Nikander, Jussi; Manninen, Onni; Laajalahti, Mikko

Requirements for cybersecurity in agricultural communication networks

Published in:
Computers and Electronics in Agriculture

DOI:
10.1016/j.compag.2020.105776

Published: 01/12/2020

Document Version
Publisher's PDF, also known as Version of record

Computers and Electronics in Agriculture 179 (2020) 105776

Contents lists available at ScienceDirect

Computers and Electronics in Agriculture

journal homepage: www.elsevier.com/locate/compag

Requirements for cybersecurity in agricultural communication networks

Jussi Nikander[a,*], Onni Manninen[b], Mikko Laajalahti[c]

[a] Aalto University, Department of Built Environment, PL 14100, 00076 Aalto, Finland
[b] Exlan Finland Oy, Pirkkalaistie 1, 37100 Nokia, Finland
[c] Natural Resources Institute Finland, Niemisenranta 113, 74140 Iisalmi, Finland

ARTICLE INFO

Keywords:
Agricultural cybersecurity
Information security
Agrotechnology
Network
Internet
Farmer skills

ABSTRACT

Agricultural cybersecurity is a rising concern because farming is becoming ever more reliant on computers and Internet access. During the last few years, the agrotechnology community, public sector, and researchers have been alerted to the problem and a significant amount of research has focused on the issue. However, the majority of the existing work focuses on external threats or specific parts of the farm technology ecosystem. This work examines the cybersecurity capabilities of individual farms and focuses on the farm local area network; the network and connected devices of six dairy farms in Finland are examined in detail. In addition, the farmers were interviewed in order to ascertain their opinions and understanding of agricultural cybersecurity. The results of the reviews were mixed. The physical cabling, for example, was all in good condition and followed appropriate regulations. On the other hand, network topology, malware protection, and system backups were not handled appropriately. Surveillance cameras typically did not work as expected. Often, the farmers did not know the network topology, the connected devices, or the details of individual devices in the network. In summary, the cybersecurity on the farms reviewed in this work was not handled optimally and significant improvements would be needed in order to secure the reviewed systems. However, since the approach of this work is qualitative in nature, care must be taken when generalizing the results. In conclusion, there is a significant need for improvements in agricultural cybersecurity on the level of individual farms. Many of the threats faced by farms are caused by their own activity or the physical environment and thus, emphasis must be put on improving their own situations.

1. Introduction

Agricultural primary production in many EU countries is still dominated by small family farms (Eurostat, 2016). Such farms are effectively small or micro enterprises where the entrepreneur works alone, with their family, or with a small number of workers. Meanwhile, the productivity of farming, both by worker and by land area, has been continually increasing due to improvements in farming practices and technologies. Currently, perhaps the most transformative aspect of these technological improvements is the digitalization of agriculture (Klerkx et al., 2019, Rotz et al., 2019, Sundmaeker et al., 2016, Wolfert et al., 2017).

The digitalization of agriculture is an ongoing process that causes an increasing number of agricultural systems to be connected to each other through the Internet (Fountas et al., 2015). The increased connectivity allows for many improvements in productivity as well as improves farming processes in other ways. However, many of these systems are mission-critical, such as ventilation or feeding systems in animal shelters, or milking systems in the dairy industry. Such systems must be constantly available as downtime can quickly cause harm to the livestock. Many of the systems are dependent on an uninterrupted supply of electricity, water and, increasingly, network connectivity. In the past few years, the agricultural sector has realized that connecting machinery to the Internet also exposes these systems to a wide range of cyber threats (Barret and Amaral, 2018, Chi et al., 2017, Cooper, 2015, DHS, 2018, Jahn et al., 2019, Javaid, 2015, West, 2018). There are numerous use cases where mission-critical systems now need an internet connection, ranging from remote monitoring and control of animal shed automation, to tractor-implements remotely connected to farm management software via the ISOBUS-10 data communications standard (ISO, 2015).

The agricultural industry (Bogaardt et al., 2016), public sector (DHS, 2018, Duncan et al., 2019, FBI, 2016), as well as researchers have recently recognized this challenge (Barret and Amaral, 2018, Cooper, 2015, Gupta et al., 2020, Jahn et al., 2019, Klerkx et al., 2019, Spaulding and Wolf, 2018), and an increasing number of publications

* Corresponding author.
E-mail addresses: jussi.nikander@aalto.fi (J. Nikander), onni.manninen@exlan.fi (O. Manninen), mikko.laajalahti@luke.fi (M. Laajalahti).

https://doi.org/10.1016/j.compag.2020.105776
Received 28 May 2020; Received in revised form 3 September 2020; Accepted 3 September 2020

related to *agricultural cybersecurity* have recently been published. An overview can be found in the work of Nakhodchi et al. (2020), who found 141 agricultural cybersecurity publications on Web of Science between 2008 and 2018.

This work contributes to these research efforts by examining the on-farm communication networks, including the problems and vulnerabilities exposed by the physical and logical topology of the network. However, the communication network itself is only a part of the whole *cyber-physical system* of a farm. This work considers the cyber-physical system to consist of all technology on a farm that can be directly connected to the Internet (through wired connection, WiFi, cellular network, etc.), or that can create and/or use data stored on the Internet (through manual data transfer via USB stick or similar means). This work defines *agricultural cybersecurity* based on the definition of cybersecurity from the Finnish government (The Security Committee, 2018): *Agricultural cybersecurity consists of the activities and processes whose goal is to provide the farm a cyber-physical system that can be trusted to work as planned.*

Furthermore, the majority of the currently available literature on agricultural cybersecurity is focused on external attacks on the agricultural IT infrastructure, perhaps even focusing just on the farm computers, or it approaches the topic from the point of view of the whole food production chain. Perhaps as a consequence of this, many of current publications either implicitly or explicitly overlook the parts of farm cyber-physical system that are not traditional computers, as well as the individual farms' ability to prepare and their level of preparedness. The amount of resources available for cybersecurity can be limited on small family farms especially. This work focuses on the situation of individual farms and puts special emphasis on small family farms where the resources available for developing the cyber-physical environment of the farm are often limited, and thus, complements the existing literature.

This work argues that, currently, the most likely threats to the cyber-physical systems of small-to-medium farms are not external attacks. Instead, the most common problems in farm-level cyber-physical environment are the consequences of a lack of foresight or errors by the farm staff or are caused by the natural environment. In the context of farm communication networks, human errors include topological problems created by badly installed or mismanaged equipment, whereas the natural environment can cause problems via extreme temperatures, humidity, animal contact, or extreme weather.

The research question in this work is as follows. *What kinds of cybersecurity threats can be found in modern small and medium farms' telecommunication networks?* The goal of this question is to map possible threat scenarios for small farms' basic telecommunication infrastructure and the equipment and machinery connected to it. This work will answer the question using qualitative methods by having a telecommunications expert evaluate the telecommunication network of six farms in southeast Finland. Furthermore, the results of the evaluation will be assessed in order to find the level of preparedness for the farms in question and generate possible threat scenarios.

