jamk.fi

Cybersecurity in Agricultural Communication Networks

Case Dairy Farms

Onni Manninen

Master's thesis
December 2018
School of Technology, Communication and Transport
Degree Programme in Information and Communication Technology
Cyber Security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s)	Type of publication	Date
Manninen, Onni	Master's thesis	December 2018
		Language of publication: English
	Number of pages 73	Permission for web publication: x

Title of publication
Cybersecurity in Agricultural Communication Networks
Case Dairy Farms

Degree programme
Master's Degree Program in Information Technology, Cybersecurity

Supervisor(s)
Kotikoski, Sampo; Saharinen, Karo

Assigned by
Natural Resources Institute Finland,
Nikander, Jussi; Laajalahti, Mikko

Abstract

Agricultural industry in Finland has used modern computing since the late 1950s, however, in the last decade digitalization in the industry has started to grow like never before. There is little public conversation about cybersecurity concerning agriculture. While there have been some earlier publications around the subject, there has not been any research focusing on networks in primary production.

The following questions needed to be answered: what kind of threats can be found in a farm's telecommunication networks, is it possible to find threats which are unique only to the agricultural industry? How is it possible to fix threats found on case farms and is it possible to generalize farm telecommunication networks' cyber threats based on the farms chosen for this case study?

The research method was chosen to be qualitative research based on data gathered during visits at carefully selected dairy farms. During the visits, farm network environment was documented and entrepreneurs were interviewed.

Findings from the case farms corresponded to the findings and observations from other research. Various kind of threats in telecommunication implementations were found, and protection against cyberattacks was at very basic level.

As a conclusion, the research confirmed that there is a real need for cybersecurity training and common guidelines to primary production about how farms should protect themselves against modern cyber threats.

Keywords/tags
Agriculture industry, primary production, communication networks, cybersecurity

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Manninen, Onni	Opinnäytetyö, ylempi AMK	Joulukuu 2018
		Julkaisun kieli: Englanti
	Sivumäärä 73	Verkkojulkaisulupa myönnetty: x

Työn nimi
Kyberturvallisuus maatalouden tietoliikenneverkoissa
Tapaustutkimus: maitotilat

Tutkinto-ohjelma
Master's Degree Program in Information Technology, Cybersecurity

Työn ohjaaja(t)
Kotikoski, Sampo; Saharinen, Karo

Toimeksiantaja(t)
Luonnonvarakeskus,
Nikander, Jussi; Laajalahti, Mikko

Tiivistelmä

Maatalouden toimiala Suomessa on käyttänyt tietotekniikkaa aina 1950-luvun lopulta saakka, mutta viimeisen vuosikymmenen aikana alan digitalisoituminen on alkanut kiihtyä ennennäkemättömällä vauhdilla. Tästä huolimatta julkisuudessa on ollut vain vähän keskustelua kyberturvallisuudesta aiheen ympärillä. Vaikka joitain aiempia julkaisuja aiheesta löytyykin, ei tutkimustyötä, joka keskittyy alkutuotannon tietoliikenneverkkoihin, ole tehty.

Tutkimustyö ottaa kantaa seuraaviin tutkimuskysymyksiin: millaisia uhkia maatilojen tietoliikenneverkoista voidaan löytää, onko mahdollista löytää uhkia, jotka koskevat erityisesti maataloutta, kuinka löydettyjä uhkia voidaan korjata ja torjua sekä onko mahdollista tehdä yleistyksiä maatilojen tietoliikenneverkkojen kyberuhista pohjautuen löydöksiin valituilta maatiloilta?

Tutkimusmetodiksi valittiin laadullinen tutkimus perustuen tietoon, joka kerättiin käyntien aikana huolella valituilta maitotalouden maatiloilta. Käyntien aikana maatilojen verkkoympäristöt dokumentoitiin ja yrittäjiä haastateltiin.

Löydökset maatiloilta vastaavat muiden julkaisujen löydöksiä ja havaintoja. Erilaisia uhkia maatilojen tietoliikenneverkkojen toteutuksista löytyi, ja suojautumisen taso kyberhyökkäyksiä vastaan oli alhainen.

Lopputuloksena tutkimus vahvisti oletukset siitä, että maatalouden toimialalla on todellinen tarve tietoturvakoulutukselle sekä yleisille ohjeistuksille siitä, kuinka maatilat voivat suojautua moderneja kyberuhkia vastaan.

Avainsanat
Maatalous, alkutuotanto, tietoliikenneverkot, kyberturvallisuus

Contents

Figures

Tables

Acronyms

ADSL	Asymmetric Digital Subscriber Line
AP	Access Point
ARP	Address Resolution Protocol
CIA	Confidentiality, Integrity, Availability
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol (data protocol), Foiled Twisted Pair (cable type)
FTTH	Fiber to the Home
Gbps	Gigabit per second
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
IMAP	Internet Message Access Protocol
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LAN	Local Area Network
Mbps	Megabit per second
MM	Multi Mode (Optical fiber type)
MTBF	Mean Time Between Failures
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
NAS	Network Attached Storage
NFS	Network File System
OSI	Open Systems Interconnection
PC	Personal Computer
PoE	Power over Ethernet
POP3	Post Office Protocol 3

RAID	Redundant Array of Inexpensive Disks
RFID	Radio Frequency Identification
RIP	Routing Information Protocol
RPC	Remote Procedure Call
RTO	Recovery Time Objective
SLA	Service Level Agreement
SM	Single Mode (Optical fiber type)
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
UTP	Unshielded Twisted Pair (cable type)
VDSL	Very-high-bit-rate Digital Subscriber Line
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WiFi	Wireless Local Area Network technology
WLAN	Wireless Local Area Network

1 Introduction

1.1 Digitalization of agrigultural industry and farms

Agriculture is one of the oldest industries in the world. In Finland, agricultural industry has been using computer technology since the late 1950s for counting genomes and breeing data with central computers. In the beginning of the 1980s, remote terminals were introduced which could connect directly from farms to central computer using modem connection. It was the early stage of the internet we know today. (Syväjärvi 2016)

Although agricultural Industry has used computer technology for a long time, digitalization in the industry has started to increase over the last decade like never before. Digital farming describes the evolution in agriculture and agricultural engineering. Nowadays computing and telecommunication networks are a mandatory part of modern farming, and without modern technology, it is almost impossible to compete in the farming business. (CEMA / European Agricultural Machinery 2017)

While IoT, robots, automation and other technical inventions are getting a larger and larger foothold in the agricultural industry, and demands for secure, reliable and durable IT solutions are needed more than ever before, there is quite little public conversation about cybersecurity around the topic.

In the last five years manure cleaning robots and cow activity sensors have increased their popularity in cow dairy farms. Activity sensor data combined with automated milking systems' milk analytics makes it possible to get vital health information about cows in real time. The new technology can help farmers respond faster to their cows' health problems and increase milk production by optimizing their work based on data analytics from automation data and cow sensors.

1.2 Cybersecurity challenges in farms

In 2013, there were over 50 000 agricultural businesses in Finland. (National Resources Institute Finland 2015) Even though the agricultural industry has used modern computing alonside daily work for several decades, overall technical skills to master challenges of information technolgy are usually at the basic level.

The core of primary production business is to grow biomass like plants, vegetables, grain or animals. A typical operating environment in primary production is a farm. An average business is classified as a micro- or small size business and is usually run within the family or in co-operation with a small group of other families. Besides the fact that employee count is usually small in primary production businesses, challenges in cybersecurity do not necessary differ significantly from other type businesses. (Laajalahti & Nikander 2017)

Like in other businesses, there is also information that should be protected. Businesses in agriculture do not run without computers or smart phones, emails, bookkeeping and devices where all business-critical data is stored. There can also be for example surveillance systems, production robots or even GPS guided vehicles in use. Almost every modern technical device is connected to a network or supports a network connection, and in the worst-case scenario, stops working or at least will work with limited features without a network connection.

Although information technology is nowadays a mandatory part of primary production, technical skill level of the employees can vary from a non-technical person to a medium skill-level person. In case of a computer or network fault in the IT system, an average farm employee may not be able to fix the problems by themselves, which can pose a major threat to business. To lower this kind of threat, entrepreneurs can always outsource IT services to professional service providers.

According to the research of Mikko Laajalahti & Jussi Nikander (2017) from Natural Resources Institute Finland, technical environment in farms is rarely designed in advance or built by the design. It is more usual that technical environment is built organically during the years as needed, and the result can be something that is hard to understand, maintain or upgrade. (Laajalahti & Nikander 2017)

1.3 Threats against primary production IT and network security

As with other industries, even in primary production farms' information technology solutions and networks may face various threats to business continuity including environmental and physical threats as well as technical, social and third party threats.

Environmental and physical threats to the business may include threats such as thunderstorms, fire, floods or water damage, dust and dirt (Figure 1) on equipment, animals causing physical damage to hardware and cables, or activists and burglars.

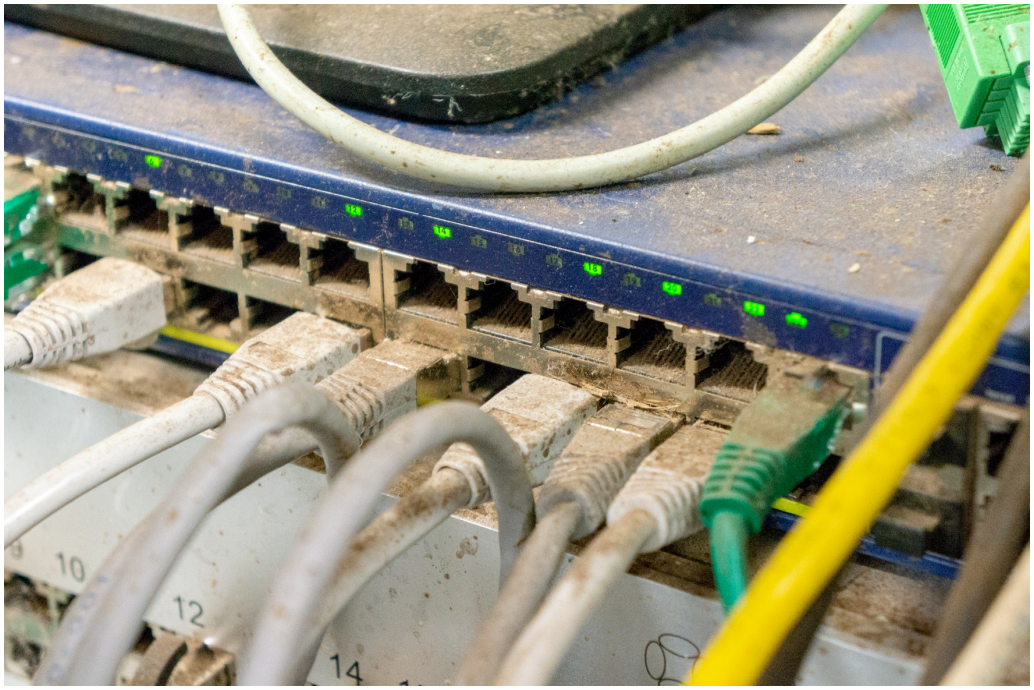

Figure 1. Example of a physical threat to network availability

Cyber threats through the internet connection are often invisible. Even though primary production is by nature a less technical industry than many other types of businesses, it does not necessary mean that it is protected against modern cyber threats. Poor endpoint protection against malware and viruses, phishing emails, ransomware and other modern cyberattacks can also affect farms and their employees.

Nowadays it is mandatory to have modern computers and telecommunication networks in farms. In order to run a farm business, employees need to use computers, smart phones and tablets to access and send data, place orders, keep in touch with other parties and fulfill legal regulations. Sending email, accessing the internet, making online orders or for example reporting born or deceased animals to the authorities makes farm businesses vulnerable to online cyberattacks.

Examples of third-party threats can be interferences with water or electricity distribution, network outages or disruptions in food supply chain during emergency situations. Third-party threats can also include house guests, barn visitors, caretakers, service provider technicians and other external parties who are visiting the farms and need to connect their laptops and other network devices to the farm network. If the third-party device is contaminated, connecting the device to the farm network will jeopardize the security of other devices on the network.

Social threats are one of the biggest cybersecurity threats in the normal business and they cannot be underestimated in agricultural industry. A social threat usually comes from inside the organization and is caused by the personnel. The employees' lack of technical education, inadequate guidance, poor password management of devices, and lack of understanding the cyber risks can cause a significant risk to the business in primary production.

1.4 Previous publications on primary production and cybersecurity

There have been only a few publications about primary production and cybersecurity in the past few years. In 2016, Capgemini Consulting published a short article discussing cybersecurity in the agrifood sector in general. The article states that the agrifood sector has many data-driven innovations, and that many parts of modern farming have been digitalized so that data which previously existed on paper is nowadays digitalized to computer data. Data needs to be continuously available, so its vulnerability is a threat to the primary process. (Capgemini Consulting 2016)

In the article, Capgemini (2016, 4) predicts that growing digital requirements and trends like mobility, cloud computing, IoT and Big Data will continuously pose new challenges when it comes to cybersecurity. New technology in agricultural industry,

such as data platforms, wireless sensor networks, RFID, GPS and business management systems, can be vulnerable to breakdown, abuse or misuse.

At the end of the article, very topical questions were raised about who should take responsibility on cybersecurity in primary production, how the different cultural biases and legal systems between the US, Europe and Asia on cybercrimes should be considered, and who will organize cybersecurity guidelines in primary production. (Capgemini Consulting 2016)

Nicola Russell from Tufts University published an article called “Cybersecurity and Our Food Systems” in December 2017. Russell addressed the topic at a general level, but he mentioned in his article that there are at least two large areas of concern regarding food systems: disruption of distribution, and the malicious tampering or adulteration of the food supply. In February of 2013, the US Department of Homeland Security identified the Food and Agriculture industry as one of the sixteen national critical infrastructures. (Russell 2017)

Jason West from University of Queensland also published in December 2017 an article “A Prediction Model Framework for Cyberattacks to Precision Agriculture Technologies”. In his article West states that “There are two types of precision agriculture systems – those that have been hacked, and those that will be.” He introduced modern cyberattack methods and addressed a system for evaluating the vulnerability level of precision agriculture through CVSS scoring in his article. (West 2017)

In 2017, Natural Resources Institute Finland’s researchers Laajalahti and Nikander published an article about “Cyberthreats in primary production”. The article discussed cyberthreats in the agricultural industry, including an introduction to a digital farm work environment, vulnerable devices and equipment, information systems in primary production and solutions to the threats in general. (Laajalahti & Nikander 2017)

One of the most recent publications on the agriculture cybersecurity genre is “Threats to Precision Agriculture” from Public-Private Analytic Exchange Program, which was published by US Department of Homeland Security in October 2018. In this article, cybersecurity in agriculture was discussed through key threats to

confidentiality, integrity and availability; precision agriculture was explained in detail, and a prediction was made about who would be targeted when precision agriculture is impacted by cyber criminals. The article also contained different hypothetical threat case scenarios and addressed further areas of additional research in the future. (US Department of Homeland Security (DHS) 2018)

2 Theory

2.1 Fundamentals of Information Systems Security

Farms in general are run by a small group of people and their IT systems are not as complex as those of larger, more technology-oriented companies. Even though the basics of information security apply to every company, there is no need to dig too deep in advanced information security guidelines to raise the level of cybersecurity and awareness in the agricultural industry.

There are several standards and guides that can be used to achieve and audit security techniques and methods. Here are some of the well-known standards and guides:

- ISO/IEC 27001 and 27002 standards– Information security management systems
- Finnish Ministry of Finance, VAHTI guides – Information security instructions
- Finnish Ministry of Defense, KATAKRI – Information security audit tool for authorities
- NIST Cybersecurity Framework – Guidance how to protect critical infrastructures

Even though all the current standards and audit tools are undoubtedly the best way to design and audit information security systems, they were too complicated to use in simple network environments such as small farms where information security must be approached with a simpler, more easily understandable and down-to-earth method.

Confidentiality, Integrity and Availability combined form the basic ground of information security and is a widely applicable cybersecurity model. These tenets are often called the CIA triad which is presented in Figure 2 on page 13.

The CIA triad is used to plan information security controls. When designing and using security controls, one or more of these tenets are addressed in the design depending on the purpose of security control. (Kim & Solomon 2012, 10)

Figure 2. CIA triad

According to Kim and Solomon (2012) these three tenets are

- **Availability** – Information is accessible by authorized users whenever they request the information
- **Integrity** – Only authorized users can change information
- **Confidentiality** – Only authorized users can view information.

