Master's thesis

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

Karianne Kjønås

How cyber security incidents can affect Norwegian food production

Master's thesis in Master in Information Security
Supervisor: Gaute Wangen
June 2023

NTNU
Norwegian University of
Science and Technology

Karianne Kjønås

How cyber security incidents can affect Norwegian food production

Master's thesis in Master in Information Security
Supervisor: Gaute Wangen
June 2023

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

NTNU
Norwegian University of
Science and Technology

Acknowledgements

Thank you to my supervisor Gaute Wangen for giving great advice and helping me both with the master thesis and all the work beforehand. Your continuous excitement over the topic and my findings has been great for keeping me motivated throughout the whole process. Thank you to all those who participated in the interviews and took time out of their day to help me. This thesis would not have happened without you. Thank you also to those who helped in the process of gathering interview participants.

Abstract

Cyber security in agriculture is becoming more important from a social security perspective because food supply can be targeted. The use of technology within agriculture has increased over the years, which leads to a rise in vulnerabilities in farm systems. The goal of this research is to discover how cyber attacks can impact food production on Norwegian farms. This research was conducted through 14 one-on-one interviews with cattle and pig farmers in Norway, and two service technicians from the two different milking robot brands used by the dairy farmers. The results are a case study of which technologies are used on Norwegian cattle and pig farms, and a risk assessment in relation to these technologies. The results show that dairy cow farms are critically dependent only on the milking robot for production, the pig farms are heavily dependent on the feeding systems, and the suckler cow farms can still continue production mostly as normal without technology. The risk scenarios identified during the interviews are mostly centered around availability, and some on integrity. None are related to confidentiality because there is very little data that is confidential on these types of farms. Infecting milking robots or feeding systems with computer viruses, or performing denial of service attacks on farmhouse networks are not difficult attacks for a cyber criminal or state actor to perform, and these can impact the individual farms' ability to produce their products. Threat actors looking to impact food production on a national scale might look more at farm suppliers like Felleskøpet and Norsvin, data processors like Animalia, and the market regulators of meat and dairy, Nortura and Tine, because attacks on this level can have consequences for farms throughout the country. Organizations such as Felleskjøpet, Nortura and Tine are crucial for Norwegian cattle and pig farms, which is why further research into their role in the supply chain and their vulnerabilities should be prioritized, in order to fully understand how much a serious cyber attack on one of these organizations can impact Norwegian food production.

Sammendrag

Cybersikkerhet i landbruket blir mer og mer viktig fra et samfunnsikkerhetsperspektiv fordi matforsyningen kan være et mål for nasjonale trusler. Bruken av teknologi i landbruket har økt med årene, som fører til en økning i sårbarheter i gårdssystemer. Målet med denne forskningen er å oppdage hvordan cyberangrep kan påvirke matproduksjon på norske gårder. Forskningen ble gjennomført gjennom 14 en-til-en intervjuer med norske ku- og grisebønder, og to service teknikere fra de to melkerobot merkene som brukes av melkekyrbøndene. Resultatet er et casestudie om hvilke teknologier som brukes av norske ku- og grisebønder, og en risikovurdering knyttet til disse teknologiene. Resultatet viser at melkekyrgårder er kritisk avhengige av melkeroboten for produksjon, grisebøndene er sterkt avhengig av foringssystemene, mens ammekyrbøndene kan produsere nesten som normalt uten teknologi. Risikoscenariene identifisert gjennom intervjuene er først og fremst relatert til tilgjengelighet, men også noen relatert til integritet. Ingen av riskioscenariene går på konfidensialitet, fordi det er veldig lite data som er konfidensiell på disse gårdstypene. Infisering av melkeroboten eller foringssystemer for gris med datavirus, eller tjenestenektangrep mot fjøsnettverk er ikke angrep som er vanskelig for en nettkriminell eller statlig aktør å gjennomføre, og disse type angrep kan påvirke de individuelle gårdenes evne til å produsere deres produkt. Trusselaktører som ønsker å påvirke matproduksjonen på et nasjonal nivå ser kanskje mer mot gårdleverandører som Felleskjøpet og Norsvin, dataprosesserere som Animalia, og markedsregulatorene for melk og kjøtt, Tine og Nortura, fordi angrep på dette nivået kan ha konsekvenser for gårder i hele landet. Organisasjoner som Felleskjøpet, Nortura og Tine er kritiske for norske ku- og grisegårder, og videre forskning på deres rolle i leverandørkjeden og sårbarheter er derfor viktig å prioritere, for å virkelig forstå hvor mye et seriøst cyberangrep på en av disse organisasjonene kan påvirke norsk matproduksjon.

Contents

Figures

Tables

Chapter 1

Introduction

1.1 Topic covered by the project

Cyber security in agriculture is becoming more important from a social security perspective because food supply can targeted. According to NSM in their risk 2022 report, state actors have an interest in targeting the food supply chain, but cyber criminals and activist are also potential threats [1].

The agricultural sector uses a lot of technology in their day-to-day operations [2]. Technological solutions are a part of many different aspects, such as water management, crop fertigation, livestock monitoring and e-commerce to name a few [2, 3]. Internet of Things (IoT) sensors are placed all around the farm and can also be used for specialized tasks such as detecting plant illness, or they can be placed on equipment such as tractors and drones [4]. The use of technology has also increased in recent years along with the rise of smart farming and precision agriculture [5].

Smart farming is a technological concept within agriculture where big data and IoT devices are used to perform tasks on the farm and improve the agricultural process [2]. Precision agriculture is a more specialized concept where tools are used to increase granularity of decision making in order to improve the efficiency of input use though IoT-based approaches [5]. Precision agriculture allows the farmer to tailor crop management within one square meter or for individual plants. Both smart farming and precision agriculture are a part of the fourth agricultural revolution [6]. The agricultural revolutions follows the industrial revolutions on the evolution from traditional agriculture using human and animal resources all the way to the smart agriculture methods used today [6].

1.2 Keywords

Security, Agriculture, Automation, Technology, Risk analysis, Threat assessment, Farming

1.3 Problem description

The increase in technology leads to a rise in vulnerabilities in the farm systems. Because the dependency on these technologies has increased, the potential consequence of a cyber attack has also escalated. This makes it even more important to be aware of the biggest threats to agriculture technology in the case of the risk owner. Additionally, NSM, in their risk 2022 report, specify the need for an overview of assets, supply chains and dependencies in order to implement the correct protective measures against state threat actors [1].

The issue is further complicated by the fact that different types of farms use different systems in their production. Some use more technology than others, and how reliant the different farmers are on the different technologies will also vary, both between the different types of productions, but also between the farms that produce the same product. In order to gain a full overview of their specific needs and limitations, each type of farm needs to be analyzed.

A literary review of cyber security within agriculture research papers revealed several gaps in the research [7]. Topics such as threats and vulnerabilities in the technology was covered quite well, but research into farmers' knowledge and perspectives, as well as their technological dependencies is lacking. The consequences of potential incidents are discussed in terms of confidentiality, integrity and availability (CIA), but the practical implications of such a consequence is not discussed [5]. For example, Gupta et al. mention that a denial of service (DoS) attack will lead to loss of availability, but does not discuss how this may affect the farmer [8]. A full risk assessment that considers the consequences for the farmer and the likelihood of cyber attacks is not present in the research, even though some of the components of a risk assessment are.

If the attack is performed on a system the farmer is not heavily dependent on, the practical consequence of the attack is lower than if an integral component is attacked in the same way. How much the farmer relies on the technology will influence the consequence more than the scope of the attack. Understanding which technologies are more critical for production is integral in order to perform a complete risk assessment and understand the practical consequences of a potential attack.

1.4 Justification, motivation and benefits

Knowing the consequences for farmers in different attack scenarios can give a clearer view of the true threats to Norwegian agriculture technology. Understanding the threats to one of the main components of the supply chain can highlight what threats are important to protect against from a societal point of view. The attack on the food production company Nortura in December of 2021 illustrates some of the consequences of a cyber attack in the supply chain, and what these types of attacks can mean for consumers [1, 9].

In order to understand the resource needs within cyber security and knowing what security aspects to put resources into, the risks at the base of the supply chain must be understood. Highlighting the need for cyber security in agriculture is also important to get the government to understand the importance of attack prevention or consequence reducing activities.

1.5 Research questions

In order to find the societal consequences of cyber attacks to agriculture technology, the first step is to look at what technologies are used by farmers today, and mapping the dependency on them. While there are multiple avenues for researching this topic, such as looking at specific farm production systems in detail, or looking at the technological dependencies of the whole supply chain, this research will focus on the farm in general. Examining multiple farms, their use of technology and reliance on suppliers will give insight into what kind of damage a cyber attack can do. In order to understand the consequences of a cyber attack, the focus does not need to be on all the technologies that are used, so much as how reliant the farmer is on the technology. However, it might be easier to miss certain dependencies unless there is a clear understanding of what technologies are used, and so this also needs to be part of the research. Cattle and pig farms are the chosen types in this research because of their role in the Norwegian food production. This leads to three research questions.

- *What technologies are used by Norwegian cattle and pig farmers to produce and deliver their produce?*
- *What are the main cyber risks to the production and delivery of produce on these Norwegian farms?*
- *How can a threat exploit the vulnerabilities of individual farms to affect food production on a national scale?*

1.6 Summary of contributions

The master thesis will provide first a mapping of the technological dependencies of Norwegian farms, in terms of which technologies are used the most, and which are most important for production. Further, the master thesis will do a risk analysis in order to give an overview of the main threats to Norwegian agriculture with specific focus on what attacks to confidentiality, integrity and availability can lead to on pig and cattle farms. Lastly, there will be a discussion on which of the identified risks can be used on a national scale to affect food production in Norway. At the end of the discussion comes the suggestion of future work, both in terms of doing the same research on other farm types, and other research opportunities within the same sector.

1.7 Report structure

This thesis is split into five chapters, the first being this introduction. This chapter introduces the topic, and highlights why there is a need for this research. Chapter 2 is the theory chapter, where information that is relevant in order to understand the topic and perform the research analysis is presented. Chapter 3 presents the methodology used, both which research methodology was chosen and why, and how the method was applied. Chapter 4 contains the results of the research, a case study and a risk assessment. The last chapter, chapter 5 is the discussion, where the research questions are answered and discussed, and the limitations and recommendations for future work is presented.

Chapter 2

Theory

This chapter starts by describing smart farming, its development over time, and how it is used on farms today. It then moves on to describe farming in Norway in terms of production and farm sizes, and how these have changed over time, and describe some important parts of the supply chain. These two sections are important to understand the basics of modern farming, and the specifics of farming in Norway today. The next section goes into detail on technological vulnerabilities and potential attack scenarios for different technologies that are used on farms. Last is a state of the art analysis, where different research articles that looks at cyber security in agriculture are described, to show why this research is necessary.

2.1 Smart Farming

Smart farming is about using software and hardware solutions to improve the work and outcome on a farm [10]. What types of technologies used can vary greatly, but technologies such as sensors, IoT, machine learning, artificial intelligence and unmanned vehicles are often associated with the smart farming term [2, 11]. A lot of farm systems and productions can be run, monitored and optimized using these processes, such as precise weeding and spraying of pesticides only when needed [11].

Farming technology has changed a lot over the years, from traditional manual labor to the technological solutions of modern agriculture [6]. According to Ferrag, Shu, Friha and Yang, the agriculture sector has developed along with the industrial revolution, which is split into four separate revolutions. From ancient times until the middle of the 20th century, farmers used indigenous tools and and manual labor. The techniques and practices have evolved over time, such as crop rotation, but the tools have stayed unmotorized [11].

The first industrial revolution brought the steam-based mechanical production, and contributed to the move from an agriculture based society into a manufacturing based society with new emerging industries such as textile and steel [12]. The

late 19th century and early 20th century brought the second industrial revolution, and electricity and electrical mass-based production. In agriculture, this meant a transition from manual and animal labor into the use of powered machinery [6]. The third industrial revolution spans the mid 20th century to the early 21st, according to Taiwo and Vezi-Magigaba, and is defined by the use of automation by means of electronics and information technology [12]. The third revolution introduced the use of information technology in agriculture, but its range of capabilities were not fully realized until the fourth agricultural revolution where big data, artificial intelligence, unmanned vehicles and Internet of Things are in use [6].

Unmanned farms has emerged as a new production mode which does not require human labor to perform production activities, where everything is run by a collection of technologies such as IoT, AI, fifth generation technology (5G), robots and big data [13]. Sensors and IoT devices collect data, which is then analyzed and processed using Big Data and AI technologies, which generate a production plan and then instructs the robots on what to do. Not all farming is going to become unmanned yet, but some of these automated and analytical technologies are in use today, such as smart collars for cows and sheep that can track fertility cycles and detect health problems, and alert the farmer on when insemination should be performed, and if a cow shows early signs of sickness.

Among the unmanned farm technologies mentioned by Wang et al. is also precision feeding, where the amount of feed given to the animals is precisely calculated based on need and production optimization [13]. The milking robot is also among the unmanned farm technologies, where each cow has specific settings in relation to the robot in terms of udder placement, typical flow rate and expected milk quality. Barn ventilation has also become more automatic, where sensors for temperature and humidity can be used to adjust ventilation automatically as needed and process pollutants in the air [14]. According to Kim and Lee, proper ventilation can significantly impact livestock productivity, and can be detrimental to livestock health.

2.2 Farming in Norway

In 2021, there were 38 076 farms in Norway, according to Statistics Norway [15]. The amount of farms in Norway has been steadily decreasing since 1979 when there were 125 302 farms, however, the amount of small farms is much lower now than before. In 1979, there were 62 017 farms with less than 50 acres of land, and in 2021 this number was down to 5 460. There are also a lot more larger farms today, with 5 031 farms with over 500 acres of land in 2021 compared to 709 in 1979. Figure 2.1 shows a comparison of the amount of farms in different size categories over the years. The most common size of a farm in 2021 was between 100 and 199 acres.

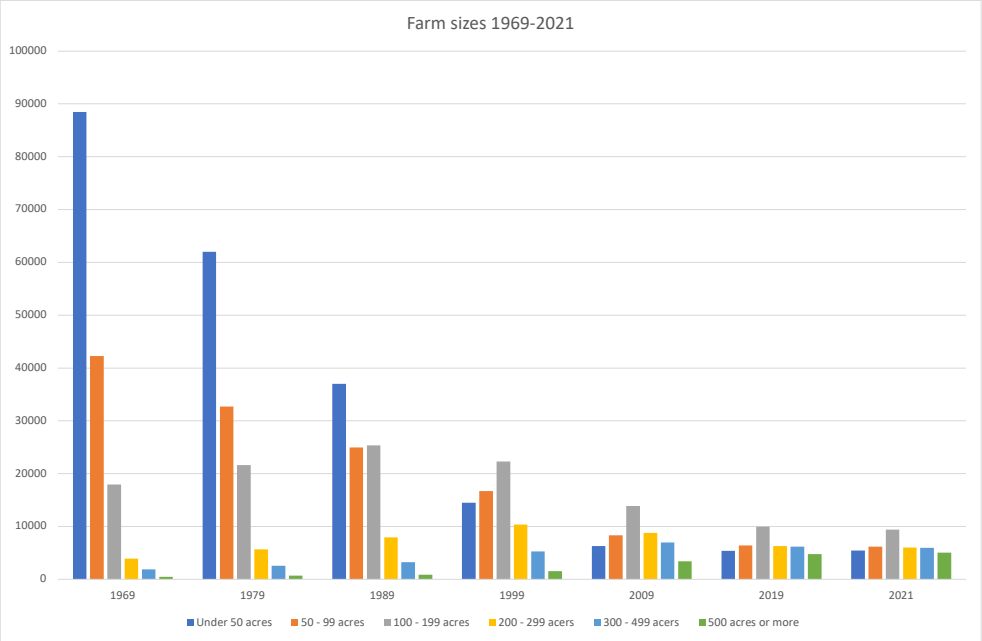


Figure 2.1: The change in farm size from 1969 to 2021. Data from Statistics Norway [15]

The are more animal farms than plant producing farms in Norway today. In 2020, there where 11 421 plant producing farms, 23 636 milk and meat producing farms and 1 451 that produce both animal and plant products [15]. Meat production has increased drastically in Norway from 1950 until more recent years [16]. The largest increase happened up until 1984 because of the agricultural revolution which improved the efficiency of the farmers. This also meant that less people were needed to work on the farms, and over time this has led to a significant reduction in the amount of employees on each farm, even though the size of the farms have increased.

In 2005, the work efficiency per person had increased by more than eightfold compared to 1950, which can be attributed to new knowledge and new technology [16]. This increase in efficiency meant that smaller farms had less to gain because they have less potential to expand, and the investment in newer technology was more profitable for the larger farms as they had the opportunity to increase production much more. Increased production of meat and vegetables is also a sign of growing affluence in society.

What types of meats that are produced and how much of each has changed over time is shown in figure 2.2, with chicken having the highest increase. The figure shows the amount of livestock in Norway over time separated into type of animal.