2. Theories and techniques

The Confidentiality, Integrity, Availability (CIA) model, seen in Fig. 1, is a fundamental element of information security (DHS, 2018, Kim and Solomon, 2012). In the model, *confidentiality* covers data privacy; only authorized users can access each system or view each piece of information. *Integrity* covers the data stored in a system being valid and accurate; only authorized users can use a system and modify the data. *Availability* covers the data or services being accessible; authorized users can use the system and access the data. In a proper cybersecurity environment, these three aspects of information security are guaranteed. A cybersecurity threat is an event that risks any of the three aspects in any part of the system.

When discussing telecommunication networks, it is useful to focus on the concepts of access control as well as network stability and reliability (Kim and Salomon, 2012). A working Local Area Network (LAN) is a requirement for modern, advanced farm technology to work properly. All systems and computers connected to the farm's LAN should be able to access all other devices, data sources, and services they need for functioning properly. Furthermore, only those systems that need to access specific resources should be allowed access them. In addition, the farmer and other users can trust that a stable and reliable LAN is fit for its purpose.

Telecommunication networks are often modeled using the 7-layer Open Systems Interconnection (OSI) model. The model, together with example cybersecurity threats for various layers in the model, can be seen in Fig. 2.

The lowest layers of the OSI model have hardware implementing them and are therefore vulnerable to physical threats. The rest of the layers are software and are only directly threatened by software threats. The focus of this work will be on the four bottom layers of the OSI model which are concerned with transferring data between two devices.

The threat models in literature often assume that the cybersecurity threats to agriculture are malicious actors. The Department of Homeland Security (DHS, 2018) identifies data theft, leaks, and intentional data falsification as major threats, while Jahn et al. (2019) discuss a wide range of external threats and Barret and Amaral (2018) discuss threats caused by hackers. Meanwhile, Chi et al. (2017) describe threats caused by the increased use of wireless sensor networks and Sontowski et al. (2020) demonstrate an attack on a wireless device. Trendov et al. (2019) and Wolfert et al. (2017) mention data security regarding agricultural big data and West (2018) discusses predicting and identifying external cyber-attacks.

However, external attacks are not the only cybersecurity threats for agriculture. Other threats identified in the literature include human errors (Bogaardt et al., 2016, DHS, 2018), natural causes and power failures (Bogaardt et al., 2016), sensor malfunctions (DHS, 2018), and extreme weather (DHS, 2018). Some common sources of cybersecurity threats in agricultural primary production are dust and dirt, humidity, and temperature changes, as well as contact with production and pest animals, all of which can disrupt the functionality of agricultural machinery, automation, and computer systems (Laajalahti and Nikander, 2017).

Furthermore, it is not merely older farmers who require additional support. According to Spaulding and Wolf (2018) younger, more tech-savvy farmers also need help. In general, a fundamental problem in agricultural cybersecurity, especially for small and medium farms, is that the farms' staff are not trained to be technology experts, let alone cybersecurity experts. Therefore, the digitalization of agriculture brings new problems to many farms which they are not able to manage professionally. Increased automation, autonomous field machinery, UAVs, sensor networks, and the integration of all these systems together fundamentally change the nature of farm management. However, the adoption of these new technologies will also require improvements in a farm's telecommunications infrastructure and significantly increase the importance of this infrastructure for the farm, as mission-critical systems start to be more dependent on telecommunications. Therefore, in addition to research on how new and upcoming technologies will affect the cybersecurity environment of a modern farm, there is also a need to focus on what kind of cybersecurity problems existing technologies already cause.

3. Methods

A modern farm requires data networks for a wide variety of different reasons. Many agricultural automation systems are connected to the Internet in order to enable remote monitoring and control, as well as for maintenance and updates from the system providers. Many of these systems have strict requirements for performance and reliability.

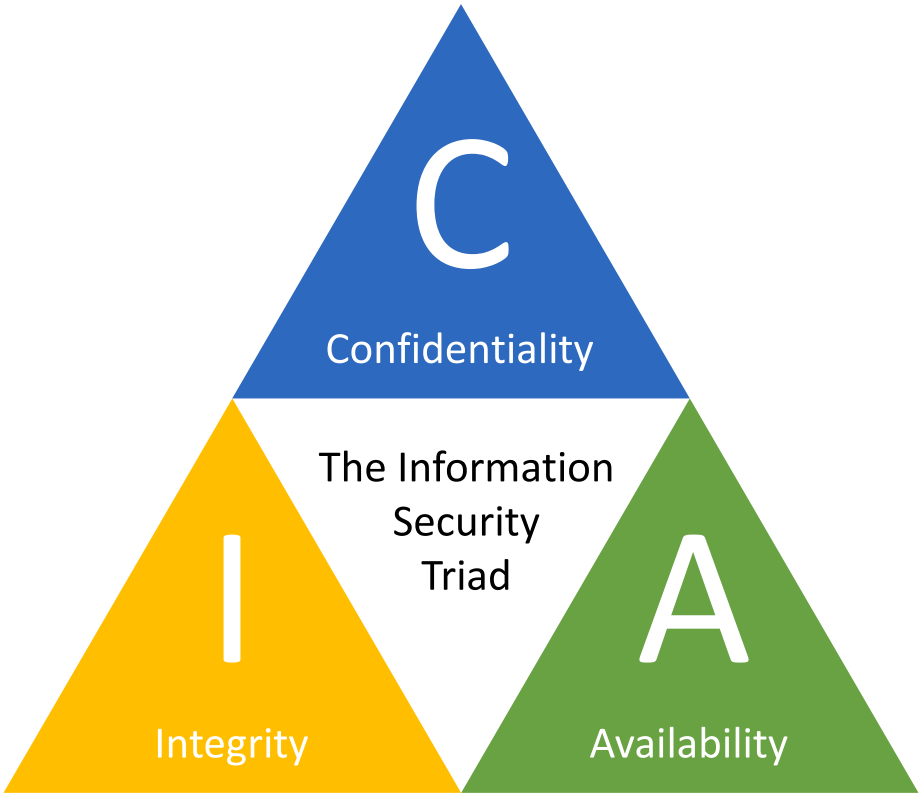

Fig. 1. The Confidentiality, Integrity, Availability (CIA) triad.

