Cyber security in the vocational education programme electrical engineering and computer technology

Marie Wilhelmsen

Thesis submitted for the degree of
Master in Information Security
60 credits

Department of Informatics
Faculty of Mathematics and Natural Sciences

UNIVERSITY OF OSLO

Spring 2022

Cyber security in the vocational education programme electrical engineering and computer technology

Marie Wilhelmsen

Cyber security in the vocational education programme electrical engineering and computer technology

http://www.duo.uio.no/

Printed: Reprosentralen, University of Oslo

Abstract

This thesis focuses on the vocational education programme electrical engineering and computer technology at the upper secondary school level. The aim is to investigate if the pupils attending said course has any need for cyber security competences. In addition, this thesis aims to investigate what solutions already exist for teaching youth cyber security. And lastly the thesis aims to determine what a possible solution could look like for the pupils of electical engineering and computer technology.

The study is based on interviews and literature reviews. The interviews provided good insight in whether or not there was a need for cyber security competences. Whilst the literature review was a good baseline for investigating existing cyber security solutions for training youth.

From the interviews performed with industry professionals, there was an indication that there was a need for cyber security competences in this educational programme. However, it cannot be clearly stated as there was not enough data, interviewees, to draw a strong conclusion. During these interviews several topics of cyber security were presented. Most notable was privacy, smart home technology, and internet of things (IoT). The main findings from the second goal of investigating existing cyber security programmes, was that there were no programmes that focused specifically on electrical engineering and computer technology, at least none that I could find. However, this goal was also used to determine effective methods for teaching cyber security, and the result here was that the most effective ways of teaching cyber security was in schools. Either through a course made for the pupils, or by teaching cyber security to teachers and allowing them to pass on the knowledge.

When determining what a possible cyber security solution could look like, there were the best method would be through a digital web application filled with interactive activities, theoretical and practical.

Acknowledgements

I would like to thank my supervisor Janne Merete Hagen for her patience, valuable input and motivational speeches.

Furthermore, I would like to thank everyone who participated in the interviews. Your input has been greatly appreciated throughout this study.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Over the past few decades, we have witnessed as most companies migrate their solutions to a digital platform. Today, everything from banking to purchasing food can be done online. This is a great movement for accessibility and usability, but it comes at a cost.

Cyber-attacks have become a daily topic for discussion, as we see an increased number of attacks due to the digital society we have made. According to NorSIS, [45], there has been an increase in incidents related to especially two types of cyber threats. The first increased threat is social engineering, where the threat agent uses fear, temptations and our trust in order to manipulate us. The second threat is ransomware, which has increased by several hundreds of percent. These types of attacks can have a massive impact on the companies that are affected. Worst-case-scenario the company can go bankrupt as a result of the attack [45].

Everyone is a potential target for these cyber-attacks. Companies, big and small, from hair salons to governments. In January of 2021 a threat actor got into the systems of Østre Toten municipality, where they deleted all backup files and encrypted all the data. None of the digital solutions were working due to this attack, and these were vital systems that were supposed to pay social help and provide medicine for the elderly [54]. With critical systems like these knocked out in one cyber attack it shows how vulnerable we are as a society due to the large amount of digital products and services.

Cyber criminals will always choose the easiest way to compromise a company, and this is often through the company's employees. According to a report made by the *Norwegian Business and Industry Security Council*, 50% of the security breaches in Norway are caused by *human error* [4]. Even though cyber criminals have become very sophisticated in their social engineering, I still believe this statistic could have been better.

That is where this thesis comes in. The aim of this thesis is to contribute to the knowledge gap of cyber security that exists in the general population. This will be done by focusing on a upper secondary vocational education programme that I believe should know cyber security - *electrical engineering and computer technology*, goes by the name of *elektro og datateknologi* in Norway.

1.1 Motivation

The motivation for focusing on this education programme is because the trades that the pupils can work in after finishing school are trades that are either directly affected by cyber-attacks or the nature of the work they do or the systems they interact with correlates with cyber security.

For instance, the pupils can become electricians, and many experiences electricians choose to start their own companies. If they do not know enough about for example, how to keep their systems safe, or how to process personal data they could be in serious trouble as they might face cyber-attacks or some serious fines. Worst-case-scenario a very profitable electrician company can go bankrupt within days if affected by a cyber-attack.

In addition, as we will be introduced to in chapter 2, trades in this education programme work with critical infrastructure, such as the power grid. They need to know cyber security to protect themselves and the work environment they are in.

1.2 Research Question

The first goal of this thesis is to figure out whether or not there is a need for competences in information security within the fields the pupils can choose. This can give a good indication of how important it will be to teach the pupils information security, at what level security should be taught and in what school year.

RQ1: What is the need for cyber security competences within the vocational education programme electrical engineering and computer technology?

Is there a need for cyber security competencies in the vocational education programme electronic engineering and computer technology?

To determine the best teaching methods for integrating information security it could be interesting to see how other countries have dealt with this issue. Perhaps there is something we can learn regarding the structure of this programme, the content, or what a solution like this can look like.

RQ2: What lessons learned can Norway benefit from other counties?

Can anything be learned from other countries information/cyber security programmes?

If we should determine that there is a need for information security competences in this educational programme and we have learned a thing or two about teaching security from other countries, we should have a look at what a Norwegian solution could look like.

RQ3: How can information security be integrated into the educational programme electrical engineering and computer technology?

Chapter 2

Background

Before diving into the research methods used to answer our research questions, we will be going through a brief description of the Norwegian school system, followed by a closer look at the education programme we will be focusing on in this thesis: *electrical engineering and computer technology*.

The goal of the chapter is to familiarise ourselves with the education programme, in order for the statements, research and conclusions made in the thesis, to make sense. We will have a look at the electrical engineering and computer technology's structure and career opportunities. In addition, we will do an initial analysis of which careers or trades can be of potential interest when it comes to cyber security.

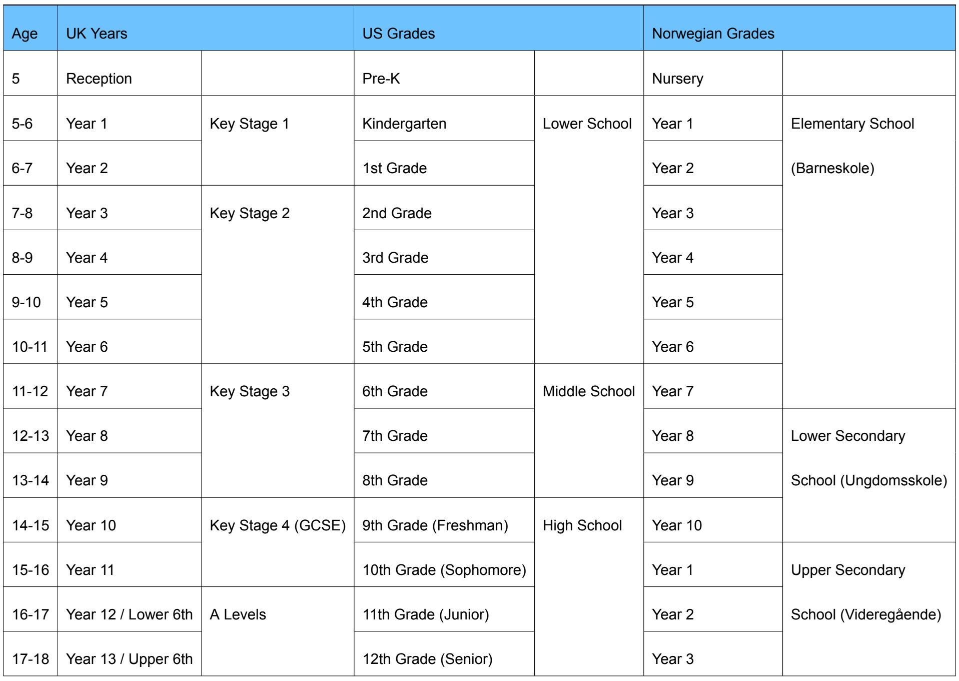
Before we delve into electrical engineering and computer technology though, we need to look at the Norwegian school system in order to understand what age group we are dealing with and where in their education the pupils are. This can help us understand what sort of previous knowledge the pupils should possess.

2.1 A brief description of the Norwegian school system

In Norway all children start school (Year 1) the year they turn six. The first ten years are mandatory, and upper secondary school (Year 11 to Year 12/13) is elective, but often needed to secure even the lowest paying jobs in Norway. In the first seven years the pupils will all be taught the same subjects. These include subjects such as Norwegian, English, Maths, Natural Sciences, and more. In Year 8 to Year 10 the pupils may choose an elective subject in addition to the standard subjects everyone is required to take. This elective subject can be picked from 16 different subjects, and this includes programming, democracy in practice, tourism, technology and design, and more.

From Year 8 to Year 10 the pupils work will be graded on a scale from one to six, where six is the highest grade and one is a failing grade. Most of these grades will be counted towards admission to Upper Secondary School (Year 11 to Year 12/13). Admission to Upper Secondary School is done purely on the grade-point-average calculated from the grades earned mostly in Year 10, but also some from Year 8 and Year 9.

To easier understand the composition of the Norwegian school system, I have created a visualisation which compares it to that of the American and English. This comparison can be seen in table 2.1.



Age	UK Years		US Grades		Norwegian Grades	
5	Reception		Pre-K		Nursery	
5-6	Year 1	Key Stage 1	Kindergarten	Lower School	Year 1	Elementary School (Barneskole)
6-7	Year 2		1st Grade		Year 2	
7-8	Year 3	Key Stage 2	2nd Grade		Year 3	
8-9	Year 4		3rd Grade		Year 4	
9-10	Year 5		4th Grade		Year 5	
10-11	Year 6		5th Grade		Year 6	
11-12	Year 7	Key Stage 3	6th Grade	Middle School	Year 7	
12-13	Year 8		7th Grade		Year 8	Lower Secondary School (Ungdomsskole)
13-14	Year 9		8th Grade		Year 9	
14-15	Year 10	Key Stage 4 (GCSE)	9th Grade (Freshman)	High School	Year 10	
15-16	Year 11		10th Grade (Sophomore)		Year 1	Upper Secondary School (Videregående)
16-17	Year 12 / Lower 6th	A Levels	11th Grade (Junior)		Year 2	
17-18	Year 13 / Upper 6th		12th Grade (Senior)		Year 3	

Table 2.1: A comparison between the school systems of England, The United States of America [57] and Norway. The ages stated in the first column are the starting ages of the pupils for the respective Years. For example, a pupil will be either five or six years when starting Year 1 in Norway [56].

When the pupils finish Year 10 and want to attend upper secondary school, they can choose from a range of different educational programmes. Some programmes focus on preparing the pupils for further study at the university (the programmes on the top row of figure 2.1), and other programmes are vocational in nature and will prepare the pupils for work life in a specific field (the remaining programmes in figure 2.1). For example, as we can see in figure2.1, pupils can choose to attend the vocational programme *building and construction*, and in doing so the pupils can become for example carpenters or any other profession within this programme.

As this thesis is only concerned with vocational education programmes, I will only be explaining the general structure of these types of programmes. The first year of any vocational programme will be the same for all pupils attending a particular programme, in Year 2 the pupils may choose between several different specialisations. An example of such a specialisation is Carpentry, in the programme building and construction programme, by choosing this specialisation the pupils can become carpenters. After Year 2 most pupils will go into an apprenticeship within their chosen specialisations. The apprenticeships are often two years long but depending on the specialisation they can be up to three years long. When the pupils complete their apprenticeships, they go through a test which if they pass, they will be granted a trade certificate as a skilled worker in their chosen trade.

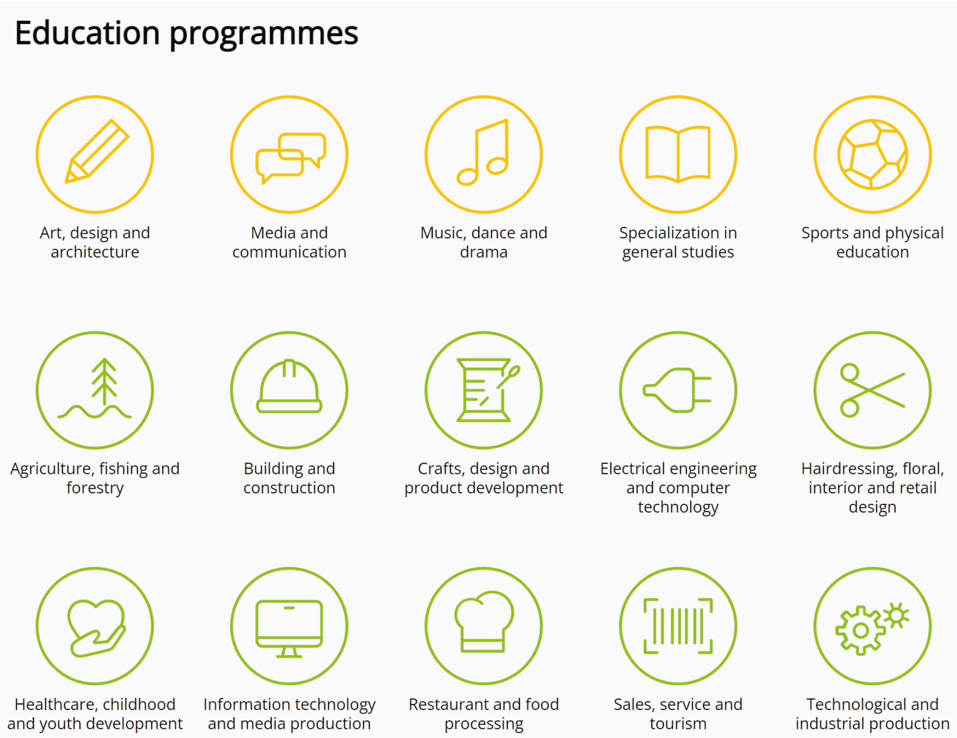

Education programmes
Art, design and architecture
Media and communication
Music, dance and drama
Specialization in general studies
Sports and physical education
Agriculture, fishing and forestry
Building and construction
Crafts, design and product development
Electrical engineering and computer technology
Hairdressing, floral, interior and retail design
Healthcare, childhood and youth development
Information technology and media production
Restaurant and food processing
Sales, service and tourism
Technological and industrial production

Figure 2.1: Illustration of the different educational programmes the pupils can choose from at an Upper Secondary school level in Norway. The top row of programmes represents the programmes that will prepare the pupils for further studies at university. The rest of the programmes are vocational programmes and will prepare the pupils for work life within a specific trade [69]

As aforementioned, in this thesis we will be focusing on the educational programme electrical engineering and computer technology. Before we take a deeper dive into the structure and possibilities of this programme let us recapitulate some of the general information gained from this subsection. From figure 2.1 we can see that this is a vocational programme. The majority of the pupils attending the programme will be in the age group 15-19, but there might be some older people attending the programme as there is no age limit. Hence, it is important to note that the solution we decide to create needs to reflect the maturity level of both groups. The pupils will be attending school for one to three years depending on the specialisation they pick. After initial training at school the pupils will enter work life as an apprentice, where they will be able to take a test which may grant them with a trade certificate in their chosen trade. The apprenticeships vary from one to three years.

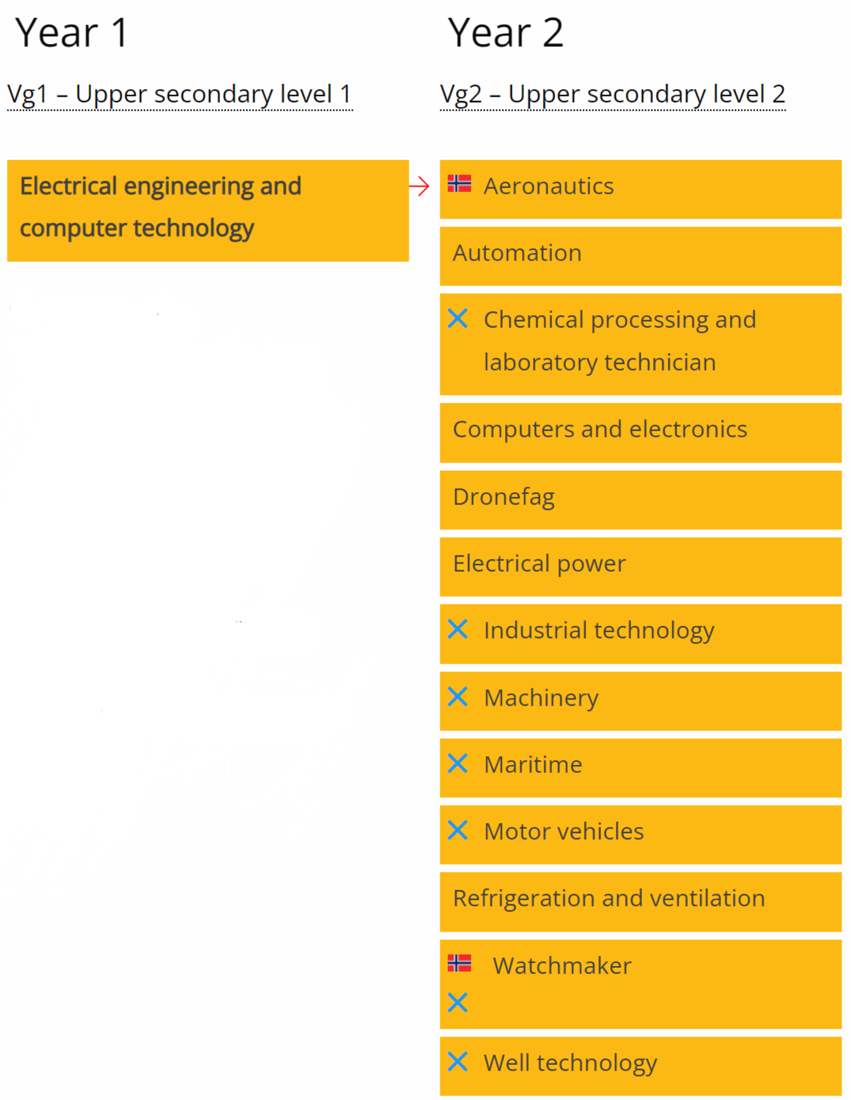
2.2 Electrical engineering and computer technology

2.2.1 Introduction

Now that we are familiar with the Norwegian school system and some general information about electrical engineering and computer technology, it is time to take a deeper dive into the structure, specialisation and the career opportunities that this programme has to offer.

Figure 2.2 portrays a rough overview of the first two years of this programme. In Year 1 all pupils will have the same subjects as each other. In Year 2 the pupils can choose between several different specialisations that all teach different subjects. In addition to subjects such as physical education and mathematics, the pupils will also have one to three subjects that are specific to the year or specialisation. For instance, in Year 1 the pupils will have a subject called *electronic circuitry and networks* which is a subject only taught in Year 1 electrical engineering and computer technology.

Note that the specialisations marked with a blue cross in figure 2.2 originally belong to a different educational programme, but the pupils may choose to swap to these programmes even with Year 1 as electrical engineering and computer technology. For instance, the Year 2 specialisation chemical processing and laboratory technician belongs to the technological and industrial production programme but may be elected as a first-year electrical engineering and computer technology pupil as they have similar knowledge to what is needed in this specialisation.



Year 1

Vg1 – Upper secondary level 1

Electrical engineering and computer technology

Year 2

Vg2 – Upper secondary level 2

- 🇳🇴 Aeronautics
- Automation
- ✕ Chemical processing and laboratory technician
- Computers and electronics
- Dronefag
- Electrical power
- ✕ Industrial technology
- ✕ Machinery
- ✕ Maritime
- ✕ Motor vehicles
- Refrigeration and ventilation
- 🇳🇴 ✕ Watchmaker
- ✕ Well technology

Figure 2.2: Illustration of Year 1 and Year 2 for a pupil attending Electrical engineering and computer technology [70].

Because the specialisations marked with a blue cross belongs to a different educational programme they will not be considered in this thesis. These specialisations should be considered when their respective educational programmes are under review, when it is time to create a cybersecurity training resource for these programmes.

In the following subsections we will have a closer look at each of the specialisation shown in figure 2.2, excluding the ones marked with a blue cross. When looking at the career opportunities that each specialisation presents, we will only have a closer look at the specialisations that I believe are most relevant in regard to cyber security. A specialisation is deemed interesting in regard to cyber security if there are any work-related tasks, interactions with systems or any interactions with customers and or colleges that require knowledge in cyber security. Work-related tasks can be the set-up of or maintenance of products which communicate using the internet. An example of a system could for example be a system locksmiths have to interact with, and this is the system that are used in access control. A system which holds the information regarding who is allowed where and when. We will have a more detailed look at these categories when we are looking at the specific specialisations.

With all this in mind, let us take a deeper dive into the following specialisations:

- Aeronautics
- Automation
- Computers and electronics
- Drones
- Electrical power
- Refrigeration and ventilation

2.2.2 Aeronautics

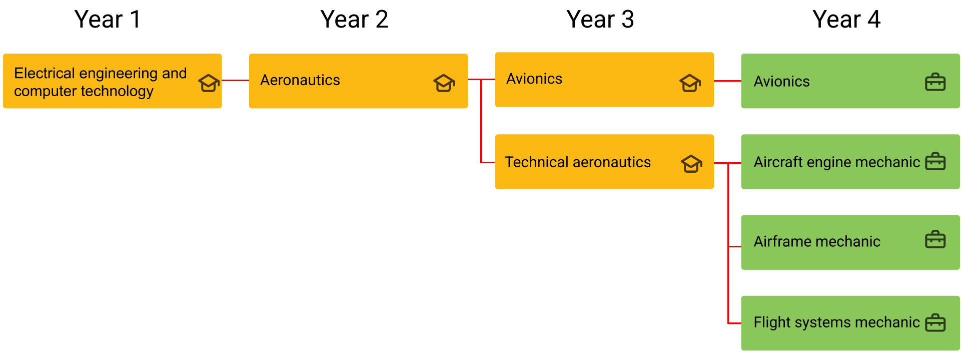


Figure 2.3: Illustration of the education path of the aeronautics specialisation. Note that this figure does not accurately represent the time spent as an apprentice [65].

In figure 2.3 we can see the full construction of the aeronautics specialisation. The yellow cards (with an academic cap icon on the right side) shows training in school, whilst the green cards (with an icon of a brief case to the right) shows the training in apprenticeships. Note that the length of the green cards is not entirely accurate, as the pupils will have to be an apprentice for more than one year before they can become certified. As mentioned previously, the length of an apprenticeship varies depending on the specialisation, but they can be two to three years.

By choosing aeronautics the pupils will be working closely with different electrical and electronic systems such as radars and navigation systems aboard an aircraft. In addition, they can work with mechanical systems such as propellers, stabilisers, winds and more [40–43]

According to a report reviewing current and future trends in the aviation industry, there has been an ongoing trend where we see increasing levels of integration of information and communication technology (ICT) equipment into mechanical devices used in the aviation industry. According to cyber.gov.au ICT equipment is described as “any device that can process, store or communicate electronic information (e.g., computers, multi-function devices, mobile phones, digital cameras, electronic storage media and other radio devices)” [2]. This is of concern to cyber security as the equipment is capable of communicating over the internet. And if this equipment is exposed on the internet as such, threat actors can find a way to take control of the devices if the devices are wrongly configured, contains vulnerabilities or if the device does not have any protection at all.

Considering the new trends with ICT equipment in the aviation industry I believe there will be need for cyber security training in this specialisation. This conclusion is derived from my initial thoughts and a research article found on the subject, further research will hence be needed to determine whether or not cyber security training will have to be created for this specialisation, and in which case what this training should entail. As for further research I would find it interesting to see if Norway has started introducing any of these ICT tools.