There is a break in the line for meat chickens in 2001 because the data is missing for that year. As the figure demonstrates, cattle and pigs have an even production throughout the years with only a small increase for pigs and a small decrease for cattle. The production of hens have also not fluctuated too much, but has a steady increase until it peaked in 2019. The chicken production has increased dramatically over the years and does fluctuate a lot more between years.

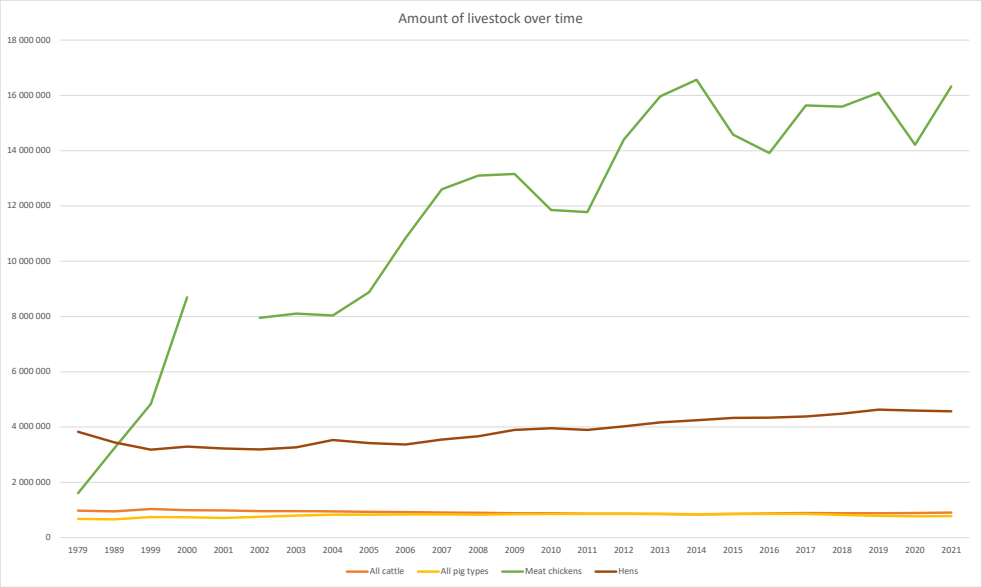


Figure 2.2: The amount of livestock types from 1979 to 2021. Data from Statistics Norway [17]

Pig is the most produced type of meat today with 134 799 tons produced in Norway in 2021 [18]. Chicken was the second most produced type of meat with 105 893 tons, and cattle is third with 87 731 tons of meat produced in 2021. In 2020, the milk farmers were paid on average 5,96 NOK per liter milk they sold [18]. As the market regulator within dairy production, Tine is bound by duty to collect milk from all the farmers in Norway that needs milk collected [19]. There are other dairies in Norway that collects milk form farmers, such as Q-meieriene, but these are smaller companies that collect from specific farms they have a deal with [20].

Tine is a cooperation, and is owned by 9000 farmers throughout the country [19]. In addition to producing and selling their own milk and dairy products, they are responsible for supplying other dairy product producers, such as Rørosmeieriene and Synnøve Finden with milk for their production. Similarly to Tine, the food production company Nortura is a cooperation, and is Norway's largest supplier of meat and eggs [21]. The company is owned by about 17 000 farmers, and is most known for its two brands Gilde, which sells red meat, and Prior, which deals

with poultry and eggs [22]. Their core business activities are the slaughter, cutting and redistribution of meat and eggs, and are, similarly to Tine, bound by duty to accept meat from all registered farms in Norway [23].

2.3 Technological vulnerabilities and attack scenarios

Because of the technological development and the increase in demand for food, farms will have to adapt to the technological advancements and increase their use of technology [24]. The traditional technologies that were used on farms are no longer capable of meeting the production demand [25]. IoT technologies are integrated into the agriculture systems to increase quality and quantity of the farm products [25].

The premise of IoT is that everything is available at all times, and in industrial systems especially, connected together [26, 27]. For agriculture, IoT devices such as sensors are heavily used for livestock safety and monitoring, crop monitoring, water management, and a lot of other operations [2]. The problem with IoT is that ensuring security and privacy becomes quite difficult, as these issues must be ensured for the whole IoT system at once, and not just for one device [27].

A large network of IoT devices can have a big attack surface [28]. An attack surface can be defined as 'the set of ways in which an adversary can enter the system and potentially cause damage.' [29]. In IoT devices, there are nine main attack surfaces identified [28]:

1. **Administrative interface:** All the means of getting access through the administrative web interface of the system.
2. **Device web interface:** Encompass the web application vulnerabilities of the web interface of the IoT device and the ways to gain access through the credential management of the interface.
3. **Cloud web interface:** The vulnerabilities of the IoT cloud components, such as the standard web application vulnerabilities, lack of two-factor authentication, credential management and transport encryption.
4. **Mobile application:** The vulnerabilities of the mobile application connected to the IoT device. Encompass the vulnerabilities of mobile applications such as username enumeration, account lockout, weak passwords and not using encryption.
5. **Device network services:** The vulnerabilities present in the network services, which can lead to attacks such as DoS, MITM, buffer overflow and malware injections.
6. **Update mechanism:** The ways the attacker can gain access by exploiting vulnerabilities in the update mechanisms of a system.
7. **Device physical interfaces:** The ways of gaining access through the physical interface of the IoT device, often through an unauthorized physical con-

nection.

8. **Device firmware:** The IoT device firmware vulnerabilities that can be exploited through for example backdoor accounts, exposed keys, and other vulnerable services.
9. **Local data storage:** The ways in which the data storage can be compromised, for example through lack of encryption or lack of integrity checks.

This increase in use of technologies means more systems to attack, which contributes to a problem that is already widespread [30]. There are a lot of different ways to attack the different technological systems on a farm, such as attacking equipment, networks, the data storage, and the supply chain [8]. Table 2.1 and 2.2 lists different attack types that can be performed on agriculture technology and describes briefly what they entail.

Attack type	**Description**
	Data attacks
Insider data leakage	Disgruntled employee leaks confidential information to outsiders [8].
Cloud data leakage	Data stored on servers in other countries can have lower security requirements or be intercepted by the foreign government [8].
False data injection	The attacker changes/falsifies data that is relevant to decision making, such as changing moisture level in soil which will lead to either overwatering or underwatering, which damages the crop [8].
Misconfiguration	Configure smart farming reporting systems in a way that reports inaccurate data to farmer [5].
Misinformation	False report about the farm is published, mimicking an actual report, with data that shows for example a disease among the livestock [8].
Ransomware	Encrypts files or entire systems with key and demands ransom money to disclose decryption key [5].
	Application attacks
Software update attacks	Disrupting the software update process or inject vulnerabilities into the patch [5].
Malware injection	Inject malware into a smart device connected to the network to propagate to as many devices as possible [8].
Buffer overflow	Insert code that overwhelms buffer, giving attacker access to system without proper authentication [5].
Indirect attacks	Insert SQL code in input fields to trick database into for example giving access or changing data [5].

Table 2.1: Attack scenarios

Attack type	**Description**
	Attacks on the Network and Related Equipment
Denial of Service	Exhausting network/device resources to disrupt the running of systems [5].
Man in the Middle (MITM)	Observe and potentially modify traffic going through the network [5]
Botnets	Infect IoT devices on farms to be part of a botnet used to attack other entities [8].
Side Channel attack	Gathers information on how a system is implemented and uses these to attack, such as analyzing voltage usage [5].
Radio Frequency Jamming	Jamming radio frequencies to disrupt systems that rely on global navigation satellite systems (GNSS) [8].
Password cracking	Cracking the Wi-Fi password of a network to gain access to data and systems [25].
Evil twin access point	Set up a rouge access point for devices to connect to in order to gain access to the devices [25].
Spoofing attacks	Spoofing DNS and ARP records to gain access to network traffic in order to intercept and/or manipulate responses [25].
Key reinstallation attacks	Trick the victim into installing a key again that is already in use in order to gain access to the network and replay, decrypt or forge packets [25].
	Supply Chain Attacks
Third party attacks	Attack third party and infiltrate network through third party access to system [5].
Data fabrication	Misuse accesses given for different purpose to create malicious data [5].
	Misuse attacks
Cyber terrorism	Attack agricultural systems to create fear [8].
Compliance and regulation	Inject false data into systems so that farm products no longer pass inspection/certification [8].

Table 2.2: Attack scenarios

2.4 State of the art analysis

In this section, different research articles within the area of cyber security and agriculture are presented. All the articles have done research specifically on cyber security within the agriculture sector, and can be separated into three main cat-

egories. First is those that have done research on a more managerial level, such as the knowledge and perspectives of the farmers and common practices. The second category is those that examine technical security aspects, such as demonstrating specific attacks or implementing security monitoring solutions. The last category encompass all those that focus on threats, vulnerabilities and attack scenarios for agriculture technologies.

Farmer knowledge and perspectives

Nikander et al. examines six dairy farms in Finland to study cyber security capabilities of individual farms in their paper 'Requirements for cybersecurity in agricultural communication networks' [31]. The LAN of the farms is examined in detail, and the farmers are interviewed about their opinions and understanding of agricultural cyber security. The result of the research was that they identified several cyber security problems with the LAN, and the interviews revealed a conceptual understanding of the importance of cyber security, but a low priority in practice.

The paper 'Cyber security on the farm: an assessment of cyber security practices in the United States agriculture industry' written by Geil et al. works to discover perceptions of cyber security, and how age, gender and education might affect these perspectives [32]. Sending out a survey built using the Health Belief Model, the researchers looked at perceived susceptibility, severity, benefits, barriers, self-efficacy, cues to action and levels of previous cyber-crime victimization and technology implementation. The results show that individuals working in agriculture can be impacted by computer crime incidents. The research also revealed that education had no effect on the choice to implement protective measures, and neither the farms size or respondent role had an effect on the adaption of computer security technology. They did find that those who had been previously impacted by a security incident were more likely to have higher levels of computer security.

Technical security aspects

In their paper 'Wireless sensor network in agriculture: Model of cyber security', Prodanovíc et al. propose a general data security model for wireless sensor networks on farms [33]. The sensors gather a lot of data that require a security mechanism to protect against adversaries. The paper analyses data security from the source to the end-user. The proposed security model is independent from communications infrastructure and is proved efficient in preventing attacks in a simulated scenario.

'Performance of machine learning-based multi-model voting ensemble methods for network threat detection in agriculture 4.0' by Peppes et al. first looks at related work within the topics of network traffic monitoring and threat classifica-

tion in relation to agriculture 4.0 application and technologies [34]. The first, and main, objective of the research paper is to present and evaluate a hard voting and soft voting ensemble model using five different machine learning classifiers such as Decision Trees and Support Vector Classification (SVC). The machine learning classifiers chosen are all suitable for network attack classification. The individual machine learning classifiers' results are compared, before a new line for research work that evaluate ensemble models in the context of network traffic classifiers in relation to agriculture 4.0 data sets is suggested.

In their paper 'Deep learning-based intrusion detection for Distributed Denial of Service attack in agriculture 4.0', from the MDPI electronics journal, Ferrag and Shu, along with two others, propose three deep-learning based Intrusion Detection System (IDS) models [35]. One neural network based, one deep neural network based, and one recurrent neural network based. These three deep learing modes are reviewed by studying their performance with binary and multiclass classification types, with focus on false alarm rate (FAR), precision, F-score, detection rate (DR), recall, True Negative Rate (TNR), False Accept Rate (FAR), Receiver Operating Characteristic (ROC) curve and accuracy.

The paper 'Security and privacy for green IoT-based agriculture: Review, blockchain solutions and challenges' by Ferrag, Shu, Yang and other researchers begins by summarizing existing surveys on smart agriculture [36]. They describe a four-tier green IoT-based architecture, which is used to classify threat models into five categories. Further, they review security and privacy solutions for IoT applications, analyze the privacy oriented blockchain-based solutions for IoT applications, and provide consensus algorithms for blockchain-based solutions, and look at how all of these will be adapted for green IoT-based agriculture. Lastly, they discuss solutions to the security and privacy challenges in agriculture.

Chaganti et al., in their paper 'Blockchain-based cloud enabled security monitoring using Internet of Things in smart agriculture', present a security monitoring framework for smart farms by implementing a prototype that can monitor device status and sensor anomalies effectively [37]. The framework can also mitigate security attacks using behavioral patterns, and they propose a community-based solution to update security alerts to neighboring farmers. The proposed architecture and prototype is evaluated to show that the network latency of the solution is negligible. Lastly, they discuss the proposed solution, and comment on future work.

Vangala et al. perform a literary review to identify the use of blockchain technology to provide information security in their paper 'Smart secure sensing for IoT-based agriculture: Blockchain perspective' [38]. The paper specifies the need for IoT technology and its applications in agriculture, before identifying security issues and requirements. They then propose a generalized blockchain-based se-

curity architecture, and perform a comparative analysis on existing schemes to uncover drawbacks in existing research. Finally, they present identified open issues and possible directions for future research.

Threats, vulnerabilities and attack scenarios

Ferrag, along with Shu and Yang have written multiple articles on cyber security in agriculture technology. In 2021, they, along with Friha, wrote a paper for IEEE on 'Cyber security Intrusion Detection for agriculture 4.0: Machine learning-based solutions, datasets and future direction' [6]. In this paper, they present cyber security threats in agriculture 4.0 categorized by CIA, and IDS evaluation metrics categorized into security based metrics and performance based metrics. They review and analyze IDS for emerging technologies in agriculture, and provide the IDS building process for agriculture 4.0. Lastly, they made implementation frameworks applicable to the IDS performance evaluation for agriculture 4.0.

In their paper 'Smart farming: Cyber security challenges', Barreto and Amaral highlight reflections regarding security challenges in smart farming using an empirical methodology [2]. They also present smart farming applications, and an overview of the security threats and challenges that the use of smart farming poses and the major security threats.

Duncan et al. have published the paper 'Cyberbiosecurity: A new perspective on protecting US food and agricultural systems', where they identify important features in broad food and agricultural production and food systems using the food safety management Hazard Analysis Critical Control Point system concept [39]. The paper explores cyber biosecurity from food production to the end product user, and consider how the integration of different levels in the supply chain such as transportation, suppliers and retailer networks can have an effect. They found that a multidisciplinary approach using expertise in agriculture, food, engineering, computer science and cyber security is needed to fill the gap in awareness, knowledge, adoption, and plans and strategies evaluations related to cyber biosecurity.

'Survey on security threats in agricultural IoT and smart farming' written by Demestichas et al. gives an overview of the main existing and potential threats to modern agriculture through a literature review on the use of Information and Communications (ICT) solutions [40]. They offer a detailed approach on cyber security and IoT related threats categorized into equipment and data vulnerabilities, cyber crime, and IoT vulnerabilities. Lastly, they summarize some of the research on mitigation measures identified during the literature review.

The paper 'Security assessment of agriculture IoT (AIoT) applications' by Kristen et al. identifies cyber vulnerabilities in agriculture trough the application of a cy-

ber security assessment process [41]. The chosen assessment model is originally made for Industrial Automation Control Systems (IACS), but has been adapted to Agriculture Automation Control Systems (AACS). In the article, they discuss initial recommendations for addressing the identified cyber vulnerabilities, along with the need for a separate cyber security standard for AACS.

Yang et al. looks at three typical development modes in agriculture in their paper 'A survey on smart agriculture: Development modes, technologies, and security and privacy challenges', and looks at security and privacy countermeasures within this [42]. The paper also looks at key technologies within smart agriculture and the applications for some of these technologies. From there, security challenges are identified. Lastly, future trends and opportunities are summarized, before security issues based on the modes, technologies and applications are discussed.

In their paper 'Security and privacy in smart farming: Challenges and opportunities', Gupta et al. provides an overview of a smart farming multi layered architecture, with focus on IoT and Cyber Physical Systems (CPS), where entry points are highlighted, as well as the communication across the layers [8]. Next, the paper looks at security and privacy in the smart farming domain, before looking at possible attacks in the ecosystem. The researchers have performed a state of the art analysis, and discuss open research challenges for improving security and privacy.

Yazdinejad et al., in their paper 'A review on security of smart farming and precision agriculture: Security aspects, attacks, threats, and countermeasures', first itemize security aspects for smart farming and precision agriculture and then study the security aspects that are violated by state of the art attacks so that they can map the attacks to the security aspects [5]. They then present a taxonomy based on the relation between cyber attacks and the stages of the Cyber-Kill Chain (CKC), and review risk mitigation strategies and countermeasures to threats to the security aspects. Further, they go deeper into Advanced Persistent Threats (APTs) by analyzing their anatomy and behavioral characteristics. Lastly, they have developed a road map for further study within security in smart farming and precision agriculture.

The paper 'Cyber attacks on smart farming infrastructure' by Sontowski et al. demonstrates a Denial of Service attack on a smart farming ecosystem by attacking deployed sensors in the field, which will hinder functionality on the smart farm [25]. Before demonstrating a specific attack, they discuss various types of attacks that are possible to perform on the network domain of a smart farm. The result of the demonstrated attack is presented, along with the use cases of such an attack. At the end, the researchers provide defense strategies against deathentication attacks before discussing future work.