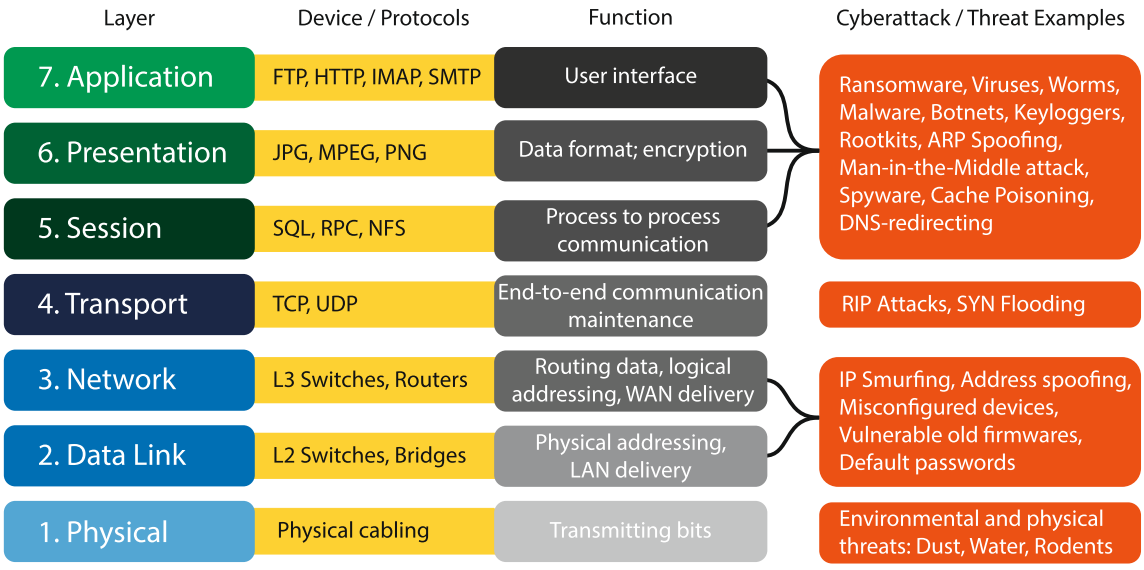

Fig. 2. The OSI model and cyber attack examples, originally published in Manninen (2018).

In animal production, for example, ventilation and watering systems must work constantly and outages can have fatal consequences to the livestock in just a few hours.

In addition to automation systems, modern farms may require access to a number of off-farm services such as farm advisory or management services or local or state authority registers for animal health or subsidy purposes. Furthermore, many farms communicate with their farming input providers, customers, or other partners through the Internet. An increasing number of farms also use web-based cameras for monitoring farm animals, premises, or other places of interest at the farm. All these require an internet connection.

Finally, in addition to all the Internet use related to the farming business, the farmer and their family also use it for leisure. This use is often through the same internal network and same ISP connection as all the farm business.

Fig. 3 shows what the local network in a generic farm might look like. The network has four important subnetworks that contain different types of computers and devices connected to the internet: the fields, the farmhouse, animal shelters, and finally other farm buildings, such as barns or grain silos.

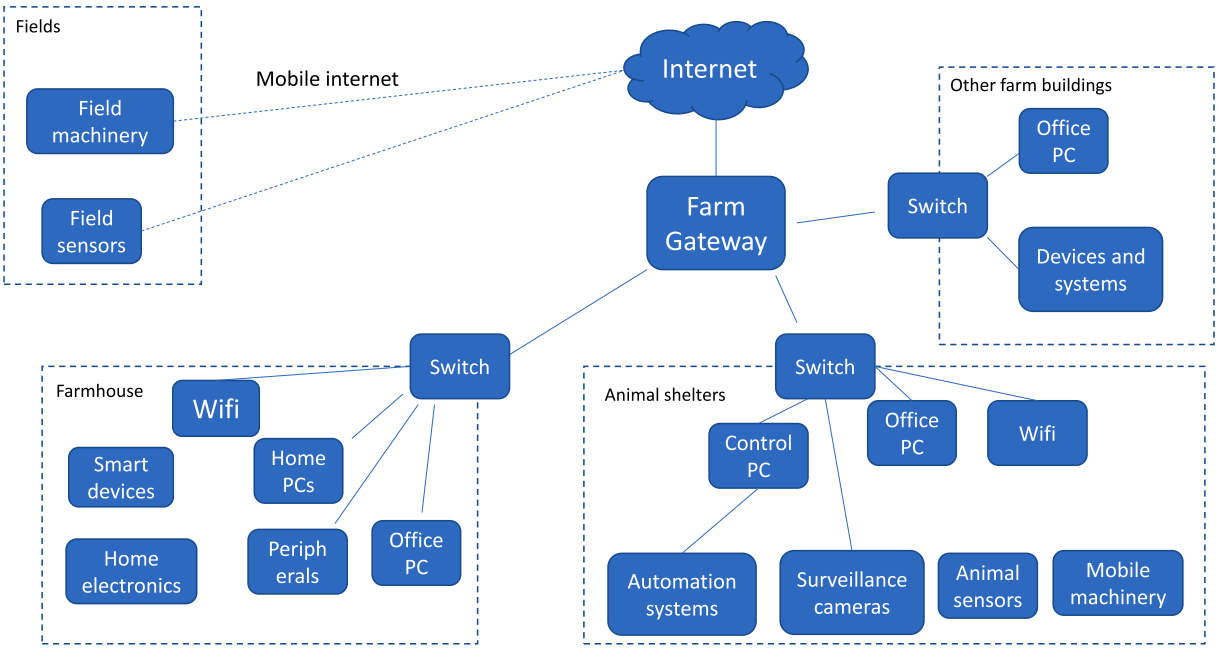

Fig. 3. Generic model for a local farm network.

On a farm, any subnetwork can have a large number of heterogeneous devices connected to it. The farmhouse most likely contains the main office PC, other work computers, and devices of the farm. In addition, the farmhouse typically also hosts private computers and devices belonging to the farmer and their family and might host devices belonging to visitors and farm workers. Thus, there is a significant need to divide the farmhouse network logically into two separate networks: one for work devices and one for private and leisure devices.

Animal shelters at a farm can also contain many devices. Most animal shelters have automation systems related to ventilation, feeding and watering the animals, and cleaning up manure. In the case of dairy farms, there are also milking systems, and farms can attach sensors to the animals for monitoring health and activity and use surveillance cameras to monitor the animals in the shelter. In addition, the animal shelters can have control and office PCs in their network.

The rest of the farm buildings can have a wide variety of computers and devices in them depending on the purpose of the building and the technology used at the farm. Similarly, a modern farm can have several sensors in the fields and use mobile machinery that are connected to the Internet. However, in many places, the field devices are more likely to be connected to the cellular network than directly to the farm's local area network.

If there are farm devices, such as tractors or field sensors, that are directly connected to the Internet, the farm local network must be able to access the data created by these devices. Furthermore, field machinery may need to be able to access data from the farm network while in the field and the farmer may have a need to access some of the on-farm services while outside the farm premises. For example, access to alerts from automation systems or the video feed from surveillance cameras may be important while the farmer is away from the farm. Therefore, it is not possible to completely close the farm local network from outside access; external devices need to be able to connect to devices on the farm LAN.