Availability refers to the availability or non-availability of the needed information or service. Whether the service is a cellular network or a network connection, it is usually expressed as the amount of time users can use the system, application and data. (ibid., 11)

Availability can be measured with calculations containing variables such as uptime, downtime, availability percent, mean time to failure (MTTF), mean time to repair (MTTR) and recovery time objective (RTO) which means the amount of time it takes to recover and make a system, application and data available again for user after an error or outage. (ibid., 11)

Service providers in information technology usually offer service level agreements (SLAs) to their customers. For example, a telecommunication company can offer to a customer a 99.993 percent uptime SLA for WAN services, which typically means a maximum of 30-minute downtime in a monthly period of time. Typically, the SLA range is between 99.5 percent to 99.999 percent availability. (ibid., 12)

Integrity of data and services means that users can trust that the accessed information is valid and accurate, and only authorized parties can alternate the information when needed. If unauthorized parties such as cybercriminals or computer virus infections alternate data or information that users need to access, the integrity of the data is compromised, and data cannot be trusted. (ibid., 12)

Examples of data integrity can be money transfers when using online bank services or accounting and personnel information on an office PC.

Confidentiality in CIA triad means that information must be protected from everyone except those with rights to it. Confidential information includes personal data, business intellectual property, and countries' and governments' national security. (ibid., 12)

2.2 Networks and Telecommunications basics

Networks and telecommunications are a critical part of business infrastructure for most businesses and organizations. Network security meets an organization's essential need for network confidentiality, integrity and availability as introduced in section 2.1. The data transmitted through the network should be protected from accidental and intentional modification, it should not be readable by unauthorized parties and its source and destination should be verifiable. (Kim & Solomon 2012, 316)

When considering network and telecommunication security, it is important to understand how traffic is sent and used through networks. One of the most basic elements of a network is the Open Systems Interconnection reference model, better known as the OSI model.

Based on Kim & Solomon (2012, 318), the OSI model is a template for building and using a network and its resources, and it presents a theoretical model of networking with seven interchangeable layers. Those seven layers are application, presentation, session, transport, network, data link and physical layer. The OSI model and cyberattack examples are introduced in Figure 3.

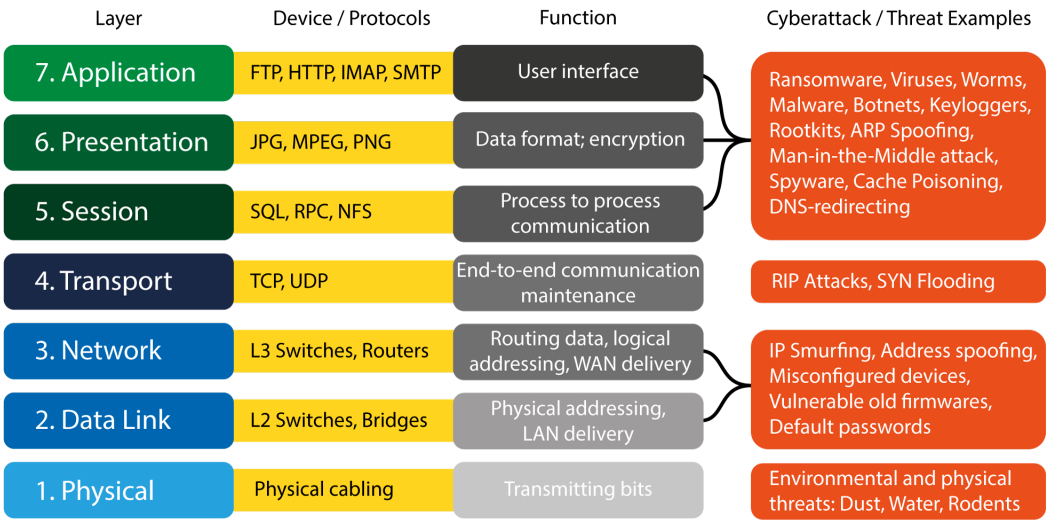

Figure 3. The OSI model and Cyberattack Examples

2.3 Regulations and guidelines in Finnish telecommunication networks

In Finland, telecommunication is regulated by the Finnish Communications Regulatory Authority. Its most recent regulation, 65C/2018, contains regulations concerning internal networks and telecommunications contracting in real estate buildings. Regulation 65C applies to internal communications networks and systems of residential properties for permanent living, office properties and public properties. (Finnish Communications Regulatory Authority 2018b)

Even though farm buildings such as barns are considered industrial buildings, and regulation 65C does not bind barn property owners to obey these regulations, these guidelines would still be very good base knowledge on how to build modern physical networks in new buildings.

Finnish Communications Regulatory Authority also provides an online service full of useful Information security guidelines and tips on their website for organizations, private individuals and service providers. The most recent articles about proper security policies and guidelines can be found there. (Finnish Communications Regulatory Authority 2018a)

Finland's Ministry of Finance published the Vahti guide for internal networks in May 2010. (Ministry of Finance 2010) Part of the recommendations in that publication are partially outdated; however, because the guidelines were drafted in a general manner, the guide still contains useful tips and hints how secure networks and IT systems can be planned and implemented.

3 Methods

3.1 Research objectives

The need for this research is based on earlier research “Cyberthreats in primary production” published by researchers Mikko Laajalahti and Jussi Nikander from Natural Resources Institute Finland. While their research focused on industry-level cyberthreats in agriculture in general, their results and findings will provide the base for this research where the goal is to dive deeper into cybersecurity in agriculture telecommunication networks as well as the devices and users using the networks.

The research questions for this study are:

- What kind of threats can be found in a farm’s telecommunication networks?
- Is it possible to find threats that are unique only to the agriculture industry?
- How it is possible to fix threats found on case farms?
- Is it possible to generalize farm telecommunication networks threats based on the farms chosen for this case study?

3.2 Research methods

This research is carried out using a qualitative approach. Even though the number of data samples – in this study, the farms – was only six, enough time was spent on each farm to survey their cybersecurity level.

The data was collected in August 2018 by visiting six different dairy farms. The targets were selected by the Natural Resources Institute Finland based on the following criteria:

- Medium size dairy farm
- Predicted business growth in the future
- A modern barn built in the 21st century (built in 2010 or later)

The visits included excursion to selected dairy farm buildings, researching how current IT and telecommunication networks have been implemented and finally, there was an interview with the entrepreneurs and employees with predetermined questions.

All six farms were located in Northern Savonia. The case farms were farms from 80 to 300 cows, and the employee count was from 3 to 10 persons.

In every case farm the following information was gathered:

- Basic information about case target business such as cow count, buildings and employee count
- Telecommunication technical implementations such as network topology, network devices, cabling categories, network cabinets, groundings and wireless network coverage
- Answers for questions by interviewing entrepreneurs about dairy farm telecommunication networks and how their business depends on networks (Appendix 1: Interview questions for entrepreneurs)

Data gathered from the farms was analyzed and categorized using the OSI model and the CIA triad method introduced in the theory section 2.1 starting on page 12. Example solutions to the threats identified on the farms are introduced at the end of the discussion in section 5.9 on page 65.

3.3 Hypothesis of case findings results

Based on the earlier research by National Resources Institute Finland, (Laajalahti & Nikander 2017) it is assumed that the findings from the case farms will support their findings concerning various kind of cybersecurity risks and threats without proper preparation against them.

Because the agricultural industry is originally less technical than for example IT industry, there may not be personnel with professional IT skills. Because of that it is assumed that understanding the needs of secure networks and IT solutions may not be at an adequate level from the perspective of cybersecurity. It is also assumed that the study would provide more detailed information about what kind of network-related hardware implementations can be found on farm environments, and how devices and other equipment are installed and configured.

After the case farm visits, based on the findings conclusions are to be made about what kind of actions should be taken to raise the farms' cybersecurity level and to promote cybersecurity awareness in primary production.

4 Results

4.1 Case farm summary

A summary of the case farm findings can is presented in Table 1: Case farm findings summary and more detailed case farm information with network topologies and network cabinet photos can be found in the next section 4.2 Detailed findings from farms starting on page 20.

Table 1: Case farm findings summary

Case farm findings summary						
	Case farm 1	**Case farm 2**	**Case farm 3**	**Case farm 4**	**Case farm 5**	**Case farm 6**
Farm basic information						
Farm size (cows)	50-100	250-300	150-200	50-100	200-250	200-250
Buildings with network	Home, Barn	Only main barn	Home, Barn	Home, Barn	Barn	Home, Barn
Cow activity monitoring	Yes	Yes	Yes	No	No	Yes
Milking method	Manual	Manual	Automated	Automated	Automated	Automated
Feeding method	Manual	Manual	Semi-automated	Manual	Manual	Automated
Manure robot	No	No	No	Yes	No	Yes
Network cabinet grounding	Yes, 16mm²	Yes, 6mm²	Yes, 6mm²	Yes, 16mm²	Yes, 6mm²	Yes, 16mm²
Backup power / surge protection	Building surge protected, no dedicated backup power	Yes, multiple UPS devices + dedicated diesel generator	Yes, multiple UPS devices + dedicated diesel generator	Building surge protected, dedicated diesel generator	Yes, multiple UPS devices + dedicated diesel generator	Partly protected with UPS devices + dedicated diesel generator
Network information						
Internet connection	Singe mode fiber 300/100M	Singe mode fiber 30/10M	Singe mode fiber 30/10M	Singe mode fiber 300/100M	Singe mode fiber 30/10M	Singe mode fiber 100/100M
LAN extension to other buildings	Single mode fiber (800m)	-	Category 5e unshielded (120m)	Single mode fiber (200m)	-	Single mode fiber (300m)
Barn LAN cabling level	Category 6, unshielded	Category 5e, unshielded	Category 5, unshielded	Category 6, unshielded	Category 6, unshielded	Category 6, unshielded
Need to connect network devices remotely	Yes, RDP + Team Viewer	No	No	No	No	Yes, RDP
Network devices						
Routers	1	1	2	1	1	3
Switches	2	1	1	2	2	1
Wireless access points	2	1	2	3	1	2
Computers, laptops	Yes, LAN + WLAN	Yes, LAN + WLAN	Yes, LAN	Yes, LAN + WLAN	Yes, LAN	Yes, LAN + WLAN
Network printers	No	Yes, LAN + WLAN	No	No	No	No
Video surveillance	Yes, analogue cameras + IP recorder	No	No	Yes, IP-cameras + IP recorder	Yes, IP-cameras + Surveillance PC	Yes, IP-cameras + IP recorder

4.2 Detailed findings from farms

4.2.1 Case farm 1

The buildings on the first case farm were located on two different sites: the main site included the farmhouse with other buildings, and the second site included a barn located 800 meters away from the main site buildings. The barn size was under 100 cows, the animals were fed manually, and the farm used a manually attached milking system.

The first case farm had a fast fiber connection with a maximum download speed of 300 Mbps and maximum upload speed was 100 Mbps. Single-mode fiber cable was installed underground between the home and the barn. A wireless fiber gateway was installed in the home building and a LAN network was extended to the barn using copper to fiber media converter in both ends.

A network cabinet was installed in the office room. (Figure 4) Both the single mode fiber from the main home building and the office category 6 unshielded Ethernet network cabling were terminated to the cabinet. The network topology of the case farm is introduced in Figure 5 on page 21.

Figure 4. Case farm 1 network cabinet

A small 5-port unmanaged network switch, video surveillance recorder and other network devices were placed on the office table outside the cabinet. The wireless access point was disconnected from the network and the device was placed at the bottom of the cabinet with power turned off. The network cabinet was properly grounded.

Farm 1 was using a cow activity service with activity meter devices on cows. The activity data was collected through cow activity receiver and the results were stored in Office PC software. In Figure 5 is presented what kind of network devices was discovered in case farm 1, how the devices were connected to each other's and what kind of users were found using the network.

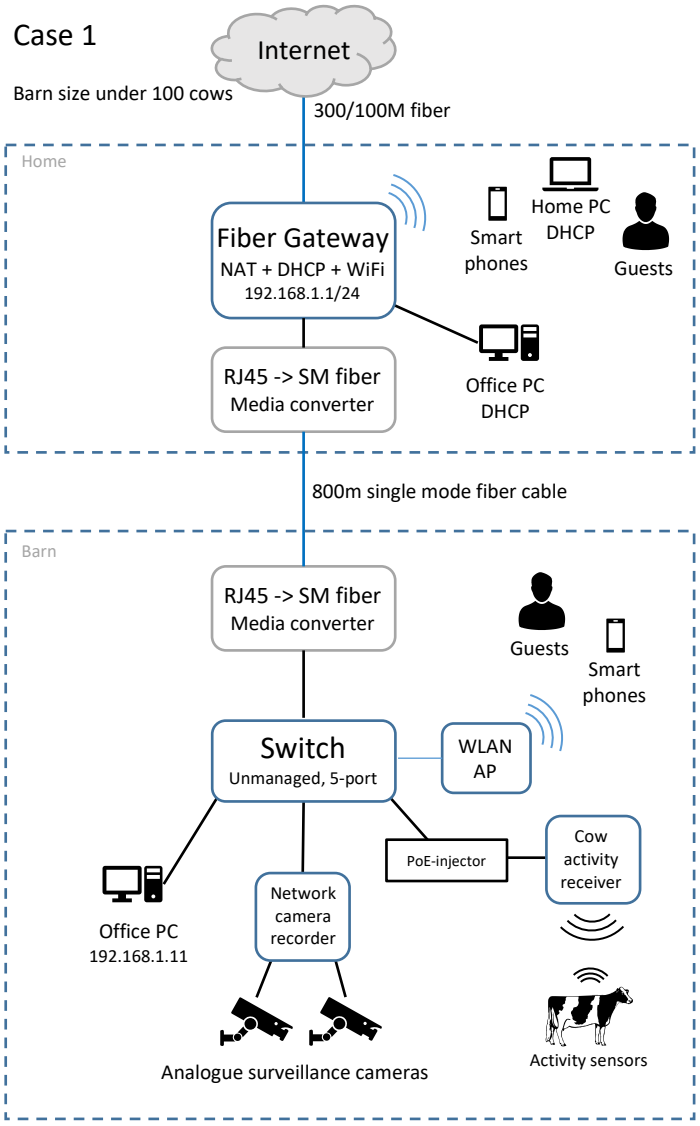

Figure 5. Case farm 1 network topology

The barn building had global surge protection; however, the computers or network devices had no dedicated surge or power protection against a power outage or thunderstorms.

During the visit it turned out that after the visit of a network service provider technician, video surveillance system's remote live video and playback had stopped working. After some on-site research, the deactivated wireless access point was identified as the cause of the problem, and after reconfiguration and re-activation the entrepreneur could once again connect to the video surveillance system using his smart phone.

The entrepreneur of the farm also wished that he could connect to the barn office PC remotely from home without travelling from home to the barn. Because the barn network was only an extension from the home wireless fiber gateway, it was only needed to manually configure an IP address to the office PC and activate Windows remote desktop services for them to start using the barn office PC from their home computer.

4.2.2 Case farm 2

The second case farm had several buildings in close proximity of each other. Even though it was one of the biggest case farms, they had one of the simplest network topologies within the farms included in this study. The size of the barn was between 250 to 300 cows, the animals were fed manually, and the farm used a manually attached milking system. Cow activity monitoring was in use and activity information was stored to the barn office computer.

The second case farm had a fiber connection with a maximum speed of 30 Mbps download and 10 Mbps upload. The business administration was conducted with one office computer, network printer, cow activity receiver and a simple switch. There were also a few laptops in the dining room using wireless connection next to the barn office.

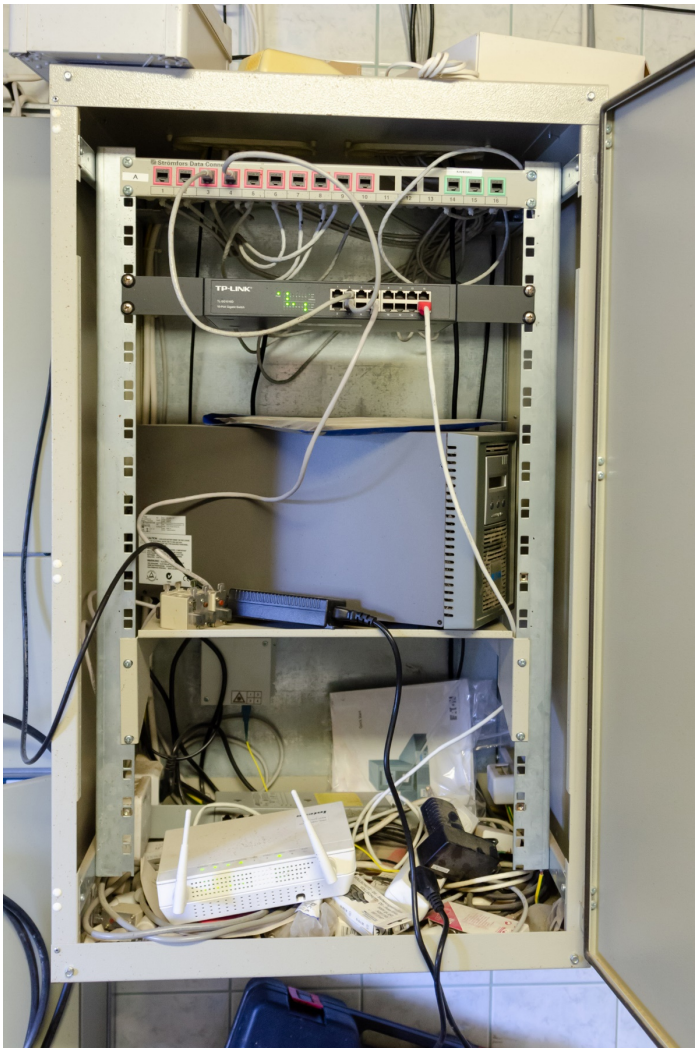

Figure 6. Case farm 2 network cabinet

The farm network cabinet was near the barn office, and barn's category 5e unshielded network cabling was terminated to the network cabinet. A wireless fiber gateway provided by the network operator was installed at the bottom of the network cabinet. The network cabinet was also properly grounded (Figure 6 on page 23).