De Araujo Zanella, da Silva and Abina first review smart agriculture and the archi-

tecture used by most systems in their paper 'Security challenges to smart agriculture: current state, key issues and future directions [24]. This review revealed four layers in the architecture, which are used to present major security threats. Further on, they summarize the current state of intelligent agriculture applications by analyzing smart agriculture projects. Lastly, they present key challenges within the topic of security challenges in smart agriculture, and point to future directions.

In the paper 'A prediction model framework for cyber-attacks to precision agriculture technologies' Jason West address the specific security challenges of precision agriculture and mobile computing, and data driven decision making in food production [43]. The paper provides a risk-based framework to counter this, that takes sacrifices of efficiency and production effectiveness into consideration. The framework is then tested against network traffic and vulnerability characteristics of the system, and is considered to give appropriate protection without compromising the efficiencies that precision agriculture provides.

Summary of state of the art analysis

As discussed in the literary review 'A survey on cyber security research in the field of agriculture technology', there are several areas where research is lacking or missing entirely [7]. Within the category of farmers' knowledge and perspectives, there is very little research, which means that empirical data on this level is missing. There are more research in the technical category, but it is not representative and does not cover the topic area well, because of the sheer amount of different agriculture technologies available. The specific infrastructures used in each of the research articles vary, and if a solution works for one type of set up, it might not work for others.

Of the three categories, the last one is where most of the research is focused. Research into threats and vulnerabilities is more general, and these results can therefore be representative for a lot of the agriculture sector. What the category is missing in terms of research is a merger of all the different aspects, and a conclusion on what these threats and vulnerabilities can lead to for the farmer. A systematic risk assessment is not present in the research, and so the practical consequence of the presented attack scenarios is not considered.

Chapter 3

Method

This chapter first describes benefits with both qualitative and quantitative research methods, before concluding on which type fits the research goals better. The project limitations are discussed in order to decide which qualitative research method is best suited for the different research question. After the choice of method is made, the applied method is presented.

3.1 Choice of Method

The first step when deciding on which research method to use, is to consider what we are trying to figure out through the research questions. With the chosen research questions, the focus is on getting an overview of the situation on Norwegian cattle and pig farms. For the first research question about what technologies are used, there needs to be several data sources, and not only one. For the other research questions, several data sources are needed, but the information needed is detailed, can take some time to gather, and can be difficult to obtain using more generalized research methods.

The first choice of method is to decide between a qualitative and quantitative study. The benefit of using quantitative research methods would be to get a more generalized results that can describe a situation as it is [44], and include several data sources. However, the goal of this research is to get a more in depth understanding of the many dimensions and layers of the subject, which is something that qualitative research methods is better at capturing.

According to Leedy and Ormrod in the book 'Practical research: planning and design', another difference between qualitative and quantitative methods is that quantitative methods often follow a waterfall model, where data collection comes first and then the analysis afterwards, whilst qualitative research methods allows for a more iterative process [44]. Moving back and fourth between data collection and data analysis can benefit the data collection phase because the researcher can

use the knowledge obtained from the first data subjects to gather even more relevant information from the later data subjects. On the basis of what the goal of this research is, which is to discover which types of technologies are used and how reliant the farmer is on them, the easiest way of gathering this information is to talk to the farmers directly. This points towards a qualitiative research method.

Project limitations

When choosing a research method, the requirements and limitations of the research project must be considered. The method should be decided based on what type of information is needed, for example if more statistics is needed, or there is a lack of empirical data. As mentioned in the summary of the state of the art analysis in chapter 2, there is a lack of empirical data and focus on the practical consequence for the farmer in case of a cyber attack. It is important to gather general insights and experience the field to understand what areas will need further study, and statistics gathered empirically gives great insight into the current situation. Therefore, the focus of this research project is to gather empirical data.

The main limitations for this research project are time and resources. The time frame is set to five months, from January until June. Writing the master thesis is individual work, and therefore the amount of people working on the project is one. Another resource limitation is contacts within the industry. Contacts will need to be gathered as part of the research process, and how many contacts that can be gathered is therefore dependent on the people contacted. This further supports the use of a qualitative research method, as fewer participants are needed for qualitative research.

Qualitative research method options

Leedy and Ormrod describe five common design methods for qualitative research [44]. The first is a case study, where an individual or situation is studied in depth over time. If two or more cases are studied, it is called a multiple or collective case study. Case studies are good for understanding situations you do not know a lot about, for example mapping dependencies of technologies on farms.

The downside of case studies are that the results cannot necessarily be generalized. A second research design is ethnography, where a group that shares a common culture is studied. Ethnography is done over several months or even years, where the goal is to identify norms, beliefs and other cultural patterns. If the goal of this research was to study the behaviors or beliefs of farmers, this could be quite useful, but that is not the goal of this research.

The third common method is a phenomenological study, where the researchers try to understand a situation from the data subjects' perspectives. The study is often conducted through unstructured interviews where the researcher works together with the participants to find the answers. Unstructured interviews fits well for research problems where getting the full answer is not very easy and may take time and consideration to obtain, for example getting a full understanding of the consequence of a cyber attack on a farm.

The fourth option is a grounded theory study where the researchers starts with data and then develops a theory, rather than having a theoretical framework and collecting data based on that. This research design fits well when existing theories on the subject are lacking or inadequate, and the important factor is that the subjects' perspectives must be included in the data collected.

The last of the five common design methods is a content analysis. This type of study typically focuses on examining forms of human communications such as books, newspapers, journals, music, films, art and more in order to identify patterns, themes or biases. The purpose of a content analysis is to identify the specific characteristics of a body of material. These types of studies can often be combined with a quantitative study in some way, for example counting the frequency of certain characteristics observed in the data.

Chosen method

To answer the first research question described in section 1.5, a case study is the chosen method. A case study can use interviews and/or appropriate documents to understand a situation in great depth, and is therefore fitting when trying to map the use of technologies on different farms. This method could also be considered when trying to answer the other research questions, but a phenomenological study can fit even better in those cases.

The farmers' experience and knowledge will affect their dependency on a technology, which in turn will affect the consequence of a potential cyber attack, and is therefore important to include in the collected data. The experienced consequence will also be somewhat subjective as different farmers can have different economical backgrounds and other differences that leads to variations in acceptable risk levels, and a phenomenological study can help capture these differences.

The unstructured characteristic of the interview can be helpful to answer all three research questions, as the goal is not to answer many specific questions, but rather answer one open question as thoroughly as possible. Therefore, the second and third research questions that looks at consequences of cyber attacks will be answered using a phenomenological study.

When using different research designs for the two questions, keeping the methods separate is not entirely obtainable, so there will be some interlapping between the methods. There will not be held separate interviews for the different methods, so the case study will also be conducted through unstructured interviews, but the data analysis and presentation will be more separate. Leedy and Ormrod recommends Creswell's data analysis spiral for the data analysis, because it can be helpful when figuring out how to proceed with qualitative data analysis [44].

3.2 Applied Method

Figure 3.1 is a flow chart showing the different steps of the research process. The green box, the literary review, was not a part of this research project, as it was performed beforehand. The first step of this research project was to choose which method to use, which the above section describes. The next step is the interviews, the planning, recruitment and execution, before the data is analyzed. The interview process and the data analysis are marked as an iterative process, because data analysis was performed during the interview process, and temporary findings were used to further the interview process. The last step is describing the results, which consists of a case study and the risk assessment.

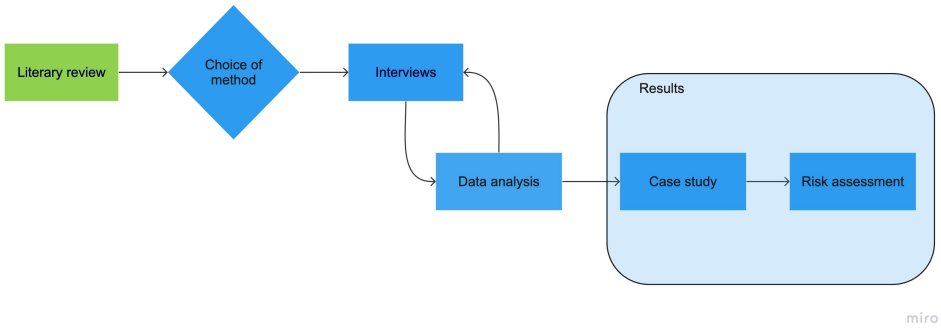


Figure 3.1: Flow chart of applied method

Preparing for interviews

According to Leedy and Ormrod, it is important to determine the interview questions beforehand also for unstructured interviews [44]. The less formal feel of this type of interview can lead to valuable insights, but for research purposes, it is important to have comparable results and not have answers to several different questions from different people. If the questions are planned beforehand, it is easier to end the interview with comprehensive answers to the questions that are needed to answer the research questions. Other questions can be asked during the interview, but they should contribute towards answering the planned questions.

Leedy and Ormrod also recommend to only have a few interview questions, and relate them to the research questions to make the analysis easier.

The first step in preparing the interviews was to decide on the research questions, and then figure out what questions were needed to answer the research questions. Table 3.1 lists the research questions and the interview questions related to each of them. When a set of interview questions was found, a trial interview was performed. This interview was conducted with a farmer that also had experience with technological equipment in many different areas of farming, and the interview was also an opportunity to ask questions about different types of farms and get more basic knowledge on typical processes on a farm. The interview also gave insight into how the study could be communicated in a good way, such as making sure the interview participants knew that no knowledge about cyber security was necessary to participate in the interviews.

Research question	**Interview question**
What technologies are used by Norwegian cattle and pig farmers to produce and deliver their produce?	Which technologies are in use on your farm?
What are the main cyber risks to the production and delivery of produce on these Norwegian farms?	For each technology, what is the consequence if it became unavailable? For each technology, what is the consequence if data in the system is not correct? For each technology, what is the consequence if data from the system became available for others? Where you affected by the cyber attack on Nortura? If yes, in what way?
How can a threat exploit the vulnerabilities of individual farms to affect food production on a national scale?	

Table 3.1: Research questions with corresponding interview questions

Recruiting interview participants

In 2021 there were 38 076 farms in Norway according to Statistics Norway [15]. Scoping the interview participants is important when there are so many possibilities. The first round of scoping removed all farms that did not produce food, as critical functions in society is an overarching theme for this project. The next round of scoping eliminated farms that did not work with animals, as there are

more animal farms than plant producing farms in Norway [15].

According to Statistics Norway, there were 23 636 milk and meat producing farms in 2020, spread over multiple different types of meat and milk. The scope was set to two different types of animals in order to research each more in depth, compared to interviewing more types of farms with fewer participants for each. Cattle was chosen as Norway was 98 % self sufficient for milk and milk products in 2022, and pigs were chosen as that was the most produced type of meat in 2022 [18].

Interviews

After the interview questions were determined, potential participants were contacted. Gathering contacts for interview participation was done through a few different means. First of, the existing contact network was contacted to see if they knew any farmers who fit the scope of the study. This yielded some contacts. The next step was to communicate more directly with farmer related organizations, such as contacting Norsk Bondelag [1] and their county offices to see if they knew anyone who could participate. This yielded another set of contacts, and some recommendations of other organizations to contact that could help both to understand more of some of the technologies used by farmers, but also give recommendations for farmers to contact for interviews. Contacting the organizations that produced some of the equipment used on the farms yielded contacts that knew more technical details about the equipment, as well as regular contacts to farms that used that organization's equipment.

When contact information for a potential interview participant was obtained, an email was sent out with basic information about the topic, goal and duration of the interview. In the beginning, interviews were expected to take up to one hour, but after several interviews were performed, the estimated time was reduced to 45 minutes. In cases where an email was not available, the person was called. If the call went unanswered, a text message was sent to explain the purpose of the call so they could call back if they so wished. The main medium used to perform the interviews was Microsoft Teams as this solution is available through NTNU, but some were conducted over the phone in cases where the participant preferred this. Before the interview, the participant was sent the interview questions so they could prepare if they wished to.

Before the interviews over Teams officially began, the participant was asked if audio recording of the session was permitted, and if not, notes were to be taken during the interview. This was also done for most interviews conducted over the phone, but some were performed in a setting where recording was not possible, and notes were taken during the interview instead in these scenarios. The parti-

[1] Website: https://www.bondelaget.no/

cipants were first asked if they wanted to know more about the goal of the research before the interview began. They were also asked if they had any questions before the interview officially began. If the participant said yes to recording, they were asked on tape to confirm that they gave permission to record.

The interview participant was asked the first question to start, and were allowed to talk freely about the topic. Whenever they were done answering the questions, follow up questions were asked to gather the necessary details. Which follow up questions were asked depended on what the participant said, and when they were interviewed. The first interviews were longer and more general, and the participants were asked more clarifying questions than ones about specific details. As the data collected was analyzed along the way, it became clearer which details where needed to perform the case study and risk assessment.

Data analysis

The data analysis was performed mainly using Creswell's data analysis spiral [44]. Leedy and Omrod recommend this process because while data analysis is a iterative process, the analysis must move foreward at some point to the later stages, and a spiral is good for this purpose. The method consists of four steps that are repeated several times until the data analysis is complete. Figure 3.2 shows the steps taken, the first being organization. The data is organized in a fashion that suits the project, either in a database, folders or otherwise. For this project, the files were uploaded into Nvivo, a qualitative study analysis tool, and labeled according to type of farm [45]. Nvivo was chosen because it is a powerful analysis tool that is available for all NTNU students to use.

The second step in Creswell's data analysis spiral is perusal, where the entire dataset is perused to get an overview, and figure out potential categories, note down thoughts and comments in general. The third step is classification, where the data is sorted into subcategories and coded. The fourth step is synthesis, where the data is integrated and summarized for readers. The data can also be organized into hypotheses, diagrams and figures. In the first round, the data units are large and general, and subcategories and codes are more general, but as you progress through the spiral multiple times, the data is broken into smaller units, and the classification codes become more specific. There will also be more data to present for each iteration of the spiral.

Because all the interviews had to be transcribed, it took quite a while to gather and organize the whole dataset. Therefore, the analysis began before all the data was available, and in order to progress as needed, the data analysis began during the data collection phase. The spiral was followed using the data currently available, and repeated whenever new data was added to the set.

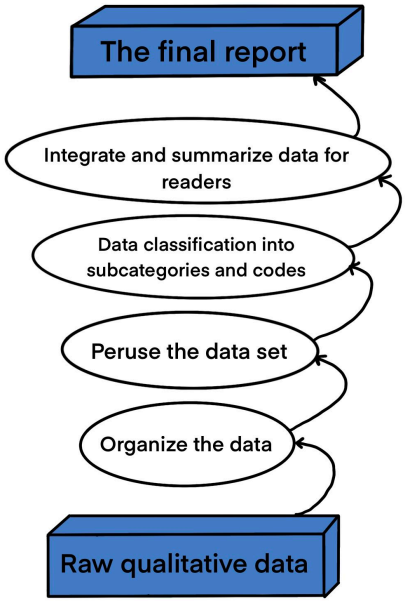


Figure 3.2: Creswell's data analysis spiral. Based on the figure by Leedy and Ormrod [44]

Risk assessment

There are many different risk assessment method to chose from, such as NIST SP800-30, FAIR and ISO 27005 [46]. All have their strengths and weaknesses, but the ISO 27005 standard was chosen in this case for its high level approach and objectives focus, which makes it adaptable to most sectors and situations, including agriculture [47]. It is also technology neutral, and is easier to use for small organizations such as farms because it has comprehensive example lists instead of questionnaires that are not as versatile, and do not rely as heavily on metrics to conduct the analysis.

The ISO 27005 standard describes two main approaches to risk assessments, an event-based approach and an asset-based approach [47]. The event-based approach identifies risk sources, and formulates risk scenarios from that, whilst the asset-based approach evaluates assets, threats and vulnerabilities to formulate risks. The asset-based approach was chosen as it can identify asset specific threats, and the bottom-up approach is more feasible when working with multiple small businesses and not one big one.

The first step of the asset-based approach is to identify assets, and then establish the value of the asset in terms of confidentiality, integrity and availability. Table 3.2 lists four levels of consequence for each of them, with a description of what

that consequence level entails. The levels are decided based on the information collected during the interviews. The specific times set for the availability levels do vary for the different farms, so the exact number of hours might not be correct for everyone. The number of hours can therefore be considered and approximation that illustrates the urgency of the unavailability.

Level	**Confidentiality**	**Description**
1	Public	No consequence for stature and public trust
2	Internal	Little consequence to stature and public trust
3	Confidential	Some consequence to stature and public trust
4	Strictly confidential	Critical consequence for stature and public trust
	Integrity	**Description**
1	No requirements	No consequence for traceability and ability to produce and deliver produce
2	Expected	Little consequence for traceability and ability to produce and deliver produce
3	Dependent	Some consequence for traceability and ability to produce and deliver produce
4	Critical	Critical consequence for traceability and ability to produce and deliver produce
	Availability	**Description**
1	2 weeks	Only consequence for operations if unavailable for a long time.
2	24 hours	Is necessary for operations, but can go without for some time.
3	12 hours	Will affect operations if unavailable for some time
4	3 hours	Critical consequence for operations if unavailable

Table 3.2: CIA consequence

The next step is to identify threats to the assets. The ISO 27005 standard presents a long list of example threats that can be relevant for an organization [47]. In the 'Information Security Risk Assessment Toolkit' book by Talabis and Martin, the threat actions are connected to a threat agent to give a bit more detail [46]. The threat actions are therefore connected to a threat agent in this study to get an insight into who or what could be the cause of damage to the farmers' assets. ISO 27005 also gives a list with examples of vulnerabilities, sorted into categor-

ies. This list was used as inspiration for determining relevant vulnerabilities, and which categories they belong to.