3.1. Examination of network infrastructure on Finnish farms

This work examines the current state of communication networks on Finnish farms. For this, the authors used an approach based on a detailed review of a small number of networks combined with in-depth interviews of the farmers. Due to the detailed approach, the authors decided to review a small number of carefully selected farms. Therefore, the results of this work do not cover the state of communication networks on farms in general; instead, it describes what kinds of implementations can be found in practice and provides insight on the types of problems encountered.

4. Results

In this work, a total of six farms from South-Eastern Finland were visited. On each farm, a communication network security expert (one of the authors) reviewed the on-premises network. After this review, an in-depth interview with the farmer was conducted. Due to space restrictions, this paper covers three of the six farms in detail. A summary of all the farms can be found in Table 1 and the full results of the reviews and interviews can be found in the work of Manninen (2018). All the farms selected for the study are planning to expand and develop their business in the future and, therefore, are expected to invest in the infrastructure of the farm. Thus, the authors assume that these are examples of farms where the IT infrastructure development is above average for Finnish dairy farms.

Only dairy farms were included in the study. The dairy industry was selected for the case study due to modern dairy farming requiring many systems connected to the Internet, and there being a large number of dairy farms in the area of study. Other branches of animal husbandry, such as poultry or swine farming, have a significantly smaller number of farms, and investigating them was not considered to be as impactful as for dairy farming. Furthermore, poultry and swine farming are even more reliant on technology and IT infrastructure than dairy farming is, and so the authors assume that these farms have at least a comparable level of technological sophistication to dairy farms.

In brief, all six farms reviewed in this work were dairy farms, with the farm size varying from 50 to 300 animals. On every farm, the barns holding the animals had an Internet connection and contained at least some of the following technologies: milking robots, automated feeding system, cow activity sensors, manure cleaning robots, and surveillance cameras.

The case farms 4, 5, and 6 found in Table 1 are described in more detail in this paper. These three farms were selected as such due to having relatively sophisticated level of automation while providing good examples of potential problems encountered in practice. As a

Table 1
Summary of the reviewed farms, originally published in Manninen (2018).

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, 16 mm^2	Yes, 6 mm^2	Yes, 6 mm^2	Yes, 16 mm^2	Yes, 6 mm^2	Yes, 16 mm^2
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 300/100 M	Singe mode fiber 30/10 M	Singe mode fiber 30/10 M	Singe mode fiber 300/100 M	Singe mode fiber 30/10 M	Singe mode fiber 100/100 M
LAN extension to other buildings	Single mode fiber (800 m)	–	Category 5e unshielded (120 m)	Single mode fiber (200 m)	–	Single mode fiber (300 m)
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

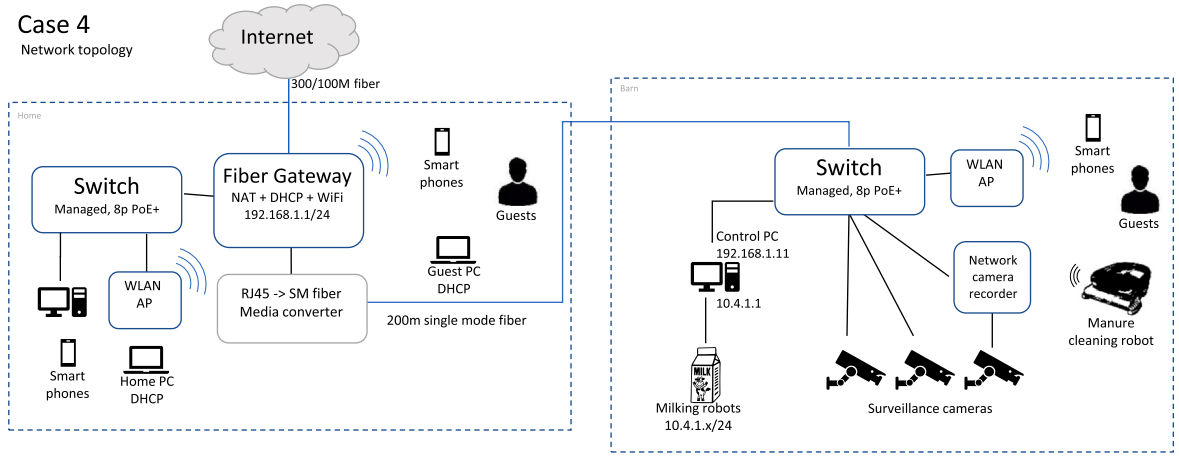

Fig. 4. Case farm 4 network topology.

result of the review, the network topologies of case farms 5 and 6 were modified. The network topology both before and after modifications are described here. The rest the farms are detailed in the work of Manninen (2018).

4.1. General observations regarding the case farms

Problems with the following were observed on practically all case farms: 1) *network equipment*, 2) *network topology*, 3) *malicious software protection*, 4) *endpoint protection*, and 5) *availability of surveillance videos*.

The basic network solutions on the case farms were found to be quite similar. Data cabling was done as part of the plan for the farm electrical wiring and the guidelines for electrical wiring for residential buildings had been followed. The materials used for the data cabling were also designed for residential buildings. The network cabinets used were not designed for the environment they were used in and were not moisture- or dustproof.

Network equipment was typically designed for consumer use and in most cases, the equipment had been left on default settings and passwords and addresses or routing had not been modified. Most of the equipment had been installed with the assumption that the device functions appropriately if it was able to connect to the Internet. In other words, proper analysis of the possible side-effects of the installation of new equipment was not done when the network was expanded. Most of the farm networks followed the chain topology, instead of the star network topology, which sometimes led to inefficiencies such as multiple devices with NAT functionality in a chain. Due to this, as well as other configuration issues, the visibility of local services in various parts of the local network was not always coherent. Furthermore, the use of consumer-grade equipment often limited the amount of flexibility in device settings. However, the equipment used was sufficient for the requirements of the farm in all cases.

The farm network topology was typically built according to need and without prior planning. Thus, the network topology had grown organically and the farmer did not have a clear understanding of: the topology, how the devices were connected to the internet, or whether the current topology was suitable for the intended purpose.

On most farms *protection against malicious software* and cyberattacks was implemented with the best-case scenario in mind. Antivirus software was installed to many, but not all, computers and laptops. On some farms, different antivirus software had been installed on different workstations at the farm. Only one farm had a hardware firewall which had been installed by the provider of the milking robot.

In this work, it was observed that *endpoint protection* is most difficult for integrated systems. It is typically not possible to install third-party software to such systems and therefore the user is entirely reliant on the equipment manufacturer and firewall solutions. On several farms it was also noted that the same computer was used both for management of on-farm integrated systems (e.g. milking or feeding) and web browsing. This increases the risk of cyberattacks against the integrated systems.