A 16-port switch was installed in the cabinet alongside with a small backup power UPS device protecting the network devices. The farm also had a diesel generator with a 12-hour running time to protect from longer power outages. The network's topology chart can be found in Figure 7.

Farm 2 was also using a cow activity service with activity meter devices on cows. Data from cow sensors was collected using a PoE-powered cow activity receiver, and the data and results were stored to Office PC's hard drive.

For technical support and assistance with equipment purchases, the farm used a third party IT provider service.

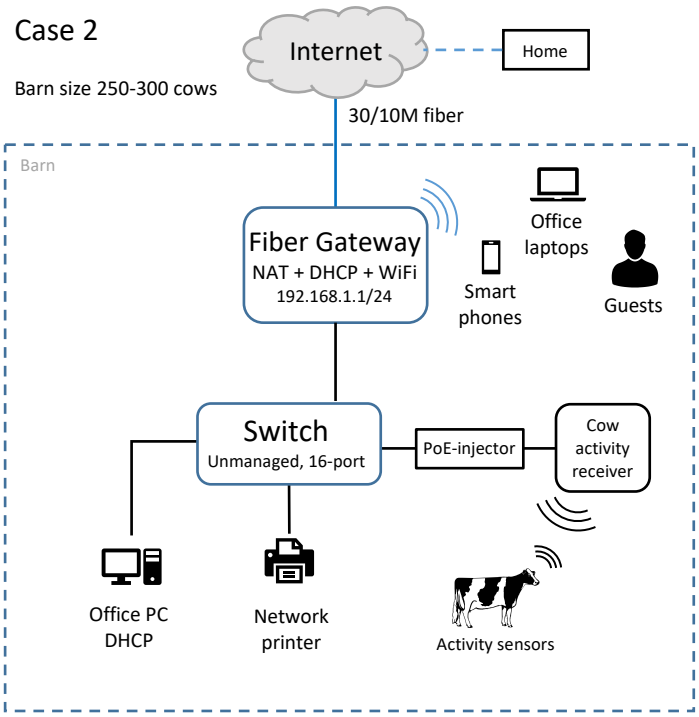

Figure 7. Case farm 2 network topology

4.2.3 Case farm 3

The third farm also had several buildings close together including the main house, the barn and other buildings. The size of the barn was between 150 to 200 cows and this was the first case farm where milking robots were used.

Internet access was provided through fiber connection with a speed of 30 Mbps download and 10 Mbps upload, and a fiber gateway was installed in the office room of the main building. From there, the local network was extended to the barn building using a Cat5e copper cable between the home building and the barn.

Figure 8. Case farm 3 network cabinet

The barn's physical network cabling level was category 5 unshielded, and cabling was terminated to a small network cabinet on the barn's office wall (Figure 8). Grounding on the cabinet was properly implemented. There was also an 8-port unmanaged switch installed in the cabinet, and another wireless router with NAT and DHCP

functionality turned on placed on the top of the cabinet. There was one small UPS device in the cabinet and another one on the office table, providing surge and backup power protection to the computers and network devices.

Milking robots were monitored and controlled through a dedicated PC with two Ethernet ports: one for connecting the PC to the existing network for internet access and updates and another port that was connected to the closed network with the milking robots.

The milking robot control PC and cow activity receiver were connected directly to an unmanaged switch; however, the Office PC and some other network devices were connected behind a second router. Data from the cow activity sensors was collected to Milking robot control PC. The farm's network topology is introduced in Figure 9.

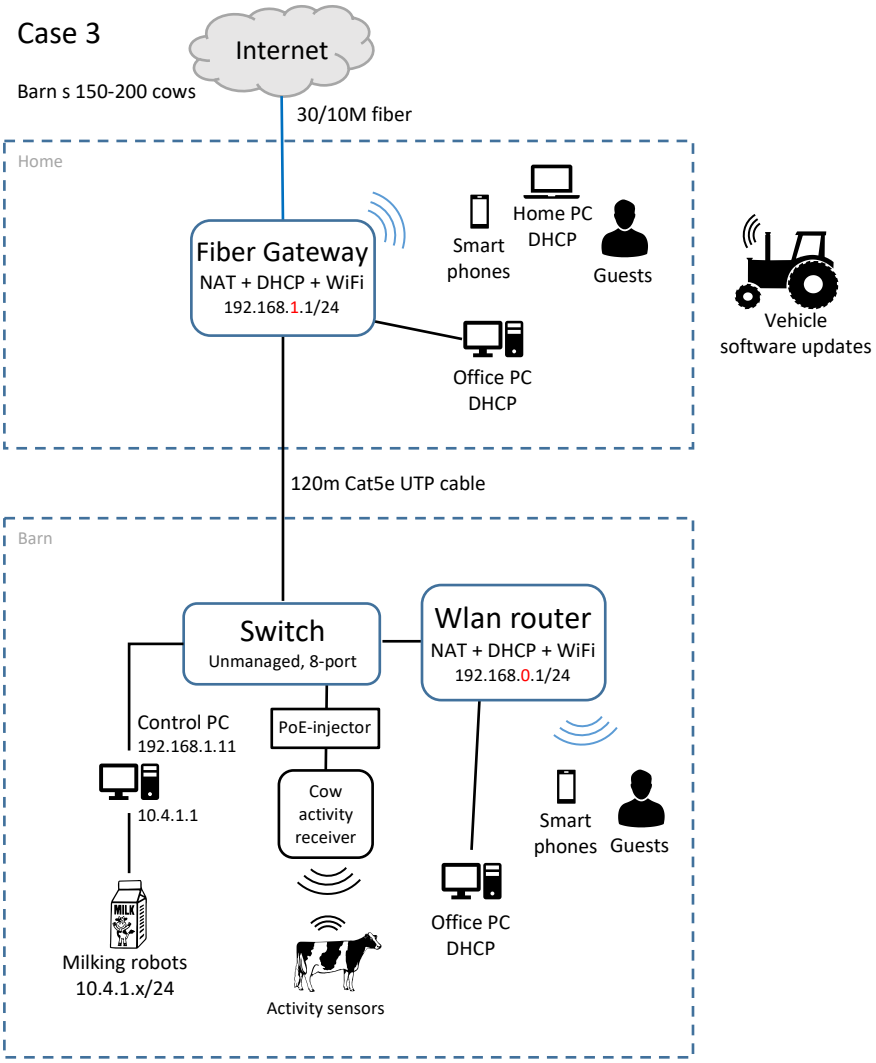

Figure 9. Case farm 3 network topology

4.2.4 Case farm 4

On the fourth case farm the distance between the house and farm buildings was about 200 meters. The size of the barn was under 100 cows, the animals were fed manually, and milking robots were in use.

A wireless fiber gateway was installed in the home building, and the home LAN network was extended to the barn via single-mode fiber cable using a copper to fiber media converter in both buildings. The fiber connection's maximum download speed was 300 Mbps and upload speed 100 Mbps. In the home building there was another wireless access point providing more wireless coverage on the home's second floor, and a third access point was installed in the barn near the milking robots.

The network cabinet was installed in the barn's office room (Figure 10). The cabling level of the barn building was category 6 level unshielded Ethernet cable, and all cabling was terminated to the cabinet. The cabinet's grounding was properly implemented.

Figure 10: Case farm 4 network cabinet

There was also a managed 10-port PoE switch in the cabinet with a network video recorder responsible for recording surveillance camera video feeds. Two IP cameras were connected to the switch and one camera was connected directly to the recorder.

The milking was carried out by a milking robot and the robot control PC was controlling the traffic between the robots and local network. As in case farm 3, there were 2 Ethernet ports on the robot control PC: one for the internet access and one for the closed network where the milking robots were installed. The farm's network topology is introduced in Figure 11.

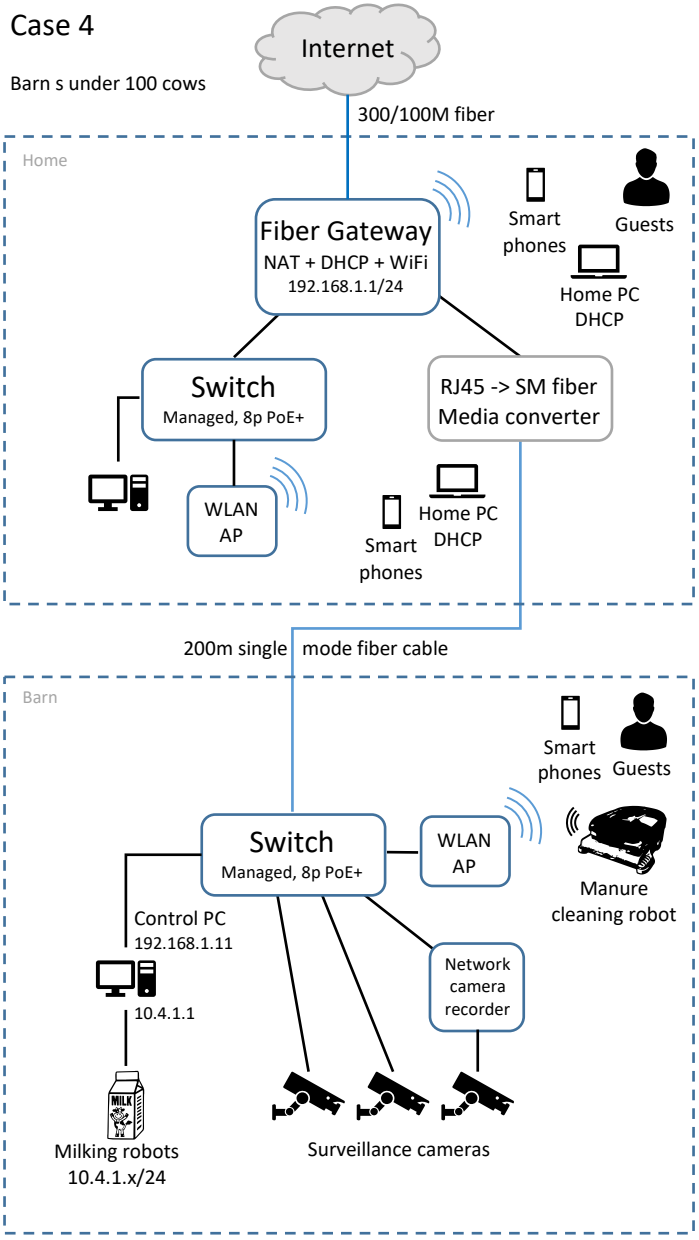

Figure 11. Case farm 4 network topology

There was no dedicated surge or backup power protection in the office for computers or network devices, but a large diesel generator provided offline backup power in the case of a power loss.

In the barn there was also an automated manure cleaning robot which was controlled by smart phone using local wireless LAN connection.

During the entrepreneur's interview, it was found out that surveillance live video monitoring using a smart phone had worked at some point after the installation but had then stopped working afterwards.

4.2.5 Case farm 5

The fifth case farm was one of the newest barn buildings in the case group. The barn size was between 200 to 250 cows, the milking was performed by a milking robot, however, the cows were fed manually.

The farm had a fiber connection with 30 Mbps download and 10 Mbps upload speed. The network cabinet was in a technical room near the office (Figure 12). The building's Ethernet cabling level was unshielded category 6 cable, and all cabling was terminated to the cabinet. The grounding was properly implemented.

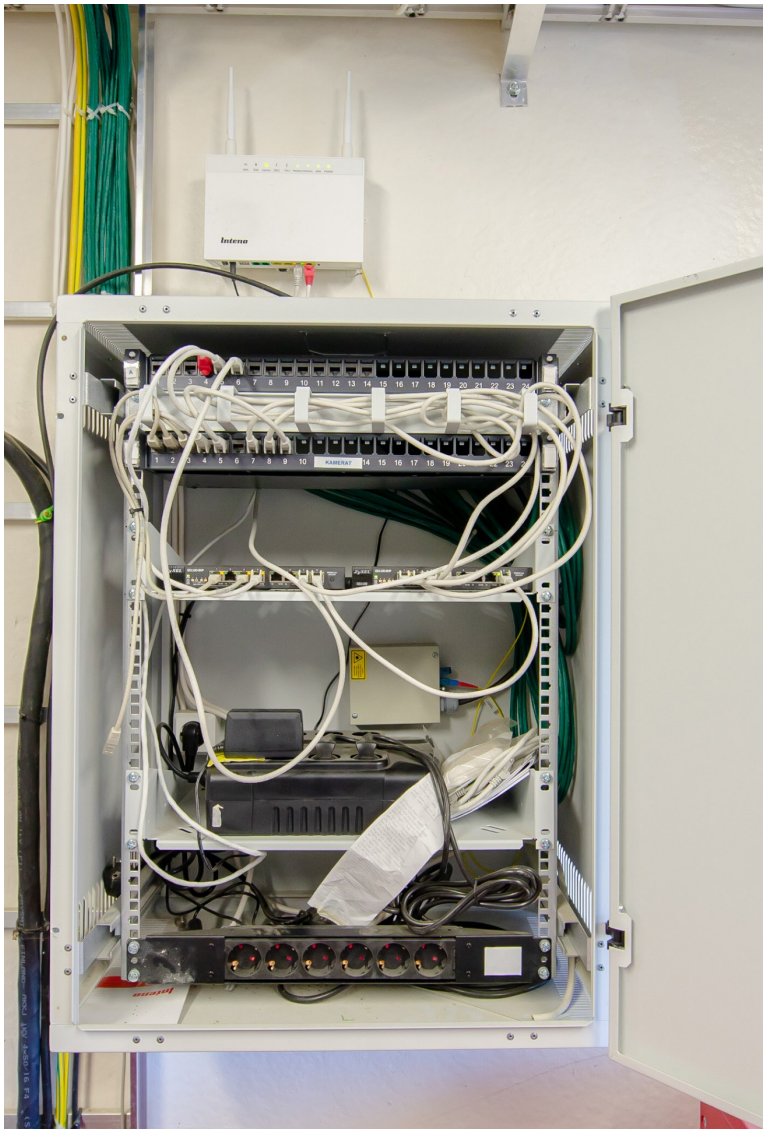

Figure 12: Case farm 5 network cabinet

A wireless fiber gateway was installed on the wall outside the network cabinet to maximize wireless coverage. Inside the cabinet, there were two unmanaged 8-port PoE switches and a small UPS device for surge protection and backup power. In case of longer power outages, there was a large diesel generator installed in a separate small building just outside the barn. The network topology of the case farm is introduced in Figure 13.

During the visit, some issues were identified concerning network device topology as seen in Figure 13. The person who had installed the surveillance cameras had also configured the same network and default gateway to both Ethernet adapters on the surveillance PC. In PC route table, both Ethernet adapters had the same gateway IP address with the same metric. The result for this configuration caused significant delay until the surveillance camera video feed started to show up after rebooting the surveillance PC.