2.2.3 Automation

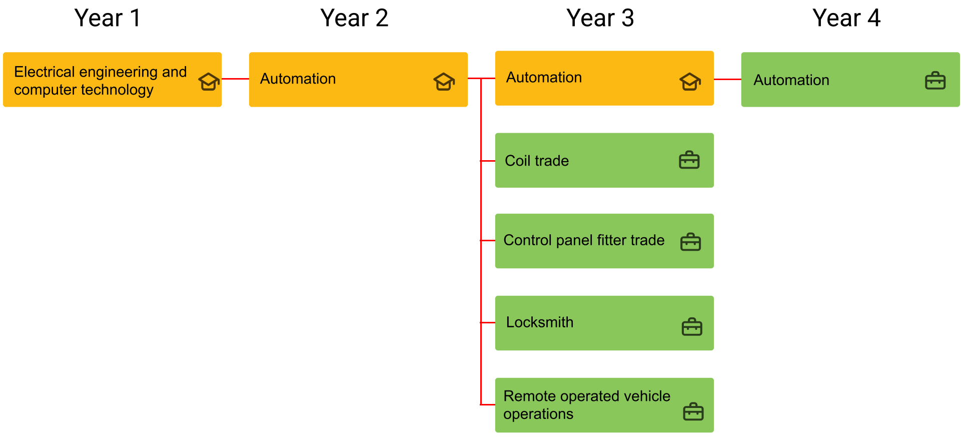

Year 1
Year 2
Year 3
Year 4
Electrical engineering and computer technology
Automation
Automation
Automation
Coil trade
Control panel fitter trade
Locksmith
Remote operated vehicle operations

Figure 2.4: Illustration of the education path of the automation specialisation. Note that this figure does not accurately represent the time spent as an apprentice [66]

As we can see in figure 2.4 the automation specialisation can lead to work in five different trades: coil trade, control panel fitter trade, locksmith, remote operated vehicle operations, and automation. These are all very different trades, which entail different work tasks and the pupils will be working with very different machinery and customers.

In regard to cyber security, the more interesting trades, in my opinion, are locksmithing and automation. The reason being the nature of the work and future development in the trades. A locksmith will have a close relationship with customers, whom can be private people or companies, and thus a locksmith will need some form of training in handling of personal data to ensure the safety of the customers data and the integrity of the locksmithing company. In addition, a locksmith can be working with important systems used for physical access control, which will need some cyber security training in order to operate in a safe fashion [21].

In the automation industry, the pupils will work with systems and devices in automated operations. The systems can be systems such as industrial control systems and regulation systems [20]. Industrial control systems are known for having vulnerabilities due their lack of built-in security controls and the fact that they are now being connected to external networks [52]. Another reason why this field might be interesting in regard to cyber security is because we are moving towards the fourth industrial revolution, industry 4.0. Industry 4.0 introduces high-tech IoT devices in processing making the factories smarter. These smart factories have advanced sensors, embedded software and robotics that are able to collect data and analyse it in order to make decision making better and faster [31]. The introduction of these smart products and smart machines which can potentially communicate via the internet into these automated processes, can introduce an increased risk of cyber-attacks which can halt the entire process. Halting an automated process can have severe consequences, especially if the factory in question is producing important medicine such as insulin. Thus, it can be important for an automation mechanic to know cyber security related to industry 4.0 production.

2.2.4 Computers and electronics

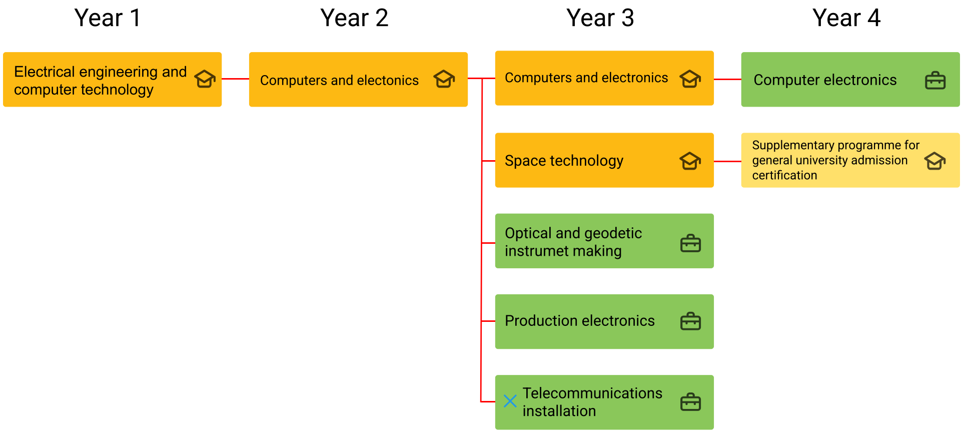

Year 1
Year 2
Year 3
Year 4
Electrical engineering and computer technology
Computers and electonics
Computers and electonics
Computer electronics
Space technology
Supplementary programme for general university admission certification
Optical and geodetic instrumet making
Production electronics
Telecommunications installation

Figure 2.5: Illustration of the education path of the automation specialisation. Note that this figure does not accurately represent the time spent as an apprentice [67]

Figure 2.5 portrays the educational path of the computers and electronics specialisation. Note that the telecommunications installation apprenticeship is marked with a blue cross, meaning one can choose to become an apprentice in this trade with the computers and electronics specialisation, but it actually belongs to a different specialisation: electrical power. Because of this, we will not be considering telecommunications installation until subsection 2.2.6.

I believe the most interesting trade in this specialisation would be computers and electronics. According to the Norwegian Directorate for Higher Education and Skills normal work assignments in this field includes maintaining information security, protect personal data and protect data and communication systems against hacking, harm, or any other form of misuse [22]. All these assignments are cyber security is all about, protecting information. The people working in this trade will more than likely need quite a lot of basic knowledge in cyber security, in addition to some deeper knowledge in network and communication security. Exactly what topics of cyber security they need to learn is yet to be determined.

The remaining trades might be of interest, but at first glance I cannot see anything particularly interesting with any of the fields. This is however yet to be determined.

2.2.5 Drones

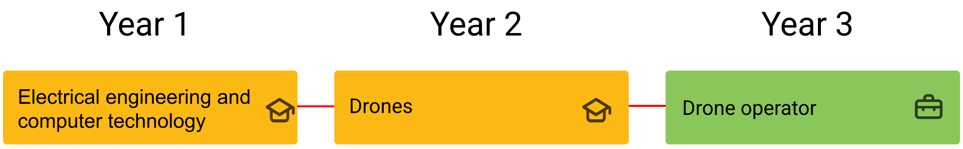


Figure 2.6: Illustration of the education path of the drones specialisation. Note that this figure does not accurately represent the time spent as an apprentice [68]

This specialisation is brand new and might see some changes in the near future, which might have an impact on the structure and content of the specialisation. Currently the pupils choosing this specialisation will be learning how to operate drones up to 25 kg, as well as learn how to maintain these drones [63]. Nothing in the current description of the specialisation indicates a need for cyber security training.

2.2.6 Electrical power

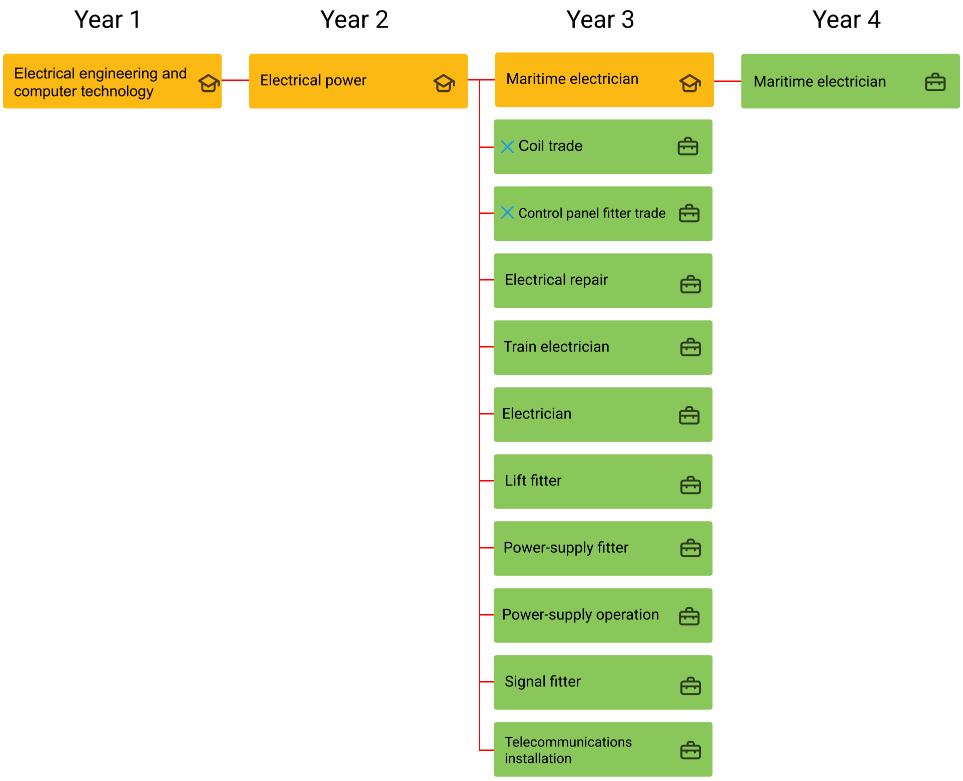


Figure 2.7: Illustration of the electrical power specialisation. Note that this figure does not accurately represent the time spent as an apprentice [71]

Electrical power is undoubtedly the specialisation with the most opportunities in terms of trades the pupils can choose from. Note that the two trades marked with a blue cross, coil trade and control panel fitter trade are already explained in subsection 2.2.3 Automation.

In the electrical power specialisation, I imagine the most interesting trades, in regard to cyber security, will be trades that work directly on the power grid, or trades working with communication networks, IoT systems and devices, and customers. Of the trades working directly on the power grid, we have the power-supply fitter trade and the power-supply operation trade. The reason why these trades should be looked at is because we are moving towards creating smarter grids. According to smartgrid.gov a smart grid is a power grid containing digital technology allowing for a two-way communication between the utilities and the customer. A smart grid consists of controls, computers, automation and other technologies working together with the power grid to respond digitally to our power needs [61].

The other trades I believe should be looked at are electricians and the telecommunication installation trade. In the past decade electricians have seen an increase in smart home products, devices and systems that are connected to the internet. These products can pose a risk to their users if they are wrongly configured, lack cyber security protection or are outdated. I believe it would be beneficial if the electricians knew more about the risks these products or systems pose in order to make a qualified decision whether or not to sell the products or recommend them. Electricians work with both private customers and companies, and the customers knowledge of the risks involved in introducing vulnerable products, systems or devices will vary immensely. The electrician should, therefore, be able to help make an informed decision and help their customers secure themselves properly.

A telecommunications installer can work with installation of and operation of local data networks such as LAN, WLAN and WIFI [24]. Exactly what this entails is unclear and should therefore be investigated further as anything to do with networks can introduce risks to cyber security. The remainder of the trades were not very interesting at first glance but should not be excluded from any further research. There might already have been introduced some interesting cyber security related systems, devices or products into these trades, which would qualify for extra training in cyber security. If not, there might be some future plans which are relevant to cyber security.

2.2.7 Refrigeration and ventilation

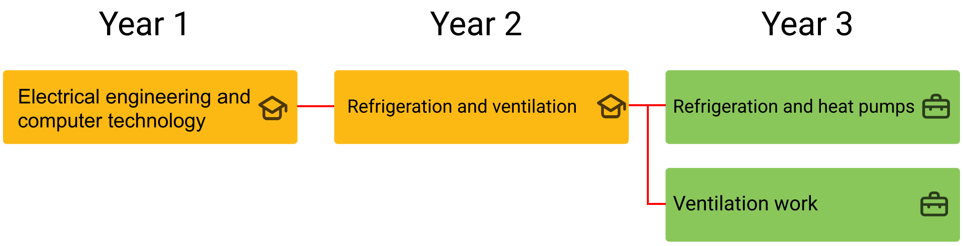

Year 1
Year 2
Year 3
Electrical engineering and computer technology
Refrigeration and ventilation
Refrigeration and heat pumps
Ventilation work

Figure 2.8: Illustration of the refrigeration and ventilation specialisation. Note that this figure does not accurately represent the time spent as an apprentice [72].

In the refrigeration and ventilation trade the pupils can work with ventilation systems, piping, automated control systems associated with refrigeration and heat pump systems, and more. Both these fields, refrigeration and heat pumps and ventilation work, might be interesting to have a closer look at as these systems are vital to many operations in our society. In these trades they do not only work on ventilation systems inside big office buildings, or some heat pumps private people have purchased, but they also work with ventilation in important research facilities where the number of airborne particles should be as low as possible, they can also work with refrigeration systems for data centres where huge amounts of data is stored, or cooling units for transporting goods such as important vaccines, and more [23, 25].

In newer times we are starting to see an influx in IoT devices being used to create smart ventilation and refrigeration systems. Where IoT solutions can help monitor the temperatures and air quality levels of a room or building. These solutions are connected to the cloud and can be controlled remotely [12, 35, 62]. If a threat actor manages to gain control of such systems, it can pose a great risk to our society. It could mean the destruction of information stored in data centres or it could be a risk to food safety if the temperature adjustments were severe enough.

I believe both trades could benefit from cyber security training in order to make informed decisions about the products they install, and they should be able to give good advice to customers about how to operate such products safely.

2.3 Reflections

At first glance, several of the trades we have looked at seem interesting in when cyber security is of concern. It is important to note that this chapter contains my initial thoughts on the matter. And whilst I decided not to investigate all the trades, I do believe all trades should be researched properly when creating a cyber security training platform. Due to the time restrictions of this study, this was not possible, but is highly recommended for future work on the subject.

Chapter 3

Research Method

The goal of this chapter is to familiarise ourselves with the different research methods used to answer the three research questions presented in the introduction. We will start by having a look at the research methods used for data collection and then we will have a look at the development method used to create a small demonstration of how a cyber security training platform can look like.

3.1 Data Collection

As previously described, in chapter 1.3, the research goals of this thesis are firstly to determine whether or not there is a need for cyber security competencies in the educational programme electrical engineering and computer technology. In addition, we are interested in having a look at how other countries have integrated solutions for training their youth in cyber security, perhaps our solution can benefit from theirs. Our last goal is to determine how cyber security can be integrated into our educational programme, what can such a solution look like and why.

Two different research methods were used to answer the three research questions of this thesis: semi-structured interview and literature research. The following subsections will describe these research methods, why they were applied, which research question they answered and what kind of limitations these methods had. As a recap, here is a list of the three research questions:

RQ1: Is there a need for cyber security competences within the vocational education programme *electrical engineering and computer technology*?

RQ2: What lessons learned can Norway benefit from other counties?

RQ3: How can information security be integrated into the educational programme *electrical engineering and computer technology*?

3.1.1 Semi-structured interview

The semi-structured interview

Semi-structured interviews are interviews where one does not follow a strict framework or schedule. Rather one has a loose set of questions, an interview guide, which is used as guidance for topics to talk about during the interview [5]. The interview itself should be a free-flowing conversation where the participants are encouraged to talk about their experiences and feelings. The questions should be open-ended inviting the participant to speak freely on the topics presented, and as the interviewer you need to be ready to ask follow-up questions if the participant presents and interesting new topic [53]. Semi-structured interviews can vary in length/time spent; they can last anything from 30 minutes to several hours. After the interview is conducted it is normal to transcribe it – that is write down everything that was said in the interview. The benefit of transcribing interviews is that you may come across something the participants said that you either forgot or did not pick up on, that is of importance to the study [79]

In this thesis, there was a total of five semi-structured interviews conducted. These five participants were asked to be interviewed because they all worked in a trade which was relevant to the educational programme in focus in this thesis. All participants were asked question from the same set of loosely defined questions, in addition to some extra questions formulated based on the trades of the participants. The interviews were supposed to last 30-45 minutes, but majority of them lasted over one hour. The participant's consent was collected on video, as the whole interview was recorded using Microsoft Teams built in recording feature. These recordings were stored on a secure server hosted by the University of Oslo, until the study's end when the recordings were deleted. In addition to collecting the consent on recorded video, the participants received a written consent in case they needed my contact information to withdraw themselves from the study. The consent form can be seen in appendix A and the interview guide in appendix B.

Only one interview was transcribed. Witnessing first-hand how long transcribing can take, I opted for a much easier and quicker summary style to gather information from the interviews. These summaries were about a page or two long and consisted of the information learned during the interview, the challenges the participants face in their daily work life, and the need for cyber security competencies within the trade of the participant. The reason I opted for a different approach than transcribing is because I did not need to know exactly what the participants said to form an opinion that could answer my research questions. And if I needed extra information on a specific topic discussed in the interview, I could simply listen to the recording again.

Research questions answered

The semi-structured interviews were used to answer our first research question, RQ1, and they were used to partly answer the last research question, RQ3. The goal of RQ1 was to determine whether or not there was a need for cyber security competencies in the educational programme electrical engineering and computer technology. I believed the best way to determine whether or not the pupils attending this educational programme needed to learn cyber security was to look to the industries and trades they would be working in. I wanted to learn how the professionals already working in these trades dealt with issues related to cyber security, and how the focus on cyber security had shifted over the years. However, my hypothesis before conducting these interviews was that the interview participants would have very limited knowledge, if any, in cyber security. The reasoning behind this hypothesis was because the Norwegian school system has previously required no cyber security training. So, I figured I could not only ask questions on this topic; I could not ask complicated questions about their infrastructure or policies in place to protect their data. Thus, I opted for asking questions about the participants daily work life, in hopes that I could derive a need for cyber security knowledge based on their work assignments, the systems they interact with daily and their general knowledge of simple terms in cyber security, such as data protection and data privacy.

The semi-structured interview was a good fit for answering RQ1 as it allowed me to have a free-flowing conversation with the participant on topics regarding what they did in their daily work life. It also allowed me to ask specific questions related to cyber security topics in order to comprehend the knowledge they already had in the field. And as I was not on a strict schedule or followed a specific questioning guide, I could ask as many follow up questions as I wanted. This turned out to be especially important when it came to cyber security topics, as some of them knew nothing about the questions asked, but others knew quite a lot – everything self-taught. All in all, the five people I spoke with were incredibly knowledgeable in their trade, and they seemed to enjoy sharing their experiences of their work life which was incredibly useful for this thesis.

The information I gained from conducting these interviews were used in part to answer RQ3. The goal of RQ3 was to figure out how we can integrate cyber security training in our educational programme electronic engineering and computer technology. From the interview participants I learned a great deal about their work and was able to derive quite a few cyber security topics which could be an integral part of the curriculum for this programme.

Even though conducting the interviews was a breeze, the semi-structured interview as a research method still came with its downsides. The most challenging part of this research method was by far the recruitment of participants. Even though the recruitment process started as early as August 2021 and ended in March of 2022, I was still only able to recruit five participants.

The participants were recruited through contacting companies either by phone or email. These companies were either found through googling the trade name or through job-recruitment websites. In total I was in contact with 26 different companies, a multitude of which I sent reminders to, to no avail. All participants that volunteered to be interviewed were recruited through calling the phone number belonging to their company, and the companies were all smaller ones. The size of the companies might have had an impact on how easy the participants were to recruit, because when contacting some of the bigger companies I had to contact either customer service or a press phone and the people answering these had no idea what I was talking about. For example, when contacting one of the big companies I was looking for a telecommunications installer, bear in mind that this company was heavily advertising this service, the customer service representative had never heard of this trade. I tried contacting this company on several other occasions, but the outcome was always the same. This happened with the majority of the trades I was trying to recruit people from, my theory as to why is because the companies I contacted, whom was either hiring or offering the services from these trades, only had small departments with few people with these specialisations. And thus, recruiting was difficult as my way in was through customer service or a press phone which normally dealt with issues related to the head office.

So, because I was only able to recruit five people from three different trades, we do not get the full picture of the cyber security competencies that pupils attending electrical engineering and computer technology should have. Although the data collected from these five participants well and truly shows that there is a need for competencies, it is still not enough to create a fully-fledged curriculum for every Year and specialisation for our educational programme, which was the original plan of the thesis. That being said, the information gathered from the participants that did volunteer to be interviewed was very valuable, but it was not enough data. A researcher is finished collecting data once data saturation is reached. Data saturation is reached when bringing in new participants to interview no longer introduce any new data to the study. Once the point of diminishing returns from the interview process is reached, one has to conduct several more interviews to make sure the dataset is indeed becoming redundant [37]. In the interviews conducted in this study, data saturation was reached in the interviews with the locksmiths by the time we came around to the second interview. So, in an ideal world a couple more interviews would be held with locksmiths in order to ensure a complete dataset.

Limitations

Even though conducting the interviews was a breeze, the semi-structured interview as a research method still came with its downsides. The most challenging part of this research method was by far the recruitment of participants. Even though the recruitment process started as early as August 2021 and ended in March of 2022, I was still only able to recruit five participants.

The participants were recruited through contacting companies either by phone or email. These companies were either found through googling the trade name or through job-recruitment websites. In total I was in contact with 26 different companies, a multitude of which I sent reminders to, to no avail. All participants that volunteered to be interviewed were recruited through calling the phone number belonging to their company, and the companies were all smaller ones. The size of the companies might have had an impact on how easy the participants were to recruit, because when contacting some of the bigger companies I had to contact either customer service or a press phone and the people answering these had no idea what I was talking about. For example, when contacting one of the big companies I was looking for a telecommunications installer, bear in mind that this company was heavily advertising this service, the customer service representative had never heard of this trade. I tried contacting this company on several other occasions, but the outcome was always the same. This happened with the majority of the trades I was trying to recruit people from, my theory as to why is because the companies I contacted, whom was either hiring or offering the services from these trades, only had small departments with few people with these specialisations. And thus, recruiting was difficult as my way in was through customer service or a press phone which normally dealt with issues related to the head office.

So, because I was only able to recruit five people from three different trades, we do not get the full picture of the cyber security competencies that pupils attending electrical engineering and computer technology should have. Although the data collected from these five participants well and truly shows that there is a need for competencies, it is still not enough to create a fully-fledged curriculum for every Year and specialisation for our educational programme, which was the original plan of the thesis. That being said, the information gathered from the participants that did volunteer to be interviewed was very valuable, but it was not enough data. A researcher is finished collecting data once data saturation is reached. Data saturation is reached when bringing in new participants to interview no longer introduce any new data to the study. Once the point of diminishing returns from the interview process is reached, one has to conduct several more interviews to make sure the dataset is indeed becoming redundant [37]. In the interviews conducted in this study, data saturation was reached in the interviews with the locksmiths by the time we came around to the second interview. So, in an ideal world a couple more interviews would be held with locksmiths in order to ensure a complete dataset.

Ethical considerations

When we are dealing with people in our studies there are always some ethical considerations to take into account. Firstly, the people who volunteer to be a part of the study need to be informed of their rights when it comes to the handling of their personal data. Secondly, they need to provide their consent to this data handling, so that the data they provide can be used.

To ensure the participants personal data was collected, processed, stored and shared in a safe and legal manner, I sent an application containing this information to the Norwegian Centre for Research Data (NSD). NSD is an organisation that gives advice on data management and data protection in research and sending such an application is often a required process of research in Norway, as it ensures correct handling of personal data. In addition to information such as encryption of data and the length of the study, I also sent an interview guide and the consent form given to interview participants. After a bit of backwards and forwards, this application was accepted in the end, and I had a guideline as to how I would collect, process, store and share data in a safe and legal manner.

For data collection, Microsoft Teams was used to conduct interviews. These interviews were recorded, and the recordings were stored encrypted on a cloud server hosted by the University of Oslo (UiO). I was the only one with access to these recordings. When processing the data and addressing the interview participants in later parts of the study, no real names were used, only pseudonyms that would protect their identity. Their names and the recording never left the cloud server until the end of the study when they were safely deleted.

3.1.2 Literature review

Literature reviews were used throughout this entire thesis. In the very start the literature review was used to gain an overview of the information that already existed on the topic. As it turns out I was not able to find a single study that focus on cyber security training in vocational education programmes at Upper Secondary school. And there was certainly nothing in regard to all the different specialisations one can choose when attending our educational programme electrical engineering and computer technology. However, there was one research paper which addressed the cyber security challenges in the aviation industry, which could be used when assessing the aeronautics specialisation. Other than this report, I had to specifically search for cyber security related topics in specific objects, products or processes related to the different specialisations and trades of the educational programme. These cyber security related topics where for instance internet of things, which is known in the cyber security industry for being vulnerable products and devices which are connected to the internet allowing them to receive and send messages [34]. Other noteworthy cyber security related topics used as search words include threat analysis, risk assessment and vulnerability. In addition, I also opted for just searching for "cyber security in xxxx" where xxxx was swapped out with either the trade or products, processed or devices found in the trade.

