Agriculture is key to Canadian prosperity and wellbeing, but it is under threat.

The agri-food system is a vital sector of the Canadian economy and our global position.

Farmers, as business people and entrepreneurs, are at the front lines of maintaining strong and resilient rural communities.

The food supply chain – from farm to fork – is essential to the health and wellbeing of every Canadian. Evolving food systems to be capable of supporting nine billion people in the face of climate change is one of the 21st century's big challenges. Digital technologies are helping agriculture to become more productive and efficient, and they can support sustainable food production practices.

Like other critical infrastructures, the agri-food sector is becoming a growing target for cyber attacks.

Digital technologies are changing how we produce food and how we distribute it

Next-generation equipment – along with agronomic and other data services – allows producers to manage each hectare of land and each individual animal in near real-time. These "precision agriculture" or "smart farming" technologies provide opportunities to boost productivity and profitability, and to enhance traceability.

Digitalization also can help farmers use inputs such as antibiotics or fertilizers more precisely, and lessen harmful outputs (emissions, waste and land disturbance), reducing agriculture's environmental footprint.

New technologies to address the food system challenges of the 21st century[1]

Digital Building Blocks

- New computing technologies
- The Internet of Things (IoT)
- Blockchain
- Cloud computing
- Big data and advanced analytics
- Artificial intelligence and machine learning
- Virtual reality and augmented reality
- 5G mobility

Advances in Sciences

- Next generation biotechnologies and genomics
- Energy creation, capture, storage and transmission

Reforming the physical

- Autonomous and near autonomous vehicles
- Additive manufacturing and multidimensional printing
- Advanced, smart robotics
- Advanced materials and nano-technologies

1. Adapted from World Economic Forum (2018)

Digital on-farm technologies

Wireless sensor networks
e.g., soil moisture, animal movement and health

Industrial control systems, automated and robotic processes and autonomous and semi-autonomous vehicles and equipment
e.g., GPS controlled seeding and harvesting equipment, environmental control systems in livestock barns, robotic milking parlours, irrigation systems, spraying by UAVs (drones)

Big data-based decision support systems
e.g., collection and analysis of farm yield data to support decision about inputs and practices, feedback to directional control systems

Supply chains and farm services
e.g., supplier deliveries and transactions, food traceability, purchaser systems (finishers, processors)

Energy management systems
e.g., renewable energy generations supplying power to outdoor sensors and charging stations

"There are two types of precision agriculture systems – those that have been hacked, and those that will be." [2]

New and important threats are developing

A series of ransomware attacks in Canada, the US and Australia in 2021 showed just how vulnerable the agri-food infrastructure can be. The attack on the Australian wool exchange system in February stopped trading for several days, resulting in millions of dollars of lost value and impacts on commodity prices. The attack on the world's largest meat producer in the summer threatened to cause disruptions to consumers on a global scale. And disruptions of two grain buyers in the United States at harvest time sent shock-waves through that sector. The attacks were attributed to cyber crime gangs based in Russia. One of these warned the agricultural sector in the fall of 2020 that it would be targeting it in the coming year.

Cyber disruptions can impact seeding and harvesting, affecting food availability and commodity prices. They can also affect animal health by: disabling milking systems; disrupting environmental controls in livestock barns; or interfering with biosecurity systems. Supply chain attacks can cause massive knock-on impacts on regional and national economies, animal welfare and local producers.

Cyber threats[3]

CYBER THREAT ACTOR	MOTIVATION	ATTACK FOCUS
Nation States	Geopolitical, economic and technological power	Disinformation, supply chain control, influence or interference, trade secrets, theft of intellectual property
Cyber Criminals	Profit/privateering for nation state	Financial data, personally identifiable information or ransomware, extortion
Hacktivists	Ideological causes inspired hacking	Sensitive business data, client and supplier data
Extremist Groups	Ideological inspired violence	Disruption of critical systems or data for physical effect
Hackers	Thrill seeking	Penetration and control of systems and devices
Insider Threats	Discontent/ retribution	Destruction/damage of business systems or profiteering of intellectual property

2. West (2018)
3. Adapted from Canadian Centre for Cyber Security (https://www.cyber.gc.ca/sites/default/files/publications/Intro-ncta-2020_e.pdf)

On-farm networks can be susceptible to attack

Farm network vulnerabilities[4]