However, it should also be noted that modern farm automation typically requires remote access from the device manufacturer. This can expose the integrated systems to cyberattacks even if the local control computer is not used to access locations outside the farm. For remote management, two technology solutions are typically used; the first is a remote desktop solution, such as LogMein or TeamViewer, and the second is the use of a VPN between the device manufacturer and the farm.

On all reviewed farms that used video surveillance, *there were problems with the availability of the video*. Typically, the video feed was not available everywhere it was needed and nor to all devices the farmer wanted to use for viewing it. The cause for these problems was often related to changes in the network topology done after the installation of the video system. Furthermore, if the farmer wanted to access the video from outside the farm, this was often impossible due to the service agreement they had with their network operator. Most farms used consumer-grade network services, where on-site services were all blocked by default, and the network operator offered no support should a service be exposed outside the local network.

4.2. Case farm 4

The network topology for case farm 4 can be found in Fig. 4. The farm had under 100 cows which were fed manually and milked with milking robots. The farm also used video surveillance equipment and had a manure cleaning robot in the barn. The network setup was relatively complicated and included many systems connected to the Internet.

The farm network consisted of two separate switches, one in the farmhouse and on in the barn. In addition, there were WLAN access points in both the farmhouse and the barn, and the fiber gateway device had a third WLAN AP.

When the farmer was interviewed, they revealed that they had trouble with accessing the video surveillance equipment using smart phone. Wireless access to the video had worked when the system was installed but had stopped working at some point.

4.3. Case farm 5

The network topology for case farm 5 is shown in Fig. 5. The left side of the figure shows the original topology, and the modified topology is shown on the right side. The size of the farm was between 200 and 250 cows, which were fed manually and milked with milking robots. The barn also had a surveillance camera system. This farm had

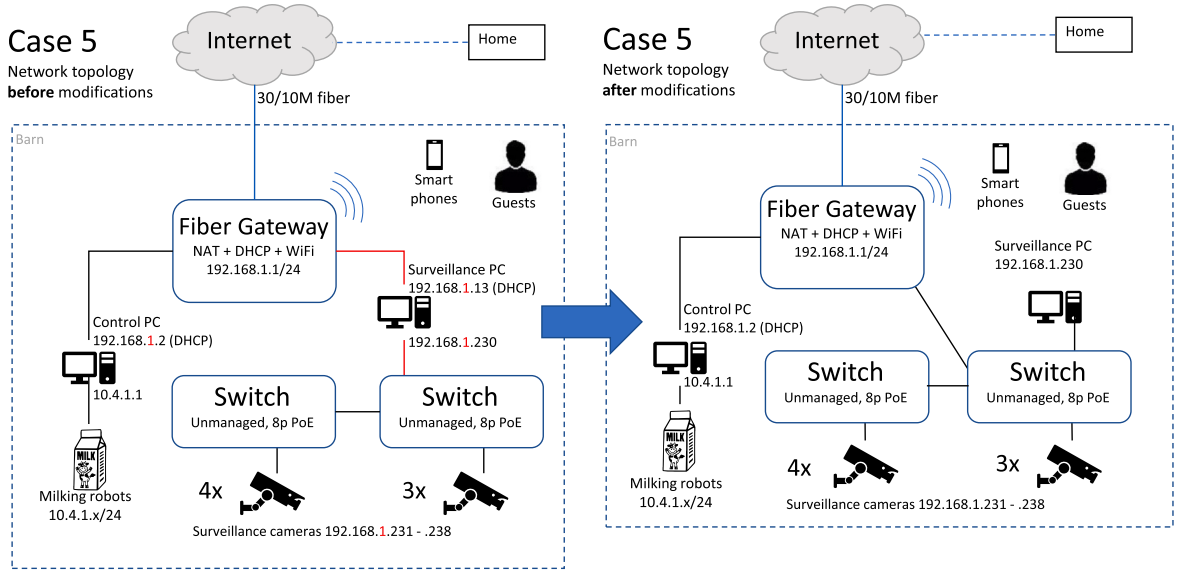

Fig. 5. Network topology for case farm 5.

separate Internet access for the barn and the farmhouse, and therefore the home network is left out of the figure.

The surveillance camera video feed in the barn went through a dedicated PC which had two ethernet adapters: one for the surveillance cameras and one for the rest of the barn network. The adapters had been configured with the same network and default gateway which caused them to have the same gateway IP in the route table of the surveillance PC. This, in turn, caused significant delays in the startup of the surveillance video feed after the surveillance PC was rebooted. The problem was resolved by connecting one of the two switches used for the surveillance cameras directly to the fiber gateway and connecting the surveillance PC there. The secondary ethernet adapter on the PC was disabled.

4.4. Case farm 6

The left side of Fig. 6 shows the original network topology for case farm 6. The size of the farm was between 200 and 250 animals and it used milking robots, automatic feeding systems, video surveillance, cow activity monitors, and manure cleaning robots. It had the largest number of different systems of all the farms in the study. As shown in Fig. 6, the Internet connection for the farm was a 100/100 M fiber which goes through the farmhouse into the barn.

The farm network used the chain model with three routers connected to the chain. One router was in the farm's main building and two in the barn, and all three had NAT functionality activated. In the interview, the farmer discussed some problems he had with the equipment at his farm. The main complaint was that the live video feed had stopped working after maintenance of the milking robot. The reason for this was that the three nested routers hid the surveillance camera network from the rest of the farm local network. As a solution, one of the routers was replaced with a switch and the surveillance cameras were connected directly to it. The modified topology for the case farm network is shown on the right side of Fig. 6.

4.5. Farmer interviews

On all case farms, the farmer was interviewed after the review of the farm network. They were asked about how they utilize IT in the farm operations, how important IT and network connection is for the farm work, how they see the role of cybersecurity, how they have prepared for problems in the farm network and equipment, and how important they see IT for their business in the future.

Information technology and network services were seen as critically or extremely important by all interviewees. Compulsory communication with authorities (related to e.g. animal health), business deals, bookkeeping, automation, and surveillance were mentioned as being daily uses of network and IT services. Despite this, most farmers did not see network failures as significant threats to their business; only one considered a day's downtime as a serious threat for their business. The rest considered a few days of downtime as manageable, and a week's worth as a catastrophic threat.

The farmers had a lot of concerns related to cybersecurity at the farm, such as endpoint or wireless security, but not all were aware of the state of cybersecurity in their own network. For example, not all farmers knew whether they had firewalls or malware protection installed on their computers. Data protection was not necessarily properly implemented; often backups were taken by hand and stored on local computers and some used cloud services for backup.