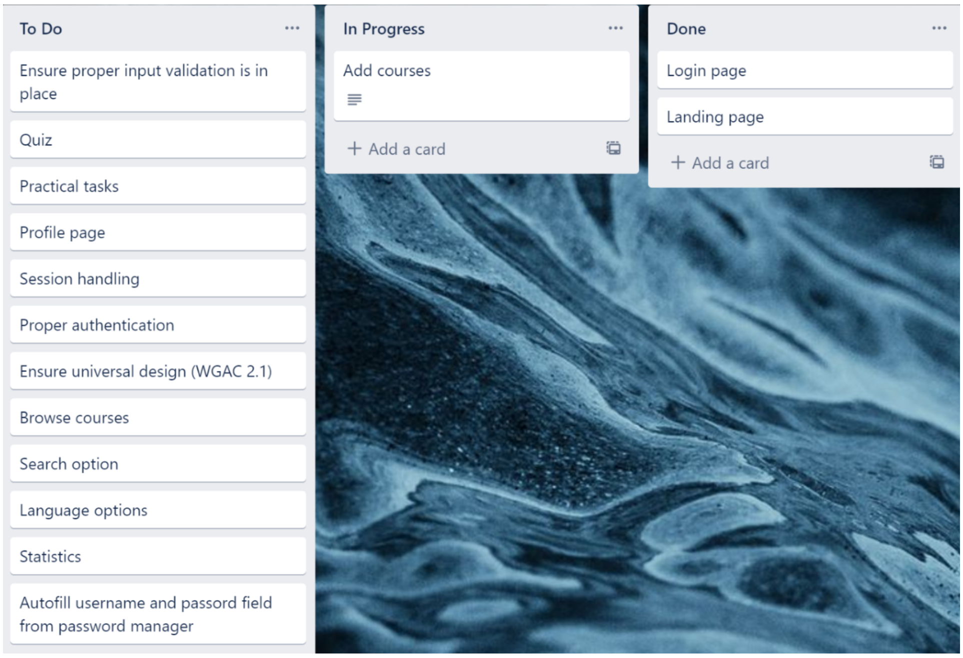
In the end I found quite a few sources of interest, which were all research reports and research papers. The search engines used to procure these specific reports and papers were Google Scholar and Oria. In addition to using search engines, I also went directly to websites of interest. These websites belonged to The Norwegian Water Resources and Energy Directorate (NVE), The Norwegian National Security Authority (NSM), The Norwegian Center for Information Security (NorSIS) and The Norwegian Defence Research Establishment (FFI).

The research reports and papers were used when collecting data for the introduction of this thesis, the research methods chapter we are currently in, and to answer both RQ2 and RQ3. The goal of RQ2 was to see if Norway could benefit from any of the cyber security programmes created for youth in other countries. The reports used to answer this question was evaluations of the different cyber security programmes. These also helped determine the way to integrate cyber security training in our educational programme, answering the last research question, RQ3. Reports and papers regarding cyber security in specific specialisations in our educational programme was also used to answer RQ3.

In addition to research reports and papers, new articles and websites were also used. The websites very especially helpful when answering RQ2, as I could go directly into the other countries cyber security programmes website and learn how these programmes were structured, and what parts the programmes consisted of. Websites were also used to explain certain terms throughout this thesis. When using the new articles, I made sure to use trustworthy news organisations such as nrk.no.

3.2 Development method

An application demonstrating a way to integrate cyber security training in our educational programme was developed during the course of this study. And as research needs methods to control the madness, so does development. The development method chosen for the development of this application was Kanban. Kanban is a framework which does not work on increments, such as sprints in the development framework Scrum, rather one focuses on the tasks at hand without considering a deadline. In Kanban, all work is centred around the Kanban boards. There is one Kanban board per project, and it consists of the columns To Do, In Progress and Done, indicating which stage the task placed in each column is in [50]. The reason behind the choice of Kanban was because I was very unsure how long each task would take, as I was completely new to the world of frontend development. And as suspected each task took much longer than first anticipated. I restricted myself to one task as work-in-progress as to not have too many balls in the air. An example of how the Kanban board looked at one point can be seen in figure 3.1.



To Do

- Ensure proper input validation is in place
- Quiz
- Practical tasks
- Profile page
- Session handling
- Proper authentication
- Ensure universal design (WGAC 2.1)
- Browse courses
- Search option
- Language options
- Statistics
- Autofill username and passord field from password manager

In Progress

- Add courses

Done

- Login page
- Landing page

Figure 3.1: Illustration of how the Kanban board looked at a point in this study. The online tool Trello was used to visualise the board.

Chapter 4

Need for competence

The purpose of this chapter is to explain how the first research question, RQ1, was answered. As a recap, the goal of RQ1 was to determine whether or not there was a need for cyber security competence in our education programme electrical engineering and computer technology.

To answer this research question, I saw three possible strategies. The first strategy was to derive the cyber security competence needed from what is called competence goals of the programme specific subjects in electrical engineering and computer technology. For clearance, competence goals are goals that portray what knowledge the pupils should have after completing the subject. The second strategy was deriving cyber security competence from the curriculum of the programme specific subjects, this includes textbooks and other teaching materials. The third strategy would be to talk to industry professionals with a trade certificate, in order to understand what the work the pupils will do in the future entails and based on that derive the cyber security needed to create a safe work environment in the different trades.

I suspected the most difficult, yet rewarding, strategy would be strategy three. With strategy three we could get some insights into what the industry professionals work entail. From the systems, devices, products and assignments that are interacted with and done in their everyday work life, we could derive what cyber security competences are needed to keep themselves and their company safe. This information would be found through interviews with these industry professionals. Now the difficult part of this strategy would be to find the right people to interview. Exactly how difficult this turned out to be, can be read all about in subsection 3.1.1.3 limitations. Because of the suspected difficulty of strategy three, I decided to see what kind of information strategies one and two would yield before committing to strategy three.

The only issue with relying on strategy one and two was that the Norwegian school system has never focused on cyber security, until recently. Luckily for us the Norwegian government introduced a national strategy for digital security expertise in 2019. This report included a section dedicated to the vocational education programmes in upper secondary school, programmes such as the one this thesis focuses on. The objective introduced in this strategy was that “digital security should be included in relevant vocational education programmes to a sufficient degree” and that The Directorate of Education would work through the curriculum of these vocational programmes in order to assess which programmes it would be relevant to incorporate cyber security into [59]. This meant that, in theory, the competence goals and the curriculum should have been updated to include cyber security by the time this thesis is being worked on which is between 2021 to 2022.

The competence goals could help with two things. Firstly, to see if the coverage of cyber security was already at a satisfactory level. This would mean that the work being done in this thesis would be useless, as the work is already done. Secondly, the competence goals could help give us an indicator of what topics in cyber security that other people have deemed important for the pupils attending this education programme to learn. Before we have a look at the official competence goals, bear in mind that when going through the different specialisations in Year 2 and Year 3 in chapter 2 Background, I found that of 11 specialisations (excluding space technology) 9 of then were interesting candidates for extra cyber security training.

Competence goals are connected to a specific subject, so when going through the competence goals of the different specialisations, and the base specialisation in Year 1, I was looking at the programme specific subjects. The Year 3 specialisation space technology did not have any competence goals in its subject, space technology, meaning the space technology specialisation was excluded from my search. With that in mind, I found a total of 31 subjects, which had a total of 330 competence goals. Of these 330 competence goals, only 8 were related to cyber security. There was one goal in the base specialisation in Year 1, three in Year 2 computers and electronics, one in Year 3 computers and electronics, two in Year 2 electrical power and the last one was found in Year 3 maritime electrician. A translation of the goals can be found in the list below.

- Perform risk assessment and carry out work in accordance with routines for electrical and ICT safety and health, environment and safety. (Year 1) [75]

- Manage users, access and rights in computer and information technology systems according to defined needs and describe routines for hardware and software updates. (Year 2 computers and electronics) [74]

- Configure and deploy physical and virtually segmented networks in accordance to the defined needs and requests, describe security routines and routines to maintain the operation of a network (Year 2 computers and electronics) [74]

- Describe routines and methods for secure data deletion to prevent personal information or other sensitive data from getting lost (Year 2 computers and electronics) [74]

- Install, configure and put into operation, information and communication systems with different operating systems, manage users, access and rights in accordance with defined needs and automate operational tasks and assess measures to ensure personal and communication security. (Year 3 computers and electronics) [73]

- Handle waste according to your own work in a professional, environmentally friendly and economical way, safeguard privacy and delete sensitive data when disposing of digital equipment (Year 2 electrical power) [76]

- Install and configure wired and wireless control systems with sensors for controlling equipment in electrical installations and consider measures to ensure privacy and data security (Year 2 electrical power) [76]

- Install and configure networked radio-based and wired equipment for custom and energy-efficient installations and assess whether data security and privacy are maintained (Year 3 maritime electrician) [77]

Competence goals tend to be quite general, in order to cover the whole curriculum in a few points. These security goals are no different. The competence goal for Year 1 is in fact so general that it would be very difficult to derive the exact topics of cyber security that needs to be followed in order to “perform the work in compliance with ICT-security”. What work are they referring to here? And what does it mean to perform the work in compliance with ICT-security? The cyber security needed very much depends on the work being done and the systems, devices and products the worker works with.

A fair few of the goals talk about routines and security routines in relation to ICT-security, updating software, upkeep of computer networks, and deletion of data. There is no explanation for what is meant with these so called “routines” and “security routines”. Personally, I have not heard of any official routines for any of the above-mentioned assignments. So, what kind of routines are referred to here? Are the people writing the textbooks and creating the curriculum supposed to create their own routines?

I was not able to derive much from these competence goals, other than the fact that privacy seems to be of importance and that the specialisation maritime electrician is of interest, which I did not initially find very interesting in chapter 2 Background. That privacy is of importance is not ground-breaking news, as we are working with quite a lot of trades that deal with personal data in some form through customer service or through the systems they set up and deal with. And as we know, breaking the law when it comes to personal data and privacy can be very expensive, and could in worst-case-scenario cause the company to go bankrupt. That a maritime electrician is of interest however, that is something we need to look more into. It would make sense as the sole electrician, or at least one of few, aboard a vessel that you would be in charge of the devices connected to a network and the digital infrastructure as a whole.

As suspected, only looking at the competence goals are not enough to derive the cyber security needed across all specialisations in our education programme. They are simply too vague, and I believe there are more than five specialisations that need cyber security training. Without further ado, let us look at what information strategy two can give us about the cyber security competences needed.

As a reminder, strategy two was looking at the curriculum of the specialised subjects. This included teaching materials such as for example textbooks. This strategy turned out to be a lot more challenging to follow than I initially thought. My thought was to start by having a look at the textbooks created for each specialised subject for all the years. Finding the textbooks though, was a challenging task. Firstly, the textbooks were not readily available, meaning that getting a hold of one either physically or digitally was difficult. Secondly, I was not able to find an official website or document that stated what exact textbook was currently in use for each of the subjects, so I had to guess. I found a website brettboka.no, which contained a quite a few textbooks for some of the specialisations, but not all. Some of these textbooks where for the same subject, just older versions. There was another issue with the website, and that was that the content was locked behind a paywall. But, through a campaign code I was able to acquire one of the books for a period of two weeks. The book I acquired was the newest textbook for the Year 1 subject electronic circuits and networks. This book was released in 2021 which means it may or may not have taken into account the national strategy when it was written, and the competence goal may or may not have existed when the book was written. However, the textbook did, to my surprise, contain a subsection called "computer security".

This subsection was one and a half pages long, and contained content such as security challenges companies face, "securing different" networks, recommendations for use of IT devices, and lastly computer security for when you are travelling. In the section about security challenges companies face, we find issues such as workers using the company computers for personal use, and statements such as that there is a need for knowledge of how to process large amounts of data, the company's system has to be set-up its IT-system in a way that a fault on a central unit will not cause the company's IT-system to go down, and "the need for cyber security knowledge has increased radically the past few years, and in 2018 EU brought out the privacy regulation GDPR (General Data Protection Regulation)". I agree with the issue that workers should not use their companies' computers for private use, as this could introduce some risks to the company's security. The worker could for example accidentally download a ransomware virus which can encrypt all the company's equipment [64].

In the section about securing different networks, they talk about routers provided by your network provider, how these routers come with the necessary security settings, and how you should use the network providers guidelines when choosing a secure password. They also talk about friends coming over and that anyone who knows your router password can, with some competence, connect to your pc, if it is not secured. Correct me if I am wrong, but that has nothing to do with securing different networks. Throughout the rest of the chapter things like not storing sensitive data on your pc, do not get fooled by scammers, use a personal firewall, create passwords with at least 8 characters, multi-factor authentication and more. Nothing is explained in a satisfactory detail.

But is there anything to be learned from this chapter? No, not in my opinion. Some of the issues brought up in the chapter is indeed relevant, but the way it is explained is not good enough. It is clearly written by someone who does not know much about cyber security. But that does not mean we should blame the authors. They were given an impossible task of interpreting the Year 1 competence goal, which as we have discussed previously made it very difficult to derive the cyber security that needs to be taught in this subject. In addition, writing about cyber security when you are not yourself properly acquainted with the field is near impossible. There is clearly a need for someone with cyber security competence to create the cyber security teaching material.

In the end I was not able to look at any other textbooks. The same fate befell the other teaching materials I tried to get a hold of, such as the Year 2 and 3 automation courses on the digital platform Norsk Industri [32].

Strategy three was to interview industry professionals with trade certificates to see if we could derive some cyber security topics from their everyday work life and the challenges they face in their daily lives. The details about the interview process can be found in chapter 3 Research methods. I ended up interviewing five participants: two electricians, two locksmiths, and a lift fitter. The interview process was explained in chapter 3.

From the lift fitter I learned that lifts themselves are still pretty primitive. New lift models are still introduced, but not many of these are connected to the internet or have smart devices in them. The lifts that are connected to the internet can be used to warn the lift fitter company about faults that occur, or they can be used to display the weather which is contained in its own module. An interesting thing that was brought up is that even tough the lifts are primitive, many of them still come with a login system, which can be used to for example troubleshoot the lift. These login systems are usually protected with a four digit pin or a default password. The lift fitter also mentioned the fact that they can work with quite a few high security clients. The interesting thing he brought up here was the fact that when the lift fitters have finished a service job on a lift they have to take a picture of said life. With a high security client, one should be careful with what is posted online, and posting a picture of a lift that reveals classified information could be bad news.

When interviewing the electricians, there were several interesting points raised. Firstly, the electricians work closely with both private customers and larger company's. And secondly, they work with all kinds of IoT devices and smart products. One of the electricians mentioned that it would be a good idea to learn more about the security of things such as smart home products, as they did not know of any of the security vulnerabilities, a part from the fact that one of their products had a default password. The issue with default passwords is that people forget to change them. The same thing happens at this electricians work where even the people coming to programme the smart home system, forgets to change the default password. Having insecure smart home products exposed to the internet like this, it could result in people tampering with your products. An example the electrician gave during the interview was that if you had a insecure product like that one of your neighbours could connect to it and control, for example your lights.

In the interview with the locksmiths, I learned about how they set-up and control the access in a physical access control system. I learned how they are, sometimes, the manager of the access control system. This system logs all the activity when someone is using their card, in addition to storing information about who has access to what. They protected the system by having it run on a PC that was used for nothing else, in addition to the PC running on its own network.

I was also introduced to smart home locks, the locks that you can install in your home, that opens codes, cards or tokens. All these access control systems worked on cryptography. There was a cryptographic algorithms that made it possible for the card and tokens to authenticate with the door. The locksmiths did not know any details surrounding the cryptographic algorithms that were used, but they knew the different products came with varying levels of security due to prices. The cheaper products had worse security than the expensive.

Based on these five interviews, I managed to derive a few topics of cyber security that would be relevant for these people to learn. First of all, all these trades could do with learning more about privacy. All three trades are what we call *service* trades, meaning they provide a service to their customers. Which means they will at some point be handling personal data, and thus they should do so in accordance with law.

Another few topics that could be useful to learn more about are the *smart home, internet of things and industrial internet of things*. It seems IoT products have come to say, and as the people who install most of these products they should learn what kind of vulnerabilities some of the products have. They should be able to recommend products that are safe to install.

Another topic is cryptography. I believe the locksmiths could benefit from learning *basic cryptography*, as they could give better recommendations as to which product you should go for, with different arguments than price.

A topic that is not necessarily directly derived from the interviews, but I still think should be a part of the curriculum, is *virus theory*. As we saw in chapter 1, ransomware attacks are growing in number. What should be learned in this topic is how to avoid getting viruses. This could mean learning topics such as *how does one get a virus*, *how do viruses spread* and what can of mitigations one can do to keep themselves and their company safe from viruses.

The last topic that was derived from the interviews was *password safety, social media and internet hygiene*. Although the electricians cannot do anything in regard to the default password on the smart home products, they should still know how to secure themselves with a good password. Tough, I do believe this theory should be introduced at a much earlier stage than upper secondary, it can still be recapitulated.

When it comes to social media and internet hygiene they should know what is OK to share and what is not. Like with the lift fitter, other trades might have to deal with high security customers. When this is the case, you should not post a picture online stating what client you are working with. Nor should you post pictures of classified places. They should also learn what is OK to do and what is not when it comes to browsing the internet on a work device versus a home device.

As we have seen there is indeed a need for cyber security training for all three of the trades, in order for them to perform their jobs as safely as possible and in order for them to be able to give good recommendations on security products such as the different level of access control.

Chapter 5

Existing programmes

The purpose of this chapter is to explain how the second research question, RQ2, was answered. The goal of RQ2 was to explore how other countries have elected to teach their youth cyber security, and whether or not we can learn something from the methods these countries have used.

In my research I found two cyber security training programmes which looked interesting, GenCyber and CyberFirst, which are programmes from The United States of America and The United Kingdom respectively. The hope was that these two programmes would help us when choosing how cyber security training should be integrated into the teaching programmes in Norway. Let us start by having a look at the American programme first, GenCyber.

5.1 GenCyber

5.1.1 Background and motivation

The *Gencyber programme* was created by the National Security Agency (NSA) as an initiative to solve the shortfall of skilled cyber security experts in the United States of America [29]. The programme strives to accomplish three goals; increase the interest and diversity in the US cyber security workforce, teach the participants correct and safe online behaviour and lastly to improve the teaching methods of cyber security in the K-12 curricula [18]. K-12 curricula refers to the subjects taught from kindergarten (4-7-year-olds) all the way through twelfth grade (17-18-year-olds).

GenCyber was inspired and modelled after a very successful *summer camp programme* by the name STARTALK, which has since 2007 increased the interest and educated students in less common languages such as

Chinese, Arabic, Russian, and so on [28]. GenCyber had its trial run in 2014 with eight different prototype camps. Since then, the programme has grown massively and was already, after just six years, offering 154 camps in 44 different states, plus the District of Columbia and Puerto Rico. The people behind GenCyber are currently working on providing camps in all 50 states [28].

5.1.2 Programme structure

The camps are hosted by different universities and colleges across the country. They are often given in the form of summer camps or some other out-of-school time activity. Each camp lasts for at least five days or at least 30 hours of activities and may contain a varied lesson plan based on what the universities or colleges want to teach [28]. The lesson plan is proposed by the institution and sent to GenCyber for approval. If the proposal is accepted, the institution will get a grant to cover the cost of hosting the camps, so that the camps themselves can come free of charge to all participants.

To join a camp, the participants apply to the specific institutions via their website, these websites are listed on the GenCyber website. Because the camps are free of charge there are some restrictions on how many participants the different institutions can host at one time, and thus the participants must fill out a form with information about themselves and the motivation for joining the camp and go through a selection process. Exactly what makes a person qualified to join a camp is not specified, but the GenCyber goals suggest the institutions try to achieve a diverse group of people.

The camps are offered for students at middle school and high school level, as well as for teachers at the K-12 level (teachers at kindergarten level all the way through twelfth grade). One of the three main goals of the GenCyber programme was to improve teaching methods for delivering cyber security content in K-12 curricula, this is tackled by providing the camps for the teachers. The camps provided for the teachers offers the teachers money in return for participating, and the goal is to inspire the teachers to include topics of cyber security in their curriculum and teach it to their pupils. This way the pupils can be introduced to cyber security at an early age, preparing them to behave safely online, learn different topics of cyber security and perhaps get to know their career opportunities within the cyber security field [29]. The goal of the student camps is to increase the awareness of cyber security and inspire the pupils to choose a career within the field of cyber security.

As mentioned previously, the topics presented at these camps differ between the institutions. Some camps focus on a deeper understanding in topics such as online safety, ethical hacking, and other topics [51], whereas other camps offer quite a broad lesson plan with focus on a general understanding of different cyber security topics [60]. Some camps focus on the idea of diversifying the cyber security workforce by offering camps for specific parts of the population, such as girls only camps [15], or camps designs for pupils who are deaf or hard of hearing [58].

5.1.3 Programme evaluation

The GenCyber programme is currently running in its ninth year. The first year, 2014, was the trial run of GenCyber, testing whether or not this programme could be a successful endeavour and could help the US reach its goal of growing their cyber security workforce, diversifying it, increase awareness of cyber security in the general population and improve the teaching of cyber security in the K-12 curricula. 2014 proved to be a very successful proof-of-concept year, and the GenCyber programme grew rapidly in 2015. In its trial run, there was only eight camps hosted at six different universities, in 2015 this number increased to 43 camps hosted by 29 universities [36].

In 2015 there was 240 teachers and around 1300 pupils attending the camps. Of the 240 teachers, 55% were females and 30% were from underrepresented minorities. Of the pupils attending the camps, 50% were females and 50% were from underrepresented minorities. So, the programme did an excellent job reaching a diverse group of teachers and pupils. The camps also succeeded in generating an interest in cyber security among its participants. In figure 5.1 we see the data collected from 90.4% of the teachers and 86.2% of the pupils who attended the GenCyber camps in 2015. Of the teachers we see that majority of them found cyber security to be an interesting subject, and the majority intended to teach cyber security to their own pupils after the camps. In the pupils' responses we see that most of them as cyber security to be an interesting subject as well. The fourth column in figure 5.1 is the pupils' intent to pursue cyber security as a career before the camp, and the last column shows the response to this question after the camp. We can see that there was quite a large increase in the pupils' intent to pursue cyber security as a career, which is exactly what the GenCyber camps were trying to achieve [36].

