Creating a Farm Network Typology Map[1]

Why having a diagram of your farm network makes good farm business sense

To operate a profitable and sustainable business, farmers have to know how to manage risk. Many farm business owners have plans for managing pests, biosecurity, fire protection, irrigation needs, and threats having to do with extreme weather and animal welfare.

1 J. Botschner with R. Kotak (2023)

Producers know that good risk management equals good farm business management

Today, new farm business opportunities are coming around the corner: these involve digital agricultural technologies – things like control systems, computer networks and data for decision support. AgTech promises to help Canadian producers feed the world in sustainable ways, adapt to climate change and increase profitability through 'precision farming'. But, like any new technology, AgTech has risks to understand and manage. Even though most farms are located in rural areas, a farm business can be just as vulnerable to cybersecurity incidents as any other business. In today's connected world, "security through obscurity" isn't enough anymore to protect a farm business from criminals or others who may want to cause harm.

Farm businesses use and produce all kinds of data that could be attractive targets for theft or ransom by criminals. Farms are also connected to critical infrastructures (like energy, finance, and water) that create value and contribute to food security and economic prosperity. If foreign powers or ideologically motivated extremists want to cause disruptions, critical infrastructures and supply chains (that bring in your inputs and take away your outputs) are some of the first things they look at for potential targets. Because most Canadian families have less than than three days' supply of food on-hand, interfering with our food system can create big problems and lots of attention. At the farm level, disruptions to critical conditions or timeframes for growing and gathering crops and animals can create big pressures for producers and their families.

In livestock operations, industrial control systems handle everything from environmental conditions to feeding and milking. They need to be secure and reliable so that animals can be safe, healthy and productive. The same goes for greenhouse operations. If any of these systems are disrupted, a producer could lose an entire quota or crop within a matter of hours or days. Field crop producers have more time to fix a problem, but there are still critical periods for planting and harvesting that have to be met. If fertilizer, pest control or irrigation systems are affected, an entire growing season could be at risk. If a disruption targets buyers of farm products, both producers and the public can be hurt through price changes, interrupted food supplies and sometimes livestock losses and crop spoilage. In all cases, the human costs of dealing with a cyber attack or a system failure can be hard on a farm business and a farm family.

But, there's good news. There are things that can be done to strengthen farm business risk management, and these can also make it easier to manage the bottom-line. One of these is to have a map of your farm network — also known as a network typology diagram. Understanding your farm network typology can help you understand your farm operations at a deeper level, so you can better manage the bottom line and manage farm business risk. The way your farm network is set up can make the difference between being 'open for business' for bad guys or being able to conduct your business with a lower risk of a cyber security incident. Being able to create a very simple farm network typology can help you when you're talking to IT or cyber security service providers. They can use the map you make to communicate more clearly with you and to plan the most cost-effective approach that makes sense for your business.

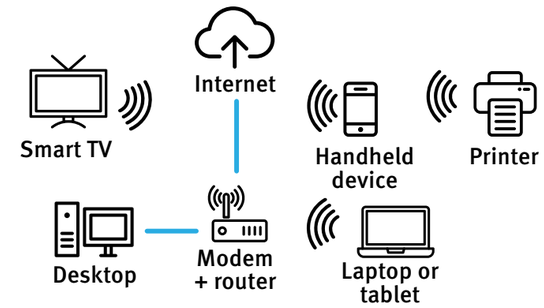
A network map can be used together with a cyber security policy , a business continuity plan, good on-farm cyber-hygiene practices (including questions for vendors) and regular cyber fire drills to help build farm business resilience. More confidence around risk management, and more insights into farm operations, can set the stage for better decisions benefitting the business in the long-run.

Additional CyberAg Infosheets that are available to help producers strengthen the cyber security capacity of their farm businesses

What is a network and a network typology?

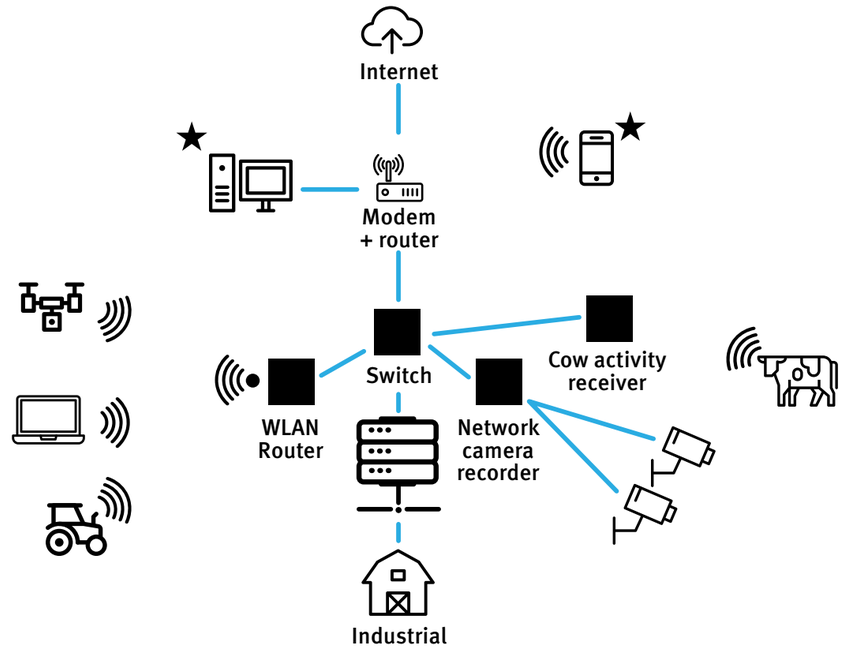
If you connect more than two digital devices together, you've created a network. Most home networks easily have more than three connected devices, like a desktop computer, a laptop or tablet, a handheld device, a printer and maybe a TV.