4.6. Summary of findings

An overview of the problems observed in this work can be found in Table 2. The table is divided into five categories as described in Section 4.1: 1) *network equipment*, 2) *network topology*, 3) *malicious software protection*, 4) *endpoint protection*, and 5) *availability of surveillance video*. The first four categories describe vulnerabilities that expose the farm network to faults. Of these, the two first categories – network equipment and topology - are general in the sense that they can cause many different problems. Examples can be seen on case farms 5 and 6 where significant problems in the network topology were fixed as a part of this work. The two next categories – malicious software and endpoint protection - are less wide in scope. However, examples of both were encountered on several farms in this work. The final problem category - availability of surveillance video - is a problem often caused by the network topology. However, it is mentioned separately here for two reasons. First, the problem appears to be very common and thus was encountered several times during this study, and second, it is easily noticed by the farmer. As a result, problems with on-farm video surveillance can act as an indicator of wider problems in a farm's network.

5. Discussion

Overall, the results of this research were mixed. Some elements on

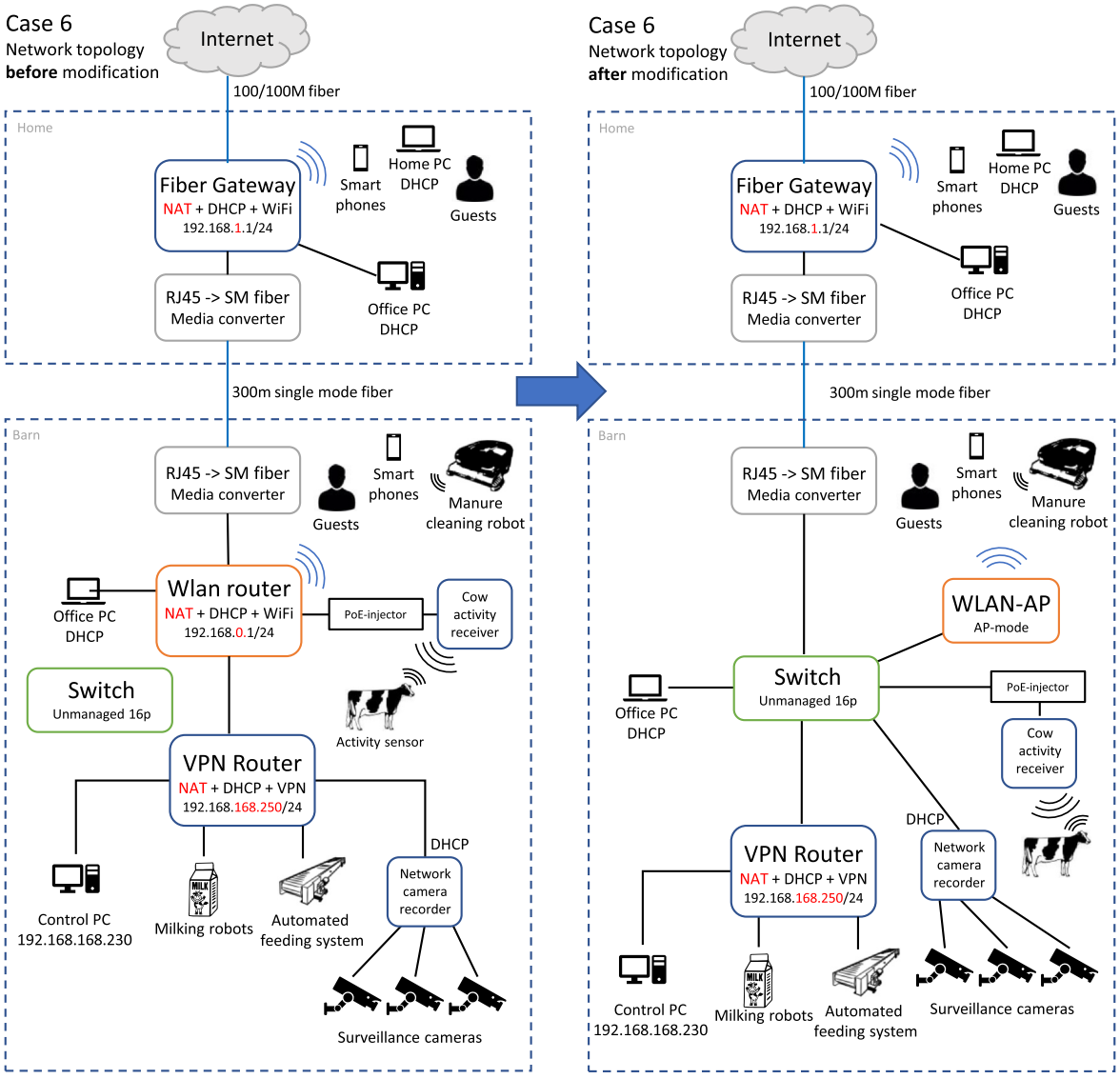

Fig. 6. Network topology for Case Farm 6.

the case farms were better handled than the authors expected, such as backup power systems and grounding of the cabling and devices. All the farms reviewed in this work had relatively modern barn buildings so, all the electrical work on these buildings, including network cabling, followed the Finnish Standards Association SFS 6000 series regulation for electrical installation (SFS, 2018). The network cabinets for most farms were messy and thus difficult to figure out. As demonstrated by the example in Fig. 7, many reviewed network cabinets had all sorts of

Table 2
Summary of cybersecurity problems observed in this work.

Problem category	Threats
Network equipment	• Consumer-grade equipment is not suitable for the physical farm environment and breaks easily • Equipment is left on default configurations and is vulnerable to intrusions and malicious software • Equipment is exposed to dust, humidity, and other environmental hazards, which can break it
Network topology	• Network topology has not been planned beforehand, so the network has grown organically, sometimes preventing equipment from working properly • Network topology is not known to the farmer, so they are unable to maintain it or plan expansions • The farmer is not aware of all devices attached to the network, and so cannot maintain them
Malicious software protection	• Malicious software protection is installed only on some of the devices leaving others vulnerable • Some devices may have multiple, superfluous protection software installed which affects device efficiency and functionality • The farm has no plan for malicious software protection and so maintenance is not done properly
Endpoint protection	• There is no firewall or network access control in the farm internet access, thus allowing outside actors easier access to the farm network • Individual devices may have their own firewalls • There is no endpoint protection plan
Surveillance video availability	• Video is unavailable for the farmer in some locations • Video is available for unauthorized users