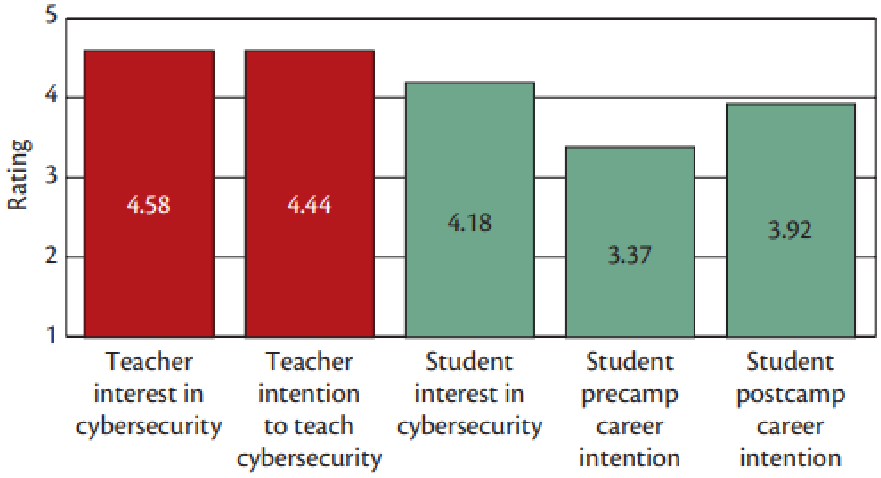


Figure 5.1: Teacher and student interest in cybersecurity after 2015 GenCyber camp participation. Average scores portrayed (1 = strongly disagree, 5 = strongly agree) [36]

GenCyber was also successful in the reaching the second goal of achieving cyber security awareness. Both teachers and pupils reported that they understood the importance of cyber security, and strongly agreed that they learned a lot when attending the camps. A visualisation of this assessment can be seen in figure 5.2. In GenCybers' third goal of improving the teaching of cyber security in the K-12 curricula, GenCyber was pretty successful as 62% of teachers who attended camps in 2015 said they had indeed implemented cyber security training in their K-12 classes, which in turn reached more than 13,000 pupils [36].

n 2021 a report containing the five-year evaluation of the GenCyber programme was released. This report covered the results of the camps from 2015 to 2019. Let us have a look at some key findings from five years with GenCyber. The first goal was to increase the interest and diversity of cyber security. There was a total of 15,545 pupils attending the GenCyber camps from 2015 to 2019. Of these pupils 46% (7,160) took part in the five-year evaluation. It is important to note that these were the pupils who graduated high school. Of the 7,160 pupils, 1,350 pupils are pursuing a career in cyber security, that is 18.9% of the pupils who took part in the evaluation. In my opinion this is not a great outcome. If the goal is to increase the cyber security workforce in the US, then a total of 1,350 pupils over the course of

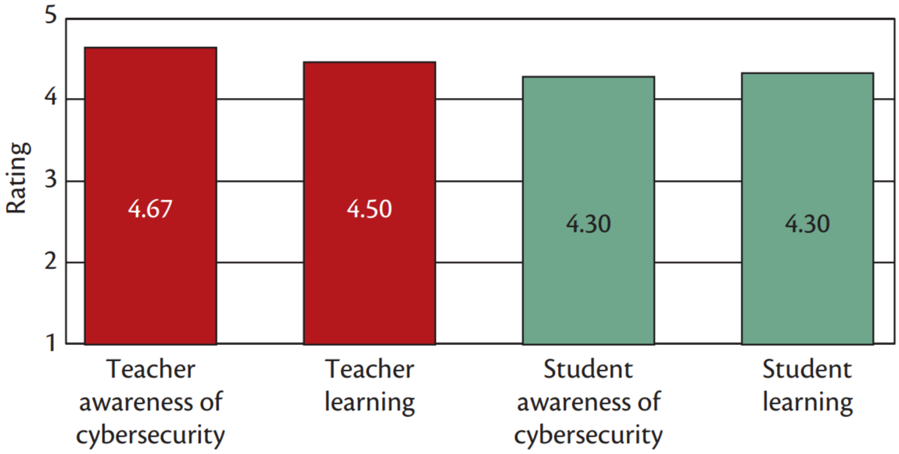


Figure 5.2: An illustration of teachers and pupils' awareness and learning about cyber security after the 2015 GenCyber camps [36].

five years is not really an increase [18].

As of 2020 there were around 331 million people living in the US [3]. And according to Cyberseek, a project ran by the National Institute of Standards and Technology (NIST), there are currently 1,053,468 people currently employed in the US cyber security workforce, with 597,767 total job openings [14]. The 1,350 pupils pursuing a career in cyber security make up about 0.2% of the jobs that are currently available. If the GenCyber programme continues to generate only 1,350 pupils for the workforce over the course of five years and the job openings remained the same over the years, it would take around 2,214 years to fill all the vacant positions (if the US was relying solely on the GenCyber programme).

In terms of the diversity in the workforce, a key finding here was that for every female pursuing a career in cyber security there are 3.5 males. This means that, of the group of 1,350 people, there were 300 females and 1,050 males. That in my opinion is not great. The females represent 22.2% of the pupils pursuing a career in cyber security, this is quite far away from the equality GenCyber wants to achieve. A visualisation of the gender representation can be seen in figure 5.3. Another finding was that for every pupil of an underrepresented minority, there are 5 Caucasians. That means we have 225 pupils with a minority background and 1,125 Caucasians pursuing a career in cyber security. The group of underrepresented minorities make up 16.7% of the total 1350. That is, again, nowhere near the equality that GenCyber wants to achieve.

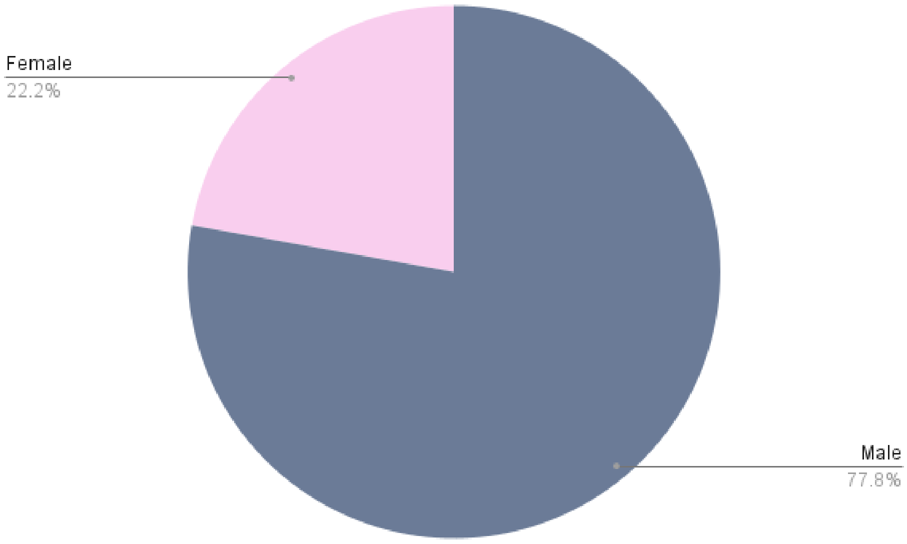


Figure 5.3: Gender representation of the 1,350 pupils pursuing cyber security. Over three quarters are males.

For the second goal, teaching participants correct and safe online behaviour, the key findings were that 87% of the respondents agree that GenCyber has indeed increased their awareness of cyber security and deemed cyber security important to their everyday lives. 13% of the respondents reported feeling the same way about cyber security as before attending a GenCyber camp. In addition, the respondents were showed a list 18 different safe online behaviours and asked to recite how many of them they were taught at the GenCyber camp. The respondents were taught 60% of the list, and they reported that they still enact 90.3% of the safe online behaviours they were taught [18]. In my opinion, the fact that they were taught 60% of the list of 18 safe online behaviours is pretty decent, as the GenCyber camps teach both safe online behaviour and other topics of cyber security in the span of minimum five days or 30 hours of activities. The respondents still enacting 90.3% of these safe online behaviours is a great outcome.

GenCybers' third goal was to improve the teaching of cyber security or cyber safety in the K-12 curricula. A total of 3,711 teachers have attended the GenCyber camps since 2015. The data in the five-year evaluation was collected from 2,664 of these teachers. The key findings of the report state that, of these 2,664 teachers, only 973 (36.5%) reported teaching cyber security or cyber safety the following school year as a result of attending the GenCyber camps. A visualisation of this can be seen in figure 5.4.

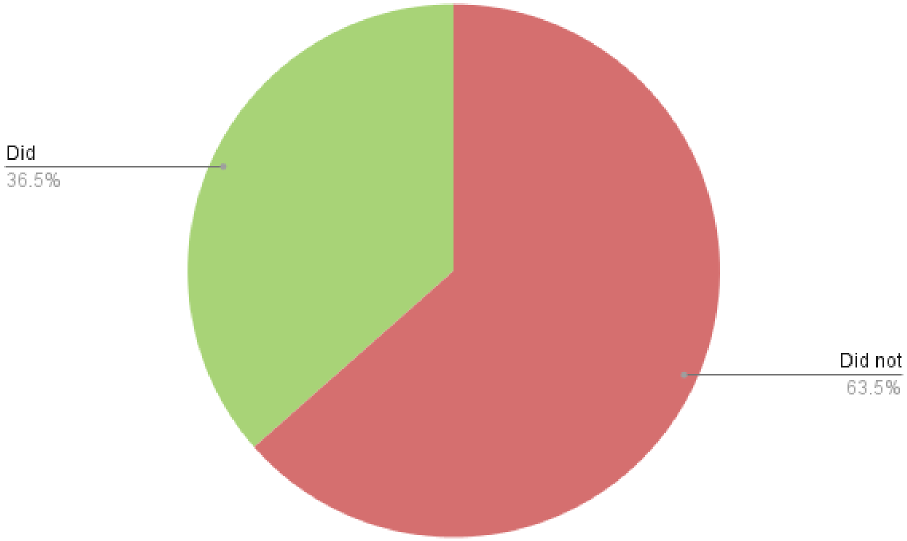


Figure 5.4: Pie chart showing the percentage of teacher who taught cyber security or cyber safety to their pupils the year following their participation to the GenCyber camp.

Although 36.5% does not seem like that much, these 973 teachers taught 26,149 hours of cyber safety or cyber security to over 145,000 pupils [18]. This goes to show that teaching the teachers has a far greater reach than the summer camps designed for the pupils themselves. A total of 15,545 pupils and 3,711 teachers attended the GenCyber camps from 2015 to 2019. Of the 3,711 we know of 973 teachers that taught their pupils cyber security or cyber safety and managed to reach 145,579 pupils. That is a total of 161,124 pupils reached through both the GenCyber camps and through the teachers themselves. The teachers make up 90.4% of the pupils reached as a result of the GenCyber camp participations. Bearing in mind that this was only 36.5% of the teachers actually teaching cyber security or cyber safety, I would say that method is pretty solid. A visualisation of the percentage of students reached through the GenCyber programme can be seen in figure 5.5.

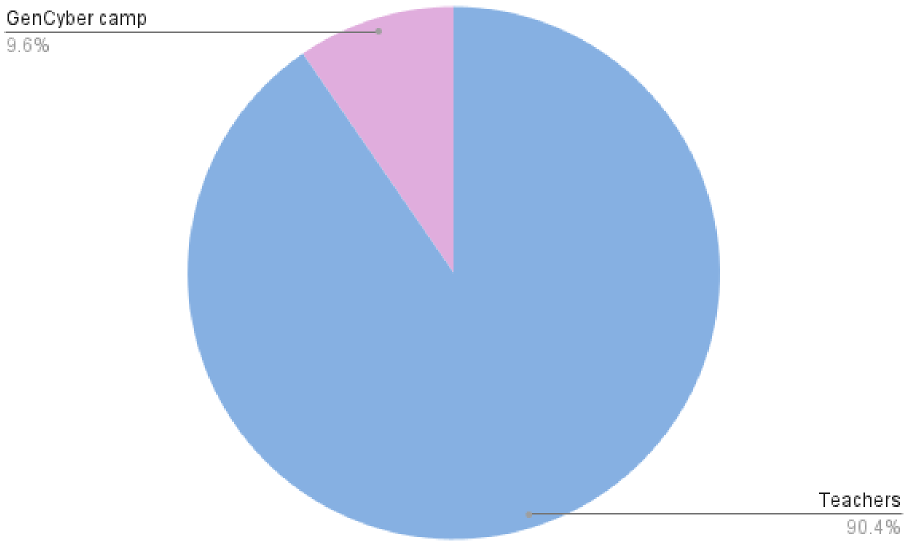


Figure 5.5: Pupils reached through the GenCyber programme. 90.4% of the pupils were reached through their teachers teaching them cyber security or cyber safety they learned from attending the GenCyber teacher camps.

All things considered; I would say the GenCyber programme has been moderately successful at reaching its goals. The first evaluation we looked at from 2015 looked very promising, but as it stands after the five-year evaluation, I would not say GenCyber has been a massive success by any means. My judgement might seem harsh, but as someone who is trying to determine whether or not this method for teaching cyber security is something worth adopting in Norway, I need to focus on the methods that benefit Norway most. I believe the best outcome from the GenCyber programme has been the number of pupils taught cyber security or cyber safety from the teachers who have attended the GenCyber camps, although the number of teachers teaching cyber security or cyber safety was rather small. I do however believe that GenCyber is onto something when it comes to teaching the teachers cyber security. In addition, I believe that GenCyber had quite successful in reaching their second goal; teaching the participants correct and safe online behaviour. Where 87% of the respondents reported that GenCyber increased their awareness of cyber security. So, the GenCyber camps clearly work, but do not reach a massive number of pupils.

Let is have a look at how the UK has decided to solve similar problems with its cyber security programme CyberFirst, before we start determining the best way to implement such a solution in Norway.

5.2 CyberFirst

5.2.1 Background and motivation

CyberFirst is a very different programme to the GenCyber programme. It was created and led by the National Cyber Security Centre (NCSC), which is a part of the Government Communication Headquarters (GCHQ) - one of the three UK intelligence and security agencies [78]. CyberFirst was created on the same basis as GenCyber, which was to solve the shortfall of skilled cyber security professionals. It was officially launched in May of 2016 with a trial run being held in 2015.

The goals of CyberFirst are similar to that of GenCyber; inspiring the next generation to pursue a career within the field of cyber security and increase the diversity in the cyber security workforce. The difference between these two programmes is that GenCyber focuses on improving teaching methods of cyber security for the pupils in kindergarten all the way through Year 12, in addition to the other two goals. Another difference is the approach to solving the shortfall in the cyber security workforce and the approach to reach their goals.

5.2.2 Programme structure

CyberFirst provides what they call *CyberFirst summer courses* (similar to the camp concept of GenCyber) of varying difficulty. CyberFirst also provides other means of learning cyber security such as through *bursaries*, a *degree apprenticeship*, *girls only cyber security competitions*, online extracurricular programmes called *Cyber Discovery*, and through cyber security curriculum and courses at specialised schools [10]. In addition, we have *CyberFirst Academy*, which is a free online where people can get free affordable training, whether you are already working in the cyber security field or not [1]. An illustration of the pipeline if activities CyberFirst provides can be seen in figure 5.6.

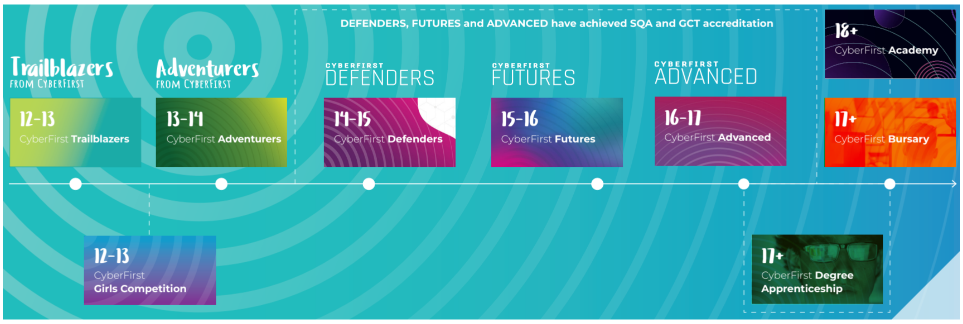
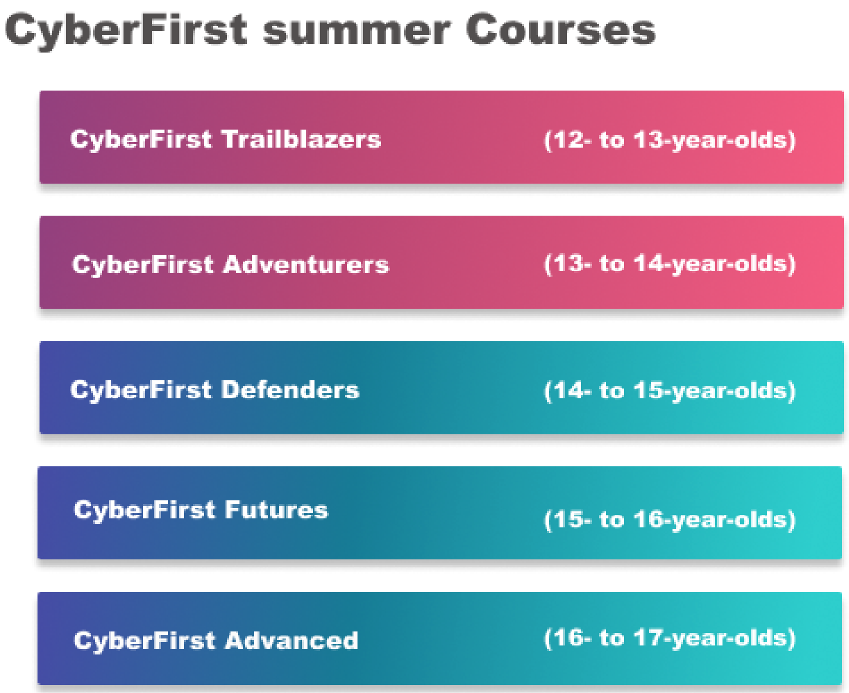

DEFENDERS, FUTURES and ADVANCED have achieved SQA and GCT accreditation
Trailblazers FROM CYBERFIRST
Adventurers FROM CYBERFIRST
CYBERFIRST DEFENDERS
CYBERFIRST FUTURES
CYBERFIRST ADVANCED
18+ CyberFirst Academy
12-13 CyberFirst Trailblazers
13-14 CyberFirst Adventurers
14-15 CyberFirst Defenders
15-16 CyberFirst Futures
16-17 CyberFirst Advanced
17+ CyberFirst Bursary
12-13 CyberFirst Girls Competition
17+ CyberFirst Degree Apprenticeship

Figure 5.6: Illustration of the pipeline of activities CyberFirst provides [6]

The CyberFirst summer courses are all free and are provided for pupils of the ages 12-17 with five different courses: *CyberFirst Trailblazers*, *CyberFirst Adventurers*, *CyberFirst Defenders*, *CyberFirst Futures*, and *CyberFirst Advanced*. The courses vary in length, recommended ages, and degree of difficulty. The two courses' Trailblazers and Adventurers are both half day courses aimed at pupils in Year 8/9 (12- to 14-year-olds) and Year 9/10 (13- to 15-year-olds), respectively. Some cyber security topics introduced in these courses include digital forensics, basic cryptography, and a general introduction to some basic cyber security terms. The last three courses' Defenders (14- to 15-year-olds), Futures (15- to 16-year-olds), and Advanced (16- to 17-year-olds) are all five-day courses where you can choose whether you would like to stay at site (similar to a summer camp) or stay elsewhere. The Defenders course focuses on the source and impact of common cyber security threats, incident response, security in home networks, and managing personal digital footprints. In the Futures course the pupils will learn about understanding and protecting networks, exploring motivations for cyber-attacks, protecting themselves from cyber-attacks, and some basic cryptology. In the last summer camp, Advanced, the pupils will be taught digital forensics, encryption technologies, penetration testing and open-source intelligence techniques [8]. See figure 5.7 for a visualisation of the CyberFirst summer courses.



CyberFirst summer Courses

CyberFirst Trailblazers (12- to 13-year-olds)

CyberFirst Adventurers (13- to 14-year-olds)

CyberFirst Defenders (14- to 15-year-olds)

CyberFirst Futures (15- to 16-year-olds)

CyberFirst Advanced (16- to 17-year-olds)

Figure 5.7: Illustration of the CyberFirst courses. The top two courses are half-day courses and the bottom three are five-day courses.

The bursary programme offers undergraduates (students who have completed their A-Level of whilst at university) £4,000 financial assistance per year and paid cyber security training each summer to help the students get a career in the cyber security field. The degree apprenticeship option offers the undergraduate an apprenticeship at a company working in the cyber security field and a recognized degree once the three-year programme is completed [7].

The girls only competitions are held every year and consist of three different phases. In phase one is an online qualifying round, phase two is the semi-finals, and phase three is the Grand Final where the top ten teams from across the UK compete for the title of UK CyberFirst Girls Competition Winners. The teams are made up of pupils of ages 12 to 13 from either England, Wales, Northern Ireland, or Scotland [9]. This competition is an initiative to increase the gender diversity in the UK cyber security workforce.

Cyber Discovery is a free online extracurricular programme for pupils aged 13 to 18 across the whole of the UK. Cyber Discovery is a newer addition to the CyberFirst roster of activities and was launched in 2017. It was created and delivered by SANS Institute and is a platform containing lectures, challenges, tasks and games related to cyber security. The Cyber Discovery journey consist of four different stages, the assessment stage, the game stage, the essential stage and the elite camp. In the assessment stage the pupils' get a set of 14 interactive challenges on a web platform, assessed to test the pupils existing knowledge of cyber security [33]. he quicker you complete these challenges the quicker you can move on to the next stage [17]. The game stage involves over 200 online challenges and focuses on self-learning, if the pupil completes a specific level they are invited to the next stage. In the essentials stage, the pupils gain access to a set of exercises, videos, challenges and more designed to test the pupil's knowledge of more advanced topics of cyber security. The last stage, the elite stage, has seen changes every year since the launch of the CyberFirst discovery programme. In the first year this stage consisted of a regional face-to-face residential camp, where further cyber security training, inspirational talks, career advice and other activities were held. In year two and three the pupils could, among other activities, attain recognized cyber security certification. In the latest year, 2020, stage four was replaced with a final Capture The Flag (CTF) challenge, where pupils must use their hacking skills in order to exploit vulnerabilities found in CTF challenges to find the "flags". This even was hosted online, and 500 pupils were invited to play [17].

The last initiative is the CyberFirst Schools and Colleges. This initiative was introduced in 2018 and encourages schools to provide more technology- and cyber security-based subjects and curriculums. The schools doing this will gain recognition from the NCSC and are awarded with one of three certificates: gold, silver or bronze. The certificates reflect the schools' current stage in the cyber security teaching, strategic ambition, and development plans. This is valuable for the schools as these certificates make them more attractive for applicants, and thus the school can become more profitable [11].

5.2.3 Programme evaluation

In 2021 CyberFirst released two evaluation reports, one evaluating the CyberFirst summer courses that ran in 2019 and the other evaluating the CyberFirst Discovery during the first four years – 2017 to 2021. Let us start with going through the statistics presented in the first report, the CyberFirst summer courses.

The total number of participants attending the summer courses in 2019 was 1,627. The data collected for the evaluation of the summer courses were collected from 549 participants who did the pre-survey (34%) and of these 549, the 255 who completed the post-survey (23%) [16]. It is important to note that in 2019 the SARS-CoV-2 pandemic hit the world, and thus the number of participants might have been affected.

Of the 1,627 participants 52% were males, 47% females and the remaining 3% did not disclose their gender. To achieve this equal gender split, CyberFirst targeted females under the recruitment process for the summer courses and the quotas were set in place in order to ensure as equal of a split as possible. When it comes to minority representation, 27% reported they were from an underrepresented minority, 8% did not provide their ethnicity and 65% were white. When asked why the participants choose to participate, they were given five different statements and asked to what degree they agreed with each statement. The first statement as to why they were attending the course was “to improve cyber security skills”, to which 62% strongly agreed and 35% agreed. When asked if they were attending “to gain knowledge of cyber security issues” 51% strongly agreed and 41% agreed. 50% strongly agreed and 42% agreed that they attended to improve their computer science skills. When it came to increasing cyber security career knowledge only 37% strongly agreed, and 46% agreed that this was the reason they attended. The most split statement was if they attended to help get a job, only 18% strongly agreed to this, and 37% agreed [16]. The visualisation of these statistics can be seen in figure 5.8.

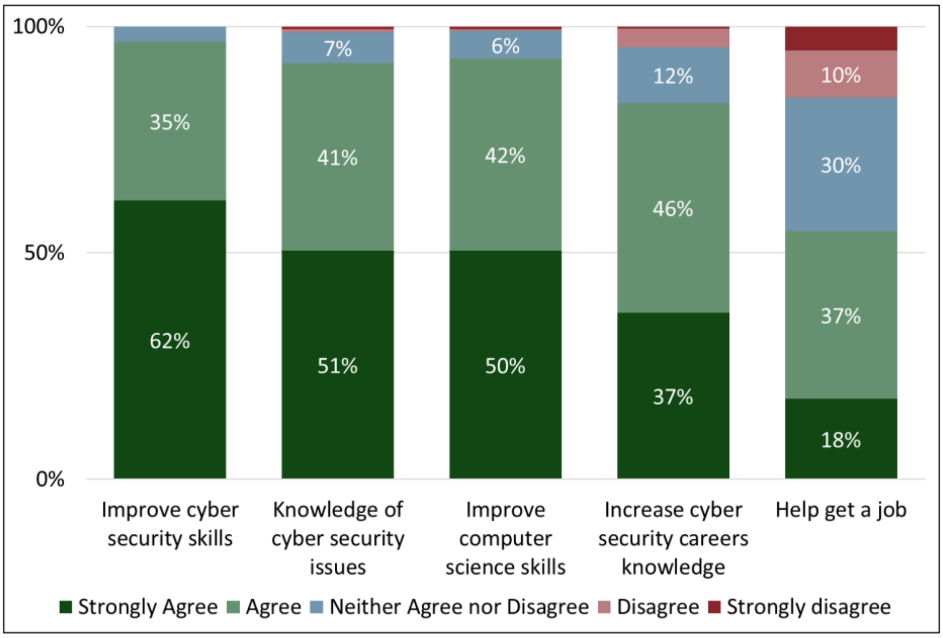


Figure 5.8: Statistics of why the participants chose to participate [16].

n the pre-survey the participants were asked if they wanted to pursue a career in cyber security, to which 43% were very interested and 48% were fairly interested. Displaying a huge interest in cyber security already before attending the summer courses. Interestingly, there was a much larger percentage of males (49%) who wanted to pursue a career in cyber security versus females (37%). When asked if they had participated in cyber security courses or event previously, 76% answered that they had, with most of these having participated in the Cyber Discovery course. Even though the interest in cyber security was already high, the participants were more likely to consider further training in form of a cyber security degree, CyberFirst bursary, CyberFirst apprenticeship and more than before the summer course. Figure 5.9 displays the interest in further education prior to and after the summer course attendance [16].