In addition to describing threat actions, the threat agents' capability and capacity is determined in order to decide the likelihood of a threat performing a threat action. The capability of the threat actor is, according to Wangen et al. their know how and ability, whilst the capacity is the resources of the threat actor [48]. Other characteristics of the threat agent, such as motivation, intention, breach type and willingness to attack is not considered here, as these can differ depending on the scope. The motivation and willingness to attack of a state actor can be quite different when looking at each farm individually compared to attacks on a larger scale that will affect multiple farms simultaneously. As this study considers both the individual farms and the national context, choosing one scope is not pertinent.

To determine the risk score, the likelihood of the risk is considered. The categories of likelihood should be unambiguous, and should be scaled into ranges that fit the situation, according to ISO 27005 [47]. However, the scope and limitations of this project is different from a risk analysis within an organization, and the likelihood is therefore determined in a different way. Based on previous knowledge and the data obtained during the interviews, the likelihood is categorized into an ordinal scale, based on how likely it is for the threat actor to be able to exploit the vulnerability at present. Table 3.3 shows the determined likelihood levels.

Level	Likelihood	Description
1	Very unlikely	Very unlikely that threat actor will be able to exploit vulnerability
2	Unlikely	Unlikely that threat actor will be able to exploit vulnerability
3	Likely	Likely that threat actor will be able to exploit vulnerability
4	Very likely	Very likely that threat actor will be able to exploit vulnerability

Table 3.3: Levels of likelihood

In the risk evaluation in chapter 4, the identified risks are described with a general description of the scenario, which threat actor(s) could exploit the vulnerability, which asset is at risk, and the total risk score, which is made up of the likelihood score multiplied by the consequence score. The risks are then placed into a risk matrix, to illustrate the criticality of each risk compared to the others.

Chapter 4

Results

This chapter presents all the the results of the research project. First the demographics are presented, where the different interview participants are described with information about their type, size and location. Then, the results of the case study is described, before the risk assessment is performed, with the asset, threat, and vulnerability assessment that creates the foundation for the risk evaluation.

4.1 Demographics

In total, 14 farmers were interviewed about their use of technology on the farm. Of these, eight were dairy farms, two were suckler cow farms, and four were pig farms. The 14 farms are described in table 4.1 by type of farm, the county the farms is located in, and information related to the size of the farm. The amount of animals on the farm is an approximation in most cases, as it is affected by several factors. How many animals, and to some extent the amount of diary cows, is affected by the calving season. Some farms plan to have calves at certain times of the years, whilst others have calves spread throughout the year. Therefore, the capacity of the milking tank is included for the dairy farms to give a more precise picture.

There are five different counties represented in the study. Innlandet county is represented most heavily due to the fact that the university I am attending is located in this county. The people contacted over email were informed of the university location, and some therefore recommended farmers in the area. Additionally, several of the people I reached out to personally are from the area, and therefore know more local farmers.

In addition to the 14 farmers, two service technicians related to dairy farm technology was interviewed. The two were from each of the largest milking robot manufacturers, and were interviewed to get a better insight into the technologies, how they perform service on the machines, vulnerabilities, and some insight into the data collected by the organizations they work for.

Interview	Type	Location	Size
1	Dairy farm	Trøndelag	2000 liters 40 dairy cows - 80 young cows
2	Dairy farm	Innlandet	6000 liters capacity 40 dairy cows - 164 in total
3	Dairy farm	Viken	72 dairy cows 120 calves and heifers
4	Dairy farm	Troms og Finnmark	3000 liters 40 dairy cows
5	Dairy farm	Rogaland	8000 liters capacity 475 cows - 80 suckler cows
6	Dairy farm	Innlandet	Up to 5000 liters
7	Dairy farm	Innlandet	Up to 10 000 liters 115 dairy cows
8	Dairy farm	Innlandet	42 dairy cows
9	Suckler cow	Innlandet	50 mother cows
10	Suckler cow	Viken	50 mother cows
11	Pig	Innlandet	1200-1600 during a year
12	Pig	Trøndelag	Up to 1000 at a time
13	Pig	Innlandet	600 at a time
14	Pig	Innlandet	1600 currently

Table 4.1: Demographics

4.2 Case study

Section 4.2 presents the results of the conducted case study. The data presented was collected during the interviews, and any information used that is collected from other sources is referenced. Only the digital technologies are included, such as those connected to the Internet, a PC, or that uses wireless signals such as GPS. Technologies that are used on the farms but are only connected to other systems trough physical wires are therefore not included.

Dairy cow farms

Figure 4.1 shows what technologies are used on the different dairy farms that were interviewed, and how they are connected to the Internet. Not all farms use the same types of technologies, but these are all the technologies that were mentioned that are used in the farm house. Each technology is marked with how many of the eight specifically mentioned using that technology. All farms that produce cow's milk depend on a milking robot. This is connected to a farm PC where the machine management software is located. This PC is often used to manage other machines such as feeding robots, as well as ordering supplies, uploading data to relevant websites and accessing software used to manage production.

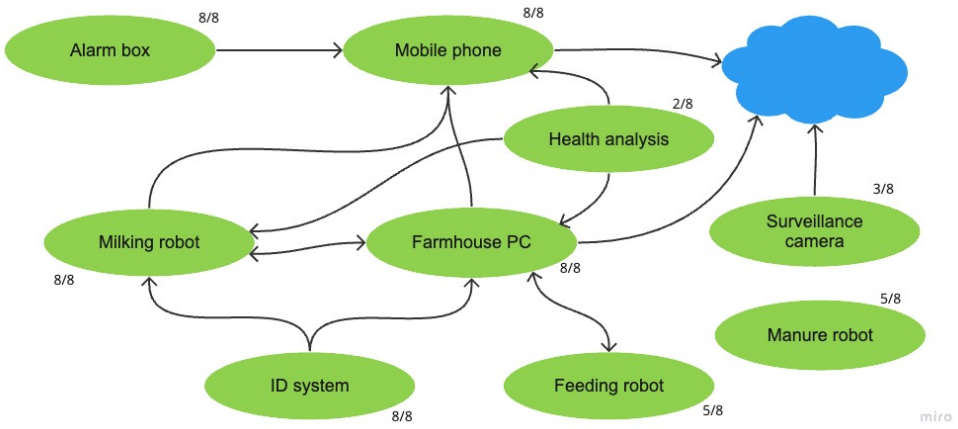


Figure 4.1: Overview of use of technology on the dairy farms

Some of these programs are also connected to the farmers' mobile phone so that they can check on progress remotely, and set alarms for events such as equipment failure or a power outage. All the farms also have a fire alarm system that will call the farmers' phone in case of fire. A dedicated robot is used by some of the farmers to remove manure, but the machine runs on its own system and is not managed through the farm PC. Overall, the only technologies all the dairy farmers use is the milking robot, farm PC, and a milking robot identification solution. The use of other technologies varies by size and farm house layout as well as location and simply choice.

There are two major suppliers of milking robots that are used in Norway, Lely and DeLaval. Six of the dairy farmers interviewed have a milking robot from DeLaval, and the last two have one from Lely. Figure 4.2 shows a cow in a DeLaval milking robot. Most farms have only one milking robot for production, but the two largest farms in this study have two machines to manage the large number of animals. These milking robots run 24/7, so the cows can go and get milked whenever. Whilst milking, the cow will be able to feed on concentrate as an incentive to stay. This feeding is connected to the milking robot, and is controlled alongside the rest of the machine from the farm PC.

To keep track of who has been milked and not, if their milk should be sent to the production tank or not, and the individual milking settings, each cow is wearing some form of identification that the robot can read. This can be either a RFID chip in an ear tag, or on a necklace around the cows' neck. This allows the machine to separate the cows into categories based on need for milking. These ID tags can also be used to steer access to certain areas of the farm, for example if a cow is on antibiotics and therefore gets milked manually, the ID tag will not let them

Figure 4.2: Image of a cow in a DeLaval milking robot

through the fencing to the main milking robot. Some use smart gates to steer the cows to set locations to perform health checks, insemination, and other similar functions. These are connected to the milking robot and the ID of the cow, so the farmer can 'order' the capture of a certain cow through the machine software, and as the milking robot has its own mobile modem, it can call the farmer directly.

The farms have different levels of alarm functions, both emergency functions such as a fire alarm, and alarms related to problems with the milking and feeding robots. Both the fire alarms and the milking robots have the ability to call the farmers' mobile phone in cases of emergency. The farmer can set up as few or many alarm scenarios as they wish for the milking and feeding robots, and some have chosen to get alerts though text message instead. Some of the applications can also give notifications directly to the mobile phone, especially for those systems that have a phone application to access services remotely. Three of the farms also have surveillance cameras that can be accessed remotely to keep an eye on the farm house and the cows.

The two other types of robots that are commonly in use on dairy farms in Norway are robots to remove or scrape manure, and various feeding robots. Five out of eight have a robot to manage manure that is either connected to the farm PC or runs on its own through a predetermined route. Those that do not have a robot use a hydraulic draft to remove manure, though some that use a robot has such a

draft as well.

Where concentrate is fed to the cows mostly during milking and is restricted in amount, fodder, or forage, is given at feeding stations in the areas where the cows stay, and is available at all times. This type of feed is often distributed through a feeding robot, as five of the dairy farmers do, or distributed using a machine connected to the back of a tractor as the other three farms use. The feeding robots are managed either by software on the farmhouse PC or by predetermined settings so that it is not connected to the LAN. Three of the farms managed their robots though software, whilst the other two configure them manually. Two of the eight farms have an automatic feeder for calves that can be connected to the same software that manages the milking robot, or programmed manually.

Farmers in Norway use a lot of different software and websites to manage the farm, both mandatory systems and optional software solutions. All farmers that have cows in Norway have to report certain information to the Norwegian food authority, Mattilsynet, through the national livestock register 'Husdyrregisteret'. This register keeps track of all cows in Norway, each with an individual identification number, and a farmer therefore need to report all new calves born, if they get any new cows from other farms, and all deaths of cows, including those sent to slaughter [49]. The Norwegian food authority also require that all cows have two ID tags with their unique identification number, one in each ear so that the cows' identity is known at all times. Each farm with cattle must also keep a journal either physically or digitally with detailed information about each cow on the farm, and information on productions types, health information, infection control measures and more [50]. All these requirements are set to have control over production in Norway, ensure animal rights and have traceability in cases of disease outbreaks, among other reasons.

Lely and DeLaval have their own software solution to manage the machines on the farm. Lely has T4C management system to control their milking machines, and DeLaval has DelPro. DelPro is not just for managing the milking machine, and can be connected to feeding robots and manure robots as well. Figure 4.3 shows an image from the DelPro application. The intention is to manage and control most activities and tasks on the farms through one solution [51]. Health analysis and heat detection and planning is also a part of DelPro, as the software is also intended to give substantial decision support. T4C is more specific to managing the milking robot, though Lely has Lely Horizon for farmers that want a more comprehensive management system more similar to DelPro [52, 53]. These are systems the farmers use every time they are in the farmhouse, to check on milking status, make sure all systems are working, checking the feeding robot supply if they use this, and they can be synced to Kukontrollen and other software used by the farmers.

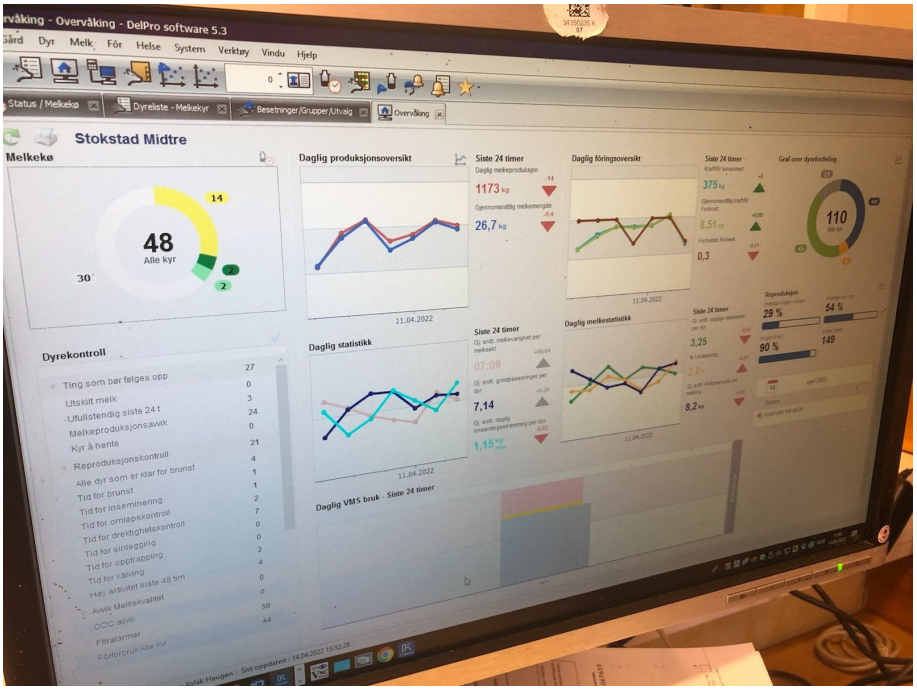


Figure 4.3: Image of DelPro on a farmhouse PC

Beyond the required software and registers, approximately 97% of dairy farmers in Norway use Tine's Kukontrollen, according to Tine [54]. This is a solution where data from all the animals are registered, processed, quality controlled and compiled for the farmer's benefit, and is an important basis for decision making. The program can gather data from many different sources, such as Geno, a website used for breeding, the individual slaughterhouses and Dyrhelseportalen by Animalia, which has information about health and insemination, where for example the veterinary can upload their report. Figure 4.4 shows how Geno's breeding plan page looks.

Other online services that Norwegian dairy farms rely on are Felleskøpet for purchasing animal feed, and the website of their chosen slaughterhouse. These, along with Tine or other dairy producers, are an essential part of the supply chain, and the farmers are dependent on these to produce or deliver their produce. Felleskjøpet delivers multiple products, but the main product for dairy farmers is concentrate feed and supplementary fodder if the farm does not produce grass, or do not have enough grass for the upcoming season. There are other companies that sell animal feed, but Felleskjøpet is one of the largest companies.

The dairy producers, such as Tine, collect milk from the tank on the farm about every three days. The collection of milk is very time sensitive, and if the milk is not collected, the tanks will become full and the farmers will have to trow away

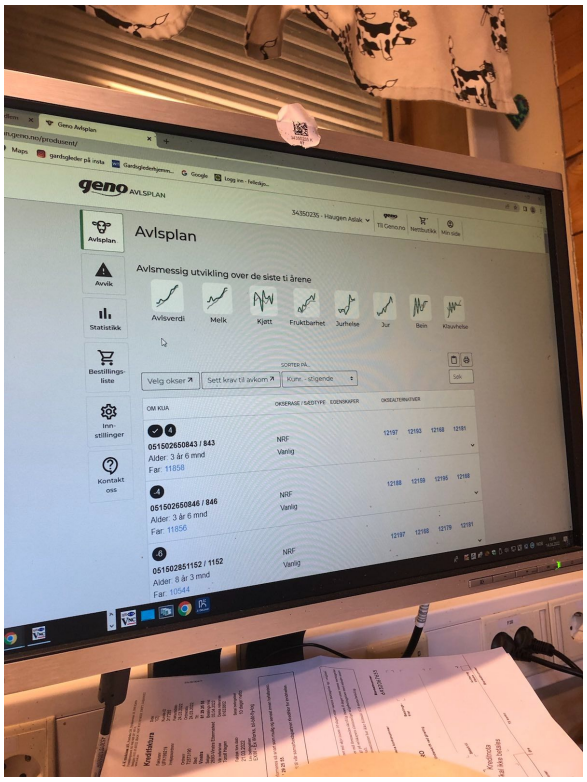


Figure 4.4: Image from the Geno application on a farmhouse PC

the milk they have collected. Ordering slaughter of cows is a less time sensitive function, as they are generally ordered 5 to 7 weeks in advance, but if they become unavailable at a crucial point in the season, many farms can face big problems. Keeping a lot of cows that should have been slaughtered will require more resources in terms of food and space, which means unplanned and increased expenses for the farmers, and a lack of income until the cows can be slaughtered. Slaughterhouses such as Nortura also give reports on the slaughter, with information about weight, fat percentages and more that the farmers use to plan and optimize for the next round of slaughter, though some of this functionality is still not available after the cyber attack that took down Nortura's services.

Health analysis services have also become more popular among dairy farmers in Norway. Lely delivers a health analysis system that connects to the necklace of the cow, whilst other companies use an ear tag [55, 56]. These sensors can analyze multiple different aspects of the cow, such as rumination, activity and length of mealtimes for early detection of health problems and detecting the different stages of heat for optimal insemination. Only two of the farmers mentioned the use of these solutions specifically, and they were both among the largest farms in terms

of milking tank capacity.