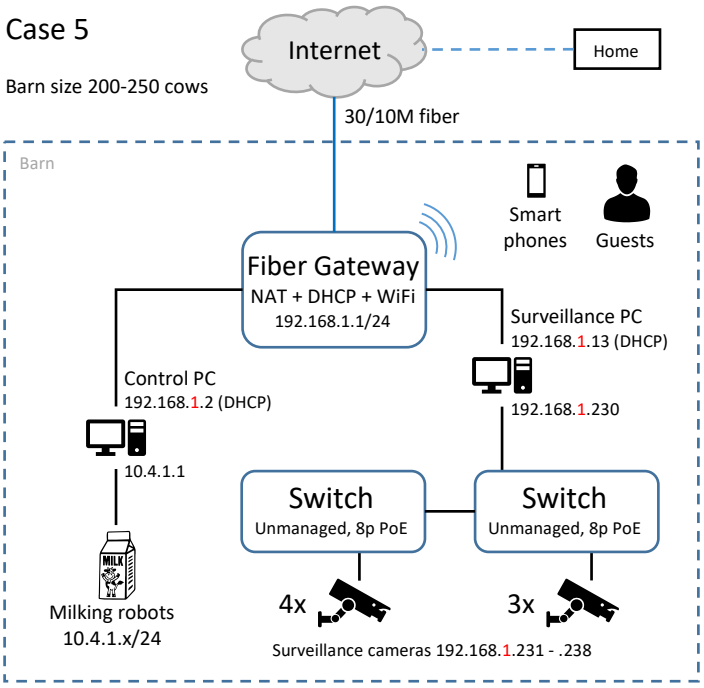

Figure 13. Case farm 5 network topology

4.2.6 Case farm 6

The sixth case farm also had several buildings close to each other. The barn size was 200 to 250 cows, and this was the first case farm where both milking robots and automated feeding robot were in use.

Internet connection was provided using fiber connection, and a wireless fiber gateway was installed in the main house. Connection speed was 100 Mbps download and 100 Mbps upload. Distance between the home building and the barn was approximately 400 meters, and there was a single mode fiber installed between the two buildings. LAN network was extended to the barn using copper to fiber media converters.

The network cabinet was installed in the office on the second floor of the barn. The barn's physical network cabling level was unshielded category 6 cable. All network cables were terminated to the network cabinet, and cabinet grounding was properly done. Network cabinet is introduced in Figure 14.

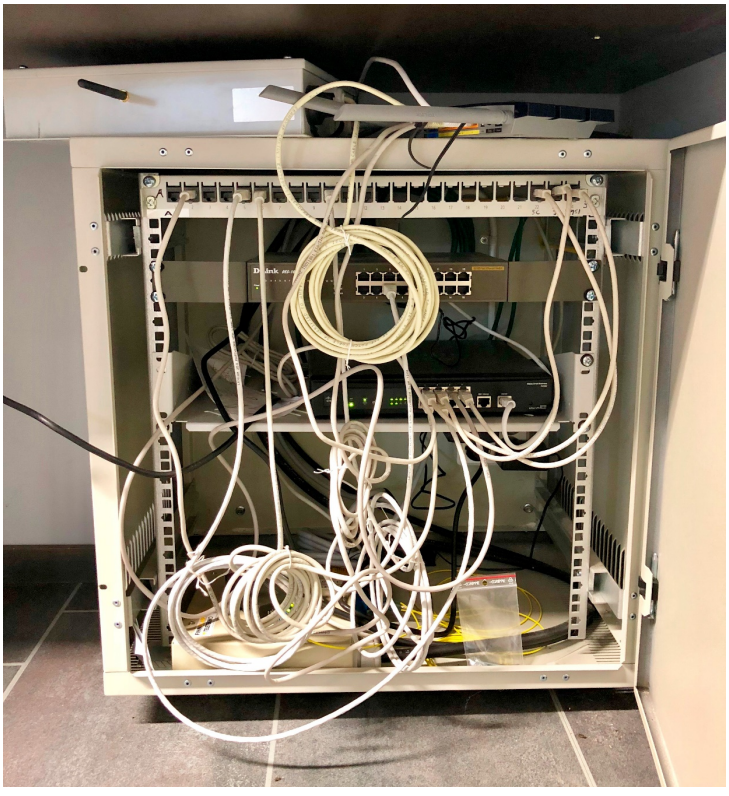

Figure 14. Case farm 6 network cabinet

A second wireless router was placed on the roof of the network cabinet and inside the cabinet there was a third router and a 16-port unmanaged switch; however, the switch was not in use for some reason. Farm office laptop and the cow activity receiver were connected directly to the second router. The manure cleaning robot was controlled by smart phones using the barn's wireless connection.

Milking robots, automated feeding system and robot control PC were connected to the third router provided by the robot manufacturer. The farm also had an IP-based video surveillance system where surveillance cameras were connected directly to the network video recorder and the recorder was connected behind the third router. the network topology of case farm 6 is introduced in Figure 15 on page 34.

The barn had global surge protection; however, the UPS battery backup for computers and network devices was limited and covered only a part of the devices. For longer power outages, there was a large offline diesel generator that could be manually activated when needed to cover the whole barn's electrical needs.

During the interview, the entrepreneur reported that the mobile connection to the video feed had stopped working after robot maintenance service. It was found out that removing the network video recorder behind the third NAT device and connecting it directly to the main house fiber gateway LAN network solved the problem.

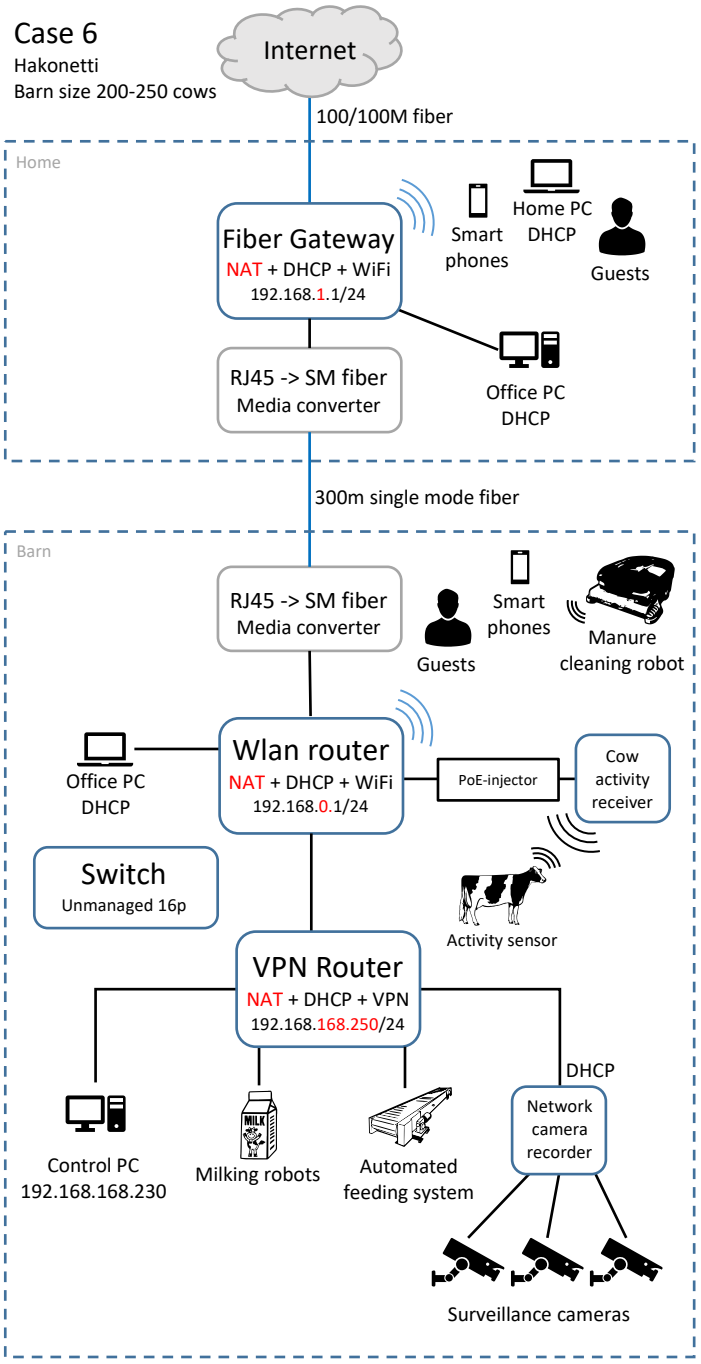

Figure 15. Case farm 6 network topology

4.3 Entrepreneur interviews

During the case farm visits, every entrepreneur was interviewed with the same set of questions. The complete list of questions can be found at the end of this master´s thesis. (Appendix 1: Interview questions for entrepreneurs.) The questions were related to information technology utilization in day-to-day operations e.g. how important network connection is in modern farming, how farms are prepared for technical problems or their opinions how they feel information technology will be used in their business in the future.

4.3.1 Telecommunications and cybersecurity in farm everyday life

The first question was related to how often information technology and network connection was needed in the farm's daily operations. Every single interviewee described the importance of information technology and network connection as mandatory, critical or extremely important. Computers were used e.g. to send compulsory official notices of birth and death to the authorities, to update animal registers, to connect to customers and service providers, for bookkeeping and updating, web browsing and emails, automation and surveillance.

When asking the entrepreneurs about what thoughts came up on their mind when thinking about their farm business and cybersecurity, there was more variety in the answers. There were concerns about endpoint security, wireless security, passwords and overall concern about cyberattacks and viruses and how to prevent from them. Even though every case farm had their concerns, not all were aware if they had a firewall or antivirus software installed on their computers.

The questions about data protection or backups resulted in predictable answers: most of the case farms stored their important data to local computers and only few knew if backups were properly taken. Some entrepreneurs used cloud storage to store business data.

The question about the potential need of remote access to farm network devices or data resulted in different answers: in most cases, there was need but only few had found a way to access devices remotely. Some entrepreneurs used Team Viewer to

get access to the barn control PC, some wanted to see live video from surveillance cameras using phone.

When asking about the fault impact of network connection to the business, all case farms except one estimated that there would be no significant impact when the network failure was between hours to one day. One exception estimated that there cannot be even a one day's network failure. Other farms estimated that from one to three days would cause real problems and a one-week disconnection would cause catastrophic impact to the business. None of the case farms had prepared for possible network failures with backup internet connection besides a smart phone's hotspot function.

4.3.2 Thoughts about existing IT systems and fault planning

Almost every farm network implementation was mostly based on barn physical network copper cabling implemented according to building electrical drawings and fiber cabling and network hardware from internet operator or third party solution provider. Most of the case farms had some third party service provider for technical support when needed.

When there was need to purchase new IT- or network devices, two farms answered that they had asked for devices with good reliability and value. The rest of the case farms trusted their service provider's decisions on which equipment is worth the investment.

Almost all case farms had been generally satisfied with the working of IT- and network equipment. Most network problems had been related to thunderstorms, physical threats e.g. an excavator accidently cutting the underground fiber or for example, after misconfiguration by a third party IT technician.

Concerning backups, two case farms knew that their data was saved to a cloud service in case of a computer malfunction. Three case farms relied on the milking robot manufacturer to keep their automation PC data protected and backed up properly because the service fee of the robot system's annual maintenance included maintenance and updates of automation PC.

All case farms had grounding in buildings properly installed; the main reason for this was the Finnish regulation for the 21st century barn buildings. In case of a power failure, most of the case farms used small UPS backup powers for surge protection and backup power. Five case farms also owned a diesel backup generator for longer power failures from a few hours to 12 hours of running time without refueling.

4.3.3 Entrepreneur's thoughts about future

The last section of entrepreneur interviews included questions about how they see their network related future and if they have any plans to build new buildings or renovate old buildings including a renewal of electrical and telecommunication implementations. The last question was related to the entrepreneur's willingness to pay for security and network services to a professional IT service company.

All case farms predicted that their need for IT services and telecommunication networks will increase in the future. Two case farms considered expanding the wireless network coverage from barn to other buildings to enable using and accessing their software and data from other buildings as well. Additionally, need to expand coverage of cow activity receiver to other buildings and outside areas was mentioned.

One case farm was planning to expand the video surveillance and add surveillance cameras also outside and other buildings besides the current cameras inside the barn.

One farm was hoping to receive more guidance with IT- and network security from The Central Union of Agricultural Producers and Forest Owners. There was also clear intent for service containing periodical maintenance for computers and network hardware since milking robot maintenance service covered only the devices related to the milking automation system and control computers.

5 Discussion

Case farm excursions revealed several interesting findings regarding a farm's cybersecurity levels, technical implementations and use of technology in primary production. This section presents the discussion and analytics on findings by organizing the findings through the OSI model layers introduced in section 2.2 on page 14 and by categorizing the found threats with the CIA triad model introduced in section 2.1 on page 12. Examples of key findings with suggested solutions to the found threats are presented at the end of this chapter in Table 4 in section 5.9 on page 65.

5.1 Findings on physical level implementations

5.1.1 Remarks regarding electrical solutions on case farms

Grounding and backup power systems were better taken care of than assumed beforehand. Almost all farms had a diesel-powered backup generator in case of power outage and the barns were surge protected. In some cases, also computers and other network devices were protected with small UPS backup power devices and the network cabinets were properly grounded.

The reason for the electrical implementation and findings is most likely due to the modern building age of the barns in the case farms. Finnish Standards Association regulation SFS 6000 series regulates low-voltage electrical installations including regulations concerning modern buildings grounding of electrical equipment's and building potential equalization. (Finnish Standards Association SFS 2018)

5.1.2 Network cabling levels and implementations on case farms

Agricultural communication networks consist of physical network cabling, network equipment and both users and devices connected to network. The network traffic needs either a wired or a wireless solution to transmit data.

The internet connections of all case farms were implemented with a single mode fiber which is currently the most modern method for a WAN connection. Electrical interferences, such as thunderstorms, do not cause negative effect on data

transmission through fiber cables. Fiber solution is also future proof because the maximum transmit speed in a single mode fiber optic cable is basically unlimited.

When reflecting fiber WAN connection to CIA triad, fiber provides better availability compared to modem connections such as ADSL or VDSL which uses copper cable where the maximum transmit speed decreases greatly over the distance.

Even though fiber is currently the best option for transmitting data, it is still vulnerable to physical damage such as excavator accidentally cutting off the fiber on the ground. To raise the level of a farm's network availability, redundant backup WAN connection, such as 4G backup is needed. A backup network connection was not found on any case farm even though all case farms estimated that more than a day's network break would cause damage to the business continuity.

Local network Ethernet cabling level varies and category 5, 5e and 6 implementations were found where category 5 is meant for data rates up to 100 Mbps and category 5e and 6 are meant for data rates up to 1 Gbps with full permanent link 90-meter length. All Ethernet cabling was implemented with unshielded Ethernet cables.

The backbone cabling between buildings was implemented with fiber cable, except in case farm 3 where category 5e unshielded cable was used for 120 m distance, which was slightly over-length based on existing cabling standards.

Based on European cabling standard EN 50173-1, the maximum length for permanent link using Ethernet cabling between buildings must not exceed 90 meters with category D (100 MHz) or E cable (250 MHz). When extending the network from one building to another and the overall length exceeds 90 meters, Single Mode or Multi Mode fiber between the buildings is required. (Finnish Communications Regulatory Authority 2018b)

If these stated maximum distances are exceeded, there may be problems with data link performance. One scenario can be two switches where the data link between switches changes constantly from 1 Gbps link to 100 Mbps link and back to 1 Gbps if the cable between switches does not pass the performance needed for solid link speed, which would cause speed problems and delays in the network.

5.2 Findings on data link and network level implementations

Even though network topologies were usually relatively simple, and the amount of data samples was limited to six case farms, there were still good examples how network devices were installed, used or configured improperly, causing direct or indirect threat to network availability. It was also found out that none of the case farms had network topology documentation and other documents about installed network devices of configurations were missing or were insufficient.

5.2.1 Accessing the internet

All case farms used a fiber gateway provided by the local network operator. There were two different network operators providing fiber connections and all FTTH (Fiber to the Home) gateways were the same model from the same brand on each case farm. Fiber gateway was responsible for converting fiber WAN connection to NAT-enabled LAN connection. The router also provided routing and both built-in wireless network and DHCP to its users.

All case farms used fiber gateway with out-of-the-box settings as the internet provider installation technician left the device after initial installation. With those two farms where more investigation to fiber gateway was made, it was found out that the default user name and password were left to the devices and the HTTP administration's login page was visible to the public internet when router public IP address was tried with internet browser outside the LAN network. It can be assumed that all or at least almost all of the six fiber gateways were left with the same security level after initial setup.

When trying to log in from the public internet to the fiber gateway using the same default administrator credentials, which were working from the LAN login page, the login attempts were unsuccessful. It is assumed that even though the administration login page was visible from the public internet, the network operator had configured to the gateway predetermined IP address list from which a user can log in to the unit remotely. It is also assumed that the network operator uses a public login page to remotely update the devices but leaving login visible to public internet relies on the fact that the login page and mechanisms security level should be hack proof.

If someone figures out some security flaw in the device and can bypass the fiber gateway login page without proper credentials, it could make an automated attack possible where an outsider party could update automatically all the devices found on the internet with infected firmware which would compromise the users' network traffic availability, integrity and confidentiality.

5.2.2 Farm LAN implementations and findings from network topologies

A fiber gateway provided by internet operator was responsible for routing and translating traffic from public internet to local network (NAT), providing IP addresses for LAN devices (DHCP) and for creating a wireless LAN connection to nearby users in all case farms.