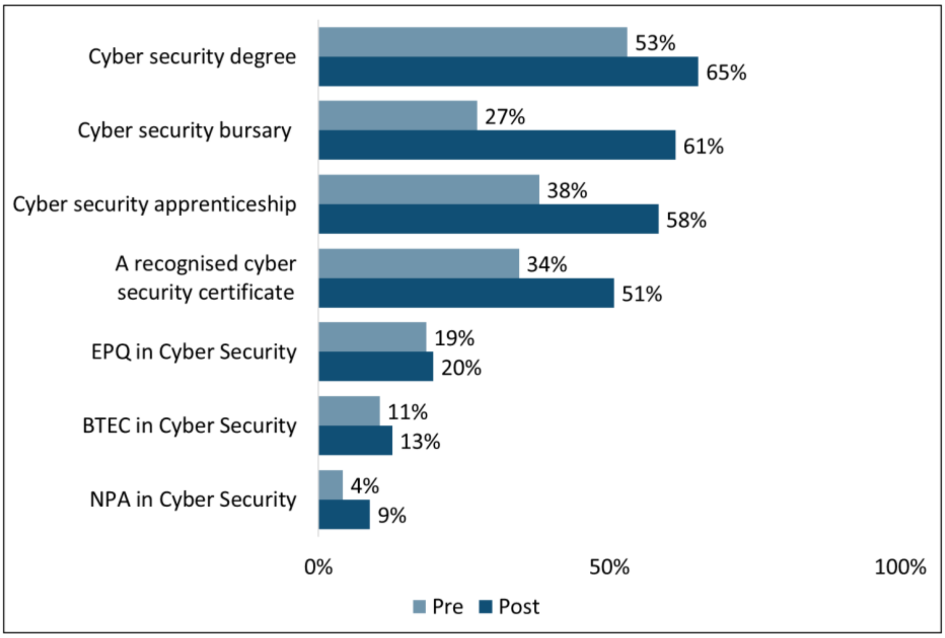


Figure 5.9: Interest in different future education options pre- and post-attending the summer courses [16].

Let us move on to the CyberFirst Discovery evaluation. As a reminder, the CyberFirst Discovery course was a four stage, free online extracurricular programme for pupils aged 13 to 18. The evaluation we are going to have a look at is evaluating the courses achievements from 2017 to 2021. The CyberFirst Discovery course has seen a total of 115,712 pupils over the course of four years since the start in 2017 to 2021. In year one (2017) there was 23,636 pupils, where 21% of them were girls. In year two (2018) there were 27,903 pupils, 25% girls. In year four (2019) there were 35,941 pupils, 32% of which were girls. And in the fourth year (2020) there was 28,232 pupils, 33% girls. It is speculated that the decline of pupils from year three to four was due to the school closures caused by the ongoing SARS-CoV-2 pandemic [17].

In table 5.1 we can see how the students fared in the different stages of CyberFirst Discovery. Of the 21,834 participants who were registered for the assess stage in year one, 32.7% progressed all the way to the game stage, 17.2% progressed to the essential stage and 1.3% identified as an elite in the end. In year two 20.5% progressed to the game stage, 14.9% to the essential stage, and 1.9% ended up as elites. In year three 31.6% of the participants progressed to the game stage, 10.5% to the essential stage and again 1.9% ended up as elites. In the last year, year four, 26.5% ended up progressing to the game stage, 11.5% progressed to the essential stage and 2.8% ended up as elites.

	Year One	Year Two	Year Three	Year Four
Registered Discovery	23,636	27,903	35,941	NA
Registered Assess	21,834	25,904	33,427	28,232
Registered Game	7,146	5,320	10,564	7,471
Registered Essentials	3,759	3,851	3,497	3,250
Identifies as ’Elite’	287	487	624	778
Attended Elite Camp	170	180	240	NA

Table 5.1: Participation in the different stages of the CyberFirst Discovery programme over the course of four years. In year four, there was no pre-registration campaign, everyone who wanted access got access, hence there is no number on how many people signed up in year four. There was also no stage four in year four, leaving this space blank as well [17].

Determining how successful the CyberFirst programme has been in reaching its goals is a bit more difficult than that of the GenCyber programme. The reason being that there is not that many statistics available for the CyberFirst programme. We only have statistics for two of the seven different activities CyberFirst provides, the summer courses and CyberFirst Discovery. It is important to bear in mind that the summer courses we have statistic from ran in 2019, during the SARS-CoV-2 pandemic. The pandemic might have had an impact on the amount of people attending the summer courses. Nevertheless, I am still not impressed with the outcome of the summer courses. There was a total of 1,627 participants across all the different difficulty levels of the summer courses in 2019. There are about 68.5 million people living in the UK [81], with an estimated 100,000 vacant cyber security positions [49]. There were no statistics provided which could say anything on exactly how many of the participants are actually pursuing a cyber security career. This makes it difficult to estimate how well the CyberFirst programme is doing to fill these vacancies. All we know is that there was an already high interest in cyber security among the participants attending the summer courses. Thus, the summer courses seem to work better for people who are already interested in working with cyber security and not so much in recruiting new people to join the cyber security workforce. This does make sense as the CyberFirst programme has created a pipeline with activities every year from the age of 12/13 all the way to a job in cyber security.

Although the CyberFirst summer courses do not seem very successful in the recruitment of new people for the cyber security workforce, they did do a good job on the male-female gender ratio, and it is a brilliant set-up for pipelining people into the workforce. It seems the recruitment of females in addition to the gender quotas put in place has been successful in achieving male-female gender equality, as 52% of the participants were males and 47% were females. As for how the CyberFirst programme is set up, it makes it easier for someone who is interested in pursuing a career in cyber security to hone their skills and do cyber security related activities throughout most of their schooling years. It is definitely a better way of doing it compared to the GenCyber programme where the pupils can go to multiple camps if they so choose, but they are not tailored to the different difficulty level the pupils might be at.

All in all, I think it is difficult to state exactly how successful the CyberFirst summer courses have been. That being said, the results from 2019 suggest that the programme is successful in reaching male-female gender equality and in providing activities for pupils to do throughout their schooling years and all the way to a career in cyber security.

The CyberFirst Discovery course was a lot more successful in the amount of people taught cyber security. A total of 115,712 pupils attended the course from 2017 to 2020. As a reminder the CyberFirst Discovery course consisted of three stages in 2017 to 2019 and three stages in 2020. That being said, there was a huge discrepancy in the amount of people participating in the first stage versus the next stages. This might indicate that the programme is a bit too difficult for the participants or perhaps it is not interesting enough for the participants to continue. Over the course of four years a total of 2,176 people go to the stage where they identify as an “elite”. That is 1.9% of the total participants. Do not get me wrong, it should definitely be a difficulty level to getting to this elite stage, but 1.9% is a very small amount. As for getting to stage two, the game stage, this in my opinion should be something almost every pupil manages, but only 26.4% of all CyberFirst Discovery participants were able to progress to this stage. There was nothing in the evaluation that stated why there were so few participants progressing through the different stages.

As for the female to male ratio, this was not as good as for the summer courses. This is most likely due to there not being a restriction in how many can participate as this is an online extracurricular activity. In 2017 only 21% of the participants were females, but by 2020 this was increased to 33%. An increase of 12% over four years is decent. They are still working on recruiting more females to participate in the CyberFirst Discovery course.

The CyberFirst Discovery course seemed to be more successful at providing cyber security training for more people than the summer courses. I would imagine this is the case because the Discovery course is available for any pupil who wants to attend. It is an online web application that is available at any time for its participants.

5.3 The Norwegian approach

Now that we are familiar with both the GenCyber and the CyberFirst programme it is time to figure out what such a cyber security programme could look like in Norway. What can be learned from the GenCyber and CyberFirst programmes? What approach will suit Norway best?

What have we learned from GenCyber and CyberFirst? From GenCyber we learned that the most effective method for reaching as many people as possible was through the teachers. Having teachers relay the teachings of cyber security to their own pupils was way more effective than providing a summer camp for pupils to join. It should be mentioned that the GenCyber camps are also a part of the initiative to recruit more people to the cyber security workforce, which it still did not seem to be very successful at. From CyberFirst we learned that providing a course in school was the most effective way to reach a large number of pupils. The Discovery course was provided through a digital platform which, in my opinion, might have contributed to its success. Digital platforms can make it easier for pupils to study the material in their own time as it is available at any point in time as long as you have internet.

To be able to use what we have learned from these programmes to figure out what a Norwegian approach can look like, we should probably set some goals of what we want to achieve with cyber security training in Norway. According to the Ministry of Justice and Public Security's national strategy for digital security competences, there is a need for general knowledge of cyber security for the whole nation, in addition there is a need for people with an expertise in cyber security [59]. So, our two goals in Norway are to:

- Increase the cyber security knowledge of the whole nation
- Inspire more people to pursue a career in cyber security

To reach the first goal, in increasing the cyber security knowledge of the general population, I believe we should focus on teaching cyber security in schools. Both GenCyber and CyberFirst showed us how many more people are reached because cyber security is provided closer to the pupils, in school. Besides, what better way is there than to force everyone to learn cyber security? I believe cyber security should be introduced from the year the pupils start getting phones, Year 3 or Year 4 perhaps, all the way through upper secondary school. In the earlier years, the pupils should learn how to use the internet and digital devices in a safe way. The need to learn about the consequences of posting pictures and videos online, and they need to learn their rights when it comes to their personal information. When they get older, they should continue learning about privacy and safe online behaviour on a more in-depth level. An in-depth topic of safe online behaviour could for example be how viruses are obtained and how they spread. In addition, they should be introduced to topics such as cryptography, as cryptography is such a vital part of cyber security. Nothing in the online world would be safe without some form of cryptography.

When it comes to upper secondary school, the cyber security topics should reflect the education programmes. For instance, in this thesis we are focusing on the education programme electrical engineering and computer technology and the cyber security topics introduced to these pupils should reflect the assignments and issues they will be faced in their work. It would for example not make a lot of sense to teach an electrician how to hack a website, they would probably benefit more from learn about security vulnerabilities in smart home products.

But it is not that simple to introduce cyber security, because the teachers might not know enough about the different topics of cyber security to be able to teach about them. There are several points that need to be determined in order to solve this issue. Is cyber security going to be its own subject? If not, which subject should it be a part of? This is not something that can be addressed by myself, rather it is a debate that the government needs to have. Though, in upper secondary school, it would make sense to integrate cyber security in the specialised subjects. When the pupils learn about the systems, devices, assignments and products that might pose a risk to security, it would make sense to address this risk and explain how to keep security intact. Nevertheless, cyber security should be taught at university level to the students who are studying to become teachers. Since they specialise in different subjects they want to teach, it is difficult to say exactly how this integration should be done.

The second goal of inspiring more people to pursue a career in cyber security is not that easy to reach. We saw both GenCyber and CyberFirst introducing summer camps/courses as a means to reach this goal. But this is not a viable option in Norway, in my opinion. Norway is a big country relative to the size of inhabitants, 5.5 million people [80]. Introducing summer camps would mean either several camps across the country or a lot of travelling for some participants. Considering the US with 331 million inhabitants managed to host the GenCyber camps for only 15,545 people over a period of five years and the UK with 68.5 million inhabitants managed to host the CyberFirst summer courses for a total number of 1,627 people in 2019, I do not see how a country with 5.5 million people could inspire a good amount of people to attend summer camps. Of course, we could try to market the summer camps well, but to be honest I do not see this endeavour being economically worth it. Another issue with recruiting people for the summer camps is that Norwegians value their freedom, I do not believe the youth would want to attend camps designed for learning skills that could be learned in school. Children want to spend their summers doing something fun, and the only camps I see working for Norwegian children are football camps, riding camps or other outdoor activity camps. And rightly so, I believe the children should spend their summer holiday outside playing, soaking up the sun that we do not see for half a year.

I believe the best way to inspire the youth to pursue a career in cyber security is to market it better. When cyber security is taught in school, it should be introduced as a possible career opportunity. Perhaps a cyber security expert could come and talk about the field in school. If introduced at an early level as something one can work with, I believe a lot more people would choose this career option. For instance, I might have chosen this career path earlier if it was presented to me as an option. I was in my second bachelor, fifth year of study when I realised what a broad and interesting field cyber security was. I have always had an interest in cyber security, always thinking critically when using the internet and sharing information online, I just did not know it was a career opportunity.

When the time comes, in Year 10, for all pupils to choose what they want to do for the rest of their life, they are hardly introduced to any of the possibilities they have. Many pupils choose the education programmes of upper secondary school that prepare them for further studies, because they simply do not know what to do with their lives. The same issue presents itself when the pupils graduate from upper secondary school as they are yet again not introduced to enough career possibilities to make an informed decision. I am not saying that every single career should be presented for the pupils, but it could be beneficial to present the careers of which Norway is missing expertise, such as cyber security expertise.

With all this in mind, the Norwegian approach would be to introduce cyber security in school as a part of the curriculum. Exactly what subject the cyber security should be a part of is unclear in Year 1 to Year 10, but in at least vocational education programmes in upper secondary school it would make sense for cyber security to be introduced in the subjects relevant to the specialisations. This approach would help solve the first goal of increasing the knowledge of cyber security in the general population. As for the second goal of inspiring more people to pursue cyber security, it could be beneficial to market the field more. Present it as a career opportunity to pupils in who are choosing the next step in their education, be that moving from Year 10 to upper secondary school or upper secondary to university level. Perhaps some cyber security experts could come during the national cyber security month, October, to educate the pupils about cyber security in addition to promoting a career in cyber security.

Chapter 6

Suggested solution

In this chapter we will have a look at the journey from the selection process of the type of solution all the way through the final demonstrative product. This type of solution is the type that has been elected the best way to integrate cyber security training in the education programme electrical engineering and computer technology, more on this in subsection 6.1. The goal of this chapter is to answer our third research question, RQ3. As a recollection, here is the third research question:

RQ3: How can cyber security be integrated into the educational programme electrical engineering and computer technology?

We will start by having a look at the choice of application type and why this type fits our purpose, educating the vocational education programme electrical engineering and computer technology, best. After that we will have a look at the different frameworks used to develop the application, the reasons for why these frameworks were chosen, and the limitations of the chosen frameworks.

After deciding the application type, we will have a look at the development process, including the requirements phase, design phase, development- and testing phase. In addition, we will have a look at the security and privacy measures that need to be in place and the ones that should be in place to create an application that is safe to use according to the Norwegian law and industry recommendations.

When we have had a look at the development process, we will have a look at the actual content of the application. This is the content that has currently been deemed important to learn for the pupils following the educational programme electrical engineering and computer technology.

The content has been derived from the interviews conducted in relation to the first and third research question. The third research question being the one we are attempting to solve in this chapter. In addition to the interviews conducted, scientific reports and threat analysis reports have been used to derive suitable cyber security content for the application.

Without further ado, let us start by having a look at the type of application that has been selected and why.

6.1 Type of solution

The intention with this subsection is to describe the type of solutions that fits our purpose best and explain the reasons for choosing this type. In addition, we will have a look at different ways of applying this type of solution and decide which way is the preferred when our goal is to discuss a possible solution to integrate cyber security training in the educational programme electrical engineering and computer technology.

Before we start looking into what type of solution fits best for our purpose, I think an explanation for what I mean by type is in order. When integrating new teaching material into an education programmes curriculum there are several different ways of doing so. Some ways include through textbooks, articles and films/videos, or as we have seen an influx of in newer times, through digital tools such as mobile applications and online web platforms. All these different ways of integrating new teaching materials into the existing curriculum are what I refer to as type when discussing the type of solution.

So, with that out of the way, what type of solution would fit the purpose of this thesis the best? The purpose being to determine the best way of integrating cyber security training in the Upper Secondary education programme electrical engineering and computer technology. Throughout the next subsections we will discuss the benefits and limitations of different types of solutions and determine which one will be used. Let us start with discussing if we should have a digital or a non-digital solution.

6.1.1 Digital or non-digital?

The first thing we need to know is whether we want to have a digital or a non-digital solution. A digital solution could for example be a cyber security learning platform via a mobile application or through a web application. A non-digital solution could be a textbook or one or more research papers that the pupils would have to read throughout the year. I do believe textbooks are much better than a bunch of research papers, especially when provided to pupils who already have a lot of learning material due to the large number of classes they need to attend. Textbooks are easier to relate to, as they are already familiar with the concept. In addition, textbooks provide a great structure to the subjects as you would normally go through them quite chronologically, chapter by chapter. They are also a great medium for teachers, who can use them to plan lessons and, in some cases, learn more about the different topics the textbook covers.

But there are some disadvantages to using textbooks as well. First of all, the information in them can quickly become out-dated, especially in a field like cyber security, which is in constant development. They also have a very limited format for giving the pupils assignments. These assignments are either relatively easy questions, with answers often provided at the end of the book, or the assignments are given in the form of a case where the pupils have to discuss their way to a solution. When we decide upon the solution type, we have to bear in mind who we are creating this solution for. We are creating the solution for pupils who have chosen a vocational education, in most cases this means that the pupils are seeking practical education. In my experience, a lot of these pupils choose a practical education because they are tired of the traditional school, where reading and doing such assignments as was just described is in focus.

Thus, I believe we should create a digital solution, because it would suit the kind of pupils we are dealing with more, in addition it is easier to implement practical assignments into the application and, last but not least, the digital medium allows for a constant update of its contents. So, whether there is a grammatical flaw or some out-dated or wrong information present in the digital solution, it can easily be rectified by its developer(s).

There are multiple different types of digital solutions. Some digital learning materials include electronic textbooks, educational videos, electronic quizzes, mobile applications, websites and web applications. Of these digital mediums I only see websites, mobile and web applications as viable options as the other ones can be integrated into these types of applications to create a more comprehensive product. So, our next task is to figure out which of these two digital teaching mediums will suit the purpose of this thesis the best.

6.1.2 Mobile application vs. web application vs. website

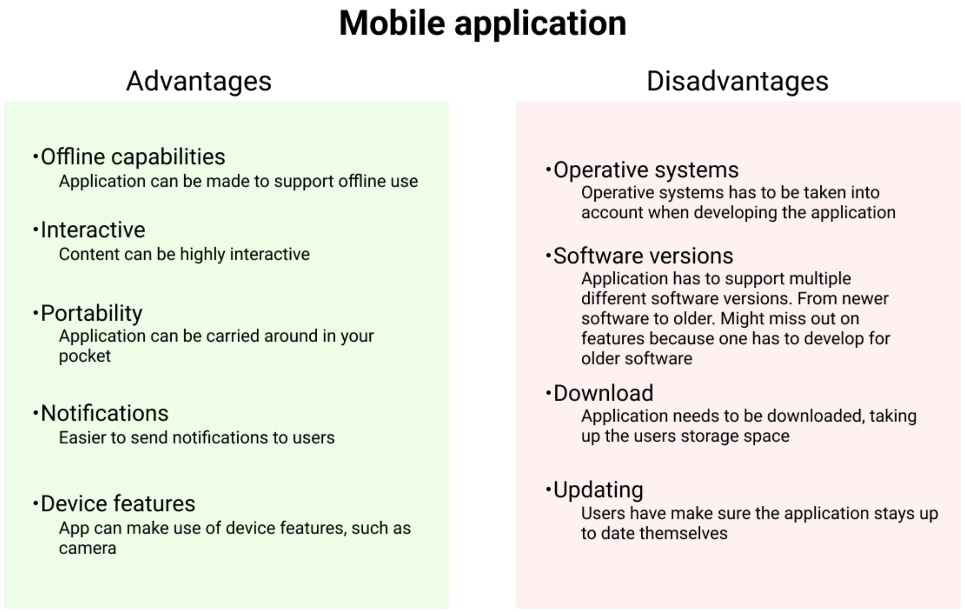
To be able to decide which of the three, mobile application, web application or website, suits the purpose of this thesis the best, we need to have a look at the advantages and disadvantages of these methods. But before we can look at the advantages and disadvantages, we need to know what these methods are.

Mobile applications are something most of us have some kind of relation to. They are often referred to as "apps" and are a type of software that run on mobile devices such as smartphones (for example iPhone, Samsung Galaxy or Google Pixel) or tablets/iPads. They can be downloaded from what is often referred to as "the App Store" which is the store on Apple devices with the Android equivalent being "Google Play Store".

emphWeb applications on the other hand, are a bit trickier to explain. Many of us are probably more familiar with the term website, but that is in fact not the same as a web application. A web application is a software or program that is accessible online through any web browser (for example Google Chrome, Mozilla Firefox or Microsoft Edge). The web applications are generally designed for interaction with the end user, unlike websites which generally consists of static content; this is content that is not changed or updated, this can be for example plain text or images. In a web application the content can change based on user interaction [38]. An example of a web application which we all can, hopefully, relate to is an email program such as Outlook or Gmail. These email programs update when email is received in the inbox, or when they are sent. An example of a website can be online newspapers such as "nrk.no" or "bbc.co.uk". In order to make an informed decision on which of these methods we should use, we will have a look at the advantages and disadvantages of each method. Figure 6.1, 6.2 and 6.3 contain the advantages and disadvantages of each method in conjunction with my assessment of each statement. Note that these advantages and disadvantages are my own beliefs, this, there might exist more advantages and disadvantages that are not taken into account. When creating these advantages and disadvantages I was bearing in mind the use of the application, which is as a learning tool.

In order to make an informed decision on which of these methods we should use, we will have a look at the advantages and disadvantages of each method. Figure 6.1, 6.2 and 6.3 contain the advantages and disadvantages of each method in conjunction with my assessment of each statement. Note that these advantages and disadvantages are my

own beliefs, this, there might exist more advantages and disadvantages that are not taken into account. When creating these advantages and disadvantages I was bearing in mind the use of the application, which is as a learning tool.



Mobile application

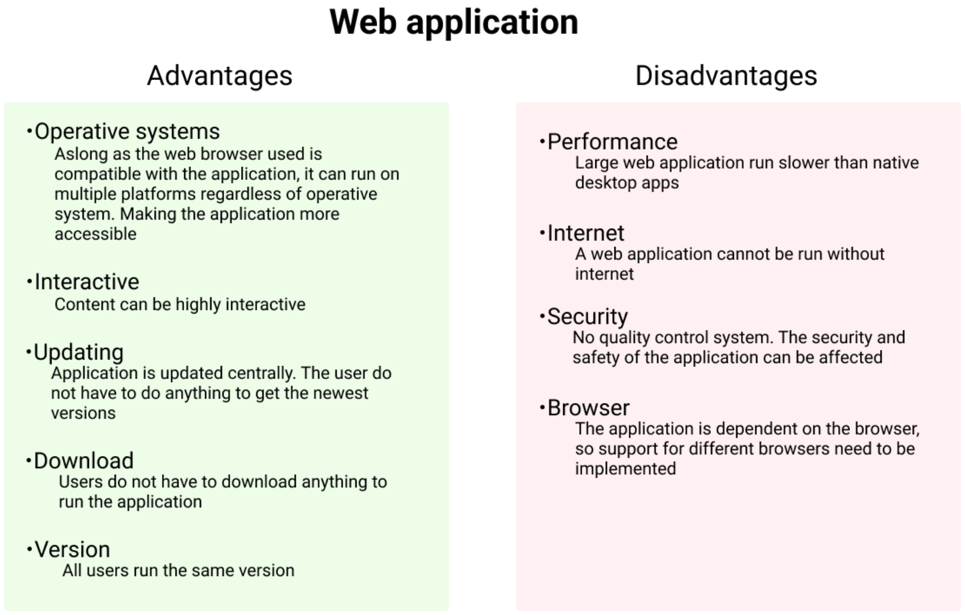
Advantages

- Offline capabilities
  Application can be made to support offline use
- Interactive
  Content can be highly interactive
- Portability
  Application can be carried around in your pocket
- Notifications
  Easier to send notifications to users
- Device features
  App can make use of device features, such as camera

Disadvantages

- Operative systems
  Operative systems has to be taken into account when developing the application
- Software versions
  Application has to support multiple different software versions. From newer software to older. Might miss out on features because one has to develop for older software
- Download
  Application needs to be downloaded, taking up the users storage space
- Updating
  Users have make sure the application stays up to date themselves

Figure 6.1: Advantages and disadvantages of using mobile applications.