Suckler cow farms

The use of technology on suckler cow farms differs from dairy cow farms mostly by the lack of the milking robot. Both types of farms produce cattle and grows cows for beef production, but the dairy farmers produce cattle to induce milk production, whilst the suckler cow farms produces calves to sells them to other beef or dairy farms. Some of the calves are kept for beef production, others are kept for breeding, and the rest are sold to other farms.

Figure 4.5 shows an overview of the technologies used by the two suckler cow farmers interviewed in this study. There is also less use of software systems because they do not have the same need to optimize milking, but they are still required to give information to the national livestock register, and do use solutions such as Storfekjøttkontrollen to keep track of beef cattle. The cows still have ID tags as required by the national food authority, but they do not use RFID to control access rights and keep track of the cows in the same manner as the dairy farms. The farms still have a farmhouse PC for ordering food, keeping track of the herd, ordering slaughter, and accessing the applications and websites of various other online services.

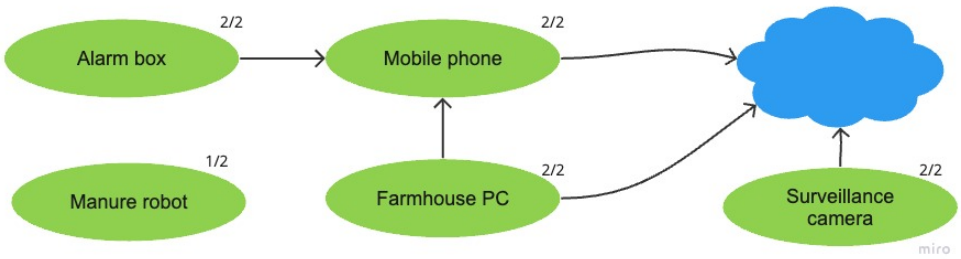


Figure 4.5: Overview of the use of technology on suckler cow farms

None of the two suckler cow farms uses a feeding robot, but one of them does use a robot to remove manure. As feeding and cleaning is needed for both dairy and suckler cow farms, the use of robots for these functions is more about preference than difference in the use cases. When it comes to alarm functions, there is less need for it on suckler cow farms as they do not have any robots or machines they are critically dependent on. Both farmers do have fire alarms similarly to the dairy farms.

Both farmers use surveillance cameras to monitor the cows, especially during calving season, to make sure that things go smoothly. One of the farms also use the surveillance cameras to monitor heat. The two farms do insemination in different

ways, where one farm orders semen online, the other farm purchases the sire and does the insemination naturally. Because they work with the same animals, the suckler cow farms use many of the same services as the dairy farms. Both farmers need to order feed and sell the cows to a slaughterhouse. As they produce calves, they also need to sell the calves, which both farms do through Nortura.

Pig farms

Figure 4.6 shows the use of technologies on the pig farms interviewed in this study. The feeding systems are the most critical technologies, and they are controlled through a dedicated management computer. The other main technology used is the ventilation system, which is also managed through a dedicated computer. The barns are required to have alarm functions in place in case the temperature or humidity reaches unsafe levels, or there is a power outage. The feeding station is also connected to the alarm system in cases of malfunction or power outages. The pig farmers also rely on online solutions to manage the farm, mainly Ingris by Animalia, and purchase from and sell to other companies in the supply chain.

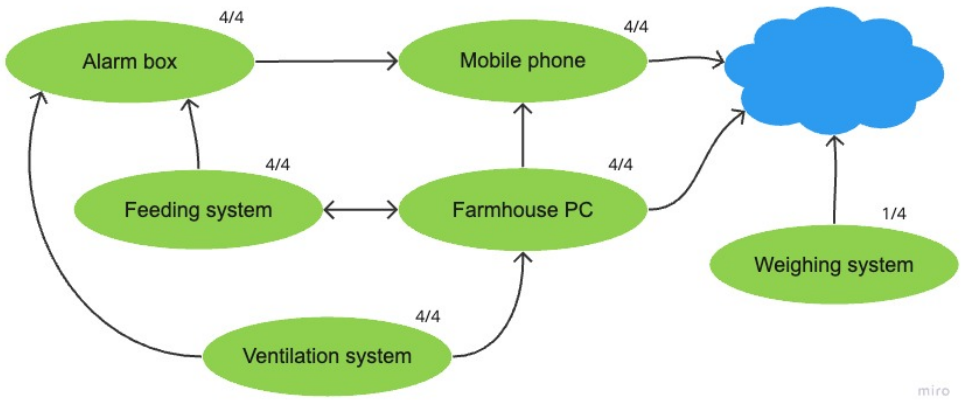


Figure 4.6: Overview of the use of technology on pig farms

Pigs are either fed dry or liquid feed, and in some cases a combination. The different types of feed requires different machines, because in liquid feeding, the consentrate is mixed with water, whilst the dry feeding machines distributes the feed mix directly. Two of the farmers in this study uses both, one uses only dry feed, and the fourth uses only liquid feed. The pigs are fed twice a day, and the law requires that the feeding system is checked once daily to make sure it works [57]. Three of the four have one feeding station delivered by BigDutchman, which can be controlled through a separate screen connected to the machine. Some of the feeding machines are connected to the Internet, whilst others are not, but all are connected to an alarm system that will alert the farmer in cases of power outages or malfunctions.

The ventilation systems are generally more mechanical, where not all can be connected to the Internet. Most of the ventilation systems delivered by Fjøssystemer do have remote access control configured. The ventilation systems are critical for pig farming, as poor air quality and temperature will affect the animals' welfare. Therefore, the farms are required by law to have emergency openings that are battery operated in case of power outages if the farmhouse itself does not have sufficient natural ventilation [57]. The ventilation systems are also controlled through a separate computer, and this is connected to the alarm system, so that the farmer is alerted if the humidity or temperature is too high.

Pigs do have ear tags that they are required by law to wear for identification [58], but they are not used in connection with machines such as the cows are connected to the milking robot. Also, none of the pig farmers use sensors to monitor animal health. One of the farmers mentioned using an automatic weighing system connected to the internet to monitor growth and gather data.

In terms of software, three of the four pig farmers uses Ingris to keep track of the animals and register production results. Nortura and other slaughterhouses are used to sell products to, and the two farms that also produce pigs use Norsvin to order semen for insemination. The other two farms purchase the young pigs through for example Nortura. Felleskjøpet also sells feed to pig farmers, which is where three of the interviewed farmers purchase their feed, whilst the fourth uses a local mill.

4.3 Assets

The asset evaluation constitutes the first part of the risk assessment. The analysis is based on the data collected during the interview process. The values set may vary somewhat from farm to farm based on which of the technologies they use, and how reliant they are on them differs, so the values given are an approximation.

Dairy cow farm assets

The milking robot is the most critical element on a dairy farm. The data on it is not confidential, but if the machine is unavailable, the farm will not be able to produce milk, and it is harmful for the animals to go too long without milking. If integrity is breached so that the milk of a cow on antibiotics goes to the production tank, the tank will have to be emptied, or if it is not discovered before the milk is collected, the farmer will receive a fine as well.

The farmhouse PC and mobile phone are both used a lot in production, but the devices themselves are not very critical for production. The feeding and manure robots are not critical, as the farmers have manual routines in cases of failure.

Asset		**CIA**
Hardware	Milking robot	Confidentiality: 1 Integrity: 4 Availability: 4
	Farmhouse PC	Confidentiality: 2 Integrity: 1 Availability: 2
	Feeding robot	Confidentiality: 1 Integrity: 2 Availability: 1
	Manure robot	Confidentiality: 1 Integrity: 1 Availability: 1
	Mobile phone	Confidentiality: 2 Integrity: 1 Availability: 2
	Machine ID tag/necklace	Confidentiality: 1 Integrity: 4 Availability: 4
	Alarm box	Confidentiality: 1 Integrity: 4 Availability: 4
	Health application sensor	Confidentiality: 2 Integrity: 3 Availability: 1
	Surveillance camera	Confidentiality: 2 Integrity: 2 Availability: 1
Software	Milking machine software and application	Confidentiality: 2 Integrity: 4 Availability: 2
	Husdyrregisteret	Confidentiality: 2 Integrity: 4 Availability: 2
	Felleskjøpet	Confidentiality: 1 Integrity: 3 Availability: 2
	Slaughterhouse website	Confidentiality: 2 Integrity: 3 Availability: 1
	Kukontrollen	Confidentiality: 2 Integrity: 3 Availability: 2

Table 4.2: Asset assessment for dairy farms

Lack of integrity with the feeding robot will have some consequences, but they will quickly be discovered, as the animals will communicate if they are lacking in food. There is a higher consequence if the animals are given too much food, because then there will be leftovers, which is a waste of money.

The machine ID tag or necklace are very important for production because they are needed for the milking, and must therefor be fixed if unavailable. If the integrity is breached so that a cow on antibiotics is mislabeled as healthy, there is a significant economic loss for the farmer. The alarm box is only important if there is an emergency, but it is critical that it is available and does sound the alarm in case of an emergency. The surveillance cameras and health application sensors are not necessary for production, but if the farm does rely on them, there can be issues with integrity mostly, where sick, or in other ways distressed animals are not discovered and treated in time.

In terms of software, the milking robot software and applications are the most critical, again with the potential financial loss if integrity is breached. There is a lower requirement for availability of the software, as the robot can work without the managing system for a couple of days. The software listed are those that are used the most, but other software will have a similar consequence assessment. If the information on these sites is incorrect, it will affect production as the information sites like Kukontrollen and the slaughterhouse websites are used to plan further production. However, the requirements for availability are lower as they are not detrimental to the farms ability to produce their product. Husdyrregisteret is also critical in terms of integrity, because if a cow is not registered correctly, the slaughterhouses will have to discard the meat instead of selling it to consumers.

In general, there is very little consequence in relation to confidentiality over all. The biggest consequence mentioned is if data is manipulated, or that the value of the data is reduced if made public, but it will not affect profitability or ability to produce if confidentiality is breached.

Suckler cow farm assets

The consequence assessment for the technologies used on suckler cow farms is very similar to the dairy farms. They do rely on surveillance cameras more in their business, but other than that, the use cases are very similar. Other than the alarm box, there are no critical consequences in terms of availability, because they do not rely on technology in order to produce cows, only to manage and optimize production. Similarly, breaches of integrity will not have critical consequences economically, but it can affect traceability. Only Husdyrregisteret has a critical integrity consequence, because this can affect production if the meat has to be discarded.

Asset		**CIA**
Hardware	Farmhouse PC	Confidentiality: 2 Integrity: 1 Availability: 2
	Manure robot	Confidentiality: 1 Integrity: 1 Availability: 1
	Mobile phone	Confidentiality: 2 Integrity: 1 Availability: 2
	Alarm box	Confidentiality: 1 Integrity: 4 Availability: 4
	Surveillance camera	Confidentiality: 2 Integrity: 2 Availability: 2
Software	Husdyrregisteret	Confidentiality: 2 Integrity: 4 Availability: 2
	Felleskjøpet	Confidentiality: 1 Integrity: 3 Availability: 2
	Slaughterhouse website	Confidentiality: 2 Integrity: 3 Availability: 1
	Storfekjøttkontrollen	Confidentiality: 2 Integrity: 3 Availability: 2

Table 4.3: Asset assessment for suckler cow farms

Pig farm assets

The feeding systems are the most critical assets for pig farmers in terms of everyday operations. The data on it is not confidential, but if it is unavailable, the pigs will not be able to receive enough food. The machines can be unavailable for a certain amount of hours, as pigs are used to going without food for about eight hours throughout the night, but if it is unavailable for more than 12 hours, the pigs will be quite unhappy. The farms interviewed in this study were all large enough that feeding all the pigs manually would be quite difficult, as the amount of kilos needed will require a lot of physical labor. As with the cows, integrity is not as important, because the farmer will quickly notice if the pigs have received too little food. If they are fed too much however, food will be left uneaten, which will lead to some economic loss for the farmer.

The alarm function is again critical in terms of integrity and availability, because it can have fatal consequences for the animals if it does not work properly in emergency situations. The consequences related to the farmhouse PC and mobile phone are no different from dairy and suckler cow farms, as pig farmers are not more or less dependent on these. The weighing system connected to the Internet is used regularly to plan feeding, and the task will have to be performed manually if the system is down for a while. However, manual weighing is a laborious task, so a malfunction of the weighing system will mean less data collection, which will somewhat affect planning and production.

The software solutions score similarly to the dairy and suckler cow farms also, because the farmers depend on these in a similar way. They are all mostly in the middle levels of consequence, because they are all used regularly in production, but are not required to be available at all times. Having correct data on these sites are more important, as wrong data can affect production negatively. The farmers are dependent on organizations such as Felleskjøpet as part of the supply chain, but these organizations can take orders over the phone as Nortura did after their cyber attack, so that the farmers can still receive and deliver products as needed.

4.4 Threat assessment

Table 4.5 lists relevant threat agents, their capability and capacity, and potential actions they can perform. These threats are general, and can apply to all the different types of farms interviewed in this study. A cyber criminal is an agent that performs malicious activities either because they simply want to cause harm, or for financial gain through for example a ransomware attack. Cyber criminals generally have some capabilities to perform cyber attacks, and their capacity is set to medium as they often earn money and make their living by hacking, and therefore have the time and resources to perform cyber attacks, especially if the attack will earn them money.

Asset		**CIA**
Hardware	Feeding system	Confidentiality: 1 Integrity: 2 Availability: 3
	Ventilation system	Confidentiality: 1 Integrity: 2 Availability: 2
	Farmhouse PC	Confidentiality: 2 Integrity: 1 Availability: 2
	Alarm box	Confidentiality: 1 Integrity: 4 Availability: 4
	Mobile phone	Confidentiality: 2 Integrity: 1 Availability: 2
	Weighing system	Confidentiality: 1 Integrity: 3 Availability: 2
Software	Norsvin	Confidentiality: 2 Integrity: 3 Availability: 2
	Slaughterhouse website	Confidentiality: 2 Integrity: 3 Availability: 1
	Felleskjøpet	Confidentiality: 1 Integrity: 3 Availability: 2
	Ingris	Confidentiality: 2 Integrity: 3 Availability: 2

Table 4.4: Asset assessment for pig farms

A state actor can be motivated to attack farmers in order to affect food production in Norway, and is therefore more interested in sabotage, but can also be looking to gain information through theft of media or documents. Because they are supported by the state they work for, and are hired specifically to perform cyber attacks, their capability and capacity is high. An activist can be interested in attacking Norwegian farmers to paint the food production industry in a negative light, or sabotage or steal equipment to prevent production. Their capability depends largely on the goal of the group, but in the farm setting, they are not expected to have a lot of capabilities. Their capacity is also limited as they do not have a lot of money, time or other resources to dedicate to the cause, because they are generally regular people with jobs and other responsibilities.

Lastly, natural causes are also a threat to Norwegian farming, especially natural occurrences that affect the power supply in some way or damage equipment. Natural causes can not control its capability and capacity to do damage. The capability of natural causes is set to low because they do not happen very often, and the event would need to happen in the right area as well to cause the specific damage. Their capacity is set to high because a natural disaster can cause extreme damage.

Threat actor	**Capability**	**Capacity**	**Threat action**
Cyber criminal	Medium	Medium	Intentional denial of service event
			Corruption of data
			Theft of digital identity or credentials
State actor	High	High	System sabotage or software failure or malfunction
			Sabotage of supply system
			Theft of media or documents
Activist	Low	Low	Eavesdropping and interception of data
			Theft of equipment and sensitive media through unauthorized physical access
			Unchecked data viewing or alteration
Natural	Low	High	Equipment damage or destruction due to natural causes (fire, lightning, etc.)
			Loss of power

Table 4.5: Threat assessment

4.5 Vulnerability assessment

Table 4.6 lists some potential vulnerabilities identified from the interviews, as well as findings from Nikander, Manninen and Laajalahti's work on dairy farms in Finland [31]. The vulnerabilities can vary quite a bit depending on the equipment used, the knowledge and experience of the farmer, the size of the farm and such. Not all farms interviewed had equipment that could be accessed remotely, but most did as the milking robot from DeLaval, and a lot of the feeding and ventilation systems for pigs, have this functionality. In many cases, remote access control is beneficial as it allows for remote reparation of the equipment, but it does make the equipment vulnerable to unauthorized access and tampering.

Category	**Vulnerability description**
Software	Remote access control
	Same login service on multiple sites
	Lack of malware protection
Network	Unprotected communication lines
	Insecure network architecture
	Lack of equipment maintenance
Personnel	Lack of security awareness
	Insufficient security training
Site	Inadequate physical access control
	Susceptible to damage in cases of lightning

Table 4.6: Vulnerability assessment

Several of the websites and software solutions used in Norwegian farming, such as Kukontrollen, Geno, Animalia and Nortura, are logged into through Produsentregisteret, a national register over agricultural producers [59]. The benefit of such a solution is that the farmers need fewer unique login credentials, however, this can cause issues if Produsentregisteret is unavailable, and the farmers can not access all the services they rely on.