A **network typology** is a **type of map or schematic diagram** that shows what digital devices are connected to make up a network, and how they are connected. A basic network typology for a simple home network might look something like this:



More and more, we're also seeing WiFi-enabled refrigerators, washers and dryers, thermostats and security systems connected to a home network. The physical devices that are connected together and share information in a computer network are called 'endpoints' or 'nodes'. Many telecommunications companies offer apps that allow you to see all of the nodes connected inside your home network. If you have one of these, open it up and have a look — you might be surprised by just how many things are connected!

Any farm that uses connected digital agricultural technologies (sensors, control systems, autonomous vehicles, cameras, business data systems) also has a network. A farm network might look something like this:



These networks can differ in size and complexity. Adding more nodes and connections in a network can allow you to bring together information from a variety of sources into a single system that helps you monitor and control the different parts of your operations.

Another tool for breaking all of this complexity into understandable pieces is the Open Systems Interconnection (OSI) model created by the International Standards Organization[2]. The OSI model is a way of thinking about the different ways that information moves inside a network, and the different functions that are created. The model, which is in its fourth decade of use, is a standard model of computer system communications across a network. It usually describes seven layers that can be used to visualize how networks operate and to identify networking issues. Picturing the different communication functions inside a network can make it easier to see how it is organized and how to troubleshoot problems when they happen.

Layer		Functions
7	**Application**	Human-computer interface for accessing network services
6	**Presentation**	Provides data in usable format, and may include encryption
5	**Session**	Maintain connections for communications among processes
4	**Transport**	Data transmission protocols for end-to-end communications
3	**Network**	Provides routing by deciding which physical path data will take using various switches and routers
2	**Data Link**	Defines where data will be stored in memory on the network (in newer models, such as TCP, this and the physical layer are known together as the data access layer
1	**Physical**	Transmission of raw data bits

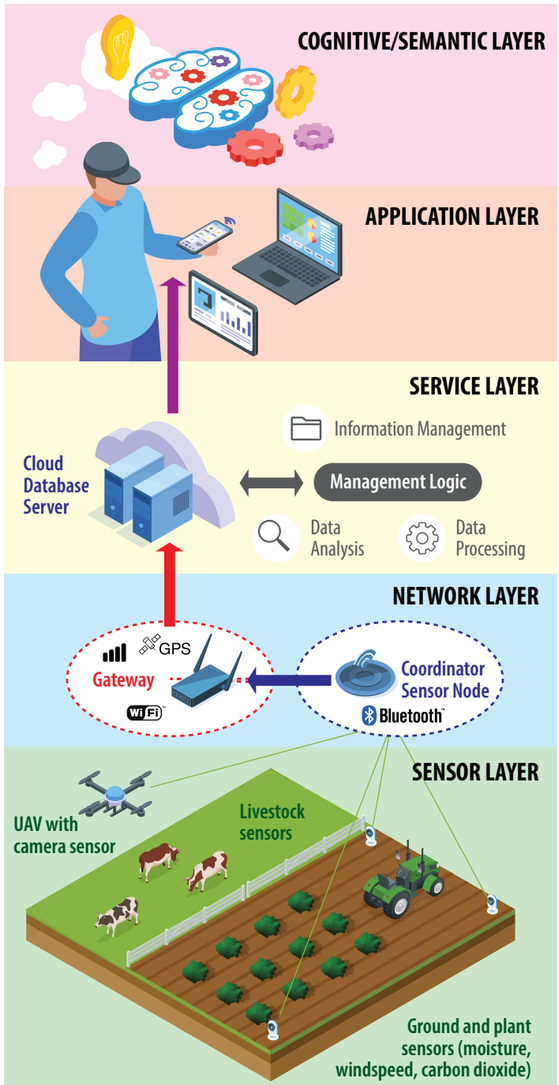
Other groups have proposed different versions of this similar architecture for precision farming, emphasizing parts that are relevant to the kinds of technologies used in agriculture. These include things like networks of different kinds of sensors (like ones that are ground-based, aerial, or wearable)[3].