In case farm 3 there was also a second router with NAT, DHCP and WLAN enabled installed in the barn, which meant that the devices connected behind the second router were behind double NAT. In the last case farm three different routers were found installed in the network. It was found out that e.g. the surveillance camera network recorder was installed behind three NAT devices, which meant that the traffic from recorder to internet had to travel through three different LAN networks before accessing the internet.

Multiple routers in chain do not cause direct threats to network security; however, this may cause threats to the availability of network device when routing problems occur between nested LAN networks. If a network printer and network backup drive are connected to different routers behind each other, it could cause availability problems for network users. Usually the traffic from devices behind multiple NAT to internet works decently; nevertheless, problems may occur in the future if new network devices are installed behind different LAN routers and these new devices should be available to all LAN users.

Avoiding multiple routers in general is a commonly used advice when planning and installing LAN networks and it is also recommended to keep the network topology as simple as possible. Preferring the star network topology will ease maintenance, increase network performance and minimize routing problems in local network. The difference between chain and star networks is introduced in Figure 16 on page 42.

In some scenarios, it is impossible to avoid multiple NAT networks; however, the findings from these case farms suggest rather a lack of understanding how networks should be installed and lack of understanding what kind of problems multiple routers could cause in LAN environments.

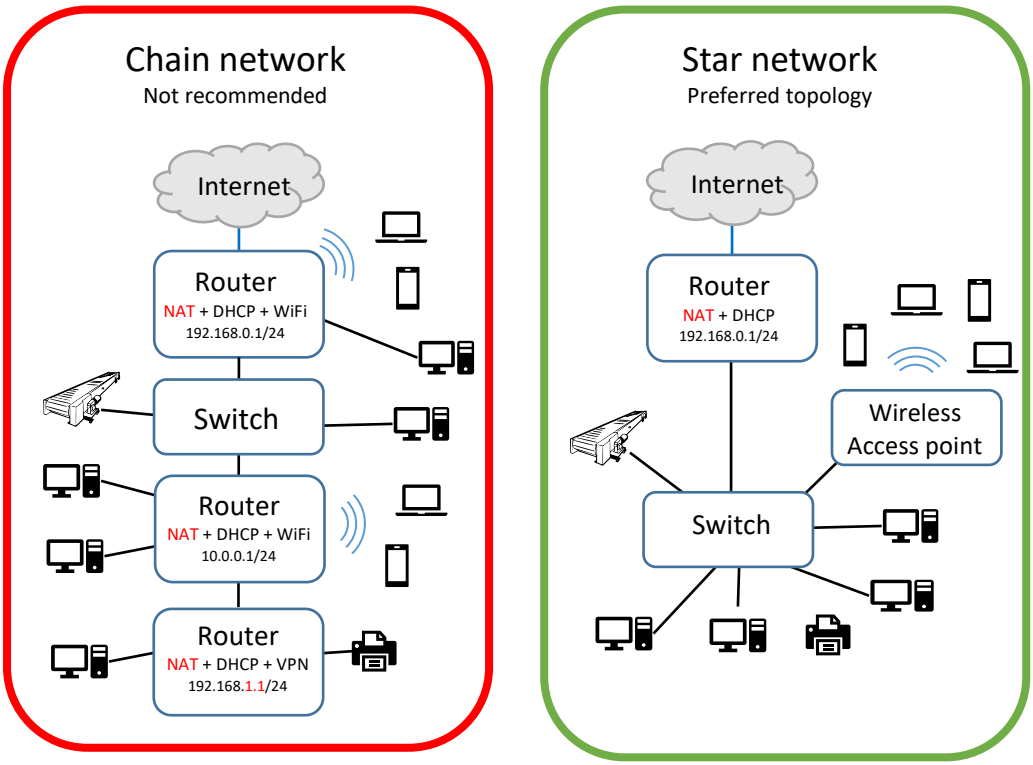

Figure 16. Difference between chain and star network topology

5.2.3 Importance of router in local networks

Router is an OSI model layer 3 network device responsible for connecting two or more networks, and it selectively interchanges packets of data between them. Affordable consumer-level routers usually contain only basic routing features with built-in network address translation (NAT), DHCP, firewall features and wireless access point.

Typically, a router is responsible for connecting a local network to the internet (WAN). In some cases, in corporate environments it is necessary to install multiple routers in the same network; however, without proper configuration multiple routers can cause problems with the availability of network assets. (Kim & Solomon

2012, 320-232) A router by itself does not necessary cause availability problems; however, installing multiple consumer-level routers including NAT, DHCP and firewall features will cause multiple nested networks behind each other and the availability problems may occur between network users.

Every data packet travelling through a network contains information from sender and destination IP addresses. Based on that information, a router delivers data packets towards the right destination using routing tables where the information is stored in which direction the network is located. If the received packet destination is unknown, the router uses the configured default route and delivers the packet to a default gateway, which is usually a device connected to a router's WAN port.

In the scenario where there are three consumer-level routers installed in a chain, (Figure 17 on page 44) there is a total of three different networks A, B and C:

- Network A is 192.168.0.0 with subnet mask 255.255.255.0
- Network B is 10.0.0.0 with subnet mask 255.255.255.0
- Network C is 192.168.1.0 with subnet mask 255.255.255.0

In this scenario, there are network drives installed in network A with the IP address 192.168.0.200 and a network printer in network C with the IP address 192.168.1.50.

Users in network A can see each other and access the network drive and internet. However, a network printer located in network C will be unavailable because the router in network A does not have the information where network C is located and the router in network A will send all unknown packets towards the default gateway, in this case the internet operator.

Users in network B can see each other and they can also access network drive in network A. The reason for this is that the router in network B will deliver unknown packets to its default gateway which is router A, and router A knows where the internet and network drive A are located. Users in network B are still not able to reach network C devices.

Users in network C can access the Internet, network B and network A devices.

By replacing routers with switches and using wireless access points rather than wireless routers, the same network would be faster, healthier and all devices would be available for authorized access as illustrated in Figure 17.

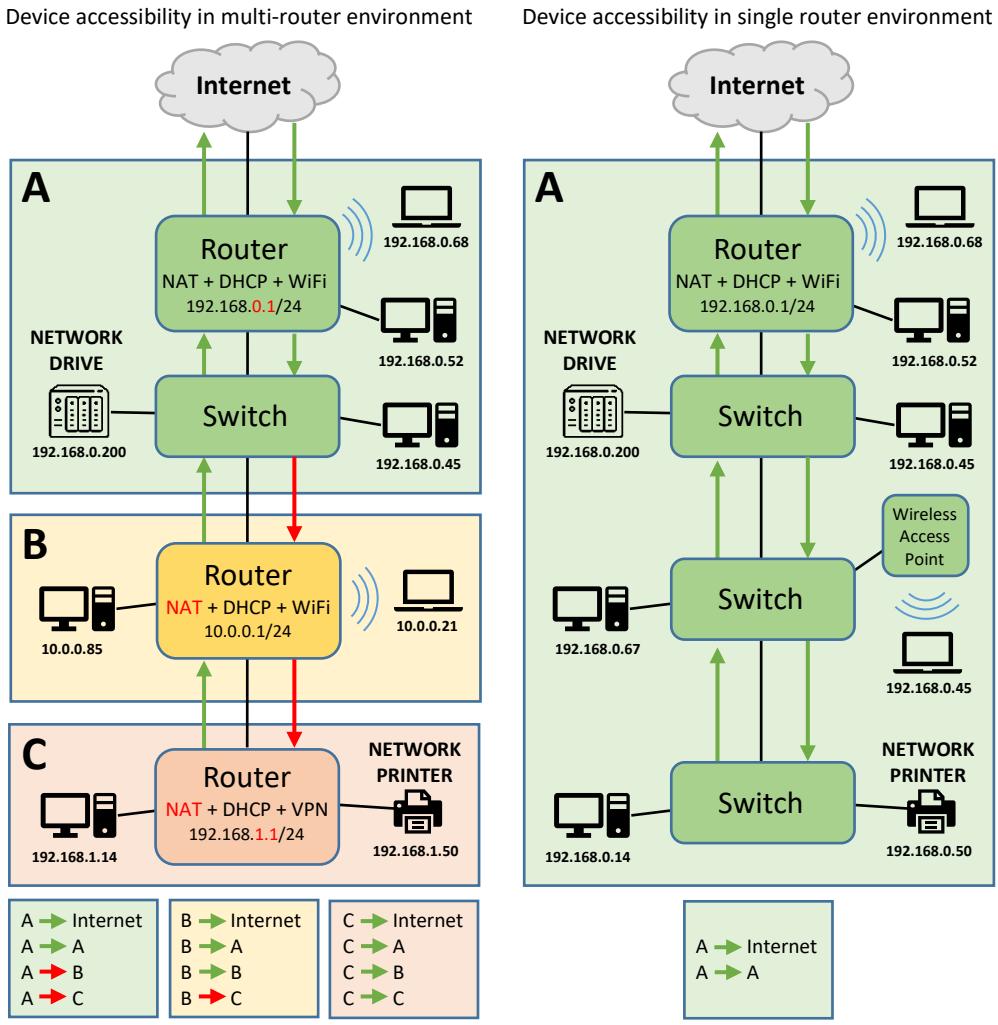

Figure 17. Device accessibility examples between multi- and single router network

5.3 Findings on software level implementations and ways how networks are used in farm

The devices connected to the dairy farm's network can include devices e.g. manure cleaning robots, IoT devices, automation devices, surveillance cameras, network drives and printers, servers, desktop and laptop computers and smart devices. Because they all need to either be able to transmit and receive data from another

device in the local network or access the internet, they are the most vulnerable part of networks on farms regarding cybersecurity.

Nowadays almost all devices can be hacked or infected with malicious code, and modern virus and malware infections occur caused by network crawlers scanning the public internet and trying to find vulnerable devices connected to the network.

In October 2016, massive distributed denial of service attack (DDoS) was malformed against GitHub, Twitter, Reddit, Netflix and Airbnb by infected surveillance cameras connected to public Internet and even fish tank could be hackable to gain access to corporate valuable data. (Jha & White 2016; Mathews 2017)

5.3.1 Findings concerning protection against malware and cyberattacks

During the visits in case farms it was found out that protection against malicious software and cyberattacks was implemented in the best-case scenario with endpoint antivirus software installed to computers and laptops. No hardware firewalls were found except on one case farm where the service provider for the milking robot automation was installed with a small firewall for automation devices inside the farm's local network.

Fiber gateway provided by the internet operator contained basic firewall function with NAT translation between WAN and LAN; however, it would raise the security level significantly if a hardware firewall with dedicated security licenses were used for analyzing the network traffic. A modern dedicated firewall with paid security licenses can detect and prevent cyberattacks and intrusions, stop malicious code and software from entering local network, analyzing and categorizing network traffic and providing a secure way to connect to local network from anywhere (using a VPN connection). With a dedicated firewall it is easier to gain better awareness of one's own local network, e.g. which devices are using the network and what kind of data they are transmitting.

Even though the farms' networks were protected with hardware firewall, proper endpoint antivirus software is also necessary. In some case farms, different endpoint antivirus software was found installed between the farm's workstations, and there were also in some case farms workstations without proper antivirus protection.

Many security software companies providing antivirus software for businesses offer centralized device management with security information summary graphics, which can help the company to keep the same security level in all computers and get alerts in a case when some endpoint device is infected.

5.3.2 Findings regarding plans in case of network or data loss

Based on the findings during the visits and from the interviews, it was found out that farms must report to authorities within five days after a new animal is born or has died, or they will face noticeable penalty and decrease of government funding. None of the case farms had prepared for longer network outages by investing in a backup connection or planning how to perform mandatory reports to authorities in a case that the network problems are longer than expected.

It is recommendable to plan and implement backup network connection to the internet in case of network outages. The Internet operator can offer backup connection as an additional service and it is also possible to configure backup connection with dedicated hardware firewall using another internet operator connection as a seamless automatic backup in a case that the primary connection is not working.

Important data created by users and used on a daily basis in farms contains usually documents, e-mails, accounting data, shift plans, supply orders and other kind of documents. Based on the visited case farms, no kind of dedicated secure device was found, such as a network drive where data was stored. In some case the cloud services of the farms were used to store some of the documents; however, the data was mainly stored in the office PC or home PC without proper backups, which is a clear threat to data availability. During the interviews, one entrepreneur answered that the accounting software on home PC was making backups to a USB memory stick, however, this memory stick was never replaced, which meant that there were no offline backups available in case of a ransomware infection.

It is recommended to invest in an automatic backup solution where important files are automatically synchronized from the needed devices to a cloud service or to a local network-attached storage (NAS) which can keep data safe after hard drive

malfunction. For example, NAS with two or more drives configured in RAID 1, 5 or 6 mode (Redundant Array of Inexpensive Disks) can survive after one drive failure without data loss. Regarding the implemented RAID configuration, it is recommended to make additional offline backups periodically from important data in case of a ransomware attack where all data would be hijacked and encrypted.

Planning and implementing a proper backup solution can keep the integrity of important data untouched, stop unauthorized access to data and keep data available to authorized users.

5.3.3 Findings on third party solutions and installations

When a barn is built, the farmer usually selects one where all equipment and automation solutions are ordered. Usually the manufacturer also provides all technical devices and installations needed to run an automation system such as is the case of milking robots, when there is usually a control PC delivered where the system can be used and where information is stored.

Automation systems delivered by a manufacturer typically contain some level of maintenance service with an annual cost. This leads to the situation where farmers assume and trust that the technical solution of the automation system delivered by a major manufacturer meets today's cybersecurity requirements.

When interviewing the case farms, it was found out that almost in every farm where milking production control PC was in use, it was also used to browse the internet, read emails and other office tasks against the guidance from the service provider. This can make the control PC more vulnerable to malware infections even though the manufacturer's service technicians were to perform periodic updates and other maintenance to automation systems and control PC remotely.

During the visits in the case farms, two different ways were discovered how milking automation service provider makes the remote connection to the farm's automation system. The difference between two different topology solutions is introduced in Figure 18.

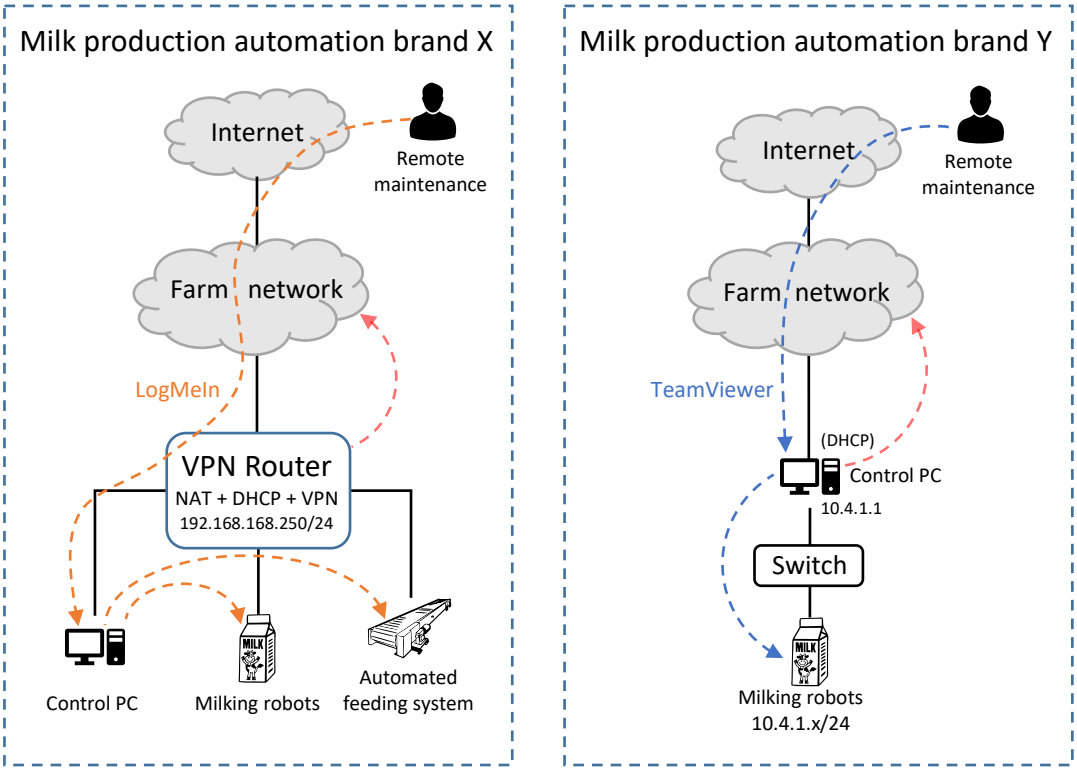

Figure 18. Remote maintenance difference between two automation brands

The first manufacturer had delivered a dedicated VPN router, and all automation devices were connected directly to the device. Even though the VPN router technically would allow the manufacturer to create a secure site-to-site VPN connection from inside the farm network to manufacturer data center, this possibility was not used. Instead, another third party remote connection software was used called LogMeIn.