How well the farmhouse PC and network architecture is protected will depend on the security awareness and training of the farmer, their economic resources and personal experience. One of the dairy farmers had previously experienced a ransomware attack, but managed to save the data. After the incident, they implemented more security regulations for use of the farmhouse PC to prevent similar situations in the future. The vulnerabilities listed in the software and network categories are typical for small businesses without dedicated security personnel, and are based on some of the cyber security problems identified by Nikander et al. [31]. Inadequate physical access control is a vulnerability because according to one of the technicians interviewed, almost none of the farmhouses in Norway are locked. Here location will affect how vulnerable the farm is to attacks conducted

through physical access, because farms in remote areas will be more suspicious to any unknown vehicles approaching. Susceptible to damage by lightning is a vulnerability that one of the technicians mentioned, as they have experience with farmhouse PC's and data cards being damaged by lightning strikes.

4.6 Risk evaluation

The risks included here are those related to the assets that are most important, and follows the template 'A threat exploits a vulnerability of an asset to compromise the confidentially, integrity and/or availability of corresponding information.' stated in the ISO 27005 standard [47]. For each risk, a description is given, along with which threat actor could pull off and be interested in performing such an attack, and which asset is at risk in the scenario. The risk score is determined by the likelihood score multiplied with the consequence score.

Dairy cow farm risk evaluation

Risk 1: Virus on the milking robot
Description: The milking robot is hit by a virus and becomes unavailable
Threat actor: Cyber criminal, state actor
Assets at risk: Milking robot
Risk score: 4 x 4

Risk 2: Denial of Service attack on farmhouse network
Description: The LAN is hit with a denial of service attack so that connecting to the Internet is not possible
Threat actor: Cyber criminal, state actor
Assets at risk: Online software solutions
Risk score: 4 x 2

Risk 3: Ransomware attack on Tine
Description: Tine is hit by a ransomware attack so that all their data and online services becomes unavailable
Threat actor: Cyber criminal, state actor
Assets at risk: Kukontrollen
Risk score: 4 x 2

Risk 4: Ransomware attack on farmhouse PC
Description: The farmhouse PC is hit with a ransomware attack, making it unusable and all data unavailable
Threat actor: Cyber criminal
Assets at risk: Farmhouse PC
Risk score: 3 x 2

Risk 5: Deactivated RFID tags
Description: An activist breaks in and deactivates all RFID tags
Threat actor: Activist
Assets at risk: ID tag/necklace
Risk score: 2 x 4

Risk 6: Lighting strike
Description: A lightning strike causes damage to the physical machines so that they do not work properly
Threat actor: Natural
Assets at risk: Hardware such as milking and feeding robot
Risk score: 2 x 4

Risk 7: Unauthorized access to feeding robot
Description: A cyber criminal gains access to the feeding robot through remote access and alters the data
Threat actor: Cyber criminal
Assets at risk: Feeding robot
Risk score: 2 x 2

Risk 8: Physical sabotage
Description: Activists break into the farmhouse to perform physical sabotage such as damaging the milking robot
Threat actor: Activist
Assets at risk: Hardware such as milking, feeding and manure robots
Risk score: 3 x 4

Risk 9: Unauthorized access to milking robot software
Description: Inadequately protected network allows threat actor to gain access to milking robot software on farmhouse PC in order to alter data
Threat actor: Cyber criminal, state actor, activist
Assets at risk: Milking robot software
Risk score: 4 x 4

Risk 10: Power outage
Description: The power goes out in the area, causing all electrically dependent systems to stop working
Threat actor: Natural, accidental, state actor
Assets at risk: All hardware dependent on electricity
Risk score: 3 x 4

Above is a list of ten risk scenarios that are relevant for the dairy farms interviewed as part of this research project. Table 4.7 shows a risk matrix, where all the risks are placed according to their likelihood and consequence score. The green area are for risks that have a total risk score of less than four, which are the risks that are not deemed important, because either the likelihood or consequence, or both, is so low.

Probability \Consequence	1	2	3	4
1 - Very unlikely				
2 - Unlikely		7		5, 6
3 - Likely		4		8, 10
4 - Very likely		2, 3		1, 9

Table 4.7: Dairy cow farm risk matrix

The yellow area is for the risks with a total score between four and nine, where either the likelihood or consequence is high, or they are both somewhere in the middle. The risks with scores less than 10 are all considered acceptable risks, and so mitigation strategies should be considered, at least for those that are close to 10, but they have a lower priority than those above 10. The red area is for the most critical risks that are considered unacceptable, and mitigating measures should be implemented.

The most critical risks are those that will affect the milking robot in some way. The scenarios where the integrity or availability of the milking robot are affected have the highest risk score possible, because these are attacks that are relatively easy for the threat actor to perform, and the consequences are critical for the farmer. Physical sabotage and power outages that will affect the availability of the milking robot also have high risk scores, but these are somewhat less likely to happen. Mitigation strategies that are already implemented are not brought into consideration during the risk assessment, as not all the farmers interviewed have them. Having a generator will mitigate the risk in cases of power outages by reducing the consequence, but for those that do not have a generator, the risk is as presented.

Implementing mitigating measures for the risks in the red area should be prioritized, especially those where the mitigation strategies have low costs. The likelihood of physical damage can be reduced simply by locking the farmhouse when leaving, as the activist threat actor are considered to have low capacity, and this might be enough to deter them from such an attack. The other risks are within the yellow area, and mitigation strategies should mainly be considered for these if the cost of the mitigating measures are worth it, or if the consequence is deemed unacceptable regardless of the likelihood.

Suckler cow farm risk evaluation

Risk 1: Ransomware attack on farmhouse PC
Description: The farmhouse PC is hit with a ransomware attack, making it unusable and all data unavailable
Threat actor: Cyber criminal
Assets at risk: Farmhouse PC
Risk score: 3 x 2

Risk 2: Ransomware attack on Animalia
Description: Animalia is hit by a ransomware attack so that all their data and online services becomes unavailable
Threat actor: Cyber criminal, state actor
Assets at risk: Storfekjøttkontrollen
Risk score: 4 x 2

Risk 3: Power outage
Description: The power goes out in the area, causing all electrically dependent systems to stop working
Threat actor: Natural, state actor
Assets at risk: All hardware dependent on electricity
Risk score: 3 x 2

Risk 4: Denial of Service attack on farmhouse network
Description: The LAN is hit with a denial of service attack so that connecting to the Internet is not possible
Threat actor: Cyber criminal, state actor
Assets at risk: Online software solutions
Risk score: 4 x 2

For the suckler cow farms, fewer risks are identified, both because fewer farmers were interviewed, and because the interviewed farmers were generally less dependent on technology. None of the identified risks are within the unacceptable level, and all four are centered around a higher likelihood and lower consequence, as shown in the risk matrix in table 4.8.

Probability \Consequence	1	2	3	4
1 - Very unlikely				
2 - Unlikely				
3 - Likely		1, 3		
4 - Very likely		2, 4		

Table 4.8: Suckler cow farm risk matrix

Three out of the four risks are the same as the risks for the dairy farms, but the risk scores are lower because the consequences related to the assets are lower. A

ransomware attack on Animalia and a Denial of Service (DoS) attack on the farmhouse network are the risks with the highest scores because these are the easiest attacks to perform for the threat actors. Implementing some mitigating measures that will reduce likelihood should be considered to make the risks more acceptable, but not if the costs are greater than the benefits.

Pig farm risk evaluation

Risk 1: Ransomware attack on farmhouse PC
Description: The farmhouse PC is hit with a ransomware attack, making it unusable and all data unavailable
Threat actor: Cyber criminal
Assets at risk: Farmhouse PC
Risk score: 3 x 2

Risk 2: Unauthorized access to feeding station computer
Description: A cyber criminal gains access to the feeding station control computer through remote access and alters the data
Threat actor: Cyber criminal, activist
Assets at risk: Feeding station
Risk score: 2 x 2

Risk 3: Ransomware attack on Animalia
Description: Animalia is hit by a ransomware attack so that all their data and online services becomes unavailable
Threat actor: Cyber criminal, state actor
Assets at risk: Ingris
Risk score: 4 x 2

Risk 4: Denial of Service attack on farmhouse network
Description: The LAN is hit with a denial of service attack so that connecting to the Internet is not possible
Threat actor: Cyber criminal, state actor
Assets at risk: Online software solutions
Risk score: 4 x 2

Risk 5: Lightning strike
Description: A lightning strike causes damage to the physical machines so that they do not work properly
Threat actor: Natural
Assets at risk: Hardware such as feeding robot and ventilation system
Risk score: 2 x 3

Risk 6: Power outage
Description: The power goes out in the area, causing all electrically dependent systems to stop working
Threat actor: Natural, state actor
Assets at risk: All hardware dependent on electricity
Risk score: 3 x 3

Risk 7: Virus on the feeding system control computer
Description: The feeding system control computer is hit by a virus, making the feeding system unavailable
Threat actor: Cyber criminal, state actor
Assets at risk: Feeding system
Risk score: 4 x 3

Above are seven risks identified for the pig farmers that are part of this research. Only one risk scenario is above the threshold of acceptable risk score. Table 4.9 shows the risk matrix for the risk scenarios, where all but one is located in the yellow area. Four of the risks are the same as those for the dairy farms, and the other three are similar, but customized to be specific to pig farming.

Probability \Consequence	1	2	3	4
1 - Very unlikely				
2 - Unlikely		2	5	
3 - Likely		1	6	
4 - Very likely		3, 4	7	

Table 4.9: Pig farm risk matrix

The highest scoring risk scenario is a virus on the feeding system computer, with a risk score of 12. This is because the risk scenario targets the feeding station, which is the machine the pig farmers are most dependent on for their production. The high likelihood score is because this is an easy attack for a motivated threat actor to perform. The second highest scoring risk scenario is a power outage, again because it targets the feeding system, among other hardware systems. The likelihood of a power outage is set to be higher than a lightning strike causing damage, because some of the farmers have experience with somewhat regular power outages in their area. The scenarios with the third highest risk score are a ransomware attack on Animalia and a DoS attack on the farmhouse network, again because these are attacks that are relatively easy for the threat actors to perform with their capabilities.

Chapter 5

Discussion

In this chapter, the three research question are discussed. For each of them, the research findings related to the question are summarized and discussed, and the strengths and weaknesses of the research are presented. Then, the limitations of the research is described, before the suggestions for future work are given.

5.1 What technologies are used by Norwegian cattle and pig farmers to produce and deliver their produce?

For the production itself, the dairy farmers interviewed rely mostly on the milking robot. Several other machines are involved in the keep of the animals and ensuring that everything runs smoothly, such as feeding and manure robots, but only the milking robot is critical for production, in addition to the ID system connected to it. Of the three types of farmers interviewed, the dairy farmers are most dependent on technology for their production process. Figure 5.1 shows a Venn diagram of the technologies used on the different types of farms. Only the milking robot, the ID system connected to the milking robot, and the feeding system, are critical for production on any of the farms. However, the feeding system is not as critical for the dairy farmers, because they have manual backup solutions, which the pig farmers do not have.

The technologies they all have in common are those used to manage the farm, the farmhouse PC where all the management software is accessed, the alarm box in cases of emergency, and the mobile phone where they receive the alarms and access some of the management software solutions. The suckler cow farms use the lowest number of technologies, and have none that are unique to their type of production. Both surveillance cameras and manure robots are used on some of the dairy farms as well. Besides the technologies they all have in common, the pig and dairy farmers only share the use of a feeding system. In addition to the milking robot and ID system, a few of the dairy farmers use health analysis sensors to monitor the health of the cows. This type of technology is used in order to detect

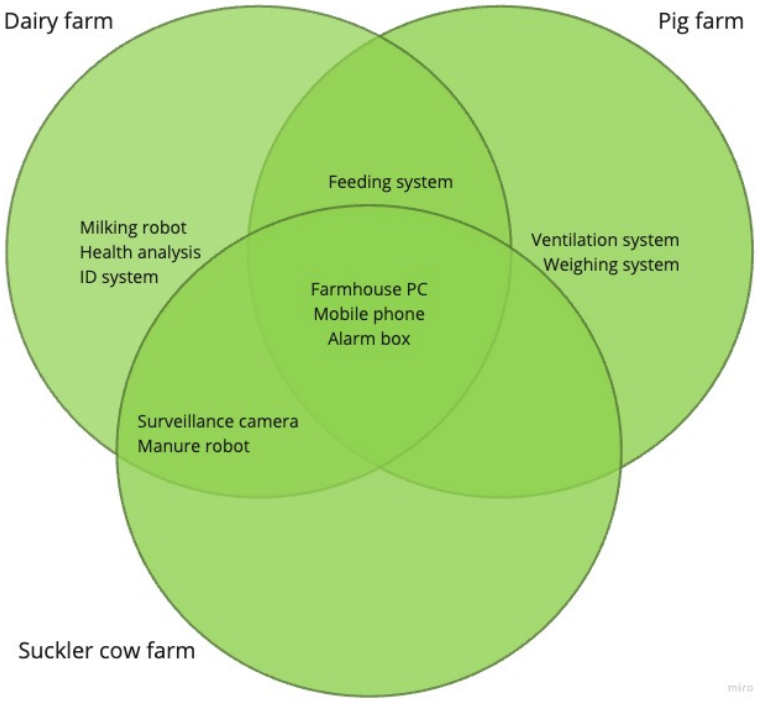


Figure 5.1: Venn diagram of the use of technology on different types of farms

illnesses early to reduce the need for medication and therefore costs, for the general welfare of the animals, and to optimize the milking production.

The pig farmers also have ventilation systems, and one of them had a weighing system connected to the Internet as well. The dairy and suckler cow farmers also have ventilation in their barn, but these are mechanical solutions that are not connected to the Internet in any way. As the ventilation system is more critical for the pigs because of the humidity and gas they produce, half of the pig farmers interviewed have remote access control to their ventilation system. The other two must enter the farmhouse to check the ventilation system, however all of them have configured alarms that will alert the farmer if the system stops working. Overall, the pigs are only critically dependent on the feeding system, as they are required by law to have battery backup solutions for ventilating the barn.

The use of technologies on these farms differ somewhat from those mentioned in the research articles on smart farming technologies presented in chapter 2. IoT and unmanned vehicles especially are mentioned a lot in the research, but none of the farmers interviewed here use this type of technology [3, 11]. This might be different for other types of farms, it might for example be more relevant for plant producing farms with acres of land to use unmanned vehicles. When it comes to IoT technology however, it might also be because it is too expensive to be worth

it, this is at least what one of the interviewed farmers said.
Not all of the technologies presented are used by all the farmers interviewed in each category. For example, not all the diary farmers use manure robots, feeding robots, health analysis systems and surveillance cameras. In addition, the versions the farmers use might be different, so that one farmer can have a feeding robot that is much newer and more technologically advanced than another. Having newer technologies often means more reliant on the Internet and possibly more vulnerable in a cyber security context, but in turn they are there to make it easier to run the farm. These differences in use and advancements of the technologies affects the risk analysis, because it means that the consequence and vulnerability analysis is not entirely correct for everyone.

The data collected and the result of the analysis might therefore not be one hundred percent correct for every farmer, but the general finding are still relevant for everyone. The criticality of the milking robot is equal for every dairy farmer, same with the feeding system for the pig farmers. How dependent the farmer is on the technology in terms of production is still the same. The findings from this research is that the dairy farmers are most dependent on technology in their production, the pigs are the second most dependent, and the suckler cow farmers are the least dependent on technology to produce their product.

5.2 What are the main cyber risks to the production and delivery of produce on these Norwegian farms?

The main risks identified for the interviewed dairy farmers were virus on the milking robot, physical sabotage, unauthorized access to milking robot software and a power outage. These were the four risks that should be considered unacceptable, and what they all have in common is that they affect the integrity or availability of the milking robot. This illustrates just how important the machine is for the production of dairy, being one of the only functions on the farm that can not be performed manually if necessary. Feeding the cows, cleaning the farmhouse and managing the animals can all be done without technology in a time of crisis on the farms that were interviewed, but not the act of milking.

The suckler cow farmers had no discernible critical risks such as the dairy farms have. The identified risks have a lower score because the consequence of the risk scenarios are low. The farmer interviewed did not rely very heavily on digital technology in their production, which makes them less susceptible to consequences that will affect production. The two risks with the highest score is a ransomware attack on Animalia and a denial of service attack on the farmhouse network, both having a total risk score of eight.

The main risks identified for the pig farmers are also not critical, except one, be-

cause they are less reliant on the machines in short time frames. A virus on the feeding system control computer is the identified risk scenario with the highest risk score, with a power outage, a ransomware attack on Animalia and DoS attack on the farmhouse network following close behind. Where the dairy farmers can only go a couple of hours without the milking robot, the pig farmers can potentially go up to twelve hours or more without the feeding machines, without having to resort to alternative solutions. Most of the farmers do not have alternatives in terms of manual solutions or generators for the feeding machines, which is why a virus or prolonged power outages is still a high risk for them.