The Sensor Layer includes all of the sensors and devices deployed to monitor crops, livestock and the environment, along with the data they collect. The Network Layer includes the communications technologies that link sensors and the internet within wireless sensor networks. The Service Layer involves the handling of data through processes and analytic activities. Finally, the Application Layer involves data visualization for human monitoring and decision support.

2 https://www.iso.org/standard/20269.html

3 Triantafyllou, A., Tsouros, D., Sarigiannidis, P. & Bibi, S. (2019). An architecture model for smart farming. 2019 15th International conference on distributed computing in sensor systems (DCOSS). DOI 10.1109/DCOSS.2019.00081.; Imperva (2021). OSI model. https://www.imperva.com/learn/application-security/osi-model/ International Organization for Standardization and International Electrotechnical Commission

We have updated the OSI model for agriculture to include another layer that is getting attention and concern. This is the layer that has to do with the ways that people see, understand and act on the different kinds of electronic information they come into contact with. Cyber security/intelligence professionals usually call this the 'cognitive/semantic' layer, but we prefer to use the everyday words, 'thinking/meaning', to discuss what is happening here. We have simplified the other naming as well – here is our updated OSI model:



Human Thinking/Meaning Layer
(also known as Cognitive/Semantic Layer)

- The minds (perceptions, beliefs, behaviours) of people accessing, transmitting and responding to information

Human-Computer Application Layer
(also known as Application Layer)

- Human-computer interface for accessing network services

Processing & Analytic Layer
(also known as Service Layer)

- Provides data in usable format, and may include encryption; includes processing and analyses of data

Connection, Transmission and Storage Layer
(also known as Network Layer)

- Maintains connections for communications among processes of IoT platform, including communications between sensors and the internet
- Data transmission protocols for end-to-end communications
- Provides routing by deciding which physical path data will take using various switches and routers
- Defines where data will be stored in memory on the network (combined with physical layer in newer TCP model as the data access layer)

Physical Sensor/Control Layer
(also known as Physical Layer)

- Transmission of raw data bits among sensors and smart devices (inclusing machinery)

An overview of different ways of organizing the OSI model for digital agriculture is located in the Appendix at the end of this document, along with examples of different kinds of cybersecurity threats that could affect each layer. The chat also shows how these different versions of the OSI model compare to the TCP/IP (Transcription Control Protocol/Internet Protocol) model, which is often used by network administrators to show how devices are connected over the Internet.

How can a farm network typology help manage cyber security risks?

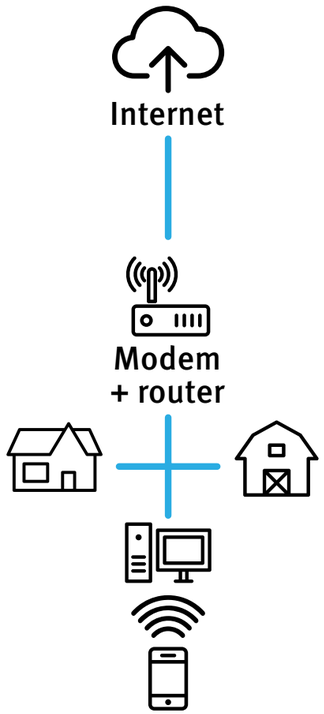
With more endpoints and connections, there are also more vulnerabilities that can be attacked to get into a farm network.

The bigger and more complex a farm network, the more vulnerabilities there are that could be exploited to gain unauthorized access

Common vulnerabilities of farm business networks are:

- Not re-setting passwords on modems and routers, or other out-of-the-box equipment, from the default manufacturers' passwords to new, unique, ones;
- Not using basic malicious software protections like firewalls, anti-malware and anti-ransomware solutions;
- No endpoint protections (such as encryption, network access controls to limit who can access different parts of a network, secure email gateways, or systems or services that monitor traffic and interrupt suspicious activity);
- Not having the right settings on connected devices (not 'configuring' them properly) or having the right software for your systems, to make sure everything works well together;
- Not having the right network equipment (such as having commercial instead of enterprise-grade equipment or using old equipment that is outdated and no longer supported by the manufacturer);
- Not allowing the system and devices to be updated, or 'patched' when these are pushed out by the vendor;
- Problems with the availability of video surveillance;
- Not having or understanding network typology; and
- Not separating ('segregating') critical networks to protect a cyber security issue in one area from spreading to all the others.

This last one can become a bigger vulnerability if a farm business network is run off the same network as the farm home:



Shared home-business networks can increase the number of opportunities 'the bad guys' have to gain access to your farm systems. The many personal uses of a home network (online gaming, social media, email, photo-sharing, working from home), and the challenge of holding family members (younger children, for example) to the same requirements as you might be able to do for yourself or your employees, can make your network more of a target. Remember, 'security through obscurity' no longer works in a connected world – households and businesses in rural areas can be just as vulnerable to cyber attacks as those in urban settings. Understanding how your particular business devices are connected will give you important insights into how to make farms less exposed to outside threats.