The other manufacturer relied on the control PC with two Ethernet interfaces where one interface was connected to automation system's closed network and another interface was connected to farm´s network. When maintenance was needed, the manufacturer technician connected to control PC remotely using third party remote software called TeamViewer.

Even though no indications were found that the remote connections were misused, some remarks must be noted:

- Because visited case farms did not have any kind of physically or virtually separated networks for automation, guests and their own business, the automation systems are usually connected directly to farm's production network alongside all other network devices used by farm's employees.
- Using remote connections from public internet to automation devices using services such as TeamViewer or LogMeIn allows a technically remote technician to access also all farm's own devices and assets in the network.
- If a third party remote login service is hacked, leaked or someone can guess its credentials (for example, ID and password in case of TeamViewer), it makes it possible for anyone to access the farm network through automation control PC.
- Using automation control PC to other tasks than controlling automation makes a PC vulnerable to malware infections (ransomware, Trojans, worms etc.)

A more secure way would be dedicated isolated networks to different needs using a proper firewall and managed switches. For example, by installing third party automation devices to a dedicated automation network will isolate automation devices from the farm's own production network and because of this, the entrepreneur can be sure that nothing on the automation network will affect the farm's own users in their local network.

Network planning and proper device implementation and configuration will require some investment and a decent level of network expertise. Once the investment and installations have been made, the network will work reliably and offer better security to its users for years to come. With proper and up to date documentation and network topology map it is easier to find possible problems and maintain the network devices.

5.4 Examples of simplifying network topologies in farms

During the visits in the case farms, incorrectly configured or improperly installed network devices were found causing a risk to network availability and operation. In this section, some examples are presented of how the founded threats and risks could be solved with small modifications to network topology and configuration.

5.4.1 Solving routing problem in case farm 5

In case farm 5, the surveillance PC was installed in the farm's office by a professional company. Through surveillance PC, the employees were able to see live video from IP cameras and watch the recorded footage. Two Ethernet adapters were installed to the PC; the primary network adapter was connected to a closed network where all network cameras were installed, and the secondary network adapter was used to connect the PC to fiber gateway for an internet connection.

If the surveillance PC was to be rebooted, it could take several minutes to get the surveillance live video back online after the surveillance software had been completely loaded. Such a long wait until the surveillance software was able to make reconnection to the cameras was alarming, and the problem needed to be investigated more closely.

It was found out that both the PC's primary and secondary Ethernet adapters were configured to use the same IP network, gateway and subnet settings. The primary Ethernet adapter was configured with a static IP address and the secondary network adapter was configured to request network settings from the fiber gateway using DHCP.

After checking the PC's routing table, it was verified that both Ethernet adapters were using the same gateway IP address 192.168.1.1 as default route 0.0.0.0 with the same metric value. This caused fundamental routing confusion because the fiber gateway could reply to the packet requests only when the packets were sent through the secondary Ethernet adapter, and the packets sent through the primary network adapter never reached the fiber gateway.

By disabling the surveillance PC's secondary Ethernet adapter and connecting camera switches directly to the fiber gateway (presented in Figure 19) solved the routing problem and all cameras live feed after rebooting PC was showing up in seconds instead of minutes.

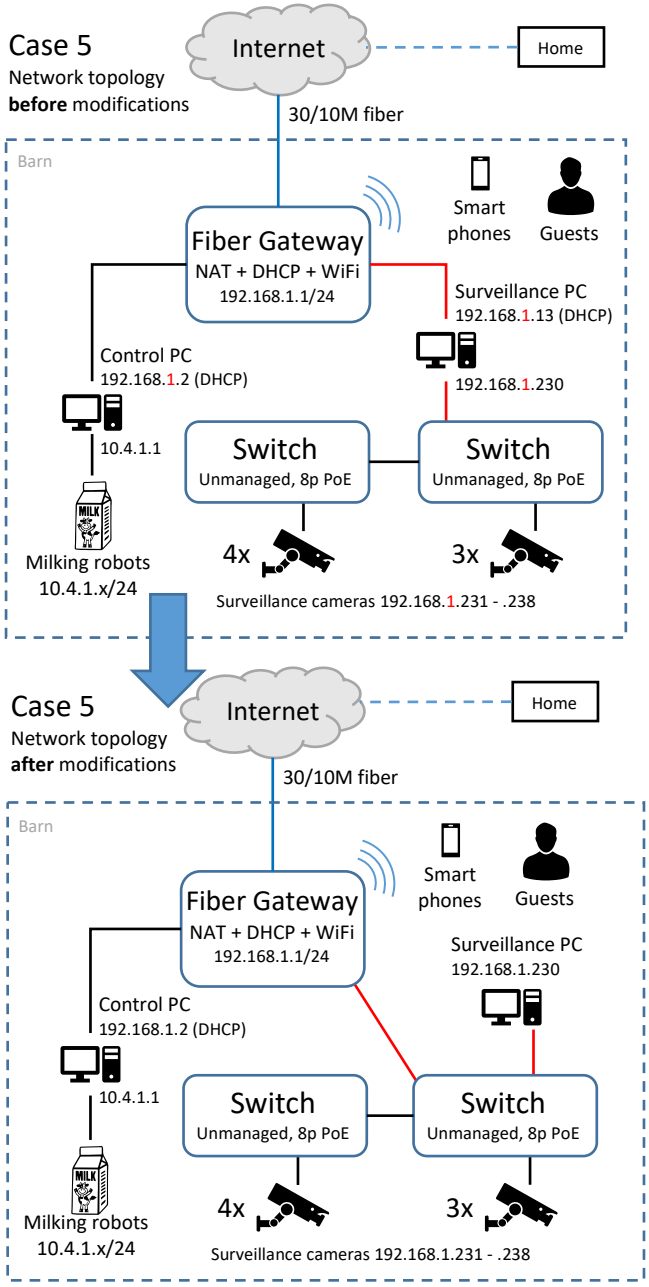

Figure 19. Removing routing problem in case farm 5

There can be various reasons why this kind of installation and configuration was implemented. It is possible that the surveillance installation technician had a limited knowledge of networks and configuring the same network to both Ethernet

interfaces was just a mistake. Another, more preferred assumption is to hope that the technician was trying to keep the IP cameras in an isolated network behind the surveillance PC; however, the results still reflect lack of routing and networking knowledge.

5.4.2 Modifying case 6 network from chain to star topology

In case farm 6, the network topology implementation was chain network topology as shown in Figure 16. With minor adjustments, it was possible to simplify the network topology to be more star-liked topology. The change in network topology is presented in Figure 20.

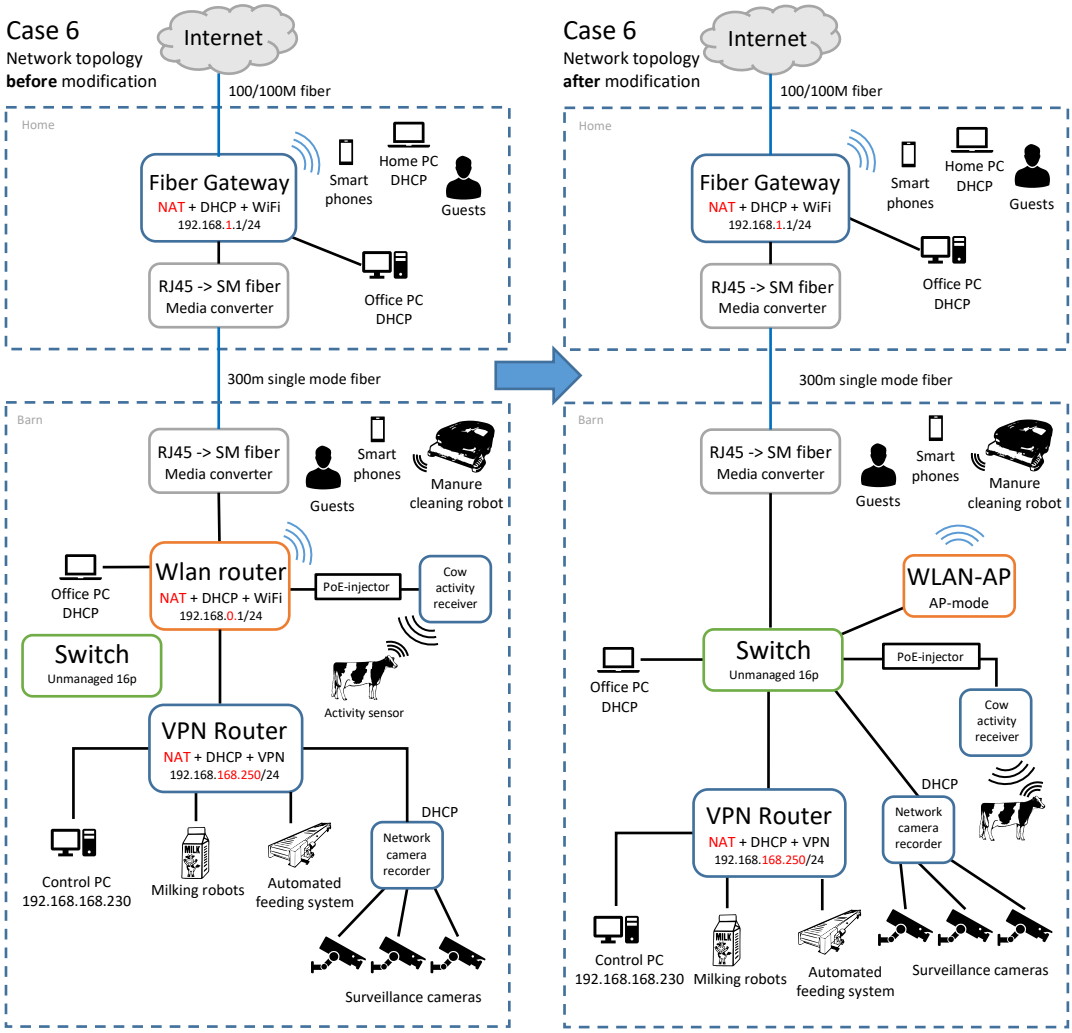

Figure 20. Simplifying case farm 6 network topology

In case farm 6, the following adjustments were made to the barn's network cabinet and devices:

- Unused and unmanaged switch was taken back to use for delivering fiber gateway DHCP and NAT to barn network devices
- The second WLAN router was reconfigured from router mode to access point mode and connected to the switch to provide wireless access to barns users
- Network camera recorder was removed from VPN router and connected to a switch
- The barn's network cabinet Ethernet cables were changed to a more suitable length
- VPN router installed by the milking automation company was connected to the switch

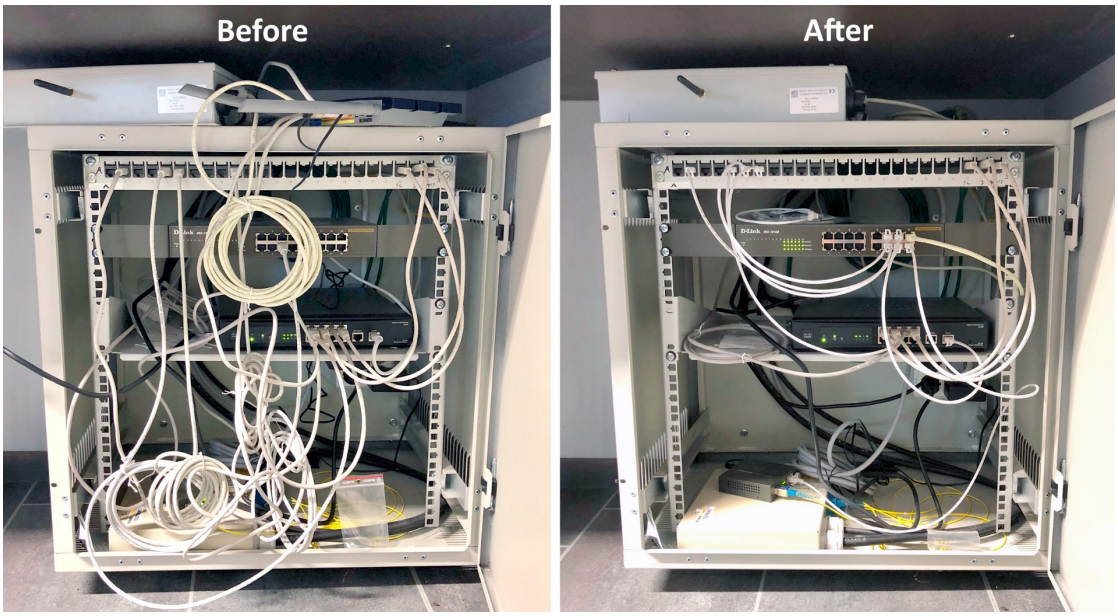

Figure 21. Network cabinet before and after modifications

The following benefits were accomplished thanks to the topology adjustments in case farm 6:

- Only one router (Fiber Gateway) is responsible for delivering the IP addresses to farm home, and the barn devices excluding milking automation company automation devices are connected directly to VPN router provided by the company.
- The barn's wireless network is created using a former WLAN router which was reconfigured to simple access point mode. Now the barn's wireless users get the IP address directly from the fiber gateway.
- The live camera feed from the network camera recorder came back online to the camera application on smart devices.
- By changing network cabinet's Ethernet cables, it is easier and faster to maintain and find out possible connection problems.

The difference between the network cabinet's over-length Ethernet patch cables and more suitable length cables is presented in Figure 21 on page 53. The result would be even cleaner if the cable management bars were installed to guide the patch cables towards the sides of the cabinet.

5.5 Advantages of enterprise-level network devices on farms

Based on the findings on farms, all the network equipment found consisted either of consumer-level devices or in some cases enterprise-level devices without advanced configuration that would take advantage of enterprise-level features.

The main difference between consumer-level and enterprise-level network device is usually level durability, reliability and network features. Enterprise-level devices are often made for more challenging environments and withstand wider environmental conditions such as changes in temperature and humidity longer than consumer-level devices. Higher price-tag also brings to the enterprise-level network features such as advanced routing tables, virtual LANs (VLAN), traffic prioritizing, advanced firewall rules, and overall enterprise-level devices are usually designed to be more secure and robust than the more affordable consumer-level devices.

From the perspective of price versus life cycle expectancy, devices designed for enterprise-level use have more often a longer warranty and MTBF expectation value (Mean Time between Failure) is often provided.

With consumer-level network routers with software firewall function and switches without management options it is usually hard or impossible to create separated virtual networks without using physically separated devices side by side. Enterprise-level switches support networking standard IEEE 802.1Q that supports virtual LANs on an IEEE 802.3 Ethernet network. This means that when using virtual LAN function, an additional 802.1Q header section is added to the network packet frame that indicates to the L2 and L3 level network devices (switches, routers, firewalls) which network segment the packet belongs to. (Shawn 2016)

Adding VLAN ID header to the network packet makes it possible to transmit and deliver network packets securely through the same network devices without the possibility that data packets mixing up with each other. Data packets containing

different VLAN information can be transmitted through the same cable between network devices using tagged data packets where data packets are sent through trunk-mode port using tagged Ethernet frames. This makes device installation simple because it is possible to transmit all segmented networks through one cable between switches and routers. (Shawn 2016)

By using segmented networks it is possible to separate home users and devices from business traffic and avoid business computers to get infected accidentally by family members actions with unsecure devices.

Firewall in the small network is usually responsible for routing traffic between network segments and for allowing or disallowing network packets to access another network segments. With firewall rules, it is possible to decide which selected networks can access internet. It is also possible to configure advanced rules like detailed access rights between segments for example to allowing users from guest network access only to home network printer besides basic internet access.

Modern firewalls also offer network traffic security features with detailed network analytics. So-called “Next-Gen” firewalls can inspect network data flow with deep packet inspection and prevent cyberattacks and malware for entering user’s network. These kinds of software security features are always paid subscriptions, however, on the other hand with firewall features e.g. gateway antivirus, antimalware, botnet detection, automatic intrusion detection and prevention, deep traffic analytics, application control and advanced network features that can raise a user´s network security to a whole new level.

Switches designed for enterprise-level use can be often managed with SSH or Telnet connection or through web user interface and support virtual LANs and fiber connections through SFP modules depending on the switch model. Enterprise-level switches can be installed to the standard 19” network cabinet, and there are switch models including Power over Ethernet feature (PoE) which is used by wireless access points and surveillance cameras. With PoE function, it is possible to transmit both power and data to a PoE supported device within the same Ethernet cable.