Web application

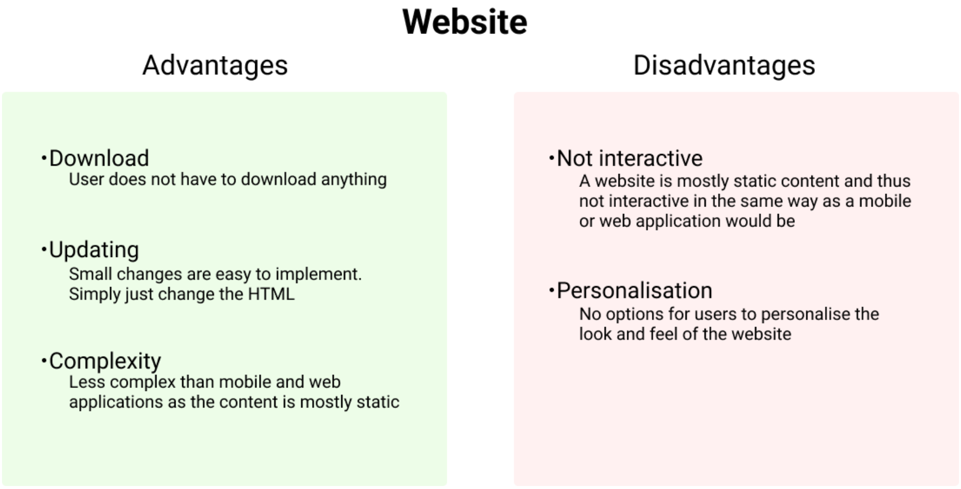
Advantages

- Operative systems
  Aslong as the web browser used is compatible with the application, it can run on multiple platforms regardless of operative system. Making the application more accessible
- Interactive
  Content can be highly interactive
- Updating
  Application is updated centrally. The user do not have to do anything to get the newest versions
- Download
  Users do not have to download anything to run the application
- Version
  All users run the same version

Disadvantages

- Performance
  Large web application run slower than native desktop apps
- Internet
  A web application cannot be run without internet
- Security
  No quality control system. The security and safety of the application can be affected
- Browser
  The application is dependent on the browser, so support for different browsers need to be implemented

Figure 6.2: Advantages and disadvantages of using web applications.



Website

Advantages

- Download
  User does not have to download anything
- Updating
  Small changes are easy to implement.
  Simply just change the HTML
- Complexity
  Less complex than mobile and web applications as the content is mostly static

Disadvantages

- Not interactive
  A website is mostly static content and thus not interactive in the same way as a mobile or web application would be
- Personalisation
  No options for users to personalise the look and feel of the website

Figure 6.3: Advantages and disadvantages of using websites

With the assessment done in figures 6.1, 6.2 and 6.3, I think we can safely say that Websites are no longer a contestant for the best solution for teaching pupils' cyber security, because they are not interactive and mostly contain static content. This does not make for an interesting and fun learning experience. As for the other two, mobile and web applications, we have a more difficult choice to make. Both mobile and web applications can offer highly interactive content which will make for a fun and interesting learning experience.

As to which one is best suited for the purpose of teaching cyber security to pupils attending electrical engineering and computer technology, I would say that would be the web application. With a web application it is easier to implement practical tasks suited for this education programme. Implementing practical tasks can indeed be done with a mobile application, but some practical tasks given in the electrical engineering and computer technology might be a bit too large to portray on the size of a mobile phone screen. I can for example see Year 2 or 3 computers and electronics needing to know how to set up a safe network, this can be taught with practical tasks where the pupil places devices in a network and simulates communication in and out of the network, much like the Cisco packet tracer [13]. With a web application it is also easier to implement a fun and interactive theoretical section to the application. Of course, this is possible in a mobile application too, but the potential in terms of looks and functionality are better in a web application. You can for instance choose to give theoretical information through videos, this would be a lot more difficult to implement on a mobile phone.

Another benefit of a web application is that it can be made to work on a phone as well. This means the pupils can have the benefit of accessing the application on their phones, and still be able to access it on the pc. This would not be possible if you chose a mobile application, as they are specially made for mobile phones. The last, but probably the most important argument for choosing a web application is what is called “the free principle in school”. This is a principle we have in Norway that states that pupils in upper secondary school have a right to receive free teaching materials, this includes textbooks and other printed materials, in addition to digital teaching aids and digital equipment, such as calculators and PCs [27]. This means that every single pupil attending an education programme in upper secondary school in Norway has access to a PC. There is no guarantee that these pupils will have a smart phone, and certainly not a newer smart phone that can be used to run newer applications. By choosing to develop a web application we make sure that the application is available to every single pupil, as long as the web browsers they use are supported by the web application which is certainly easier to see to than for a mobile application to support all operating systems and the different versions of these operating systems.

6.1.3 Web application

Now that we have decided that a web application would be best suited for teaching cyber security to the pupils attending electrical engineering and computer technology, we need to decide how we are going to make it.

There are several different ways of creating a web application. The easiest way is probably to use so-called application builders, which allow non-technical people to create their own applications. Some examples of application builders that most people might have heard about include WordPress and Shopify [30]. Web application builders are good options for start-ups that has no technically able personnel. I would personally not recommend using them unless you have to. The reason being security. No application or platform is completely secure, but if you create your own application, you will have a lot more control of the security features in place in your solution. In addition, you can update the application as soon as new vulnerabilities are found. This is not the case if the vulnerability itself is within the framework or features of the application builder. If we look at the Common Vulnerabilities and Exposure (CVE) database, which contains known vulnerabilities in a variety of different products and systems, we find a very large numbers of vulnerabilities connected to WordPress. Since 2004 there has been a total number of 344 known vulnerabilities in WordPress. Quite a few of which have obtained a high score (9-10, 10 being max score), indicating very serious issues. Already in 2022 five vulnerabilities have been found in WordPress, where the highest score obtained was 6.5 [19].

Vulnerabilities are constantly being rectified by the application builders, but if we create our own application, we have more control over the security measures and features in the application. In addition, we will have full control of the databases, which can be used to store user data. So how do we create our own web application?

A web application consists of a frontend; the part of the web application the users can see and interact with, a backend; the part of the web application that is hidden, this part is usually responsible for storing and manipulating data, and one or more databases; the part of the application used for storing data. A frontend typically consists of code written in the programming languages HTML, CSS and JavaScript. To make development faster and easier one tends to use different frameworks or libraries to help the development. Examples of frontend frameworks and libraries are Vue.js, Angular and React. These frameworks/libraries will help you structure your code and build the software. Backend frameworks work similarly to the frontend frameworks as they also help you structure your code and build the software. Some backend frameworks include Django, Flask and Ruby on rails. Generally, the backend code tends to be programmed in one programming language. Common programming languages for backend programming include Python, PHP and C#. As for the backend frameworks mentioned above the programming language used by them are python for Django and Flask and Ruby for Ruby on rails. When it comes to programming a database, they are usually written in different types of SQL, for example MariaDB or MySQL.

The plan was to develop a web application using React as the frontend tool, Flask for the backend and MySQL for the database. Due to limited time and the amount of time spent on learning frontend development, there was no time to spend on developing a backend and a database. Meaning the demonstrative product is only a shell with no connections to a backend server and thus no information from a database.

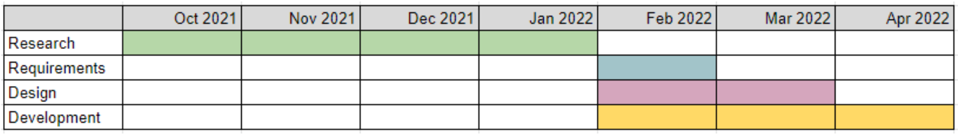
The reasons for choosing React as the frontend development tool was plenty. First of all, this was a library I already had a little bit of experience using, I also really like the natural code structure that forms because its modular structure. In addition, there are benefits in terms of performance since it was designed with performance in mind which allows even complex applications to run fast [48]. I also believe that React, in the right hands, can create beautiful interactive and fun applications.

t should also be mentioned that Node.js and npm was also used to create the frontend product. Node is a runtime environment that is used to build scalable network applications [44]. Npm is a package manager for the Node js environment. With npm, packages can be installed that can help make the user interface (UI) of the web application better. It is important to note that you need to be careful with the npm packages you install as some of them are malicious. These malicious packages can be used to spread malware. In addition, one needs to make sure the npm packages stay updated, as outdated packages can pose a risk to the security of the application if they are found to include vulnerabilities.

Now that we are familiar with the programming languages and libraries that was used to develop the demonstrative product, we will have a look at the development process.

6.2 The development process

In this subsection we will go through how the demonstrative application was developed. We will have a look at the process from the requirements phase all the way to the finished product. The finished product being the demonstrative application. We will start by looking at an overview of the process before explaining each phase of the process.



	Oct 2021	Nov 2021	Dec 2021	Jan 2022	Feb 2022	Mar 2022	Apr 2022
Research	🟩	🟩	🟩	🟩			
Requirements					🟦		
Design					🟪	🟪	
Development					🟨	🟨	🟨

Figure 6.4: Simple grantt chart showing the development process

This development process was divided into four different phases, with some of them overlapping. The phases were the requirements phase, design phase, development phase and the testing phase. The following subsections will try to explain what was done in each of phases

6.2.1 Requirements phase

According to [55, p. 83], requirements are descriptions of what a system should do, the services provided and the constraints to its operation. The requirements should reflect the needs of the customers for a system. As this is a thesis on the topic of information security, our focus will be on the security requirements of the application. However, we should establish some requirements to be able to understand what the basic functionality of the application.

The topic of this thesis was decided by the CyberSmart project. The desired outcome of the thesis would be an application that could be used by pupils at upper secondary school to learn cyber security. Because of this I saw CyberSmart as the customer of the application and as such contacted them in order to discuss the functionalities of the application itself. I had a meeting with some of the creators of the CyberSmart project, and asked questions such as what functionality they expected or wanted the application to be able to perform, or if they had any design ideas they wanted to implement into the application. They had no ideas of what they wanted the application to look like or the functionalities the app should contain. In other words, I could not this source to derive the requirements of the application. Another idea would be to use the intended users, of the application, the upper secondary pupils, to derive the requirements, but I did not think this would have any merit as it would take a lot of effort to involve such a large userbase when the time is of the essence. Though I think they should be involved at a later stage to give input on the user experience and the design of the application.

So, the requirements to the functionalities in this application was derived from what I thought would be important to include in the application. The following list contains some of the requirements that I thought would be either important or interesting features.

- The system shall display all *courses*
- The system shall display chapters in currently chosen course
- The system shall display users' chapter and course progression
- Users need to login to be able to access the features of the application
- Users shall be able to read theoretical content
- Users shall be able to watch video version of theoretical content

- Users shall be able to take chapter quizzes
- Users shall be able to do practical assignments

Based on these requirements, we can create an outline of what the application can look like: The users will start by logging in to the application. Once logged in, the users will be met by a dashboard. On the dashboard the users will find some statistics of the progression they have through the current course. The application will host multiple such courses, these will contain different chapters representing the cyber security topics relevant for the course. The courses will be designed to meet the needs of the different years and specialisations they *belong to*. For instance, Year 1 would have its own course with chapters based on the cyber security topics that would be relevant to teach in Year 1. You will also find quick-access to the different chapters of the currently chosen course available on the dashboard. The users should be able to ”sign up” to multiple different courses if they so please, as this would encourage the users to learn more. For each chapter, there will be a chapter quiz, testing their abilities to retain the curriculum. This quiz can be taken as many times as the user pleases. In addition, there will be a few practical assignments. The chapters would ideally have a theoretical part consisting of either written and/or video-recorded lectures.

Security requirements

In order to ensure our application is being built with security in mind, we should create some security requirements. To create the security requirements the ”Cigital Risk Management Framework” has been followed [39]. When using this framework we are using risk assessment to determine the requirements that should be in place to ensure that the application is safe to use. An illustration of the framework can be seen in figure 6.5.

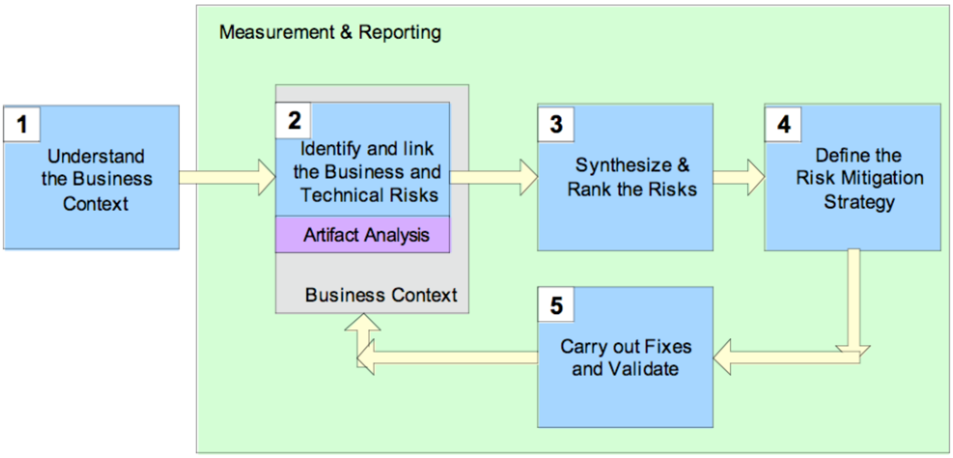

Measurement & Reporting
1
Understand the Business Context
2
Identify and link the Business and Technical Risks
Artifact Analysis
Business Context
3
Synthesize & Rank the Risks
4
Define the Risk Mitigation Strategy
5
Carry out Fixes and Validate

Figure 6.5: The Cigital risk management framework [39].

With this risk management framework, we will be going from understanding the *business context* to identifying the business risks that threaten the context, and then we will identify the technical risks before we define a mitigation strategy, thus arriving at our security requirements [39]. The business context consists of the goals, priorities and circumstances that make up the business image. To identify the business risks we first need to determine what the goals of the business are. In this thesis we are not associated with a particular business, so we will establish the business goals based on the goals and ambitions of the application we are going to make. The goal of the application is to teach pupils about cyber security, in order to achieve this goal the application has to remain available for its users, thus making that a goal too. The third goal would be to provide a safe service in regard to cyber security of the application itself. A safe service could for example be a service that processes, protects and handle personal data in a safe manner. Our three business goals are thus:

BG1 Teach pupils cyber security

BG2 Provide a reliable service

BG3 Provide a safe service

Now that the business goals are identified, it is time to identify the business risks and technical risks related to these goals. We start by identifying the business risks. The business risks can be seen in table 6.1.

	Business risk	Description	Affected business goal(s)
BR1	System is unavailable	Users are unable to access the system	BG1, BG2
BR2	Personal data breached	Users personal data is stolen or accessed by unauthorized entities	BG3
BR3	System does not work as intended	System has flaws	BG2, BG3, BG3

Table 6.1: Business risks with description

With the business risks in hand, let us identify the technical risks. Technical risks are situations that do not have the desired effect on the design or implementation of the system [39]. The technical risks can be seen in table 6.2 and they are categorised based on the STRIDE model. The STRIDE model helps categorise based on different types of threats. STRIDE stands for *spoofing, tampering, repudiation, information disclosure, denial-of-service* and *elevation of privilege*. STRIDE stands for:

- Spoofing: Pretending to be someone you are not
- Tampering: Modification of data
- Repudiation: Claiming you were not responsible for or did not do something
- Information disclosure: Unauthorized entity gets hold of data
- Denial of service: Deny users access to service

The technical risks have a risk level associated with them, this risk level can help us determine which risks we should focus on mitigating. The risk level is the product of the combined probability of an incident happening and the consequences if it were to happen. In this thesis we use a low (L), medium (M) and high (H) scale.

Technical risk	Probability	Consequence	Risk level
Spoofing			
1 Poor enforcement of access control			
1.1 Default passwords	L	H	M
1.2 Users can create weak passwords	H	M	H
1.3 Unlimited authentication attempts allowed	M	H	H
Tampering			
2 User information changed	L	M	M
3 Data at rest or in transit not encrypted	M	M	M
4 Progression data is manipulated			
4.1 SQL injection	H	M	H
4.2 Session hijacking	M	L	M
4.3 Man-in-the-middle attack	L	L	L
5 System logs are changed	L	M	M
Repudiation			
6 System logging not implemented properly	M	L	M
7 System logs are not protected	M	L	M
8 Use of someone else’s account	M	L	M

Technical risk	Probability	Consequence	Risk level
Information disclosure			
9 Information breach			
9.1 SQL injection	H	M	H
9.2 Session hijacking	M	L	M
9.3 Man-in-the-middle attack	L	L	M
10 Data at rest or in transit not encrypted	M	M	M
11 Threat actor gains access to system logs	L	L	L
Denial of service			
12 Denial-of-service attack	H	H	H
13 Server or database crash			
13.1 Servers taken out by ransomware	M	H	H
13.2 Environmental damage to servers	L	H	M
14 Backups are not tested	M	H	H
15 Backup solution not implemented properly	M	H	H
Elevation of privilege			
16 Broken authorisation, threat actor gains access to privileged system	M	M	M

Table 6.2: Technical risks with risk assessment

Under the topic *spoofing*, we identified three technical risks. The first risk "default password" addresses the risk related to users having a default password assigned to them. Nowadays I should hope there is a low probability of this happening, but the consequences are high as the threat actor can potentially gain access to all accounts. Now the probability of the users choosing a weak password for themselves is very high, the consequence would be that the attacker can log into the account with the weak password. Considering we have plans of only potentially storing emails, usernames and names of users I think the consequence would be medium. Medium because the attacker gets hold of this information for this user but cannot do anything else. The last risk identified was "system allows unlimited authentication attempts", this has been classified as high consequence as the threat actor can through brute-force attacks potentially gain access to each and every account

In the *tampering* section we identified 6 technical risks, three of which are related to the manipulation of progression data. This data could for example be tampered through SQL injection, if the input was not properly validated or sanitised. The probability of a SQL injection attack is high as these types of attacks are one of the most normal ones [47]. The consequences of such an impact is, however, classed as medium. It would be annoying to lose all progression or for the progression to show the wrong amount, but it will not cause harm to the users or the system itself. This progression data is not sensitive personal data. The session hijacking and man-in-the-middle attacks have a low consequence as they can only affect one user at the time, and the data that can be affected is not sensitive. They can tamper with the progression as the client is speaking with the server for access to the progression data, or with the user data as the server is trying to authenticate the users. Data encryption and the change of system logs has also received a medium consequence, as the amount of personal data in the application is at a minimum. If user information were to change, it would mostly be annoying not very harmful. Say the email was changed to that of the threat actor and the threat actor got access to the system, all they would have access to is the progression of the pupil they stole the account from. This very much depends on how much personal information is portrayed in the application.

There were three risks identified in the *repudiation* section. These were related to system logs and the use of someone else's account. As for the system logs, the consequences of them not being properly implemented or not protected properly is low. In the system logs you can normally find information such as system changes. This has been classed as low consequence as the system logs would not contain much information. This is a teaching application that will only provide the pupils with courses to take and the progression through these courses. There is not much interesting information for the threat actors to grab from a system log. The usage of other people accounts is nothing to fear either, you cannot do anything other than learn which means that there is nothing important we are protecting and thus we do not need the non-repudiation trait. The overall risk assessment for these technical are however medium, as the probability for the different scenarios to occur is medium.

n the *information disclosure* section, we have five risks. Again, we find technical risks related to SQL injection, session hijacking and man-in-the-middle attacks. These have received the exact same score as for the tampering section due to the same reasons. We have also seen the risk related to encryption of data in rest or transit before and this again has been rated the same due to the same reasons. Now the risk related to the attacker getting a hold of the system logs is assessed as having a low risk, as the probability of it happening is low and the consequences are also low, due to the little amount of interesting data that will be stored in the logs.

Five risks were identified as related to *denial of service*. All of these technical risks have received a consequence of high as they affect the user's ability to use the system. If a successful denial of service attack was to be launched against the web application the users would not be able to access their accounts and thus not be able to learn. As for the technical risks related backups and destruction of data in the server, these would have a high consequence because it could potentially mean losing all the data on the users, meaning they would have to sign up again or all their progression would be lost. If the servers were infected by ransomware, it could also mean the potential for losing all the data and having to start again.

In the *elevation of privilege* topic, one technical risk was identified. If the authentication of the application was broken it could lead to the threat actor gaining access to privileges, they should not have. This could potentially become more serious if there was a form of administrative user or if the users had different privileges, but as it stands now there is only one type of user and thus only one privilege to be had. The authorization could still be broken though, this could for example mean that the threat actor could gain access to accounts that they should not have access to.

With the technical and business risks identified, it is time to link them together. The result of this can be seen in table 6.3

Business risk	Technical risk
BR1: System is unavailable	12 DoS
	14, 15 Backup issues
	13 Server or database crash
BR2: Personal data is breached	1 Poor enforcement of access control
	3, 10 Data at rest or in transit not encrypted
	8 Using someone else’s account
	9 Information breached
	7 System logs are not protected
BR3: System does not work as intended	4 Progression data is manipulated
	2 User information changed (username, email)
	5 System logs are changed
	11 Threat actor gains access to system logs
	16 broken authorisation, threat actor gains access to privileged system
	6 System logging not implemented properly

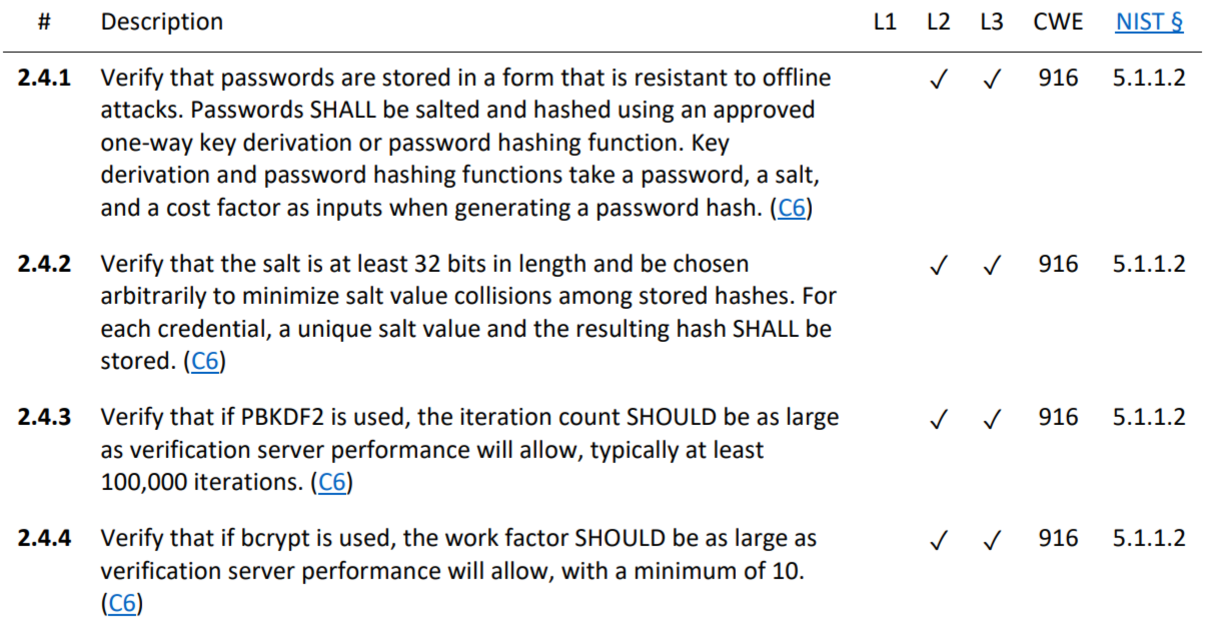
Table 6.3: Technical risks mapped to business risks

Category	Security requirement	Associated technical risk
Authentication	Any access to the system shall require authentication	1 Poor access control, 2 User information changed
	The system shall implement measures to limit the amount of unsuccessful authentication attempts	1.3 Unlimited authentication attempts allowed
	A strong password policy should be in place	1.1 Default passwords and 1.2 Users can create weak passwords
Authorization	The system shall protect confidential information from being read by unauthorized entities	3, 10 Data at rest or in transit not encrypted, 16 broken authorisation, threat actor gains access to privileged system
Availability	The system shall detect and mitigate denial-of-service attacks	12 Denial-of-service attack
	A back-up solution should be in place	13.2 Environmental damage to servers, 14 Backups are not tested and 15. Backup solution not implemented properly
Integrity		
	The system shall use up to date protocols for transporting data	3, 10 Data at rest or in transit not encrypted, 4.3, 9.3 Man-in-the-middle attack
	The system shall use up to date cryptographic schemes for protecting data at rest and in transit	3, 10 Data at rest or in transit not encrypted, 7 System logs are not protected
Miscellaneous	The system should not store personal data in system logs	6 System logging not implemented properly
	All user inputs shall be validated and sanitised	4.1, 9.1 SQL injection

Table 6.4: Security requirements

With the mapping of the business risks and the technical risks in mind, we can create some security requirements for the application. See table 6.4.