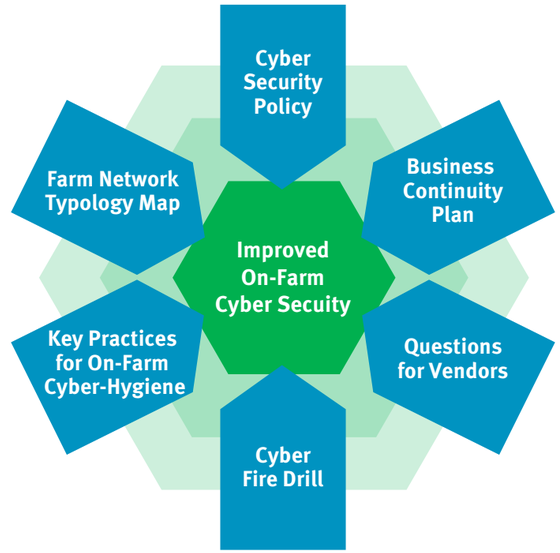
If you operate a farm gate retain store, you may also need to comply with Canadian payment card standards, known as Payment Card Industry Data Security Standards – sometimes called PCI DSS or PCI compliance. These are the standards that specify data security steps to prevent sensitive credit card information from being stolen or breached[4]. PCI compliance obligates all businesses that "accept, process, store or transmit credit card information" to maintain a secure environment[5].

A recent study of agricultural communications networks[6], identified a range of potential cyber security threats to the farm system, using the OSI model as a way of visualizing different categories and types of risks[7]. The following chart compares different versions of the OSI model in precision agriculture, to show the ways that people have 'sliced up' farm operations. Sample cybersecurity threats are shown alongside. Not all threats are going to be captured by the OSI model. But, this offers a wider view of farm-based cyber security that includes common human errors, equipment failures, environmental events and the legal-regulatory dimension of smart farming.

A farm network typology diagram can help you understand how your systems are laid out and connected to each other, where threats may be coming from and suggest areas to address to make things safer. It is of several important pieces in a set of safeguards that will help your farm be better protected and more resilient.

There is a Work Sheet for each of these. They also overlap in some areas. You can start with any one. The understanding you develop in one will help you with the others. Three additional Work Sheets will help you round out your knowledge and practices:

- Questions for Vendors and Suppliers;
- Key Practices to Strengthen On-Farm Cyber-Hygiene; and
- Conducting a Cyber Fire Drill.

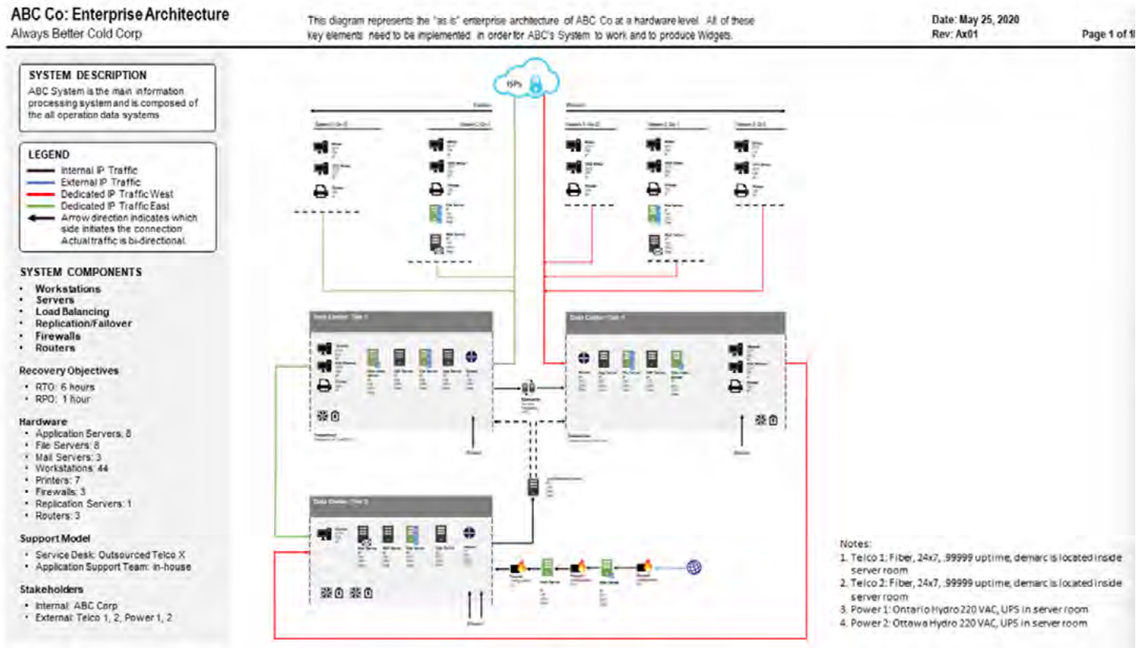


4 See, for example: https://www.ppscanada.ca/pci-compliance/
5 https://www.pcicomplianceguide.org/faq/#1
6 Nikander, J, Manninen, O & Laajalahti, M. (2020). Requirements for cybersecurity in agricultural communications networks. Computers and Electronics in Agriculture, 179. https://doi.org/10.1016/j.compag.2020.105776.
7 Overview of the OSI model, after Imperva (2021) and Nikander, et al (2020)