Open Front Door

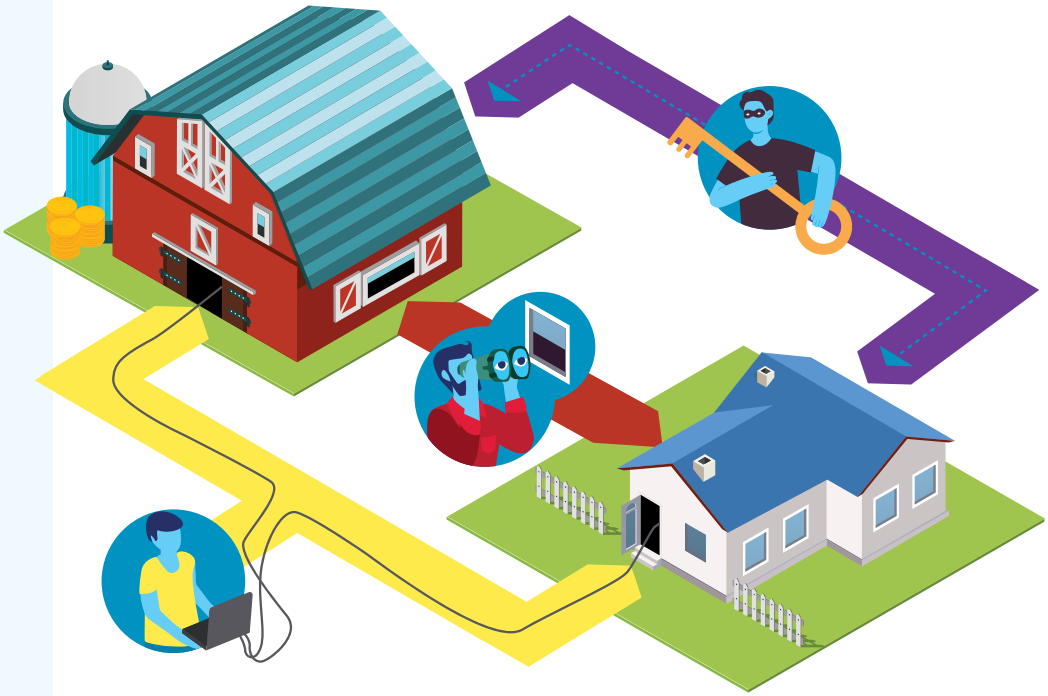
Common open ports - physical points of connection on computers that allow communication with external devices and to the Internet *(examples: for file transfer, for email retrieval and routing; for access to the World Wide Web; to allow connected applications to communicate with one another)*

Side Window

Using psychological techniques to get people to do things they shouldn't do *(examples: make a payment; click a link; or share confidential information)*

Locked Back Door

Sneaky methods for getting around normal physical and computer safeguards *(like user authentication or encryption in a computer or connected device)*



But Canadian producers are adaptable

Farmers are good risk managers. They:

- are good at noticing things that might involve risks and threats
- understand their operations and the ways the economic environment can impact their business (examples: commodity prices; the costs of inputs)
- can tolerate uncertainty and manage through disruptions
- are life-long learners
- make careful decisions to evolve their farming practices
- use information and experience to make practical decisions
- mentor and support family members and neighbours
- are self-reliant, and they also collaborate with one another ('barn-raising')
- are careful with their resources and stewards of their land and livestock
- plan for the future

4. After McCafferty (2020)

There are things farmers can do to minimize the risk of cyber disruptions, so they can continue to enjoy the business benefits of digital technologies

Take practical steps focusing on prevention, back-up and recovery:

- **Make sure hardware and software has been updated** by patches, and that they have basic physical and electronic safeguards in place (examples: locked server cabinets; strong passwords).
- **When on social media, consider** what kind, and how much, information about people and farming operations is shared.
- **Don't use public WiFi to check on farm systems when off the farm** – purchase and use a VPN (virtual private network) service for mobile devices if there's a need to monitor operations from public places OR connect monitoring apps to the cellular data service.
- **Make a sketch** of the devices, sensors, computers, servers, mobile devices, automated equipment, environmental control systems, financial systems, and other hardware that are connected within the on-farm networks – this helps to identify potential vulnerabilities.
- **List all the suppliers** whose services involve points of electronic contact with the on-farm systems.
- **Question suppliers about their information/cyber security safeguards** – for example, by using the tool, *Top Questions for AgTech Vendors*.
- **Conduct periodic cyber 'fire drills'** – to ensure you know what to do, in the event of a cyber incident.
- **Take time to understand what information is critical to the farm business**, where it sits and how it moves, and what would happen if it is corrupted or not available.
- **Consider how to get things up and running again following a disruption** – for example, pork and poultry operations have a very small timeframe to prevent big financial losses and animal welfare catastrophes if their environmental control systems go offline.
- **Back up your most important information regularly** and store it in a safe place.
- **Reach out to IT service providers and sector associations** to get technical help and to stay informed about new threats and how to manage them.
- **Most cyber attacks rely on human error or manipulation** – stay alert to the ways this can occur: don't click on un-verified links in emails or text messages; don't over-share information about operations and vacation plans; never reveal sensitive business or personal information to unsolicited callers – always check back with financial services or suppliers first – including IT service providers.

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.

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