In addition to the security requirements derived especially for this application, I would also recommend having a look at the OWASP Application Security Verification Standard (ASVS). This standard can be used for both testing purposes and to see if there are any more potential security requirements that are relevant to add to our requirements [46]. ASVS is a community driven project which contains a large set of security requirements and controls. This verification is based on what ASVS calls “application security verification levels”. There are three levels that are used to determine which controls and requirements should be present in your application. The levels specify what type of application the different requirements are made for. Our application fits the description of level 2 best, as we are dealing with an application that contains sensitive data, being potentially emails and names. This level is recommended for most applications. For each control and requirement presented in the ASVS there are ticks indicating at what level they should be implemented at. For instance, as we can see in figure 6.6, we have four requirements related to the storage of credentials. All four requirements are required to make safe applications at level 2 (L2) and Level 3 (L3) [46].



#	Description	L1	L2	L3	CWE	NIST §
2.4.1	Verify that passwords are stored in a form that is resistant to offline attacks. Passwords SHALL be salted and hashed using an approved one-way key derivation or password hashing function. Key derivation and password hashing functions take a password, a salt, and a cost factor as inputs when generating a password hash. (C6)		✓	✓	916	5.1.1.2
2.4.2	Verify that the salt is at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes. For each credential, a unique salt value and the resulting hash SHALL be stored. (C6)		✓	✓	916	5.1.1.2
2.4.3	Verify that if PBKDF2 is used, the iteration count SHOULD be as large as verification server performance will allow, typically at least 100,000 iterations. (C6)		✓	✓	916	5.1.1.2
2.4.4	Verify that if bcrypt is used, the work factor SHOULD be as large as verification server performance will allow, with a minimum of 10. (C6)		✓	✓	916	5.1.1.2

Figure 6.6: ASVS example.

6.2.2 Design phase

Creating the design

After the requirements for the application were made, the design phase commenced. I started by sketching a bit on paper, before I moved on to a digital tool for designing interfaces; Figma. Some of the initial wireframes can be seen in figures 6.7, 6.8 and 6.9

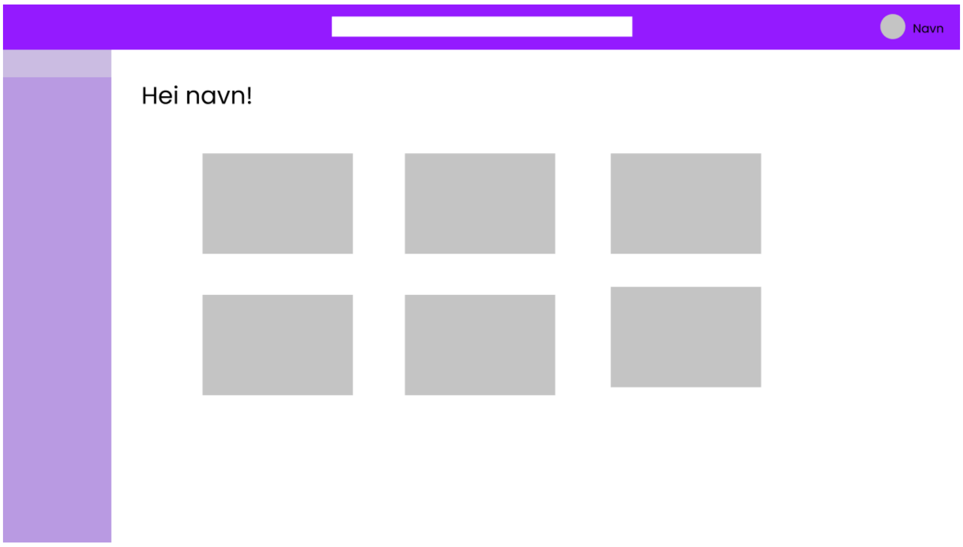


Figure 6.7: First wireframe

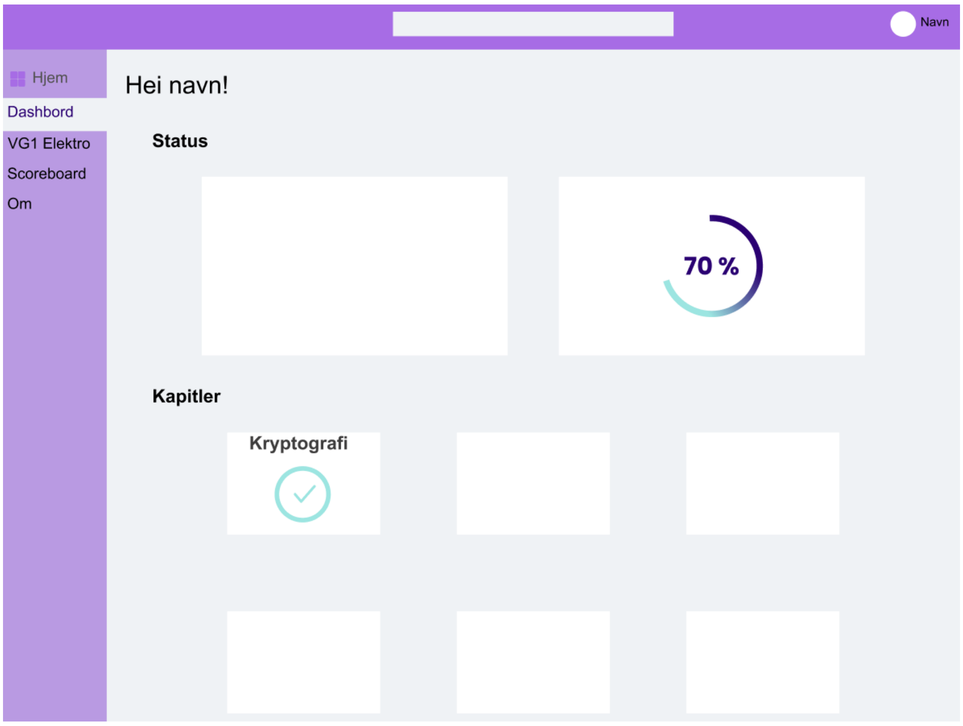


Figure 6.8: Second wireframe

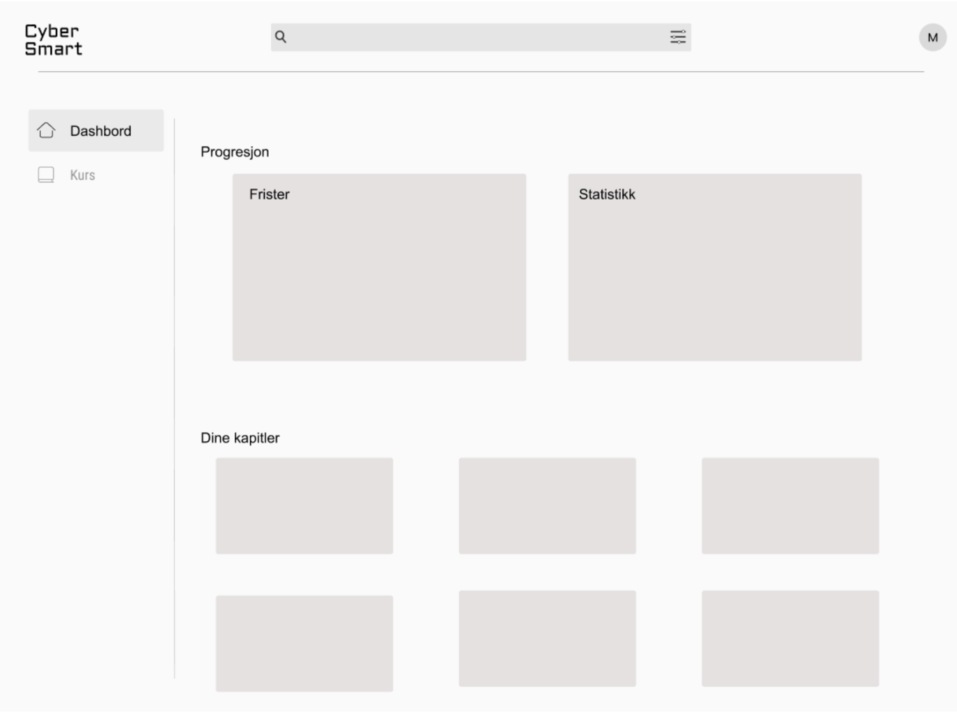


Figure 6.9: Latest wireframe

As you can see, I am by no means a designer, so this phase was quite challenging. I was aiming for a simple and modern design which would motivate the pupils to use the application. Exactly how successful I was in my task, is questionable. If this project is to be continued, I would recommend hiring a UX designer on the team.

Universal design

As this application is developed in Norway, it has to be universally designed. The essence of creating universal design is to create a solution that suits everyone, regardless of the disabilities they might have. In Norway, universal design has to be created following the WCAG 2.0 (soon to be 2.1) guideline on A and AA level, with the exception of the following principles: 1.2.3, 1.2.4, and 1.2.5 [26].

6.2.3 Development phase

The development phase lasted from February 2022 to April 2022, with the research and set-up of development environment being done from October 2021 to January 2022. The agile framework Kanban was used to structure the development phase, this development method was explained in chapter

3.2. I decided to develop using the Kanban method because I was very new to frontend and thus had to learn a new way of programming to be able to produce an application. My original plan was to create a full stack application, with a frontend, backend and a database, but I had to scrap this idea as learning a new framework took way too long. For most of the new functionalities I wanted to implement into the application hours was spent researching how to do it. The reason why the research took so long was because I was trying to develop a system that was not plagued with code that could lead to future technical debt, that could easily be handed over and used for further development. An example of a feature that was implemented to avoid future technical debt, was the ability to change language. If this was not implemented in the start of the development, then a lot of code would have to be changed.

After spending weeks on making sure the code I created was well coded and easy to read, I still did not really have anything visual to show. As this was supposed to be a demonstrative product, I had to change my focus on developing just the visuals in order to actually have something to show for. So, the remaining weeks of the development process were used on just developing functionality that was visual. In the end I managed to create a login page and a dashboard. My initial thought was to create a fully functional login page with authentication and an application with session management, but due to time constraints and the amount of time research took, I decided against it.

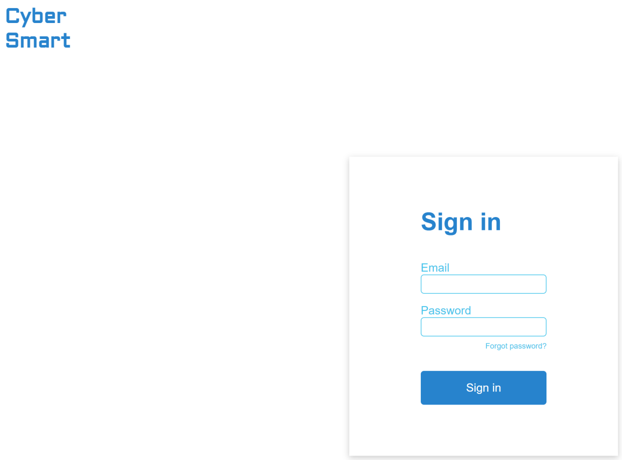


Figure 6.10: Screenshot of the developed login screen

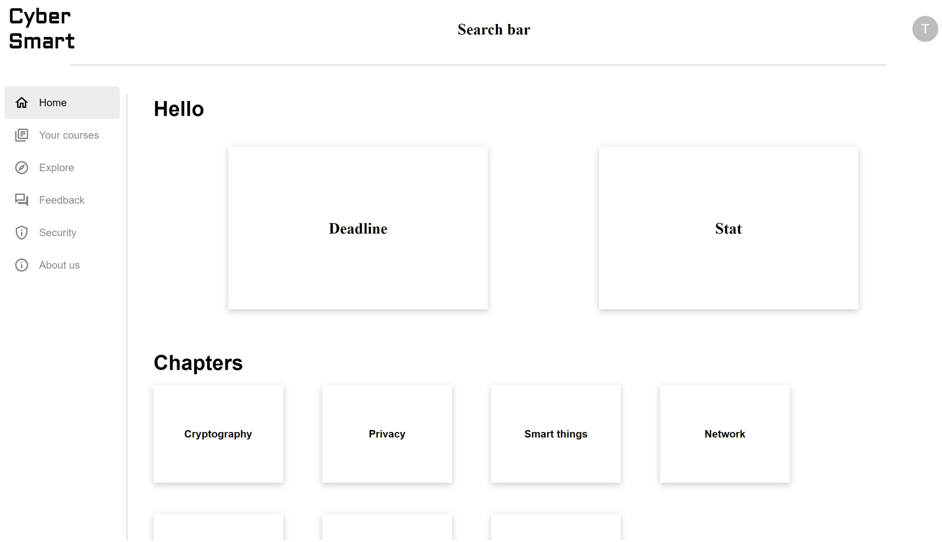


Figure 6.11: Screenshot of the dashboard from the application

Chapter 7

Discussion

The goal of this chapter is to discuss the results found during the course of this thesis. This includes looking at key findings, discussing these results and looking at the limitations of the methods and the results used and found in this thesis. As a reminder, we are focusing on the vocational education programme electrical engineering and computer technology, an education programme provied in upper secondary school. Without further ado, here is a recap of the research questions:

RQ1: What is the need for cyber security competencies within the vocational education programme electrical engineering and computer technology?

RQ2: What lessons learned can Norway benefit from other counties?

RQ3: How can information security be integrated into the educational programme electronic engineering and computer technology?

7.1 Key findings

To answer the first research question, RQ1, semi-structured interviews and literature research was used as research methods. Before the interviews were conducted, there was an attempt to solve RQ1 through looking at competence goals and the teaching material already existing for the education programme. As a recap, competence goals are goals that portray what knowledge the pupils should have after completing a specific subject.

In every year and all the different specialisation of electrical engineering and computer technology, the pupils will have one to three subjects that are specially created for the education programme and the specialisations. For instance, in year one the pupils have two specialised subjects; electronic circuitry and networks and energy and control systems. Of a total of 330 competence goals, 8 were cyber security related, and only a handful were useful in determining if there was a need for cyber security competence in the education programme.

Using the teaching materials provided for the education programme was not possible either, as they were all hiding behind a paywall that I was not able to breach. Thus, the only viable option would be to interview industry professionals and looking at existing research. In total I interviewed five participants from three different trades; two electricians, two locksmiths, and one lift fitter. In the interview with the lift fitter, they said that the lifts in Norway are very primitive and hardly any of them contain any smart products, systems or devices that communicate over the internet.

From the interviews I determined the following topics as interesting; privacy, smart home, internet of things (IoT) and industrial internet of things (IIoT), in addition to cryptography, basic virus theory, passwords, social media and internet hygiene. Exactly how these topics were derived can be found in chapter 4.

The second research question, RQ2 – what lessons can Norway learn from other country's cyber security programmes, literature research was the only research method used. The aim of this research question was to determine the best way for Norway to teach its population cyber security and inspire more people to pursue a career within the field. The cyber security programmes we looked at were GenCyber belonging to the US and CyberFirst belonging to the UK. As it turns out, Norway has much to learn, just not from any of these countries. Both programmes provided an activity during summertime, summer camps and courses. Through their approaches were a bit different, I would say the statistics provided about the success of each of the products indicate than none of them were a great success. Over a period of five years, GenCyber taught 15,545 pupils cyber security, but only 1,350 of them are pursuing a career in cyber security. There are about 331 million people living in the US [3] and a total of 597,767 job openings [14]. Adding an extra 1,350 new will not do that much, considering it accumulates to 0.23% of all job openings.

CyberFirst only provided statistics from one year of their summer courses (2019), but in this year, they had a total of 1,627 pupils where most of them were already interested in cyber security before even joining, with the majority of them portrayed an interest in further studies in cyber security. Now there are around 68.5 million people living in the UK [81]. with a about 100,000 vacant positions in cyber security [49]. If all the 1,627 people pursue a career, that would be 1.6% of all the job openings. Which is in fact much better than the results from GenCyber, but we do not know for sure if all of these pupils will pursue a cyber security career.

What was interesting with both GenCyber and CyberFirst though, was their different approaches to teaching cyber security in schools. The GenCyber programme provided summer camps for teachers, so that the teachers themselves could teach their pupils cyber security. Even though only 36.5% of the teachers who attended the summer courses actually did teach their kids cyber security, around 145,000 pupils were reached. Making this method a pretty decent one. In the UK, CyberFirst taught cyber security to pupils in school through an online course with three to four stages that the pupils had to progress through. Over the course of four years 115,712 pupils attended this course, which does sound like a great achievement. But there were some discrepancies, in my opinion, as only 26.4% of the pupils managed to go from stage one to stage two. That is only 30,547 people. Now it is hard to say whether this is a really bad thing, or just a bad thing, as we do not know the difficulty level of the stages, but one should think a stage called assessment would have a higher progression rate.

All in all, teaching pupils cyber security in school seems to work better than a summer camp type programme. And so, the Norwegian approach, in my opinion, should be to teach pupils cyber security in school. Introduce cyber security as part of subjects or its own subject already in Year 3 or 4, when the pupils start getting phones and join online forums. In the earlier years, the pupils should learn how to use the internet and digital devices in a safe way. The need to learn about the consequences of posting pictures and videos online, and they need to learn their rights when it comes to their personal information. When they get older, they should continue learning about privacy and safe online behaviour on a more in-depth level. An in-depth topic of safe online behaviour could for example be how viruses are obtained and how they spread. In addition, they should be introduced to topics such as cryptography, as cryptography is such a vital part of cyber security. Nothing in the online world would be safe without some form of cryptography.

The goal of the third research question, RQ3, was to figure out how cyber security should be integrated in the education programme electrical engineering and computer technology. To answer this question, we used literature research and the knowledge gained from the very same interviews conducted to answer RQ1. From RQ2 we learned that the Norwegian approach to teaching cyber security should probably be through some kind of teaching in school. Exactly what kind of solution we should integrate was discussed in chapter 6, and the answer we ended up with was through a web application. Some of the reasons for choosing a web application included that it was easier to implement larger practical assignments, that require more space than a mobile screen, it is an interactive application, a fun and interactive theoretical section is easier to implement, the web application can be made to work on a phone, and last but not least the free principle which states that pupils in upper secondary school have a right to receive free teaching materials, this including a PC [27]. This was kind of the tipping point as these pupils do not necessarily have access to a smartphone, at least not a smartphone with newer software than can run newer applications. So, the answer to how cyber security should be integrated into upper secondary education is through a web application.

7.2 Limitations

There are several limitations that need to be considered when looking at the results found in this thesis. First of all, when answering RQ1 – the need for competence, competence goals of the subjects related to the education programme was used. As the digital strategy for national security competence was introduced in 2019, the study on the programme might not have finished. Meaning that the amount of competence goals and the content of the existing once might change to accommodate the 2019 strategy. Another limitation was the amount of people who were interviewed. With such a low number of interviewees for so many different trades, we might not have gotten a full picture of where the competence is needed. Though, we did manage to establish that there is some need for competence in cyber security.

As for RQ2 – the lessons learned from other countries, the CyberFirst summer courses only had statistics from 2019, a year plagued with a global pandemic. Thus, the results of the evaluation might not have been representative for what the course actually can do. In addition, the response rates of both the evaluation of GenCyber and CyberFirst were decent but not great. Perhaps we would have gotten a different picture if there were more respondents.

When determining which platform should be used when integrating cyber security into the education programme electrical engineering and computer technology, my evaluation of each of the different platforms might have been biased as I derived the advantages and disadvantages of each platform myself.

My knowledge of the electrical engineering and computer technology domain was also limited. Perhaps more could have been gathered from the interview participants if my expertise on the subject was a bit better.

7.3 Further research

The research that remains to do is interviewing more people in the trades that were already interviewed, in addition to the remaining trades that there have been no interview participants from. As mentioned in chapter 3, I interviewed a total of five people: two electricians, two locksmiths and one lift fitter. The interviews with the locksmiths felt like they reached saturation level already by the second interview, as nothing new was presented. Thus, I would recommend interviewing another one or two people as this would ensure saturation was indeed reached by interview number two. As for the electricians, there was some overlapping information, but I would say there is still at least another three or four interviews to be conducted. I was only able to interview one lift fitter and thus cannot evaluate how many interviews need to be conducted to reach saturation.

As for the other trades, there are quite a few left that should be very interesting to interview in relation to cyber security. These trades are as follows:

- Avionics
- Aircraft engine mechanic
- Airframe mechanic
- Flight systems mechanic
- Control panel fitter

- Automation
- Computer electronics
- Maritime electrician
- Power-supply fitter
- Power-supply operation
- Telecommunications installation
- Refrigeration and heat pump
- Ventilation work

The rest of the trades did not look very interesting, initially. However, I believe interviewing at least one form each trade could not hurt. Perhaps there actually are some parts of the trade that do require security knowledge. If that should happen, the trade needs to be interviewed to the point a bit past saturation to ensure all data is collected.

One of the main struggles of this thesis was getting a hold of people. Thus, here are my recommendations for what gave me the possibility to interview five participants. Do not spend time emailing companies, call them

If you are unable to procure people through contact with companies, try trade associations or training offices

Find vacant positions who are searching for someone with the qualifications you are looking for and call the person responsible for the application process, if they are listed

When interviewing participants focus on understanding their work, as not many of them will be familiar with details of topics in cyber security. Understand what some of the trades common assignments are, what systems and devices they interact with and such. Ask questions regarding things that can be relevant for cyber security, such as industrial control systems; SCADA, DCS, and PLCs. Or if they are familiar with any IoT devices that are used in their trade. In addition, ask questions related to privacy, for instance do they handle customer data? Some of them are in fact self-taught on the topic of cyber security, so questions directly regarding cyber security should also be asked. For instance, do you know what cryptographic algorithms are used? How does the algorithm work?

7.4 Future development

There is still quite a bit of development left to do. We need to structure and integrate the cyber security courses. The authentication is still not possible. A backend and databases need to be developed.

There are also some things yet to be determined. For instance, are we creating a stand-alone platform or are we integrating the current code into an existing system? To answer this question some higher forces need to be involved, as there already exists too many digital teaching materials, and it is difficult for the pupils and teachers to keep track of them all.