How to create a network typology for your farm

There are a number of software different tools that you can purchase or subscribe to that will automatically create a network typology of your systems. If you have a large enough operation (hundreds or thousands of nodes), with a dedicated IT staff person, this might make sense.

Here is an example of what an automatically generated business network typology can look like[8]:



A cyber security or IT service provider should also be able to use an automated network mapping tool to help you understand your system and make informed decisions about how to improve its security. As mentioned above, your telecommunications account may also have a feature that lets you see a list of devices that are connected. This can be a good starting point.

Sometimes the easiest way to learn is to do things by hand. Taking time to make a basic drawing of your farm network on a piece of paper, or a whiteboard, will give you a feel for your system, and a set of questions that can help you be a more informed consumer of cyber security services and products.

Work through the following activities. You will likely leave out a number of nodes and connections — most businesses have a lot more than they think. You may not be able to collect all the information you need right away, but you can add to your diagram as things become clearer. As you learn more, or talk to more people, you may want to revisit your network typology and make whatever updates are necessary.

8 Courtesy of Alan MacCafferty, University of Ottawa

Sketching Your Network Typology Map[9]

STEP 1:

Decide on the shapes and names you will use for different devices of your network.
These are things like: soil sensors; autonomous equipment; milking apparatus; environmental controllers; personal computers and the roles they play (control, storage, surveillance, etc.); handheld devices; cameras; camera recorders; manure cleaners; switches (a 'hub' with physical plug-ins to connect devices within a network – or to the internet – so they can communicate with each other by transferring data through the switch; switches are in Layer 2 of the OSI model); gateways (connecting networks to one another); routers; etc. **Make a rough list of everything you know that is connected on your farm. Now check it – is there anything you might have left out?** Think about how all of these are arranged. You might consider using a number to show where several of these are connected to another node.

For example, you might use the following to show that five cameras are connected: 5 x

STEP 2:

Make a map. Name and sketch out all of the different nodes in your network. Either on the diagram, or in a separate chart, make note of the manufacturer' and the model number.
Each node will have an IP address (a multi-digit number, separated by periods, that identifies a device on the internet) or a MAC address (a multi-digit manufacturer's number for the adapter that helps connect a device to the internet). Record these addresses either on your diagram or in your chart.

STEP 3:

Draw lines to show which nodes are connected to one another.
You might use a solid line for wired devices and a dotted line to show wireless connections. If you are able to include more information about the connections – for example the 'ports' on a switch that a device is connected to, then add that as well.

Looking at your network typology diagram:

- **Does anything come to mind as a vulnerability you need to fix?**
- **What are you best opportunities to improve your cyber security position?**
- **What would you need to do to make this happen?**
- **Where do you need more information — where would input from a professional be most helpful?**

STEP 4:

Make a copy of your network typology map and store it in a safe place.
If you complete the other Work Sheets in this series, and put them in a binder (with another binder as a backup), you'll have all of the main components for making serious progress in your farm's cyber security.

STEP 5:

Review your network typology map with your IT provider or cyber security provider, as a way to find opportunities to make your farm network more secure.
Remember, this is a starting point – you can update your network typology map as you learn more, or become more familiar with the technical workings of your farm network.

Closing thoughts

We suggest that you revisit these resources from time-to-time. I can also be helpful to hire a professional to review and refine these tools based on the unique strengths and opportunities of your business. Don't forget to keep up on new developments by reading and taking advantage of training opportunities. While there's a lot that individual farm business can do to make them more cyber secure, they can't – and shouldn't – go it alone. Tell your vendors, commodity associations, federations, advisors, and elected officials about the help you feel you need. They are all in a position to listen, engage and perhaps create new opportunities for support. The success and sustainability of your farm businesses contributes to the prosperity and well-being of the entire food system, and of all Canadians!

The suggestions offered in this document are intended as education about options for further exploration. They are not a substitute for professional technical advice tailored to an individual business.