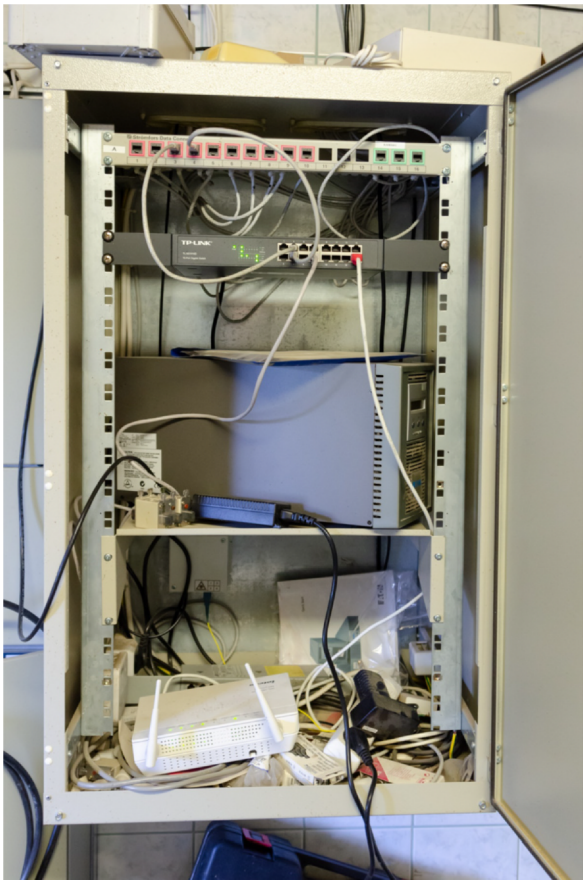

Fig. 7. Example network cabinet from a reviewed farm.

devices in them, and in many cases the farmer was not aware of the functionality of all the devices.

There are several clear causes for the state of the farm networks reviewed in this work and the following reasons were considered the most important. First, *farmers typically do not have a lot of resources*, especially time and money, to use on the farm network, as other matters at the farm are considered to take priority. Consequently, the farm network, despite its importance, is not given proper consideration. Second, the *typical farmer is not an IT expert* and therefore would not be able to properly build, secure, and maintain their network without expert assistance. Thus, the network is often left in a vulnerable state and may not work as intended. Third, due to lack of expertise, the network of a typical farm uses an Internet connection and network *devices designed for home use* which are not ideal for a system used for production in a demanding physical environment.

5.1. Network equipment and farm network topology

Based on the limited number of farms surveyed in this work, the farm local network of many farms was vulnerable to many cybersecurity threats. For example, the farms did not have dedicated firewalls and relied on the protection provided by the gateway devices. One farm was an exception and had a firewall to protect the milking robot which had been installed by the robot's provider. Malware protection was maintained on the level of individual devices and there was no general plan for malware protection for the whole farm.

The network in some of the surveyed farms used a chain topology. An example of this is case farm 6, where the network consisted of three chained WLAN routers before the modification, and a router – switch – router - chain after the modification. Chain topology was also used on other surveyed farms, including case farms 1 and 3, described in detail in Manninen (2018). Furthermore, many farms had the network connection run through the farmhouse, and the farmhouse devices were directly connected to the router that also acted as the internet gateway for the farm network. This can often lead to a network topology where the devices in the farmhouse are visible to everything on the farm. In most cases this is not needed for the farm office computer or other such devices. Additionally, unless the farmer has explicitly modified the settings of the gateway device, all of the devices in the farmhouse will be sharing the same local network. Thus visitors, workers, and consultants will have access to the network that houses all the farm's business data. In this survey, case farm 4 was the only that had separate subnetworks for work devices and other devices at the farmhouse.

For the most part, the farm networks surveyed in this work were not very complicated. Thus, even when there were problems in the network topology, such as on case farms 5 or 6, the modifications required to rationalize the topology were not time-consuming or expensive.

The surveyed farms typically lacked backup internet access, systematic and regular data backups, and many farmers were unaware of the status or structure of the network on the farm. The equipment used was often consumer-grade and therefore unsuited for many of the rigors of physical environment at the farm, which includes dust, humidity, extreme temperature, and animal contacts. Furthermore, many devices had only limited setting options which is not ideal for professional work. Clearly, the farm networks reviewed in this work had room for improvement in the design, implementation and maintenance of the farm local network and the wider cyber-physical environment.

5.2. Low-hanging fruits for improving farm cybersecurity

Based on the reviewed farms, there are several relatively simple ways to improve farm cybersecurity. All of these require at least some sort of investment from the farmer: time, training, money, or a combination of those. Due to their simplicity, these low-hanging fruits, shown in Fig. 8, can be used a starting point for improving farm cybersecurity.

The most important step for a farmer wanting to improve the cybersecurity of their farm is to *understand the importance of cybersecurity*. Based on the farmer interviews, farmers know on a conceptual level that farm cybersecurity is an important issue and that problems in the farm network may hinder farm operations significantly. Despite this, in practice, cybersecurity matters often have a very low priority and even simple improvements can be left undone. Should farmers understand the gravity of the issue, they might be more willing to invest time and money.

Many of the problems encountered in the survey were caused by farmers not knowing their network well enough. Therefore, an easy means of improving farm cybersecurity is for the farmer to *map the current topology* of their network, as well as list the devices are permanently or semi-permanently connected to it. A simple way to

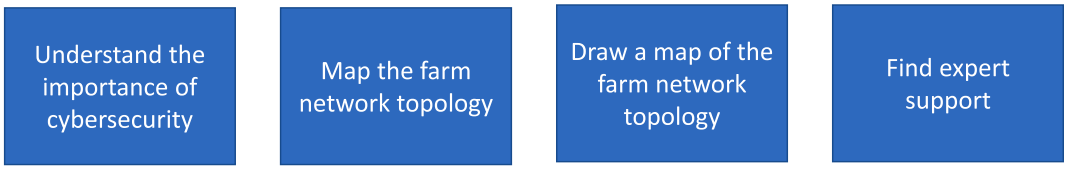

Fig. 8. The low-hanging fruit of farm cybersecurity.

maintain this knowledge on a network the size of a typical farm is to *draw a network diagram* on paper. This way the diagram is easily available and can, for example, be given to service personnel who come to the farm. It is also easy to modify, and accessible also in the case of network or electrical failures.

A proper understanding of the network topology will also allow the farmer to: better plan future additions to the farm network, understand what all the devices connected to the network are, and, for example, clean up the farm network cabinets should they be difficult to comprehend. When the farmer knows what is in the local network, they also have an easier time planning what other security measures, such as malware protection software, device backups, or similar, they need for their farm.

However, managing all this can be a daunting task for many farmers, and therefore it is important to for a farmer to *find expert support* for maintaining and developing the cybersecurity at their farm. The best providers for this support depend on the local farm business ecosystem but in the Nordic countries, farm advisory services are a possibility. Nordic farmers tend to use advisory services quite a lot and therefore adding support and advice on cybersecurity would be a natural expansion of the services provided. Of course, farm advisory services might not have enough cybersecurity experience to provide such services so it is also possible for other actors to provide this service for farmers.

6. Conclusions

This work describes the findings from research on the cybersecurity in Finnish dairy farms. The number of farms included in this study was only six, and therefore the results here cannot be directly generalized to cover all farms in Finland. Furthermore, since the farming ecosystems in various countries have many crucial differences, even more care should be given when applying these results to other countries. Nevertheless, the results of the review indicate that general level of cybersecurity readiness in agricultural primary production is likely to be relatively low. A farmer's understanding of the own local network at their farm is lacking. They may know what agricultural automation systems are included in their network but are unaware of how they are connected to each other or to the Internet.

