.
    - Grader på en skala fra 1-5 (lav-høy)
- Burde elevene bli informert om slike ting?
- Har du opplevd etiske dilemmaer knyttet til informasjonssikkerhet?
    - For eksempel å få informasjon som burde blitt rapportert, men som i så fall kunne skadet en persons verdighet/omdømme? Eller: Innsamlede data blir brukt i en annen sammenheng enn det som var hensikten, uten at 'offeret' har kjennskap til det?
- Har det forekommet uønskede hendelser der elever eller ansatte har fått skadet integritet/verdighet/omdømme pga for dårlige prosedyrer knyttet til informasjonssikkerhet?
    - Forklar. Eksempler

Political and legal level (about laws and regulation sin society and how they are implemented) :

- Hva er de viktigste juridiske aspektene du er nødt til å håndtere, med tanke på informasjonssikkerhet?
    - Personopplysningsloven. Taushetsplikt
- Foreligger det noen politiske føringer for å bruke sosiale medier i kommunikasjon med ikke-ansatte, for eksempel elever, foresatte eller eksterne aktører?
    - Omdømmebygging. Markedsføring

Administrative and managerial level (about managing and controlling operational tasks):

- Eksisterer det noen opplæring knyttet for ansatte, knyttet til informasjonssikkerhet?
    - Hvem? Bestemte grupper? Nyansatte?
    - Hva slags opplæring? Obligatorisk?
    - Når? Regelmessig? Ved bestemte hendelser?
    - Hvem er ansvarlig for slik opplæring?
- Hvem I organisasjonen håndterer sensitive eller konfidensiell informasjon?
    - Grupper? Lærere? Rådgivere, PPT? Administrativt personell?
- Hvordan er sensitiv og konfidensiell informasjon sikret?
    - Fysisk? Bygninger eller avdelinger/seksjoner atskilt fra annen aktivitet?
    - Rutiner, for eksempel låsing av kontor når man ikke er tilstede?
    - Logisk? Autentisering? Passord? Tofaktorautentisering? Annet?
- Hvordan blir uønskede hendelser knyttet til informasjonssikkerhet rapportert?
    - Skrevne prosedyrer? Eksempler?
- Finnes det eksempler der organisasjonen har forbedret informasjonssikkerheten pga sikkerhethendelser?
    - Har man lært av tidligere hendelser?
- Hvem er ansvarlig for tilganger til sensitiv informasjon, samt at informasjonen er korrekt?
    - Opplysninger om elever og ansatte. Skrevne prosedyrer? Tilgangslogger?
- Hard et forekommet uønskede hendelser der sensitiv eller konfidensiell informasjon har blitt stjålet eller kommet i gale hender ved feiltakelse?
    - Eksempler? Beskriv hendelsen(e). Konsekvenser. Personlige konsekvenser? For organisasjonen? For mulig 'offer'?
- Hvilke kommunikasjonskanaler brukes for å kommunisere med elever og foreldre?
    - Telefon. SMS. E-post. LMS. Sosiale medier
- Hvordan brukes sosiale medier I organisasjonen generelt?
    - Finnes det etiske retningslinjer for bruken? Er det tilgjengelig informasjon om sikkerhetstrusler gjennom sosiale medier? Skriftlig informasjon og retningslinjer?
    - Har alle ansatte tilgang til sosiale medier på arbeid? Hvilke (typer) sosiale medier?
- Forestill deg at du har et budsjett som er øremerket informasjonssikkerhet. Hvor mange prosent vil du bruke på hvert av de følgende nivåene: Etisk, politisk/juridisk, administrativt, operativt, teknisk?

Operational level (about directly security execution) :

- Har du vært vitne til en eller flere uønskede hendelser relater til informasjonssikkerhet?
    - Forklar. Hva? Når? Hvordan? Konsekvenser?
- Har du selv forårsaket en eller flere uønskede hendelser relater til informasjonssikkerhet?
    - Forklar. Hva? Når? Hvordan? Konsekvenser?

- Personlig spørsmål: Skolen bruker ettnivå/enfaktor autentisering (brukernavn og password) for tilgang til alle sentrale systemer. Dette spørsmålet gjelder tilgang til skolens nettverk. Bruker du samme passord til en eller flere andre, eksterne tjenester?
    - Når byttet du sist passord?
- Kjenner du passordet til en eller flere brukere (ansatte eller elver)?
    - Kjenner du til om andre gjør det?

Other:

Har du andre ting du ønsker å tilføye, som det ikke har blitt spurt om?