9 Adapted from elements described in Nikander, et al. (2020) and Domotz (https://blog.domotz.com/know-your-networks/how-to-make-a-network-topology-diagram/)

Appendix A: Comparison of OSI Models for Digital Farm Networks

List of TCP/IP Layers (For comparison)		List of OSI Layers in Digital Agriculture						Examples of malicious threats impacting confidentiality, integrity availability
		Nikander, et al (2020)[2]	Triantafyllou, et al (2019)[3]	Gupta, et al (2020)[4]	Rouzbahani, et al (2022)[5]	Botschner, et al (2023)[6]	Functions	
	8					**Human Thinking/ Meaning Layer**	The minds and actions (perceptions, beliefs, behaviours) of people accessing, transmitting & responding to information	• Influence operations • Distinformation, misinformation, malfinformation • Phishing and ransonsomware
Application Layer	7	**Application Layer**	**Application Layer**	**Edge & Cloud Layers**	**Application Layer**	**Human-Computer Application Layer**	Human-computer user interface for accessing network services	• Phishing, spoofing and ransomware • Viruses, worms, botnets, keyloggers, spyware, SQL injection • Zero-day exploits/malware inserts into vendor software • Data thefts, leaks, falsifications (third party, insider) • DNS redirection/ hijacking • Exploitation of authentication gaps to enable access to network by unauthorized devices
	6	**Presentation Layer**	**Service Layer**		**Processing Layer**	**Processing & Analytic Layer**	Provides data in usable format, and may include encryption; includes processing and analyses of data	
	5	**Session Layer**	**Network Layer**	**Network Layer**	**Communication Layer**	**Connection, Transmission & Storage Layer**	Maintains connections for communications among processes of IoT platform, including communications between sensors and the internet	
Transport Layer	4	**Transport Layer**					Data transmission protocols for end-to-end communications	• Distributed denial of service (DDOS) attacks • DNS redirection/ hijacking re man-in-the-middle attacks
Internet Layer	3	**Network Layer**					Provides routing by deciding which physical path data will take using various switches and routers	• IP address spoofing (using one trusted machine within a network to gain access to areas of the network) • Insider data leakage • False data injection (data poisoning)
Data Link Layer	2	**Data Link Layer**					Defines where data will be stored in memory on the network (combined with physical layer in newer TCP model as the data access layer)	
Hardware Layer	1	**Physical Layer**	**Sensor Layer**	**Physical Layer**	**Perception Layer**	**Physical Sensor/ Control Layer**	Transmission of raw data bits among sensors and smart devices (including machinery)	• Data theft/ interference by hackers/ hacktivists/ violent extremists • Physical interference, such as vandalism or theft of hardware

2 Nikander, J, Manninen, O & Laajalahti, M. (2020). Requirements for cybersecurity in agricultural communications networks. Computers and Electronics in Agriculture, 179. https://doi.org/10.1016/j.compag.2020.105776.
3 Gupta, M., Abdelsalam, M., Khorsandroo, S. & Mittal, S. (2020). Security and privacy in smart farming: Challenges and opportunities. IEEE Access, 8(20), 34564-34584. DOI 10.1109/ACCESS.2020.2975142.
4 Triantafyllou, A., Tsouros, D., Sarigiannidis, P. & Bibi, S. (2019). An architecture model for smart farming. 2019 15th International conference on distributed computing in sensor systems (DCOSS). DOI 10.1109/DCOSS.2019.00081. Gupta (2020)
5 Rouzbahani, H.M., Karimipour, H., Fraser, E., Dehghantanha, A., Duncan, E., Green, A., Russell, C. (2022). Communication layer security in smart farming: A survey on wireless technologies. arXiv:2203.06013v1 [cs.CR] https://doi.org/10.48550/arXiv.2203.06013
6 Botschner, J., Corley, C., Fraser, E., Kotak, R. & McMahon, D. (2021) Cybersecurity in digital agriculture. Ottawa, ON: Community Safety Knowledge Alliance.

Appendix B: Glossary of Common Terms in Cybersecurity[2]

Botnet: A collection of devices which have been established by a threat actor or compromised in order to run a remote-control agent granting an attacker the ability to remotely take advantage of the system's resources in order to perform illicit or criminal actions. These actions include DoS flooding attacks, hosting false Web services, spoofing DNS, transmitting SPAM, eavesdropping on network communications, recording VOIP communications and attempting to crack encryption or password hashes. Botnets can be comprised of dozens to over a million individual computers. The term botnet is a shortened form of robotic network

Data thefts, leaks (third party, insider): The act of intentionally stealing data. Data theft can occur via data loss (physical theft) or data leakage (logical theft) event. Data loss occurs when a storage device is lost or stolen. Data leakage occurs when copies of data is possessed by unauthorized entities.

Disinformation, misinformation, malfinformation:[3] Disinformation involves false information that is spread in order to manipulate people, cause damage, or influence people, organizations, and countries. Misinformation involves spreading false information without intending to cause harm. Malinformation involves information that is based in the truth but that is exaggerated in order to mislead and create the potential for harm.