In the risk analysis overall, there are only a few scenarios that affect integrity compared to availability. This is because attacks that affect integrity has so many factors that play into it. Farmers work with live animals and plats that can all, in some way, alert when something is not working as expected. If the animals receives too little food, they will make the farmer aware of this, same with bad ventilation. The farmers that have worked with animals for at least a couple of years know their animals, and if data they rely on for production suddenly changes, there is a higher likelihood of them noticing this compared to businesses that for example only deals with data.

The data in farming is also spread across a lot of sources and mediums. If for example Husdyrregisteret were attacked and the integrity of the data was compromised, they could gather the correct data from the farmers. A lot of the farmers have the basic information about their animals on paper, especially the cattle farmers, as they have the highest requirements when it comes to traceability. All these factors can reduce the consequence of attacks on integrity, which makes the risk scores lower.

Attacks on confidentiality is not included in the scenarios, simply because the interviewed farmers saw very little consequence tied to confidentiality breaches. In addition, they did not see what the motivation for the attacker could be, as they would not be able to use the data in a way that would affect the farm significantly. The only thing the farmers were worried about was if some activists presented the data in a wrong context to mislead the public about the welfare conditions for the animals.

The way the likelihood is calculated in this research differs from the more traditional methods using factors such as expected frequency. However, because the research is on multiple, separate, small organizations instead of one larger, the more common methods do not fit. The risk situation is also continuously changing, which means that it is important to perform this type of research on a regular bases. During the interviews, several of the farmers who did not have a generator mentioned having considered purchasing one recently, because of the war in Ukraine. They felt that the threat of Russian sabotage on critical infrastructure

in Norway has increased in light of the current political situation.

The risk of power outages is also something that varies for the different farms. Their location has a lot to say in terms of how much a power outage will affect them. One farmer was higher in the mountains, in an area where the power went out somewhat regularly, and the farmer was therefore quite used to having to turn on the generator and using manual alternatives. On the other hand, one farmer was quite close to an oil company, and the power grid in that area was therefore much more robust, and the farmer had thus never had the need for a generator.

Overall, there are some critical risks for the dairy cow and the pig farms, and some non critical but still high scoring risk scenarios for the suckler cow farms. However, the severity of the risks will vary, both because the different farms' reliance on technologies vary, and because some have mitigating measures already in place.

5.3 How can a threat exploit the vulnerabilities of individual farms to affect food production on a national scale?

A cyber attack on one farm will not affect the food industry in Norway. As the risk analysis shows, it is possible to hinder production of produce on a farm through a cyber attack, but an attack on one or a couple of farms will not have a widespread effect when there are over 38 thousand farms in Norway. Therefore, to analyze whether the food production on a national scale can be affected, the suppliers must be considered. The farmers are greatly dependent on other parts of the supply chain in order to produce and deliver their products, and if these are out of commission in some way, there are definite possibilities of there being consequences to the food production.

As the supply chain consists of many different entities, there are several possible targets for cyber attacks. There are three main sections these can be divided into, those that deliver services or products to the farms, those who the farms delivers their products to, and those that receives, analyzes and delivers data. Some, like Tine and Nortura, falls into both the second and third category, but their main business is to receive and process products from the farms. There are also some data processing services that are used by multiple of these organizations, such as LogMeIn and Produsentregisteret, which can lead to consequences for multiple parts of the supply chain in case of a cyber attack.

Farm suppliers

The power suppliers are not someone only the farmers are dependent on. Their critical role for the entire nation makes them a clear target for serious state threat actors, however, this means that they are also heavily protected against potential threats. Most of the farmers interviewed, especially the dairy cow farmers, where all but one had it, have generators as a back up for critical farm functions in cases of power outages. The two suckler cow farms did not have a need for them, and only of the pig farmers had one. Though the pig farmer had also installed solar panels to use as a power source on the farm. Some of the farmers without generators did mention having considered it more in recent times, as the war in Europe increases the view of Russia as a threat to the Norwegian power grid. So even if the Norwegian power supply were to be damaged, many farmers have backup solutions so that they are still capable of running relatively normal. How an attack on the power grid can affect other suppliers is something that can be studied further.

As the risk analysis shows, a virus on the milking robot can have a critical consequence for a dairy farmer. If an attacker could infect multiple milking robots simultaneously, this could have an effect on food production if enough farms were affected. One of the two companies that produce milking robots used by the interview participants, DeLaval, use remote access control for service purposes. This is beneficial for quickly fixing problems, but it makes the machines vulnerable to attacks through the remote access control. Therefore, it might be possible for an attacker who gains access to DeLaval's systems to affect multiple milking robots simultaneously through their remote access control service.

According to a DeLaval service technician, they have to log in to the machines one at a time to perform service, using the LogMeIn solution, and simultaneous attacks would therefore be quite difficult. An analysis and penetration test of DeLaval's systems would need to be performed to gauge if such an attack is feasible. An attack that can work on both Lely and DeLaval milking robots is if the virus is introduced through a software update, similarly to what happened with the SolarWinds cyber attack in 2020 [60]. There, the attackers gained access to Solarwinds systems, and spread their virus through a regular software update for the IT systems monitoring and management software the company supplied. The attack hit 18 000 of SolarWinds customers, and several US federal agencies, along with hundreds of big private companies such as Cisco and Microsoft.

Felleskjøpet is the main food supplier for a lot of farms in Norway. There are other companies that also produce feed, and could take over deliveries if an incident were to occur, but they likely would not be able to supply all the needed food, because there are so many animals. The pig farmers all give their animals several kilos of food per day, and though they often buy feed in bulk, they are dependent

on being able to purchase feed when they need it. One farmer mentioned having a four day buffer when purchasing food, and as they go trough about nine tons in nine days, they really have to receive the food when they need it. So, a cyber attack that stops Felleskjøpet from being able to deliver feed, can have major consequences for meat, eggs and dairy production.

Farm product distributors and processors

The nation has already seen the consequences of a cyber attack on Nortura. Nortura managed to prevent the attacker from encrypting their digital infrastructure, and so the consequences were far less serious, but the intrusion still led to delayed production and shelves empty of Prior, Gilde and Folkets products [61, 62]. If the attackers had succeeded in encrypting the infrastructure, production could have been down for a long time instead of just the 13 days it took before they were able to continue receiving animals for slaughter.

Also Norsvin was hacked in 2021, before the attack on Nortura [63]. They were hit with a ransomware attack, but the backups were not affected, and so they were able to continue mostly as normal, with only the email and order systems being affected. If Norsvin is attacked so that they are not able to operate as usual, this can have major economic consequences for the farmers. One of the pig farmers said that if Norsvin were unable to supply semen within the fertility window of the pigs, it can cost the farm about 100 000 to 150 000 NOK. The breeding of pigs does happen at different times throughout the country, so this type of attack will most likely not hinder production too bad, but the consequence is high for those affected. The fact that the Norsvin attack had so little consequence can be a good sign however, as it at least indicates that there are good incident response routines within the company.

Tine is another potential target as a market regulator because they collect most of the milk from Norwegian dairy cow farms. If they were hit by for example a ransomware attack that encrypted their entire digital infrastructure, the availability of milk in Norway would plummet. Meat can be frozen and stored, so keeping a national emergency storage is easier, but milk is a fresh product than can not be stored for months at a time. Other companies than Tine process the milk to produce diary products, but if Tine's infrastructure is down, they might not be able to collect the milk from the farmers and deliver it to the factories of these other companies.

Data processors

The core businesses of the supply chain might not be the only targets in the Norwegian food supply chain. For remote access control, services such as LogMeIn and TeamViewer are used by the service technicians and the farmers. The threat actors can exploit vulnerabilities in these systems, or weak passwords and a lack of two

factor authentication to gain access to farm systems. In 2021, a water treatment facility in Florida was attacked using remote access, most likely through TeamViewer [64].

Produsentregisteret is used by some of the organizations, such as Tine, Geno and Animalia, as a login service. This shared access makes Produsentregisteret a possible target to hinder access to the services of these companies. The extent of damage this can cause in terms of what can still be accessed and not, and whether a hacker can gain access to the other organization through this login service, should be determined in order to be more risk aware and possibly protect against such an attack.

Another joint service used by Norwegian farmers and agriculture actors is Landbrukets Dataflyt SA. Today's company is a merger between an earlier version of Landbukets Dataflyt and Produsentregisteret, and is owned by 18 organizations, such as Nortura, Gjensidige, Tine and Sparebank 1 [65]. The intention is to have one place for authentication, so that the farmer can log in only once and get access to all the different online services that are part of the collaboration. The solution is also developed to facilitate data sharing in a secure fashion with consent from the farmer to ensure ownership of the data. This shared authentication and data access makes it a potential target for cyber attacks, especially to gain access to these other organizations and the data that is shared.

In general, getting an overview of the entire supply chain can be quite beneficial when working towards discovering vulnerabilities and potential targets. Landbrukets Dataflyt facilitates data flow between the bigger organizations, but which organizations and solutions are involved in the data flow between these larger ones and their partners and suppliers should be analyzed for weaknesses. A mapping of all the individual actors involved in food production in Norway should be created to get a full overview of potential targets.

One of the farmers interviewed also works for Nibio, which is a research institute within bioeconomics in Norway. From their personal experience as a farmer, they mentioned that a cyber attack that only goes after data can have consequences on a national scale as well. The data collected on how many animals there are, where they are and such, may also be used to plan the import of food, and give an overview of how much food we are able to produce ourselves. Landbruksdirektoratet measures our degree of self-sufficiency each year, and this analysis can give valuable insights when planning our food import [18].

In summary

The conclusion is that the supply chain is a more fruitful target for state actors than individual farms, however, basic protection from cyber attacks on the indi-

vidual farms can help protect against a larger attack. For example, enabling two factor authentication and using strong passwords for remote access services can reduce the consequence of a coordinated remote access control attack by a nation state actor. The National Cyber Security Centre (NCSC) in the UK have developed a cyber security guide specifically for farmers together with the National Farmers Union in the country [66].

Overall, there are many potential scenarios where a serious an capable threat actor could affect food production in Norway. How feasible each of the possibilities mentioned are, is not a part of this research, but should be the focus of future research. Which area within agriculture is attacked will also greatly affect the consequence, as there is a difference in how large the emergency storage of different types of produce can be, and some products are also easier to import than others. Plant based food production, such as vegetables and cereals are also not analyzed, and their dependency on technology and vulnerabilities might be quite different. However, this research project shows how important it is to focus on security on the level that can cause the most damage, namely the supply chain.

5.4 Limitations

As this is a qualitative study, the data is not fully representative of the industry. Therefore, some of the details of this research may not be correct for everyone. This is noted in the research, as not all the farmers interviewed use the same technologies. However, this does not mean that the results are not sound and relevant on a general level.

The farmers interviewed in this research are all in the medium or large category in terms of size. This can be attributed to the fact that smaller farms might not use as much technology, and therefore were not interested in participating. One farmer that was contacted did not wish to participate as they felt they used too little technology to be relevant to the research project. Additionally, the larger farms might be more active in organizations such as Norsk Bondelag, Norsvin and Felleskjøpet, and therefore the participants gathered through these were of a larger size. Thus, the research is more relevant for medium and large sized farms than the smaller ones.

Chicken farms were initially a part of the scope for the thesis, but they were removed because there were too few interview participants. Only one interview with a chicken farmers was completed, and though the interview gave a lot of valuable and relevant data, one data source was not enough to be able to include the findings in the research.

5.5 Future work

The farms interviewed in this research are just two of the many different types of farms there are in Norway, which can all have different uses for technologies and dependencies on them. For example, the interview with the chicken farmer did reveal that chicken farmers are very dependent on technology, because the chickens are so sensitive to temperature changes, and need constant heat to survive. Also, some of the farmer that have cattle also have sheep, where some use technologies such as geofencing, where the animals are placed in virtually fenced in areas [67].

Other farmer also worked within plant agriculture such as cereals. Based on what the farmers said, the impression is that it seems easier to disrupt the technologies they use. Specifically the newest tractors seems to be dependent on the Internet to work as self driving vehicles. However, it seems that the consequences when the technologies do not work are lower than dairy production especially, because the farmer can operate the tractor manually. The technologies are mostly based on optimizing the crop output more than being critical for production, but research specifically into this type of farming is needed to confirm this information.

In addition, there are possible targets in the supply chain for plant farming as well. One farmer interviewed mentioned that the companies, such as Felleskjøpet, that receive cereals from farmers, can be a bottleneck, and if a fire broke out at the facility, the farmers would not be able to send the collected cereals to the facility, which means they would go to waste. How critical such a situation can become should be researched further, both in terms of plant producing farms, but also how this can affect the delivery of animal feed to livestock farms.

The farmer working at Nibio also mentioned that Kartverket's CPOS services could be a target for cyber attacks against precision agriculture [68]. These services rely on GNSS, which Gupta et al. describe as a possible target for radio frequency jamming attacks [8]. Another farmer mentioned having faced more issues with GPS, which is used by many tractors for self driving, because the Russian military takes satellites out of their regular course to use in the war effort. One farmer also knows someone who lives in an area where the American military visits somewhat regularly, where the GPS signals in the area are blocked every time they are there. The reliance on global navigation satellite system (GNSS) should be considered when analyzing the farms that produce cereal grains and vegetables.

As mentioned in the discussion, there are plenty of opportunities for further research within the supply chain of Norwegian food production. The focus can be on the individual organizations and their importance to the food production, but there should also be a focus on the services used to connect the different organizations, such as Landbrukets Dataflyt.

Chapter 6

Conclusion

The findings from the first research question about which technologies are used on Norwegian cattle and pig farms, are that Norwegian dairy cow farms are first and foremost dependent on the milking robot, and the ID tag connected to it, for their production. The farmers interviewed use other technologies as well, such as feeding and manure robots, but all the dairy cow farms in this study have manual backup routines for these other technologies. For the pig farmers, the feeding system is the most critical technology, because they have too many pigs to have the capacity for the manual labor required to feed them manually. The suckler cow farms use many of the same technologies as the dairy farmers, but none of them are critical for their type of production.

The risk assessment for the dairy farms yielded 10 risk scenarios, where the highest scoring ones are those that affect the availability of the milking robot, or the integrity of the milking robot software. The likelihood of attacks such as a computer virus or unauthorized access through remote access control systems is high, because they are relatively easy for a capable threat actor to perform. For the suckler cow farms, no critical risks were identified because they rely less on technology. The highest scoring risks for the suckler cow farm is a ransomware attack on Animalia that hinders access to their farm management software Storfekjøttkontrollen, and a denial of service attack on the farmhouse network, which again prevents access to the management software. For the pig farms, the highest scoring risk scenario was a computer virus on the feeding system control computer, because this affects the availability of their most critical asset. These risks can vary between different farms within the same production type, and some farms have more mitigating strategies in place than others, but these are generalized findings that are relevant for several medium or large sized cattle and pig farms in Norway.

Hitting just one farm will not affect food supplies, so threat actors interested in impacting food production on a national scale are more likely to focus on other elements of the supply chain. These threat actors might look more at farm suppliers like Felleskøpet and Norsvin, data processors like Animalia, and the market

regulators of meat and dairy, Nortura and Tine, because attacks on this level can have consequences for farms throughout the country. These organizations, their vulnerabilities and importance for Norwegian food production, should be studied further. Additionally, services such as Landbrukets Dataflyt, which gives a collective sign on solution to access several different agricultural software solutions, and secure sharing of data between farmers and organizations, should be studied. Research into how cyber attacks on these types of organizations can affect the food supply chain should be completed, as well as research into what the consequences of these types of attacks can be for the individual farms.

Bibliography

[1] NSM, 'Risiko 2022,' Tech. Rep., 2023.

[2] L. Barreto and A. Amaral, 'Smart farming: Cyber security challenges,' in *2018 International Conference on Intelligent Systems (IS)*, IEEE, 2018, pp. 870–876.

[3] F. Chien, A. Anwar, C.-C. Hsu, A. Sharif, A. Razzaq and A. Sinha, 'The role of information and communication technology in encountering environmental degradation: Proposing an sdg framework for the brics countries,' *Technology in Society*, vol. 65, p. 101 587, 2021.

[4] K. Grgić, D. Žagar, J. Balen and J. Vlaović, 'Internet of things in smart agriculture—possibilities and challenges,' in *2020 International Conference on Smart Systems and Technologies (SST)*, IEEE, 2020, pp. 239–244.

[5] A. Yazdinejad, B. Zolfaghari, A. Azmoodeh, A. Dehghantanha, H. Karimipour, E. Fraser, A. G. Green, C. Russell and E. Duncan, 'A review on security of smart farming and precision agriculture: Security aspects, attacks, threats and countermeasures,' *Applied Sciences*, vol. 11, no. 16, p. 7518, 2021.

[6] M. A. Ferrag, L. Shu, O. Friha and X. Yang, 'Cyber security intrusion detection for agriculture 4.0: Machine learning-based solutions, datasets, and future directions,' *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 3, pp. 407–436, 2021.

[7] K. Kjønås and G. B. Wangen, 'A survey on cyber security research in the field of agriculture technology,' IEEE, 2023.

[8] M. Gupta, M. Abdelsalam, S. Khorsandroo and S. Mittal, 'Security and privacy in smart farming: Challenges and opportunities,' *IEEE Access*, vol. 8, pp. 34 564–34 584, 2020.