The farm network is likely to be implemented without systematic design, and therefore can contain features that hinder or prevent some on-farm services from working. For the farms included in this study, a common consequence of this was problems with the visibility of surveillance camera video. Typically, the video was not available in all locations where the farmer wanted to view it. Often, the equipment connected to the farm network is consumer-grade, may not be properly configured, and is not properly protected from environmental threats (e.g. lightning, humidity, or temperature) or from malware.

However, most of these flaws, while dangerous for the cybersecurity of the farm, and therefore posing risks for farm operations, are not particularly complex to solve. The largest hurdles are likely to be a lack of farmer awareness of cybersecurity issues, lack of expertise in IT, and a lack of resources, including time, money, knowledge, and connections to outside experts who could help. None of these are insurmountable; there are some low-hanging fruits, collected in Fig. 8, which may be a good starting point when starting work on improving farming cybersecurity.

CRediT authorship contribution statement

Jussi Nikander: Conceptualization, Methodology, Validation, Writing - original draft, Supervision. **Onni Manninen:** Conceptualization, Methodology, Investigation, Writing - original draft, Visualization. **Mikko Laajalahti:** Conceptualization, Methodology, Investigation, Resources, Validation, Writing - original draft.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Barreto, L., Amaral, A., 2018, September. Smart farming: Cyber security challenges. In: 2018 International Conference on Intelligent Systems (IS). IEEE, pp. 870–876. (https://ieeexplore.ieee.org/abstract/document/8710531).

Bogaardt, M.J., Poppe, K.J., Viool, V., van Zuidam, E., 2016. Cybersecurity in the Agrifood sector. Capgemini Consulting.

Chi, H., Welch, S., Vasserman, E., Kalaimannan, E., 2017. A framework of cybersecurity approaches in precision agriculture. In: Proceedings of the ICMLG2017 5th International Conference on Management Leadership and Governance. Reading, UK: Acad. Conf. Publ. Int. (https://search.proquest.com/docview/1897672343?pq-origsite=gscholar), pp. 90–95.

Cooper, C., 2015. Cybersecurity in food and agriculture. Protecting Our Future 2.

DHS, 2018. US Department of homeland security: threats to precision agriculture (https://www.dhs.gov/sites/default/files/publications/2018%20AEP_Threats_to_Precision_Agriculture.pdf).

Duncan, S.E., Reinhard, R., Williams, R.C., Ramsey, A.F., Thomason, W., Lee, K., Dudek, N., Mostaghimi, S., Colbert, E., Murch, R.S., 2019. Cyberbiosecurity: A new perspective on protecting US food and agricultural system. Frontiers Bioeng. Biotechnol. 7, 63 (https://www.frontiersin.org/articles/10.3389/fbioe.2019.00063/full).

Eurostat, 2016. Farms and Farmland in the European Union – statistics. Available at https://ec.europa.eu/eurostat/statistics-explained/index.php/Farms_and_farmland_in_the_European_Union_-_statistics#Farms_in_2016 accessed at May 15th 2020.

FBI, 2016. Smart Farming May Increase Cyber Targeting Against US Food and Agriculture Sector. Private Industry Notification, PIN 160331-001. (https://publicintelligence.net/fbi-smart-farm-hacking/).

Fountas, S., Sorensen, C.G., Tsiropoulos, Z., Cavalaris, C., Liakos, V., Gemtos, T., 2015. Farm machinery management information system. Comput. Electron. Agric. 110, 131–138.

Gupta, M., Abdelsalam, M., Khorsandroo, S., Mittal, S., 2020. Security and privacy in smart farming: Challenges and opportunities. IEEE Access 8, 34564–34584.

ISO, 2015. Tractors and machinery for agriculture and forestry — Serial control and communications data network — Part 10: Task controller and management information system data interchange. International standard, International Organization for Standardization.

Jahn, M.M., Oemichen, W.L., Treverton, G.F., 2019. Cyber Risk and Security Implications in Smart Agriculture and Food Systems. Accessed: Nov, 14, 2019.

Javaid, A.Y., 2015. Cyber security threat analysis and attack simulation for unmanned aerial vehicle network. Doctoral dissertation. University of Toledo.

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

Klerkx, L., Jakku, E., Labarthe, P., 2019. A review of social science on digital agriculture, smart farming and agriculture 4.0: New contributions and a future research agenda. NJAS-Wageningen J. Life Sci. 90 100315.

Laajalahti, M., Nikander, J., 2017. Alkutuotannon kyberuhat [Cybersecurity threats in agricultural primary production). Research report 30/2017, Natural Resources Institute Finland.

Manninen, O., 2018. Cybersecurity in Agricultural Communication Networks: Case Diary Farms. *Master's Thesis*, School of Technology, Communication and Transport. JAMK University of Applied Sciences.

Nakhodchi, S., Dehghantanha, A., Karimipour, H., 2020. Privacy and Security in Smart and Precision Farming: A Bibliometric Analysis. In: Handbook of Big Data Privacy. Springer, Cham, pp. 305–318.

Rotz, S., Duncan, E., Small, M., Botschner, J., Dara, R., Mosby, I., Reed, M. and Fraser, E. D., The politics of digital agricultural technologies: a preliminary review. Sociologia Ruralis.

Sontowski, S., Gupta, M., Chukkapalli, S.S.L., Abdelsalam, M., Mittal, S., Joshi, A., Sandhu, R., 2020. Cyber Attacks on Smart Farming Infrastructure.

Spaulding, A.D., Wolf, J.R., 2018. Cyber-security knowledge and training needs of beginning farmers in Illinois. 2018 Agricultural & Applied Economics Association Annual Meeting, Washington, D.C., August 5-August 7.

Sundmaeker, H., Verdouw, C., Wolfert, S., Pérez Freire, L., 2016. Internet of food and farm 2020. Digitising the Industry-Internet of Things connecting physical, digital and virtual worlds, 2.

The Security Committee, 2018. Vocabulary of Cyber Security. Traficom, Sanastokeskus STK, and National Emergency Supply Agency. Available at https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/ Accessed at May 15th 2020.

Trendov, N.M., Varas, S., Zeng, M., 2019. Digital technologies in agriculture and rural areas. Briefing paper. Food and Agriculture Organization of the United Nations, Rome.

West, J., 2018. A prediction model framework for cyber-attacks to precision agriculture technologies. J. Agric. Food Inf., 19(4), pp. 307–330. (https://www.tandfonline.com/doi/abs/10.1080/10496505.2017.1417859).

Wolfert, S., Ge, L., Verdouw, C., Bogaardt, M.J., 2017. Big data in smart farming–a review. Agric. Syst. 153, 69–80.