Distributed denial of service (DDOS) attacks: An attack that attempts to block access to and use of a resource. It is a violation of availability. DOS (or DoS) attacks include flooding attacks, connection exhaustion and resource demand. A flooding attack sends massive amounts of network traffic to the target overloading the ability of network devices and servers to handle the raw load. Connection exhaustion repeatedly makes connection requests to a target to consume all system resources related to connections, which prevents any other connections from being established or maintained. A resource demand DoS repeatedly requests a resource from a server in order to keep it too busy to respond to other requests. DDoS (Distributed Denial of Service) have the same aim but the attacks are often conducted using a network of internet-connected computers (Botnet) that overwhelms the target server with even more traffic than a DoS attack.

DNS redirection/ hijacking: These are techniques that manipulate the system that connects your computer to a website when you type in the site's web address. DNS (Domain Name System) is like the phone book of the internet. It translates domain names (like google.com) into IP addresses (like 172.217.7.206) that computers use to connect to websites. DNS hijacking, DNS poisoning, and DNS redirection are all ways that attackers can manipulate the DNS system to redirect users to malicious websites. DNS hijacking occurs when an attacker gains unauthorized access to a user's computer or router and changes its DNS settings. This can cause the user's internet traffic to be redirected to a fake website that looks like the real one, but is designed to steal their sensitive information.

False data injection (data poisoning): This involves an attacker deliberately planting false or misleading data into a computer system or database. This is done trick a system into producing wrong outputs (decisions or predictions). To protect against data poisoning attacks, it is important to use strong authentication and access controls to prevent unauthorized users from modifying data. It is also important to regularly monitor system logs and network traffic for any unusual activity.

Firewall: A security tool, which may be a hardware or software solution that is used to filter network traffic. A firewall is based on an implicit deny stance where all traffic is blocked by default. Rules, filters or ACLs can be defined to indicate which traffic is allowed to cross the firewall. Advanced firewalls can make allow/ deny decisions based on user authentication, protocol, header values and even payload contents.

Hacker: A hacker uses technical knowledge to solve a problem within an electronic system by non-standard means. A white-hat hacker is a security professional legitimately hired to find vulnerabilities in a system (by the owner). A black-hat hacker is illegally breaking into a computer system simply for the thrill. Note: gaining unauthorized assess to a computer is a crime, even if there is no other purpose. Criminals are motivated by profit and may exploit computer systems for reasons other than hacking and, therefore, should be investigated along those lines. There is a grey area with criminal hackers that use the spoils of the break-in to refinance their hacking hobby. Hacktivism — Similarly, hacktivists are often a mix of hackers looking for a cause to justify their hobby or activists using hacking as a means to an end.

2 Full referencing of sources is provided in Botschner, et al (2021). Cybersecurity in Digital Agriculture. Ottawa and Saskatoon: Community Safety Knowledge Alliance. Additional references are as noted
3 Source: https://www.cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300

Hacktivists: Someone who uses computer hacking skills to for activism, to promote a political or social cause. They may vandalize a website, leak sensitive data, or try to shut down a services. Hacktivists usually want to bring attention to their cause and maybe create change. They often target organizations or websites that they believe are acting against their values or beliefs.

Ideologically motivated violent extremist: IMVE, covers individuals who hold a variety of violent and extremist beliefs from many different belief systems. Ideologically motivated violent extremists have often try to use stories of division and distrust to try to gain followers and get people to carry out acts of vandalism, violence and/or to undermine our democratic institutions and system of governance.[4]

Influence operations: Also known as psychological operations, these activities can involve creating, spreading and making use of false information, to serve political objectives locally or internationally. These false stories are spread using different kinds of media to influence beliefs, feelings, decision-making and behaviour in line with the objectives.

Interference

Foreign: The Government of Canada defines[5] foreign interference as, "deliberate and covert activity undertaken by a foreign state to advance its interests, often to the detriment of Canada's." It is often deceptive and may involve "attempt[s] to threaten our citizens, residents and institutions, or to compromise our way of life, undermine our democratic processes, or damage our economic prosperity."

Physical (damage): This could include acts like vandalism or theft of hardware.

Insider threat: The likelihood or potential that an employee or another form of internal personnel may pose a risk to the stability or security of an organization. An insider has both physical access and logical access (through their network logon credentials). These are the two types of access that an outside attacker must first gain before launching malicious attacks, whereas an insider already has both of these forms of access. Thus, an insider is potentially a bigger risk than an outsider if that insider goes rogue or is tricked into causing harm.

Keyloggers: These are malicious software or hardware that can record every keystroke made on the keyboard of a computer or mobile device. They can capture passwords, credit card numbers, and data typed into the device. The information can then be transmitted or stored so that it can be picked up by the attacker. Keyloggers can be put in place using malware, phishing, or by gaining physical access to a device. Some protections include using strong passwords and not re-using passwords across devices. Avoid clicking on unknown links or attachments. Keep security software up-to-date. Keep access to devices limited to trusted people.