Wireless access points at the enterprise-level are used only for accessing the selected network segment wirelessly. Device installation is easy because access

points supports Power over Ethernet, and only one Ethernet cable between switch and access point is enough for power and data transmit. The broadcasting of multiple wireless networks simultaneously is usually supported and different network segment users can connect securely to their own network segment because enterprise-level access points support VLAN tagged traffic.

5.6 Recommendations for planning and implementing secure networks

Network security is important despite of the size of the network. Secure networks can be achieved with up-to-date documentation of the network and its devices, properly implemented network cabling, separate virtual network segments, properly selected and configured network hardware, monitoring, analyzing and alerting the network events and user cybersecurity education.

Comprehensive and up-to-date **network documentation** makes faster fault diagnosis possible during the network fault and can be achieved by:

1. Finding all technical and certification documents concerning cabling implementations if they exist and keeping them easy accessible place
2. Identifying and documenting all network devices and network users and how network devices are connected to each other by making network topology map
3. Finding out and documenting what are the roles of existing network devices, how the devices can be accessed for management including firewalls, routers, switches, and access points
4. Keeping all usernames and passwords to network services and devices in safe place

Physical cabling is the network's backbone and a long-term investment: the life cycle of high-quality Ethernet cabling can be up to 30 years and fiber cables over 50 years. Without properly selected and installed cabling there can be problems with network availability and reliability. In the case of planning to build new building or renovation of the old building, European cabling standard EN 50173 defines the standards and regulations for Ethernet cabling. When the physical cabling is installed by a professional company, the cabling is measured with a certified cable analyzer, and the cabling performance results are documented; hence, it is safe to install network routers, switches and access points where they are needed.

European cabling standard EN 50173-1 states that in short, under 90 m distances, copper Ethernet cable can be used when cabling is implemented with category 6 and

6A copper Ethernet cable. If 90 m distance between two network devices is exceeded, the connection needs to be implemented with a fiber cable to fill the cabling standard regulations. (Finnish Communications Regulatory Authority 2018b)

Recommendations of a high quality and high-performance network cabling are:

- Use of known-brand high quality copper cables with minimum category level 6. Recommended level would be future-proof category 6A which is capable to 10 Gbps speeds with full length.
- Cabling is installed on a proper path using cable ladders, rails, trays etc.
- In industrial environments shielded F/UTP or F/FTP type copper cable is recommended.
- The fire safety regulations must be taken into account when selecting network cable products and cable paths. (European cabling standard EN 50575 regulates cable performance in the face of fire).
- Installing Ethernet cables near electrical wires must be avoided and keep Ethernet cables as far from electrical wires as possible. When low voltage copper cable run parallel besides electrical wires, it can act like transformer or inductor and induce electrical current and noise from the electrical wires. Detailed information for installation distances between Ethernet and electrical wires are presented in European cabling standard EN 50174-2.
- All permanent copper cables should be terminated to proper network cabinet which has a lockable door for preventing unauthorized access to the cabinet
- Network cabinet should be installed in dry, warm easy accessible place and when selecting cabinet size, it should include enough space for installing network devices such as router, firewall, switches inside the cabinet.
- At the end user side Ethernet cabling should be terminated to proper termination box taking into account environmental variables such as dust and moisture.
- All network cablings should be well documented and properly labeled in a way that from label it is possible to identify where precisely the cable is terminated in the network cabinet.
- Network cabling documents including performance test results should be always demanded from the installation company for future use.

Dividing network and isolating different network user groups into separate **virtual network segments** and selecting proper network hardware to support the technical features can make network in farms safer and more controllable. Before planning the network segments, the following questions needs to be answered:

- What kind of different user groups need the network? (i.e. farm own usage, Visitors, Home, Automation, Surveillance etc.)
- How many devices need the access network and where? Is the device network connection implemented with wired or wireless connection?
- What kind of network access does the selected network user group need? Is it enough that group members can transmit data with each other? Does the group need to access Internet? Does to group need to access another user group segment?

Based on these answers, it is possible to design what kind of network segments need to be created, what kind of network traffic rules between the segments needs to be configured and finally, select which enterprise-level network devices are suitable for the needs. These plans form the different network segments used in farms and basic firewall rules between the segments.

With the knowledge where, how and how many devices need to be connected to the network, it is possible to estimate what kind of network equipment is needed to provide network access for all devices. Some recommendations for selecting proper network devices and recommendations for configuration are presented as follows:

- Asking help for network device selection and installing service from professional service provider specialized for networking can ensure that the selected devices are suitable for the needs and properly configured.
- By selecting a switch with extra ports more than the current need makes future expansions easier.
- Selecting switches with Power over Ethernet support can be a good investment in case of wireless access points or surveillance cameras are needed.
- Defining the areas where wireless networks are needed can help to estimate how many wireless access points must be installed to provide reliable wireless network in defined areas.
- When selecting network devices, environmental variables must be taken into account, such as the device exposure to temperature changes, water, dust etc.
- Default credentials should always be changed to all network equipment.
- New firmware and security updates should be installed to the devices periodically.
- Wireless networks should have a strong unpredictable password with WPA2 encryption.
- The devices responsible for farm network should be configured to a static IP address for management access and document configuration changes as well as management access information comprehensively.
- If professional installation service is used, all network documents should be sent to the customer for future use.
- Surge protection and UPS backup power for network devices is recommended against thunderstorms and power surges.

Network availability and security can be disturbed for many different reasons. M**onitoring, analyzing and getting alerts from the network events** can help to anticipate future problems, find the reason for possible network problems and recover faster from the network fault. Firewall is one of the easiest ways to get deep analytics of network traffic; however, interpretation of alarms requires professional understanding of what kind of events are normal and what kind of events needs to be investigated closer.

One possibility to ensure network health and fast recovery is to outsource farm network maintenance to a third party professional company where analyzing network traffic and maintenance of network hardware is part of the paid service.

User cybersecurity education will raise users' cyber awareness and help to identify what kind of cyber threats there are. User mistakes are one of the biggest threats causing data loss, virus infections and other security threats.

5.7 Design example for segmented network in farm environment

This section presents a secure network design for hypothetical case farm using segmented networks and enterprise-level network devices. The designed network topology is presented in Figure 22 on page 61.

In this network topology, the following network devices are responsible for delivering the network to its users:

- Fiber Gateway (provided by Operator)
- Firewall
- Managed PoE Switches
- Wireless Access Points

Fiber Gateway is responsible for converting fiber internet connection to copper signal. In this design, Fiber Gateway is configured to act as a bridge and deliver public IP address without altering packets through the device to firewall WAN port. Fiber Gateway features like NAT, DHCP and Wireless LAN are disabled.

Firewall is the most important device on the design. Firewall is responsible for network segmentation and routing traffic between the segments. Firewall provides traffic network address translations (NAT), IP address delivery (DHCP), rules how traffic can pass between network segments (firewall access rules), and analyzing and securing the network data between the public traffic from WAN and the private traffic from LAN networks.

With firewall rules, it is possible to allow specific network segment only to access from LAN to WAN for internet access and deny access to all other segments. With segmentation, it can be make sure that if a computer or another device is compromised in one segment, it will not affect devices in other segments.

Firewall can also provide to authorized users a secure way to connect to farm network and access the network assets e.g. office network drive, automation control PC or surveillance feed using VPN connection (Virtual Private Network).

Switches deliver all different network segments using VLAN tags, and every switch has dedicated switch ports to different network segments. Automation devices are connected to automation network ports, the surveillance cameras are connected to surveillance network ports and so on. Between switches, it is possible to transmit all necessary network segments within one cable using switch port trunk-mode if necessary. Switches are also responsible for powering up access points and surveillance cameras with Power over Ethernet feature.

Wireless Access Points deliver secure wireless networks for wireless devices. Network segments' VLAN tagged traffic is delivered through switches to the access points allowing devices to connect wirelessly and securely to the selected network. Because of PoE support, the access points do not need additional electricity, which makes the installation easier.

In the design the following network segments are presented

- Office network
- Surveillance network
- Guest network
- Automation network
- Home network

An example of configured firewall rules between network segments is presented on Table 2 on. In the example, traffic from all segments is allowed to access the internet; however, unauthorized traffic from the internet to all networks is denied. Office network users are allowed access to all other networks besides home network; however, the traffic from other networks to office network is denied.

Table 2. Example of firewall access rules between network segments

		TO					
		Internet	Office	Home	Surveillance	Guest	Automation
From	Internet	-	Deny	Deny	Deny	Deny	Deny
	Office	Allow	Allow	Deny	Allow	Allow	Allow
	Home	Allow	Deny	Allow	Deny	Deny	Deny
	Surveillance	Allow	Deny	Deny	Allow	Deny	Deny
	Guest	Allow	Deny	Deny	Deny	Allow	Deny
	Automation	Allow	Deny	Deny	Deny	Deny	Allow

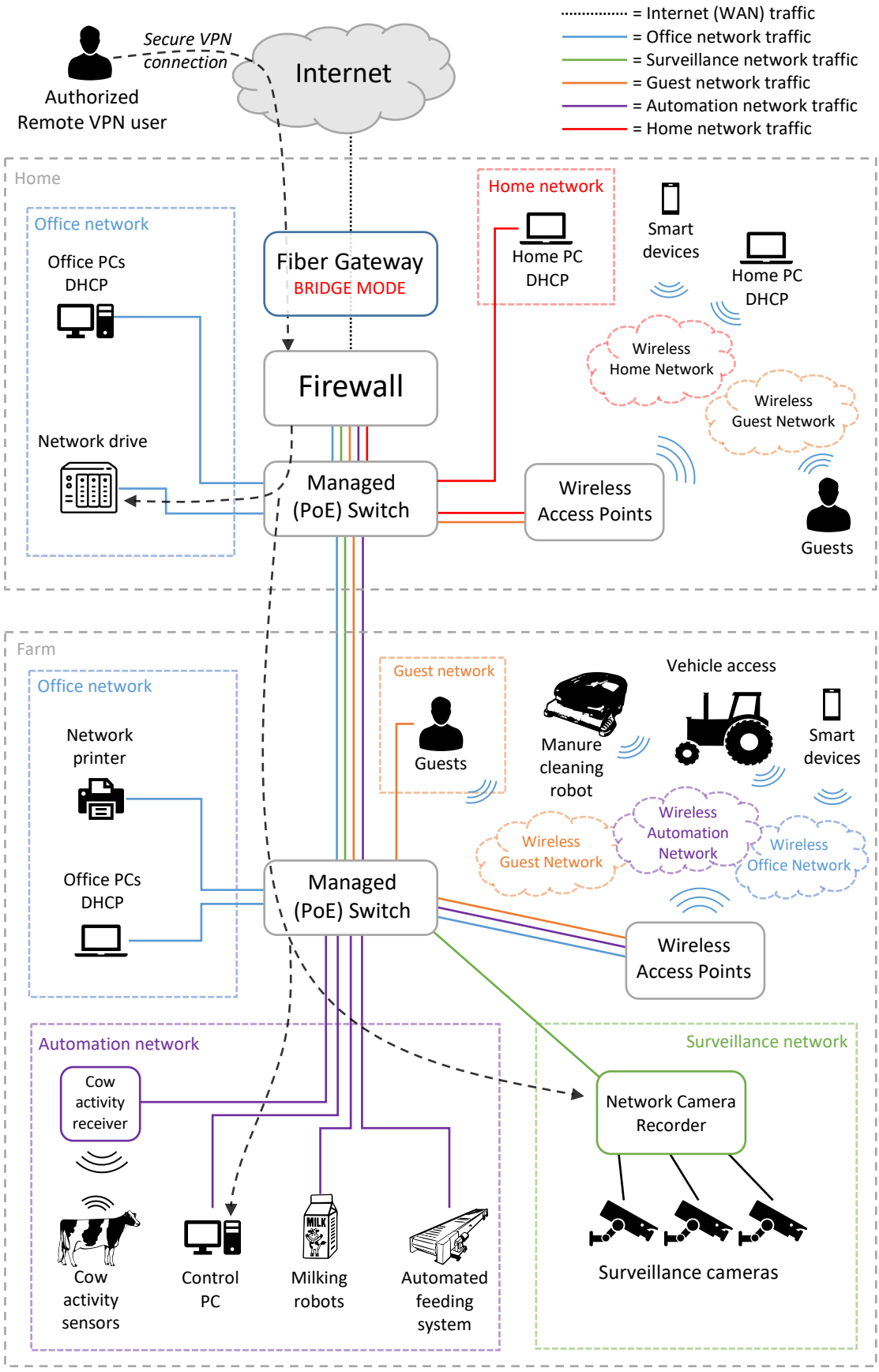

Figure 22. Example of a segmented network using a firewall and managed switch with VLANs

5.8 Possible business impact after device failure or cyber incident

Based on the findings and interviews on farms, modern farm will not run its business for a long time without automation and network access. The business impact in short term network outages is low; however, the impact caused by a long term network break is significant.

Before analyzing the business impact caused by network outage, it is important to understand what kind of reasons there can be that cause the fault in the communication networks.

Faults in network communication may affect the following network segments:

- Faults in local private network
- Faults in local internet connection
- Operator-specific network disruption
- Operator-independent nationwide network interference

Nationwide network interferences are the rarest and are caused by major faults in the internet backbone between countries or major cyberattack such as botnet attack against the world's largest DNS service operators. These disruptions can affect all internet users and a normal user cannot prepare against operator-independent interferences.

Faults in local internet connection or **operator-specific network disruptions** are usually caused by the same reasons as nationwide interferences. A local connection fault can be a result of a broken modem or fiber gateway. It is also possible that operator communication network core node fails during the maintenance or operators are targeted with DDoS attack (Distributed Denial-of-Service attack) by botnet devices.

For these kinds of network faults, it is possible to prepare for the situation by installing a secondary backup internet connection which is provided by some another operator. Firewalls are able to switch between primary and secondary internet connection automatically in case the primary connection fails.

Faults in the local private network can be the result of a faulty network device, device misconfiguration, user error or cyberattack against the business. If network

documents describing local network topology are up-to-date, recovery time from faulty network device is usually faster than without documentation.

In local private network, there are usually at least three types of devices: users, assets and network hardware responsible for delivering data between users and assets. Network asset is usually a device that should be available for user access e.g. network drive, network printer or office computer. A fault in a network drive causes disruption in accessing network drive files, a fault in network printer causes a printer to be offline and a fault in office computer can cause disruption of accessing the needed software or data stored on the computer.

Planning for actions in case of disruption of asset availability is the key for minimizing the business impact caused by the occurred fault. Examples of incident impact on business are presented in Table 3 on page 64.

Table 3. Examples of incident impact on business

Incident	Duration of impact	Impact on business	Cost	Prevention measures
Network connection failure caused by excavator accidently cutting the underground fiber near farm.	Depending on available telecommunication professionals from 1 to 5 working days.	Internet access is impossible. Emails do not work. Orders must place via phone. Remote automation maintenance is impossible.	Indirect cost amount depends on farms business.	Automated 4G backup connection provides internet access during the primary connection fault.
Automation PC gets infected by ransomware and accessing to computer data and software stops working.	Permanent, new computer or software reinstallation is needed.	Ransomware crypts all data and demands for paying ransom money. It is not guaranteed that data will be decrypted after payment. It should be assumed that all data is lost.	PC hardware and reinstallation cost. Cost of data lost cannot be estimated.	Periodically offline backups from important files.
Network switch breaks down due to thunder and power surge breaks other devices connected to switch.	If replacement hardware is not pre-purchased, replacement units are usually available within couple of working days depending distributor stock balance.	Devices connected to switch cannot access network. If device breaks by power surge impact from switch, device replacement is needed.	Replacement hardware and reinstallation cost.	All network hardware should be protected against power surges using UPS backup power devices.
Consumer-grade wireless access point stops working in barn because of high temperature and moisture.	From 1 to 3 working days depending how easy access point is to replace.	Wireless network access in barn is unavailable. Some work practices may need to be changed.	Replacement hardware and reinstallation cost.	By selecting enterprise-grade access point meant for outside use ensures reliable working in harsh conditions
Because of long-term network fault farm is unable to deliver reports about born or deceased animals to the authorities in time	Over 5 days (including holidays and weekends)	If reports are not delivered within 5 days, farm could get sanction of 3-30% decrease in agricultural subsidy	Significant	Ensuring additional methods to deliver required reports in case of long-term network fault
Someone finds out a major vulnerability on milking robots and creates a worm to find and attack milking robots automatically. Hacked robots stops milking cows.	Depending how fast worm is spreading, impact can last as long as manufacturer updates the robot software.	Catastrophically. Normally cow is milked twice a day and farms using robots do not have manual option for milking. If cow is not milked on time, it will cause pain to the animal and will be animal welfare violation.	Immeasurable. If cow is not milked on time, cow uterine inflammation (mastitis) is likely in the near future	Depending how automation robot is connected to network and worm infection is possible, next-gen firewall with security services may be able to prevent infection

5.9 Key findings summary

All security threat findings on case farms can be reflected to the CIA triad introduced in section 2.1. While various kinds of threats related to network security or cybersecurity overall were found, all findings can be evaluated with CIA triad. Table 4 provides examples of this way to reflect the threats to CIA triad.