[9] Nortura Medlem. 'Nortura er utsatt for et dataangrep, oppdatert sak.' (), [Online]. Available: `https://medlem.nortura.no/nyheter/nortura-er-utsatt-for-et-dataangrep-oppdatert-sak-article45484-11885.html` (visited on 10/10/2022).

[10] G. Idoje, T. Dagiuklas and M. Iqbal, 'Survey for smart farming technologies: Challenges and issues,' *Computers & Electrical Engineering*, vol. 92, p. 107 104, 2021.

[11] V. Moysiadis, P. Sarigiannidis, V. Vitsas and A. Khelifi, 'Smart farming in europe,' *Computer science review*, vol. 39, p. 100 345, 2021.

[12] S. Taiwo and M. Vezi-Magigaba, 'Human capital perspective of previous industrial revolutions: Review in support of 4ir and its possible impacts,' *Multicultural Education*, vol. 7, no. 8, pp. 86–96, 2021.

[13] T. Wang, X. Xu, C. Wang, Z. Li and D. Li, 'From smart farming towards unmanned farms: A new mode of agricultural production,' *Agriculture*, vol. 11, no. 2, p. 145, 2021.

[14] S. J. Kim and M. H. Lee, 'Design and implementation of a malfunction detection system for livestock ventilation devices in smart poultry farms,' *Agriculture*, vol. 12, no. 12, p. 2150, 2022.

[15] Statistics Norway. 'Fakta om jordbruk.' (), [Online]. Available: https://www.ssb.no/jord-skog-jakt-og-fiskeri/faktaside/jordbruk (visited on 06/02/2023).

[16] T. Ladstein and T. Skoglund, 'Utviklingen i norsk jordbruk 1950-2005,' Statistics Norway, Tech. Rep., 2007.

[17] Statistics Norway. 'Gardbruk, jorbruksareal og husdyr.' (), [Online]. Available: https://www.ssb.no/jord-skog-jakt-og%20fiskeri/jordbruk/statistikk/gardsbruk-jordbruksareal-og-husdyr (visited on 06/02/2023).

[18] Landbruksdirektoratet. 'Norsk landbruk - tall og fakta.' (), [Online]. Available: https://www.landbruksdirektoratet.no/nb/norsk-landbruk-tall-og-fakta (visited on 06/02/2023).

[19] Tine. 'Vi er de mange små som blir én stor.' (), [Online]. Available: https://www.tine.no/om-tine/vi-er-de-mange-sma-som-blir-en-stor (visited on 15/05/2023).

[20] Q-meieriene. 'Q-gården.' (), [Online]. Available: https://www.q-meieriene.no/q-gaarden (visited on 15/05/2023).

[21] Nortura medlem. 'Produksjonssteder.' (), [Online]. Available: https://medlem.nortura.no/organisasjon/kontaktinfo/produksjonssteder/ (visited on 15/05/2023).

[22] Nortura. 'Om oss.' (), [Online]. Available: https://www.nortura.no/om-nortura (visited on 15/05/2023).

[23] Nortura. 'Vår matproduksjon.' (), [Online]. Available: https://www.nortura.no/verden-beste-r%5C%C3%5C%A5varer/v%5C%C3%5C%A5r-matproduksjon (visited on 15/05/2023).

[24] A. R. de Araujo Zanella, E. da Silva and L. C. P. Albini, 'Security challenges to smart agriculture: Current state, key issues, and future directions,' *Array*, vol. 8, p. 100 048, 2020.

[25] S. Sontowski, M. Gupta, S. S. L. Chukkapalli, M. Abdelsalam, S. Mittal, A. Joshi and R. Sandhu, 'Cyber attacks on smart farming infrastructure,' in *2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)*, IEEE, 2020, pp. 135–143.

[26] K. Tsiknas, D. Taketzis, K. Demertzis and C. Skianis, 'Cyber threats to industrial iot: A survey on attacks and countermeasures,' *IoT*, vol. 2, no. 1, pp. 163–186, 2021.

[27] R. S. M. Joshitta and L. Arockiam, 'Security in iot environment: A survey,' *International Journal of Information Technology and Mechanical Engineering*, vol. 2, no. 7, pp. 1–8, 2016.

[28] D. Diaz Lopez, M. Blanco Uribe, C. Santiago Cely, A. Vega Torres, N. Moreno Guataquira, S. Morón Castro, P. Nespoli and F. Gómez Mármol, 'Shielding iot against cyber-attacks: An event-based approach using siem,' *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[29] C. Theisen, N. Munaiah, M. Al-Zyoud, J. C. Carver, A. Meneely and L. Williams, 'Attack surface definitions: A systematic literature review,' *Information and Software Technology*, vol. 104, pp. 94–103, 2018.

[30] D. Van Der Linden, O. A. Michalec and A. Zamansky, 'Cybersecurity for smart farming: Socio-cultural context matters,' *IEEE Technology and Society Magazine*, vol. 39, no. 4, pp. 28–35, 2020.

[31] J. Nikander, O. Manninen and M. Laajalahti, 'Requirements for cybersecurity in agricultural communication networks,' *Computers and electronics in agriculture*, vol. 179, p. 105 776, 2020.

[32] A. Geil, G. Sagers, A. D. Spaulding and J. R. Wolf, 'Cyber security on the farm: An assessment of cyber security practices in the united states agricultural industry,' *International Food and Agribusiness Management Review*, vol. 21, no. 1030-2018-1811, pp. 317–334, 2018.

[33] R. Prodanović, D. Rančić, I. Vulić, N. Zorić, D. Bogićević, G. Ostojić, S. Sarang and S. Stankovski, 'Wireless sensor network in agriculture: Model of cyber security,' *Sensors*, vol. 20, no. 23, p. 6747, 2020.

[34] N. Peppes, E. Daskalakis, T. Alexakis, E. Adamopoulou and K. Demestichas, 'Performance of machine learning-based multi-model voting ensemble methods for network threat detection in agriculture 4.0,' *Sensors*, vol. 21, no. 22, p. 7475, 2021.

[35] M. A. Ferrag, L. Shu, H. Djallel and K.-K. R. Choo, 'Deep learning-based intrusion detection for distributed denial of service attack in agriculture 4.0,' *Electronics*, vol. 10, no. 11, p. 1257, 2021.

[36] M. A. Ferrag, L. Shu, X. Yang, A. Derhab and L. Maglaras, 'Security and privacy for green iot-based agriculture: Review, blockchain solutions, and challenges,' *IEEE Access*, vol. 8, pp. 32 031–32 053, 2020. DOI: 10.1109/ACCESS.2020.2973178.

[37] R. Chaganti, V. Varadarajan, V. S. Gorantla, T. R. Gadekallu and V. Ravi, 'Blockchain-based cloud-enabled security monitoring using internet of things in smart agriculture,' *Future Internet*, vol. 14, no. 9, p. 250, 2022.

[38] A. Vangala, A. K. Das, N. Kumar and M. Alazab, 'Smart secure sensing for iot-based agriculture: Blockchain perspective,' *IEEE Sensors Journal*, vol. 21, no. 16, pp. 17 591–17 607, 2021. DOI: 10.1109/JSEN.2020.3012294.

[39] S. E. Duncan, R. Reinhard, R. C. Williams, F. Ramsey, W. Thomason, K. Lee, N. Dudek, S. Mostaghimi, E. Colbert and R. Murch, 'Cyberbiosecurity: A new perspective on protecting us food and agricultural system,' *Frontiers in bioengineering and biotechnology*, vol. 7, p. 63, 2019.

[40] K. Demestichas, N. Peppes and T. Alexakis, 'Survey on security threats in agricultural iot and smart farming,' *Sensors*, vol. 20, no. 22, 2020, ISSN: 1424-8220. DOI: 10.3390/s20226458. [Online]. Available: https://www.mdpi.com/1424-8220/20/22/6458.

[41] E. Kristen, R. Kloibhofer, V. H. Díaz and P. Castillejo, 'Security assessment of agriculture iot (aiot) applications,' *Applied Sciences*, vol. 11, no. 13, p. 5841, 2021.

[42] X. Yang, L. Shu, J. Chen, M. A. Ferrag, J. Wu, E. Nurellari and K. Huang, 'A survey on smart agriculture: Development modes, technologies, and security and privacy challenges,' *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 2, pp. 273–302, 2021.

[43] J. West, 'A prediction model framework for cyber-attacks to precision agriculture technologies,' *Journal of Agricultural & Food Information*, vol. 19, no. 4, pp. 307–330, 2018.

[44] P. D. Leedy and J. E. Ormrod, *Practical Research: Planning and Design, Global Edition*, 6th ed. Pearson, 2016.

[45] Nvivo. 'About nvivo.' (), [Online]. Available: https://help-nv.qsrinternational.com/20/win/Content/about-nvivo/about-nvivo.htm (visited on 15/05/2023).

[46] M. Talabis and J. Martin, *Information security risk assessment toolkit: Practical assessments through data collection and data analysis*. Newnes, 2012.

[47] International Organization for Standardization, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*, ISO/IEC 27005:2022(E). Vernier, Geneva, Switzerland: International Organization for Standardization, 2022.

[48] G. Wangen, A. Shalaginov and C. Hallstensen, 'Cyber security risk assessment of a ddos attack,' in *Information Security: 19th International Conference, ISC 2016, Honolulu, HI, USA, September 3-6, 2016. Proceedings 19*, Springer, 2016, pp. 183–202.

[49] Mattilsynet. 'Hva skal du rapportere til husdyrregisteret?' (), [Online]. Available: https://www.mattilsynet.no/dyr/produksjonsdyr/storfe/rapport-til-husdyrregisteret (visited on 02/05/2023).

[50] Mattilsynet. 'Krav til dyreholdjournal for storfe.' (), [Online]. Available: https://www.mattilsynet.no/dyr/produksjonsdyr/storfe/krav-til-dyreholdjournal-for-storfe (visited on 02/05/2023).

[51] DeLaval. 'Delaval delpro™ besetningsstyringsplattform.' (), [Online]. Available: https://www.delaval.com/no/utforsk/delaval-delpro/ (visited on 03/05/2023).

[52] Lely. 'T4c management system.' (), [Online]. Available: https://www.lely.com/farming-insights/t4c-management-system/ (visited on 03/05/2023).

[53] Lely. 'Lely horizon.' (), [Online]. Available: https://www.lely.com/us/solutions/farm-management/horizon/ (visited on 03/05/2023).

[54] Tine. 'Husdyrkontrollen.' (), [Online]. Available: https://medlem.tine.no/gard-og-drift/husdyrkontrollen (visited on 02/05/2023).

[55] Lely. 'Lely qwes.' (), [Online]. Available: https://www.lely.com/solutions/milking/qwes/ (visited on 03/05/2023).

[56] OS ID. 'Full oversikt, bedre lønnsomhet og mer frihet.' (), [Online]. Available: https://www.osid.no/aktivitetsmaling/ (visited on 03/05/2023).

[57] Lovdata. 'Forskrift om hold av svin.' (), [Online]. Available: https://lovdata.no/dokument/SF/forskrift/2003-02-18-175 (visited on 12/05/2023).

[58] Mattilsynet. 'Øremerking av svin.' (), [Online]. Available: https://www.mattilsynet.no/dyr/produksjonsdyr/svin/oremerking-av-svin (visited on 12/05/2023).

[59] Produsentregisteret. 'Velkommen til produsentregisteret.' (), [Online]. Available: https://sak.prodreg.no/ (visited on 13/05/2023).

[60] M. Willett, 'Lessons of the solarwinds hack,' *Survival*, vol. 63, no. 2, pp. 7–26, 2021.

[61] H. Simonsen. 'Konsekvensene ble mindre enn de kunne blitt.' (), [Online]. Available: https://medlem.nortura.no/arkiv-2022/konsekvensene-ble-mindre-enn-de-kunne-blitt-article45593-18928.html (visited on 26/05/2023).

[62] L. F. Vogt, A. Nordby and I. A. Nordrum. 'Trente på dataangrep – måneder senere ble de hacket.' (), [Online]. Available: https://www.nrk.no/innlandet/nortura-ovde-pa-dataangrep_-i-jula-ble-selskapet-hacket-1.15795956 (visited on 26/05/2023).

[63] NTB. 'Norsvin rammet av løsepengevirus.' (), [Online]. Available: https://www.digi.no/artikler/norsvin-rammet-av-losepengevirus/514970 (visited on 26/05/2023).

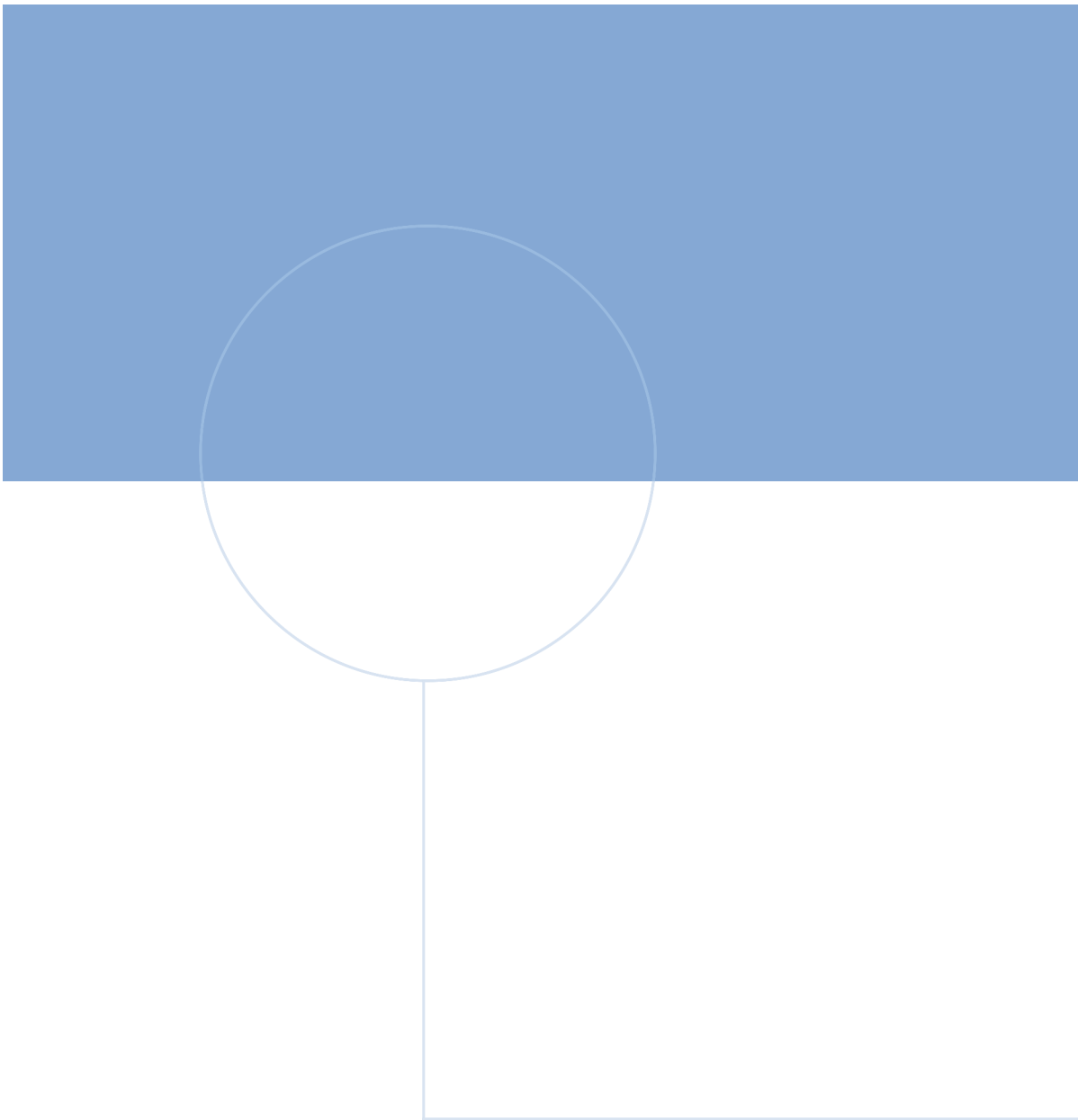
[64] Cybersecurity and Infrastructure Agency. 'Compromise of u.s. water treatment facility.' (2021), [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-042a (visited on 26/05/2023).

[65] Landbrukets Dataflyt SA. 'Om selskapet.' (), [Online]. Available: https://www.landbruketsdataflyt.com/om-oss/selskapet (visited on 26/05/2023).

[66] NCSC and NFU, 'Cyber security for farmers: Practical tips on how to stay safe,' NCSC, Tech. Rep., 2021.

[67] S. Sivakumar, B. Maruthi Shankar, M. Mahaboob, N. Adhish, R. Dineshkumar and N. Rahul, 'Sustainable farming and customized livestock management using internet of things,' in *Proceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022*, Springer, 2023, pp. 543–552.

[68] Kartverket. 'Få veiledning om cpos.' (), [Online]. Available: https://www.kartverket.no/til-lands/posisjon/hva-er-cpos (visited on 27/05/2023).



NTNU

Norwegian University of
Science and Technology