Man-in-the-middle attacks: This involves intercepting (often unencrypted) data as it moves between devices (data in transit). For example: data is intercepted by 'X' moving from 'A'-to-'B'. The intercepted data could be viewed, or altered in ways that make it hard for either A or B to know if something has happened.

Multi-factor authentication (MFA): Authentication using two or more different factors to provide increased security during log-ins. Factors may include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric)

Phishing: A social engineering attack that attempts to collect information from victims. Phishing attacks can take place over e-mail, text messages, through social networks or via smart phone apps. The goal of a phishing attack may be to learn login credentials, credit card information, system configuration details or other company, network, computer or personal identity information. Phishing attacks are often successful because they mimic legitimate communications from trusted entities or groups such as false emails from a bank or a retail website.

Ransomware: A form of malware that holds a victim's data hostage on their computer, typically through robust encryption. This is followed by a demand for payment in the form of Bitcoin (an untraceable digital currency) in order to release control of the captured data back to the user spoofing: The act of falsifying the identity of the source of a communication or interaction. It is possible to spoof IP address, MAC address and email address. IP address spoofing uses trusted equipment within a network to gain access to areas of the network.

Spyware: A form of malware that monitors user activities and reports them to an external party. Spyware can be legitimate in that it is operated by an advertising and marketing agency for the purpose of gathering customer demographics. However, spyware can also be operated by attackers using the data gathering tool to steal an identity or learn enough about a victim to harm them in other ways.

SQL injection: SQL injection is a type of cyber attack that targets websites and applications that use a database to store information. The attacker uses a technique to insert malicious code into a database inquiry, which allows them to access or modify sensitive information in the database. SQL injection attacks can be used to steal or modify information, and may sometimes take control of a website or application. Websites and applications can be protected from these attacks if they use secure coding practices and are regularly tested for vulnerabilities. Users should exercise caution when entering personal information on websites if they do not seem secure or trustworthy.

Virus: A form of malware that often attaches itself to a host file or the MBR (Master Boot Record) as a parasite. When the host file or MBR is accessed, it activates the virus enabling it to infect other objects. Most viruses spread through human activity within and between computers. A virus is typically designed to damage or destroy data, but different viruses implement their attack at different rates, speeds or targets. For example, some viruses attempt to destroy files on a computer as quickly as possible while others may do so slowly over hours or days. Others might only target images or Word documents (.doc/.docx).

Wi-Fi: A way to support network communication using radio waves rather than cables. The current Wi-Fi or wireless networking technologies are based on the IEE 802.11 standard and its numerous amendments, which address speed, frequency, authentication and encryption.

Worm: A form of malware that focuses on copying and spreading itself. A worm is a self-contained malicious program that attempts to duplicate itself and spread to other systems. Generally, the damage caused by a worm is indirect and due to the worm's replication and distribution activities consuming all system resources. A worm can be used to deposit other forms of malware on each system it encountersZero-day exploits/ malware inserts into vendor software

Zero-day: A zero-day vulnerability is a software vulnerability that is not yet known by the vendor, and therefore has not been mitigated. A zero-day exploit is an attack directed at a zero-day vulnerability.

4 Source: https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210722/013/index-en.aspx
5 https://www.canada.ca/en/security-intelligence-service/corporate/publications/foreign-interference-and-you/foreign-interference-and-you.html

About this project

The *Cyber Security Capacity in Canadian Agriculture* project is a national, multi-year, initiative funded by Public Safety Canada's Cyber Security Cooperation Program that aims to strengthen cybersecurity capacity within Canada's agricultural sector.

The agricultural sector has increasingly become a target of cyber attacks in ways that can cause serious disruption to the livelihoods of rural communities, and to critical infrastructures, including supply chains. This project is aligned to efforts to strengthen and support domestic food security and wellbeing, rural economic development and resilience, and national prosperity.

For further information

CSKA Community Safety Knowledge Alliance

www.cskacanada.ca

Partly funded by

Canada

Additional resources

The Canadian Centre for Cyber Security (Cyber Centre) is Canada's authority on cyber security. It works to protect and defend the country's valuable cyber assets.
https://www.cyber.gc.ca/en/guidance/cyber-security-small-business
https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations

Get Cyber Safe is a national public awareness campaign created to inform Canadians about cyber security and the simple steps they can take to protect themselves online.
https://www.getcybersafe.gc.ca/en

CyberSecure Canada is a voluntary federal certification program designed for small and medium-sized enterprises and other organizations in Canada to help improve cybersecurity practices.
https://www.ic.gc.ca/eic/site/137.nsf/eng/home

JusTech is a privacy breach tool. In the event of a data breach, by answering a series of questions, business owners will be provided with multiple auto-generated documents: a completed Personal Information Protection and Electronic Documents Act (PIPEDA) breach reporting form, client notification, internal communication letter, a how-to-guide for breach reporting, and sample cyber policies. The process is easy to use and completely free for small businesses.
https://www.justech.ca