Table 4. Examples of threat key findings and suggested solutions

Finding	Possible threat	CIA triad reflection	Suggested solution
In many farms, doors were unlocked and unauthorized access to network cabinet and office was possible to anyone.	Unauthorized access to network cabinet and office may endanger the devices for sabotage or theft.	Compromising device's confidentiality and availability.	By keeping doors locked with proper access control and video surveillance will keep assets safe from unauthorized access.
In case farm 3 there was both Cat5e cables coming from home office connected to the same unmanaged switch in barns network cabinet.	If someone would connect the second Ethernet cable between fiber gateway and home office free Ethernet jack, it would cause loop between home fiber gateway and barns switch and paralyze the network immediately.	Network loop affects network availability and causes for network outage could be hard to solve with the knowledge of farms own employees.	The second Ethernet cable from home office should be removed from the switch in the barn.
Fiber gateway admin login visible to public internet and admin credentials with default settings	If someone could bypass gateway login security (whitelisted IP-addresses), it is possible attackers to upgrade fiber gateway with infected firmware.	Compromising network traffic confidentiality, integrity and availability.	Network operator should be contacted and asked to reevaluate the risk of public login if there are other ways to deliver updates and keep maintenance.
Farms guests used the same LAN network than owners, no dedicated guest-networks were used	Allowing guests to join the same network where farm own devices are connected compromises all devices to unauthorized access. If guest device is infected, infection could spread to farms own network devices.	Compromising network devices' confidentiality, integrity and availability	Investing in a network equipment for business use (firewall, managed switch etc.) would make it possible to create a safe network segment for guest access.
No firewall hardware was used to protect network traffic	Without dedicated firewall, it is almost impossible to detect intrusions or suspicious network traffic. Computers, smart phones, network drives, automation devices and IoT devices connected to the internet are vulnerable to cyberattacks.	Compromising network traffic confidentiality, integrity and availability.	By investing to a real firewall would make possible to protect LAN network traffic better, raise awareness of possible attacks and for example it could be possible to create safe network segment for guest access.
Business files were often stored on a local computers without backups	Data loss after hardware failure, user error or infection by malicious software	Compromising files integrity and availability	Farms should self-valuate what kind of important data they handle and where it is stored and invest for a proper backup solution (Local backup system or cloud backup).
Multiple computers were lacking proper antivirus software	Risk of malicious software infection.	Compromising operating system and files confidentiality, integrity and availability.	Farms should keep a list of computers and smart devices and make sure that every vulnerable device has the same level of antivirus protection.
Automation control PCs provided by automation company were used against the instructions also for browsing the internet, accessing emails etc. Automation computers' hard drives were almost full (5-8GB free space)	Because PCs were used also other things than automation control, it raises the possibility to get malicious software infection. Lack of free space on hard drive could cause computer to slow down or booting problems after major Windows update.	Compromising operating system confidentiality and availability	By investing to dedicated office PC for other tasks than automation control would lower the infection risk of automation PC.
All case farms thought the longer network outage would be harmful but no backup connection were installed (like 4G backup)	If primary WAN connection (fiber) is cut off accidentally or intentionally (sabotage), it can take multiple days to get fiber fixed.	Compromising network availability	Investing in backup connection (e.g. 4G) would raise the network availability level.

These findings answer one of the research questions about the threats that can be found in the farms' telecommunication networks including some solutions how it is possible to fix the threats found in the case farms.

Based on the findings on the farms, their network solutions are implemented mainly with consumer-level devices. Most of the network devices, including WLAN routers and switches were installed to the farm network without any configuration or farmers counted on third party service provider's expertise, which was found to be lacking network skills as well.

The found problems on farms relating to IT solutions or network devices seem to be very similar compared to other small businesses in other non-IT-specific industries with the same employee size. It seems that if a company's core business is not IT related and there is no dedicated IT support person among the employees, the same kind of problems exist: documentation about IT solutions or network implementations is inadequate or missing completely, inexpensive consumer-grade network devices are used without proper configuration, and proactive planning in case of network outages and proper backups is missing.

Even though many similarities were found with the same size companies in other industries, unique threats to agriculture industry were also found. In the primary production, the required level for physical implementations is much higher than in businesses in cities, and physical threats such as dust, dirt or e.g. animals damaging physical cabling and devices demand more focus than in cleaner environments.

The distance between buildings where a network is needed in farm environments is also longer compared to other small companies, which leads to cabling implementations with fiber solutions when the cable distance between two buildings exceeds 90 meters. These regulations are introduced in European cabling standard EN 50173-1.

It was found out that in most of the case farms, the cabling between buildings was implemented with single mode cable except for farm. In other industries the companies corresponding to the employee size in agriculture industry do not necessary normally need fiber cabling in local networks.

One of the most surprising findings during the case farm visits was that all case farms were offered and implemented fiber network connection to the outside world. The network speeds were from 30/10 Mbps to 300/100 Mbps (download/upload), which is technically at the same level or better than in most small companies in cities.

When analyzing the findings from the perspective of network threats' uniqueness relating to agriculture industry, it can be stated that most of the threat differences between the same size companies with their core business not in the IT sector are caused mainly by environmental differences. In countryside areas the environmental and physical threats to network equipment and the probability of power and network outages are higher than in areas closer to cities where the power and network infrastructure is usually stronger.

Because there was only a handful of selected case farms, no strong generalizations can be made on how vulnerable telecommunication networks are in the primary production; however, based on the case farm findings and the earlier research by Laajalahti and Nikander (2017) from Natural Resources Institute Finland, the following key observations and conclusions can be made about farm telecommunication networks and cybersecurity:

- Overall cyber awareness level in agriculture is low and limited. Based on the interviews, most of the entrepreneurs or employees only understood the need of endpoint antivirus software without fear of other types of protection
- None of the case farms had proper documentation about network devices or network topology
- Networks were not protected with hardware security solutions such as dedicated firewalls
- All network devices and users were in the same network without a separation between farm's own devices, automation or visitors' needs
- All case farms used the fiber gateway provided from their internet operator and the fiber gateway was responsible for wireless network, NAT and DHCP services
- Other network devices in farms are mostly inexpensive consumer-level devices or have been provided by operator or automation service provider
- It is usual that network devices were installed with out-of-the-box configuration and default credentials
- Installation and configuration errors were found both in network devices installed by the farm's own personnel or a third party service provider
- The need for cybersecurity training and guidelines on how a network should be built and protected is required

6 Conclusions

Given that primary production is one of the major industries in our national emergency supply chain, based on observations in the case farms and earlier research it can be stated that farms are vulnerable to cyberattacks in many ways.

Because the farm size was larger, the barns were modern and technology used in the selected case farms was more advanced than on average farms in Finland, it can be expected that in many farms the findings on network implementation could be much worse than the ones found on the selected case farms.

The agriculture industry has been under the cyberattack radar for years, yet, times have changed. Cyberattacks are evolving, and automated scanners are constantly seeking the internet for vulnerable devices. The need for cybersecurity education and clear guidance from authorities as for how farmers can protect their networks, devices and data is required urgently.

Based on the observations, it can be claimed that there is also a need for professional IT- and cybersecurity services in primary production. If farmers had more education about cyber threats and ways to protect against them, it could create new business service possibilities for companies that provide expertise in these areas.

During the visits it was found that on farms the farm's own devices, automation devices and visitors were using the same network without restrictions. By using a network firewall with managed switches, it would be possible to implement multiple parallel and safe networks for each user groups where accessing from network segment to another could be controlled with firewall settings. Modern next generation firewalls can also offer network gateway level protection to all network users against viruses, cyberattacks, ransomware and deep analytics about network traffic.

Having a network topology map is one of the most important ways to document and understand how farm network is built both for the farm's own employees and third party experts. Even though a farmer does not necessary understand the role or operation of network device, it is possible even for a novice to draw a basic network topology map where it is documented which kind of devices are found on the

network and how they are connected to each other. In case of network problems, with network topology documentation it is easier and faster to understand and detect the cause of the network fault.

Christina Cooper has published Recommendations for Cybersecurity Best Practices within the Food and Agriculture Industry in 2015 (Cooper 2015) as follows:

- Create a cybersecurity culture within the Food and Agriculture Sector
- Increase the number of skilled professionals and those educated in cybersecurity
- Create and utilize assessments and other necessary tools
- Create and update applicable policies, plans and procedures
- Create and test backup and recovery plans
- Increase collaboration with other critical infrastructure sectors

The results based on the findings on the selected case farms fully support the findings and recommendations by Cooper (2015). The number of companies providing cybersecurity services is constantly increasing but the awareness of the need for these kinds of services must be raised in the primary production by educating farmers and increasing the cybersecurity culture within the agriculture industry.

From the business perspective, there is a clear need in the primary production for companies providing professional services such as auditing, planning, installation and maintenance of secure networks. While there are many potential customers in Finland within the agricultural industry, more planning is needed for what kind of services are the most needed and they should be focused on. Cooperation with known and respected players in agriculture industry could be the right way to make primary production field more secure one farm at a time.

Further research in agriculture cyber-awareness and sample solutions and guidelines to a primary production IT infrastructure is needed. It would be necessary to research deeper into which existing regulations and cybersecurity guides could fill the agriculture needs, and proper authorities should take control for cyber-education and supervising the progress of agriculture cybersecurity culture.

Future work

Even though the selected research questions were answered, more ideas for future research came up during the process of writing this master's thesis. Here are some questions that need to be answered and topics which have potential for future research:

- Cybersecurity in agricultural automation devices & proprietary software
- How will the deployment of ipv6 affect the cybersecurity of telecommunication networks at farms?
- How could farms self-assess their current cybersecurity level and identify the most vulnerable areas in their environments?
- Nationwide survey to farms for mapping the technical know-how level and the current understanding of cybersecurity and threats they are facing in business
- Detailed guidelines for planning and implementing networks in farm environments
- What kind of regulations are there on internal networks and telecommunications contracting in industrial buildings (barns)?
- Is there any authority who will take responsibility for promoting cybersecurity education in primary production?

References

Capgemini Consulting 2016. Cybersecurity in the Agrifood sector. Utrecht, Nederland. Accessed 10 October 2018. Retrieved from https://www.capgemini.com/consulting-nl/wp-content/uploads/sites/33/2017/08/02-029.16_agrifood_pov_consulting_web.pdf

CEMA / European Agricultural Machinery. (2017, February 13). Digital Farming: what does it really mean? Brussels, Belgium. Accessed 18 November 2018. Retrieved from http://old.cema-agri.org/sites/default/files/CEMA_Digital%20Farming%20-%20Agriculture%204.0_%2013%2002%202017.pdf

Cooper, C. 2015. Cybersecurity in Food and Agriculture in publication Protecting our Future, Volume 2: Educating a Cybersecurity Work Force. Hudson Whitman/ Excelsior College Press.

Finlex 2014. Tietoyhteiskuntakaari (917/2014). Helsinki, Suomi. Accessed 20 October 2018. Retrieved from http://www.finlex.fi/fi/laki/alkup/2014/20140917

Finnish Communications Regulatory Authority 2018a. Information security guidelines and tips. Accessed 10 November 2018. Retrieved from https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvaohjeet.html

Finnish Communications Regulatory Authority 2018b. Regulation on internal networks and telecommunications contracting in real estate buildings. FICORA 65 C/2018 M. Helsinki, Finland. Accessed 15 November 2018. Retrieved from https://www.viestintavirasto.fi/attachments/maaraykset/UUSI_M_65_C_2018_EN.pdf

Finnish Standards Association SFS 2018. SFS 6000 Pienjännitesähköasennukset. Accessed 10 November 2018. Retrieved from https://www.sfs.fi/sfs6000.

Jha, P. & White, J. 2018. Mirai (malware). Accessed 18 November 2018. Retrieved from https://en.wikipedia.org/wiki/Mirai_(malware)

Kim, D., & Solomon, M. 2012. Fundamentals of Information Systems Security. Jones & Bartlett Learning LLC.

Laajalahti, M., & Nikander, J. 2017. Luonnonvara- ja biotalouden tutkimus 32/217. Alkutuotannon kyberuhat. [Primary production cyberthreats] Helsinki. Accessed 5. October 2018. Retrieved from http://jukuri.luke.fi/bitstream/handle/10024/539088/luke-luobio_32_2017.pdf?sequence=1&isAllowed=y

National Institute Resources Finland, J. N. 2015. Suomen maatalous ja maaseutuelinkeinot 2015. ISBN: 978-952-326-026-9. Helsinki: Luonnonvarakeskus 2015.

Mathews, L. 2017. Criminals Hacked A Fish Tank To Steal Data From A Casino. Accessed 13 November 2018. Retrieved from

https://www.forbes.com/sites/leemathews/2017/07/27/criminals-hacked-a-fish-tank-to-steal-data-from-a-casino/

Ministry of Transport and Communications, Finland 2014. Information Society Code (917/2014). Helsinki, Finland. Accessed 1 November 2018. Retrieved from https://www.finlex.fi/en/laki/kaannokset/2014/en20140917.pdf

Russell, N. 2017. Cybersecurity and Our Food Systems. Medford, USA. Accessed 20 October 2018. Retrieved from http://www.cs.tufts.edu/comp/116/archive/fall2017/nrussell.pdf

Shawn, G. 2016. IEEE 802.1Q VLAN Tutorial. Accessed on 24 November 2018. Retrieved from http://www.microhowto.info/tutorials/802.1q.html#idp28880

Syväjärvi, J. 2016. Reikäkorteista digiaikaan: Maatalouden Laskentakeskus Oy 30 vuotta, tietojenkäsittelyä 58 vuotta. Vantaa. ISBN: 978-952-93-7315-4.

US Department of Homeland Security (DHS) 2018. Threats to Precision Agriculture. Accessed 18 October 2018. Retrieved from https://www.dhs.gov/sites/default/files/publications/2018%20AEP_Threats_to_Precision_Agriculture.pdf

Ministry of Finance 2010. Vahti sisäverkko-ohje [Vahti guide for internal networks] VM/2312/00.00.00/2010. Tampere: Juvenes Print Tampereen yliopistopaino Oy

West, J. 2017. A Prediction Model Framework for Cyber-Attacks to Precision Agriculture Technologies. (ISSN: 1049-6505). Gatton, QLD, Australia: Journal of Agricultural & Food Information. Accessed 5 November 2018. Retrieved from https://doi.org/10.1080/10496505.2017.1417859

Appendices

Appendix 1. Interview questions for entrepreneurs

Questions about telecommunication implementations and functionality in your business and thoughts about future

Telecommunications and cybersecurity in the entrepreneurs' everyday life

- How important is the role of telecommunications in the day-to-day operations of your business?
- What kind of thoughts do you have about the term "Information Security" in your business?
- Do you use any devices or software to secure your telecommunications, such as a firewall or antivirus software on computers?
- Is your business-critical data stored on a storage device in the local network or on an external service provider's cloud service?
- From the point of view of your business, is there a need to access to your devices or data remotely? (For example, remote connection from a tractor to a server on the local network)
- In case of a fault in network connection or network hardware (i.e. a fault in the farm's own hardware or a fault caused by the internet operator), what kind of negative effects would there be if the network outage lasted an hour, a day, a week or longer?

Acquisition and use of current solutions

- Have you planned and implemented your current telecommunication network by yourself, or have you had help from your internet operator or another third party service provider?
- Which of the following has most affected the acquisition of existing telecommunication solutions: The total cost of the telecommunications system, or the security and reliability of the network hardware?
- Do you have the IT skills required to configure networking devices or troubleshoot problems in case of faults?

Functionality of existing solutions

- Have you been satisfied with how your current telecommunications system's functionality and implementation?
- Have there been any sort of faults with networks? If so, what kind of faults? How have these events affected your business?
- Have you received help with solving the problems of the telecommunications network?
- Have there been any tasks or purchases that you haven't been able to do due to lacking connections, devices or cabling?

Planning for faults

- Do you have business-critical data duplicated or backed up?
- Are your IT or networking-related devices surge protected?
- Do you have an emergency power system, or do you use UPS-devices for protection?
- Is the grounding of buildings and network cabinets taken into account?

Looking to the future

- How do you see your needs regarding IT and telecommunication developing in the future?
- Do you have any plans for new construction or renovation projects where electricity or telecommunications cabling will also be renewed?
- Are you willing to pay for telecommunication or cybersecurity services, if needed? If you are willing to pay for these services, can you specify what kind of services you would need?