In addition, we need to know how the cost of development and hosting should be covered. In April of 2022 I attended a meeting regarding a new strategy for digital competence and infrastructure hosted by the Norwegian Directorate for Education, where multiple different organisations spoke about what they wanted from this strategy. In this meeting, the president of the School Student Union of Norway talked about how important it was for new and existing products to be free of charge so as many schools as possible could take use of the products. They mentioned that they did not want these teaching materials to become “pay-to-win”, meaning no one should have to purchase the products in order to get the best possible learning outcome. Thus, I suggest this project should be non-profit and receive some backing from companies or the government.

The president of the School Student Union also mentioned that a lot of the digital teaching materials are outdated, which is why I suggest we get a UX designer onboard so our application can look fit for purpose. It could also be useful to have several more people on the research and programming.

Chapter 8

Conclusion

This chapter includes a very brief summary of the findings done in this thesis. If you want a more in-depth explanation of how we came to answer the research questions and the limitations of this thesis, go to chapter 7.

The goal of this thesis was to address the following research questions:

RQ1: What is the need for cyber security competences within the vocational education programme electrical engineering and computer technology?

RQ2: What lessons learned can Norway benefit from other counties?

RQ3: How can information security be integrated into the educational programme electrical engineering and computer technology?

When researching the first research question, RQ1, we found evidence that there would be need for cyber security competences in electrical engineering and computer technology, however there was not enough data to draw a strong conclusion.

As for the second research question, RQ2, we found that the approach that was likely going to suit Norway best, was by teaching cyber security in school.

There was good indications that developing an interactive web application would be the best way of answering research question three, RQ3.

Bibliography

[1] CyberFirst Academy. *Products*. Accessed 24.05.22 [Online]. URL: https://www.cyberfirstacademy.com/.

[2] Australian Cyber Security Centre. *ICT equipment*. Accessed 19.05.22 [Online]. URL: https://www.cyber.gov.au/acsc/view-all-content/glossary/ict-equipment.

[3] United States Census Bureau. 2021 [Online]. URL: https://www2.census.gov/programs-surveys/decennial/2020/data/apportionment/apportionment-2020-table01.pdf.

[4] Norwegian Business and Industry Security Council. *Mørketallsundersøkelsen 2020*. Tech. rep.

[5] C.dearnley. 'A reflection of the use of semi-structured interviews'. In: *Nurse Researcher* 13.1 (2005). ISSN: 1351-5578. URL: https://www.deepdyve.com/lp/royal-college-of-nursing-rcn/a-reflection-on-the-use-of-semi-structured-interviews-jdDEW0B0vO?.

[6] National Cyber Security Centre. Accessed 24.05.22 [Online]. URL: https://www.ncsc.gov.uk/files/CyberFirst-programme-pipeline-v3.pdf.

[7] National Cyber Security Centre. *Bursary and Degree Apprenticeship*. Accessed 29.05.22 [Online]. URL: https://www.ncsc.gov.uk/cyberfirst/bursary-and-degree-apprenticeship.

[8] National Cyber Security Centre. *CyberFirst courses*. Accessed 29.05.22 [Online]. URL: https://www.ncsc.gov.uk/cyberfirst/courses.

[9] National Cyber Security Centre. *CyberFirst Girls Competition*. Accessed 29.05.22 [Online]. URL: https://www.ncsc.gov.uk/cyberfirst/girls-competition.

[10] National Cyber Security Centre. *CyberFirst overview*. Accessed 29.05.22 [Online]. URL: https://www.ncsc.gov.uk/cyberfirst/overview.

[11] National Cyber Security Centre. *CyberFirst Schools/Colleges*. Accessed 29.05.22 [Online]. URL: https://www.ncsc.gov.uk/cyberfirst/cyberfirst-schools.

[12] G. Chiesa et al. 'Multisensor IoT Platform for Optimising IAQ Levels in Buildings through a Smart Ventilation System'. In: *Sustainability* 11.20 (2019). ISSN: 2071-1050. URL: https://www.mdpi.com/2071-1050/11/20/5777.

[13] Cisco. *Cisco Packet Tracer*. Accessed 28.05.22. URL: https://www.netacad.com/courses/packet-tracer.

[14] Cyber Seek. *Cybersecurity supply/demand heat map*. Accessed 24.05.22 [Online]. URL: https://www.cyberseek.org/heatmap.html.

[15] Cybertech girls. *Home*. URL: https://cybertechgirls.org/.

[16] H. Bickley D. Campbell-Jack and J. Lillis. *CyberFirst Evaluation*. 2021. URL: https://www.gov.uk/government/publications/independent-evaluations-of-cyber-discovery-and-cyberfirst-programmes/cyberfirst-evaluation.

[17] H. Bickley amd J. Lillis D. Campbell-Jack. *Cyber Discovery Evaluation*. 2021. URL: https://www.gov.uk/government/publications/independent-evaluations-of-cyber-discovery-and-cyberfirst-programmes/cyber-discovery-evaluation.

[18] M. Dark et al. *5-Year Evaluation*. Dark Enterprises, Inc. 2021. URL: https://www.gen-cyber.com/static/resources/GenCyber%5C%20Five%5C%20Year%5C%20Report.pdf.

[19] CVE Details. *Wordpress vulnerability statistics*. Accessed 24.05.22 [Online]. URL: https://www.cvedetails.com/product/4096/Wordpress-Wordpress.html?vendor_id=2337.

[20] Direktoratet for høyere utdanning og kompetanse. *Yrkebeskrivelse Automatiker*. 22.03.22 [Online]. URL: https://utdanning.no/yrker/beskrivelse/automatiker.

[21] Direktoratet for høyere utdanning og kompetanse. *Yrkebeskrivelse Låsesmed*. 22.03.22 [Online]. URL: https://utdanning.no/yrker/beskrivelse/lasesmed.

[22] Direktoratet for høyere utdanning og kompetanse. *Yrkesbeskrivelse Dataelektroniker*. Accessed 23.03.22 [Online]. URL: https://utdanning.no/yrker/beskrivelse/dataelektroniker.

[23] Direktoratet for høyere utdanning og kompetanse. *Yrkesbeskrivelse Kulde- og varmepumpetekniker*. Accessed 24.03.22 [Online]. URL: https://utdanning.no/yrker/beskrivelse/kulde-_og_varmepumpetekniker.

[24] Direktoratet for høyere utdanning og kompetanse. *Yrkesbeskrivelse Telekommunikasjonsmontør*. Accessed 24.03.22 [Online]. URL: https://utdanning.no/yrker/beskrivelse/telekommunikasjonsmontor.

[25] Direktoratet for høyere utdanning og kompetanse. *Yrkesbeskrivelse Ventilasjonstekniker*. Accessed 24.03.22 [Online]. URL: https://utdanning.no/yrker/beskrivelse/ventilasjonstekniker.

[26] Kommunal- og distriktsdepartementet. *Forskrift om universell utforming av informasjons- og kommunikasjonsteknologiske (IKT)-løsninger*. URL: https://lovdata.no/dokument/SF/forskrift/2013-06-21-732.

[27] Norwegian Directorate for Education and Training. *Gratisprinsippet i skolen*. Accessed 28.05.22 [Online]. URL: https://www.udir.no/regelverk-og-tilsyn/skole-og-opplaring/gratisprinsippet/videregaende-skole/lareboker--utstyr/?path=cehmkdicehmkdl.

[28] GenCyber. *General FAQs*. Accessed 18.01.22 [Online]. URL: https://www.gen-cyber.com/faq/.

[29] GenCyber. *Welcome to GenCyber*. Accessed 18.01.22 [Online]. URL: https://www.gen-cyber.com/about/.

[30] K. Hughes. *10 Web application builders for non-technical startup founders*. Accessed 28.05.22 [Online]. URL: https://www.karllhughes.com/posts/10-web-app-builders.

[31] IBM. *How Industry 4.0 technologies are changing manufacturing*. Accessed 19.05.22 [Online]. URL: https://www.ibm.com/topics/industry-4-0.

[32] Norsk Industri. *Læremidler innen Teknologi og industrifag*. Accessed 27.05.22 [Online]. URL: https://www.norskindustri.no/kurs-og-arrangementer/digitale-laremidler-vgs/digitale-laremidler-for-vgs/.

[33] SANS Institute. *Cyber Discovery*. Accessed 23.05.22 [Online]. URL: https://joincyberdiscovery.com/.

[34] *Internet of things. Oxford Lexico*. Accessed 21.05.22. URL: https://www.lexico.com/definition/internet_of_things.

[35] C. Jui-Sheng, H. Yu-Chien and L. Liang-Tse. ‘Smart meter monitoring and data mining techniques for predicting refrigeration system performance’. In: *Expert Systems with Applications* 41.5 (2014), pp. 2144–2156. ISSN: 0957-4174. URL: https://www.sciencedirect.com/science/article/pii/S0957417413007446.

[36] T. Ladabouche and S. LaFountain. *GenCyber: Inspiring the Next Generation of Cyber Stars*. 2016.

[37] B. Marshall et al. ‘Does Sample Size Matter in Qualitative Research? A Review of Qualitative Interviews in is Research’. In: *Computer Information Systems* 54.1 (2015). URL: https://www.tandfonline.com/doi/abs/10.1080/08874417.2013.11645667.

[38] M. Martin. guru99. Mar. 2022 [Online]. URL: https://www.guru99.com/difference-web-application-website.html.

[39] G. McGraw. *Risk Management Framework (RMF)*. Cigital. Sept. 2005 [Online]. URL: https://www.cisa.gov/uscert/bsi/articles/best-practices/risk-management/risk-management-framework-%28rmf%29.

[40] NHO Luftfart. *Ønsker du å jobbe med luftfartøyets struktur?* Accessed 22.03.22 [Online]. URL: https://www.nholuftfart.no/flyfag/flymekaniker/Flystrukturmekaniker/.

[41] NHO Luftfart. *Ønsker du en spennende jobb som flymotormekaniker?* Accessed 22.03.22 [Online]. URL: https://www.nholuftfart.no/flyfag/flymekaniker/flymotormekaniker/.

[42] NHO Luftfart. *Vil du bli flymekaniker med spesialisering innen reparasjoner og vedlikehold av de fleste av luftfartøyets systemer?* Accessed 22.03.22 [Online]. URL: https://www.nholuftfart.no/flyfag/flymekaniker/flysystemmekaniker/.

[43] NHO Luftfart. *Vil du jobbe med det elektriske anlegget og navigasjons- og kommunikasjonssystemene i et luftfartøy?* Accessed 22.03.22 [Online]. URL: https://www.nholuftfart.no/flyfag/flymekaniker/avioniker/.

[44] Nodejs. *About Node.js*. Accessed 28.05.22 [Online]. URL: https://nodejs.org/en/about/.

[45] NorSIS. *Årsrapport 2021*. Tech. rep. Studievegen 2, 2022.

[46] OWASP. *OWASP Application Security Verification Standard*. Accessed 29.05.22 [Online]. URL: https://owasp.org/www-project-application-security-verification-standard/.

[47] OWASP. *OWASP Top Ten*. Accessed 29.05.22 [Online]. URL: https://owasp.org/www-project-top-ten/.

[48] U. Pisuwala. *The benefits of ReactJS and reasons to choose it for your project*. Peerbits. Feb. 2022 [Online]. URL: https://www.peerbits.com/blog/reasons-to-choose-reactjs-for-your-web-development-project.html.

[49] Prospects. *Cyber security training*. Accessed 27.05.22 [Online]. URL: https://www.prospects.ac.uk/jobs-and-work-experience/job-sectors/information-technology/cyber-security-training.

[50] D. Radigan. *What is Kanban?* Accessed 22.05.22 [Online]. URL: https://www.atlassian.com/agile/kanban.

[51] Rhode Island College. *GenCyber Camp*. Accessed 18.01.22 [Online]. URL: https://www.ric.edu/gencyber-camp.

[52] M. Rice and S. Shenoi. 'Threat analysis of an elevator control system'. In: *Critical Infrastructure Protection XI*. Ed. by K. Rannenberg. Springer, 2017, pp. 175–176.

[53] K. Rose. 'Unstructured and semi-structured interviewing'. In: *Nurse Researcher* 1.3 (1994). ISSN: 1351-5578. URL: https://www.deepdyve.com/lp/royal-college-of-nursing-rcn/unstructured-and-semi-structured-interviewing-VRRfJt1BW5.

[54] H. Solbakken. *Sensitiv pasientinformasjon kan være på avveie etter dataangrep*. Jan. 2021 [Online]. URL: In%20nrk.no/innlandet/ostre-toten-kommune-angrepet-av-hackere-_-pasientinformasjon-og-helsedata-kan-vaere-pa-avveie-1.15321398.

[55] I. Sommerville. *Software Engineering Ninth Edition*. 9th. Massachusetts, USA: Pearson Education, 2011.

[56] Study in Norway. *Education*. Accessed 15.03.22 [Online]. URL: https://www.studyinnorway.no/living-in-norway/education.

[57] The Good Schools Guide". *Comparative ages, grades and exams - US vs UK*. Accessed 15.03.22 [Online]. URL: https://www.goodschoolsguide.co.uk/international/transitions/comparative-ages-grades-and-exams-US-vs-UK.

[58] The University of Alabama in Huntsville. *GenCyber Cybersecurity Summer Camps*. Accessed 18.01.22 [Online]. URL: https://www.uah.edu/ccre/camps.

[59] I. S. Tybring-Gjedde and I. Nybø. *Nasjonal strategi for digital sikkerhetskompetanse*. Ministry of Justice and Public Security, Oslo, Norway. 2019. URL: https://www.regjeringen.no/contentassets/8ed748d37e504a469874ce936551b4f8/nasjonal-strategi-for-digital-sikkerhetskompetanse.pdf.

[60] University of Washington. *GenCyber Virtual Camp 2022*. Accessed 18.01.22 [Online]. URL: https://gencyber.uwb.edu/.

[61] US Department of Energy. *The Smart Grid*. Accessed 19.05.22 [Online]. URL: https://www.smartgrid.gov/the_smart_grid/smart_grid.html.

[62] J. Uslenghi et al. 'IoT energy monitoring of a refrigeration installation'. In: (2020). URL: https://riunet.upv.es/bitstream/handle/10251/179820/UslenghiSapena-BanoPineda-Sanchez%5C%20-%5C%20IoT%5C%20energy%5C%20monitoring%5C%20of%5C%20a%5C%20refrigeration%5C%20installation.pdf?sequence=1&isAllowed=y.

[63] Utdanningsdirektoratet. *Læreplan for Vg2 dronefag*. Accessed 23.03.22 [Online]. URL: https://hoering.udir.no/Hoering/v2/1822.

[64] H. Venås and S. Vangsnes. *Elektroniske kretser og nettverk*. 1st ed. Elforlaget, 2021.

[65] Vigo. *Aeronautics*. Accessed 22.03.22 [Online]. URL: https://www.vilbli.no/en/en/no/electrical-engineering-and-computer-technology/program/v.el/v.elele1----_v.elfly2----_/p1#kursKolonne2.

[66] Vigo. *Automation*. Accessed 22.03.22 [Online]. URL: https://www.vilbli.no/en/en/no/electrical-engineering-and-computer-technology/program/v.el/v.elele1----_v.elaut2----_/p1#kursKolonne2.

[67] Vigo. *Computers and electronics*. Accessed 22.03.22 [Online]. URL: https://www.vilbli.no/en/en/no/electrical-engineering-and-computer-technology/program/v.el/v.elele1----_v.eldel2----_/p1#kursKolonne2.

[68] Vigo. *Dronefag*. Accessed 22.03.22 [Online]. URL: https://www.vilbli.no/en/en/no/electrical-engineering-and-computer-technology/program/v.el/v.elele1----_v.eldrf2----_/p1#kursKolonne2.

[69] Vigo. *Education programmes*. Accessed 21.01.22 [Online]. URL: https://www.vilbli.no/en/en/no.

[70] Vigo. *Electrical engineering and computer technology*. Accessed 21.02.22 [Online]. URL: https://www.vilbli.no/en/en/no/fag-og-timefordeling/program/v.el/v.elele1----/p2.

[71] Vigo. *Electrical power*. Accessed 22.03.22 [Online]. URL: https://www.vilbli.no/en/en/no/electrical-engineering-and-computer-technology/program/v.el/v.elele1----_v.elele2----_/p1#kursKolonne2.

[72] Vigo. *Refrigeration and ventilation*. Accessed 22.03.22 [Online]. URL: https://www.vilbli.no/en/en/no/electrical-engineering-and-computer-technology/program/v.el/v.elele1----_v.elkvv2----_/p1#kursKolonne2.

[73] vigo. *Læreplan for dataelektronikerfaget*. Accessed 30.05.22 [Online]. URL: https://vilbli.no/nb/nb/no/laereplan-for-installering-og-drift/ul/v.el/v.dat03-03.

[74] vigo. *Læreplan for datateknologi og elektronikk*. Accessed 30.05.22 [Online]. URL: https://www.vilbli.no/nb/nb/no/laereplan-for-data-og-informasjonsteknologi/ul/v.el/v.del02-03.

[75] vigo. *Læreplan for elektro og datateknologi*. Accessed 30.05.22 [Online]. URL: https://www.vilbli.no/nb/nb/no/laereplan-for-energi-og-styresystemer/ul/v.el/v.ele01-03.

[76] vigo. *Læreplan for elenergi og ekom*. Accessed 30.05.22 [Online]. URL: https://www.vilbli.no/nb/nb/no/laereplan-for-elenergi-og-styresystemer/ul/v.el/v.ele02-03.

[77] vigo. *Læreplan for maritim elektriker*. Accessed 30.05.22 [Online]. URL: https://www.vilbli.no/nb/nb/no/laereplan-for-elektronisk-kommunikasjon/ul/v.el/v.mel03-02.

[78] *What we do*. Accessed 26.05.22 [Online]. URL: https://www.ncsc.gov.uk/section/about-ncsc/what-we-do.

[79] L. S. Whiting. 'Semi-structured interviews: guidance for novice researchers'. In: *Nursing Standard* 22.23 (2008). ISSN: 0029-6570. URL: https://www.deepdyve.com/lp/royal-college-of-nursing-rcn/semi-structured-interviews-guidance-for-novice-researchers-wbVDV0sckU.

[80] Worldometer. *Norway Population*. Accessed 28.05.22 [Online]. URL: https://www.worldometers.info/world-population/norway-population/.

[81] Worldometer. *U.K. Population*. Accessed 28.05.22 [Online]. URL: https://www.worldometers.info/world-population/uk-population/.

Appendices

Appendix A

Consent form

Masteroppgave i informasjonssikkerhet (samtykkeskjema)

Prosjektleder: Marie Wilhelmsen (mail: mariwilh@ifi.uio.no, tlf. 46613349)

Institusjon: Universitetet i Oslo, Institutt for informatikk

Bakgrunn og formål

Vår hverdag blir mer og mer preget av digitale verktøy. Med disse verktøyene har vi blitt mer tilgjengelige enn noen gang. Det positive er at vi kan enklere opprettholde kontakt med kjente og kjære verden rundt, men det negative er at vi er nå mye mer tilgjengelige for personer vi ikke ønsker å ha noe å gjøre med. Cyberangrep har blitt et emne man hører om ofte, og det er noe som skjer daglig i norske bedrifter. Den enkleste inngangsdøren til en bedrifts interne systemer er arbeidere som ikke kan noe særlig om cybersikkerhet. Vi kan ikke lengre være avhengige av at sikkerhetseksperter skal ta seg av all jobben, det norske folk må bli bedre rustet til å takle sårbare situasjoner.

I dette masterprosjektet skal jeg jobbe med å gi videregående elever på linjen “Elektro og datateknologi en verktøykasse som kan hjelpe de både i arbeidslivet og på hjemmebasis. Jeg skal først kartlegge om det faktisk finnes et behov i arbeidsmarkedet for slik opplæring, og så skal jeg konstruere en opplæringsplattform som kan lære opp elevene i de ulike momentene i cybersikkerhet som jeg mener de burde ha kompetanse i, basert på kartleggingsprosessen.

Hvorfor får du spørsmål om å delta?

Du blir invitert til å delta på intervju fordi jeg mener at akkurat du sitter på verdifull informasjon som kan hjelpe meg med kartleggingsprosessen.

Hva innebærer det for deg å delta?

Deltakelsen vil komme i form av et intervju. Under intervjuet vil enten video og/eller stemme bli tatt opp. Det kan hende jeg har behov for mer informasjon, da vil jeg eventuelt invitere til et oppfølgingsintervju eller stille oppfølgingsspørsmål via mail.

Hva skjer med informasjonen om deg?

Informasjonen om deg og eventuelle opptak av deg vil bli lagret på en sikker server, eid og driftet av Universitetet i Oslo. Det er kun prosjektleder Marie Wilhelmsen som har tilgang på disse opplysningene. Ingen persondata vil bli brukt i selve rapporten (med mindre dette er noe du ønsker selv), kun fakta du kommer med under intervju / oppfølgingsspørsmål på mail vil potensielt ende opp i ferdig rapport. Alle opplysninger om deg vil bli slettet etter endt studie, juni 2022.

Du har rett til innsyn i hvilke opplysninger som er lagret om deg, i tillegg har du rett til å korrigere eventuelle feil i opplysningene som er registrerte. Du har også rett til å få opplysninger om deg slettet (dette kan du gjøre ved å trekke ditt samtykke, se “Det er frivillig å delta”).

Skulle du ønske å se hva slags opplysninger som er lagret om deg i forbindelse med dette prosjektet, kan du sende en mail til prosjektleder Marie Wilhelmsen.

Du kan klage på behandling av dine opplysninger til Datatilsynet og institusjonens personvernombud (personvernombud@uio.no).

Det er frivillig å delta

Det er frivillig å delta og du kan trekke ditt samtykke når som helst uten å oppgi en grunn. Dersom du trekker tilbake ditt samtykke vil alle opplysninger om deg bli slettet. Du kan trekke tilbake ditt samtykke ved å sende en mail til prosjektleder. Du samtykker til å delta i prosjektet ved å skrive under på dette dokumentet.

Avslutning:

Dersom du har noen spørsmål angående prosjektet eller du skulle ønske å trekke ditt samtykke kan du sende en mail til mariwilh@ifi.uio.no eller ringe meg på 46613349.

Ved å signere under, godkjenner du at jeg kan behandle dine persondata på en sikker måte, samt at fakta du kommer med under intervju / oppfølgingsspørsmål på mail kan ende opp i ferdig rapport.

______________________________ ______________________________

Deltaker Prosjektleder

Dato for signatur: ________________

Appendix B

Interview guide

Intervjuguide fagfolk

Fase 1: Oppvarming

- Uformell prat
- Informasjon
    - Temaet for samtalen (bakgrunn og formål)
    - Hva skal intervjuet brukes til? Anonymitet i ferdig oppgave
    - Spørsmål fra respondent
    - Informer om samtykke, eventuelt om opptak (video/taleopptak)
    - Start eventuelt opptak

Fase 2: Respondents faglige bakgrunn

- Hvor mye erfaring har du med å være <stilling>?
- Hvordan ble du endte du opp med å jobbe med dette?
    - Motivasjon
    - Utdanning
- Hvordan ser en vanlig arbeidsdag ut?

Fase 3: Hoveddel

Nøkkelspørsmål: (Ikke nødvendigvis gjengitt i denne rekkefølgen)

- Oppfølgingsspørsmål til en vanlig arbeidsdag
    - Hvilke systemer interagerer du med?
        - Har dere noen systemer dere er avhengige av i hverdagen?
        - Hva gjør dere om noen av disse systemene er nede?
- Hva lærte du på skolen som du har hatt mest nytte av i arbeidslivet?
    - Er det noe du skulle ønske du lærte mer om før du startet i arbeidslivet?
- Har du hørt om begrepet cybersikkerhet?
    - Hva legger du i begrepet?
    - Har du noen gang opplevd noe du relaterer til dette begrepet?
    - Er det noe du skulle ønske du visste mer om?
    - Tror du det hadde det vært nyttig å lære om cybersikkerhet i skolen?

Fase 4: Oppsummering og avslutning

- Oppsummering av funn gjort i intervjuet
- Er det noe respondenten ønsker å legge til?
- Gjenta viktige deler med samtykke; hvordan trekke seg fra prosjektet etc.
- Takk for intervjuet