Basic Steps to Make Your Farm More Cyber Safe

Key Practices for On-Farm Cyber-Hygiene

Canada's food system, from farm to fork, is facing a growing risk from cybersecurity threats.

Most of these threats come from criminals wanting to profit from the growing use of digital technologies. Others may come from groups that want to disrupt the agri-food sector, make an ideological point, or harm Canada's prosperity and well-being.

These risks are real. But, just like taking care of pest management, biosecurity, or planning for extreme weather events, there are concrete steps that farm businesses can take to be better prepared and more resilient, in the event of a cybersecurity incident.

An important approach in cybersecurity is to create layers of protection that make it hard for attackers to penetrate an organization and cause harm. The more barriers, the more effort is required to get through. Even if one layer is compromised, the others may prevent an attack from reaching its intended target (like a control system or farm data).

Cybersecurity is a new best management practice in agriculture: it enables better farm risk management and supports new farm business opportunities involving digital technologies.

To download copies of this tool, go to:
https://cskacanada.ca/projects/strengthening-the-cyber-security-capacity-of-canadas-agricultural-sector/

CSKA Community Safety Knowledge Alliance
Research to Practice to Alignment

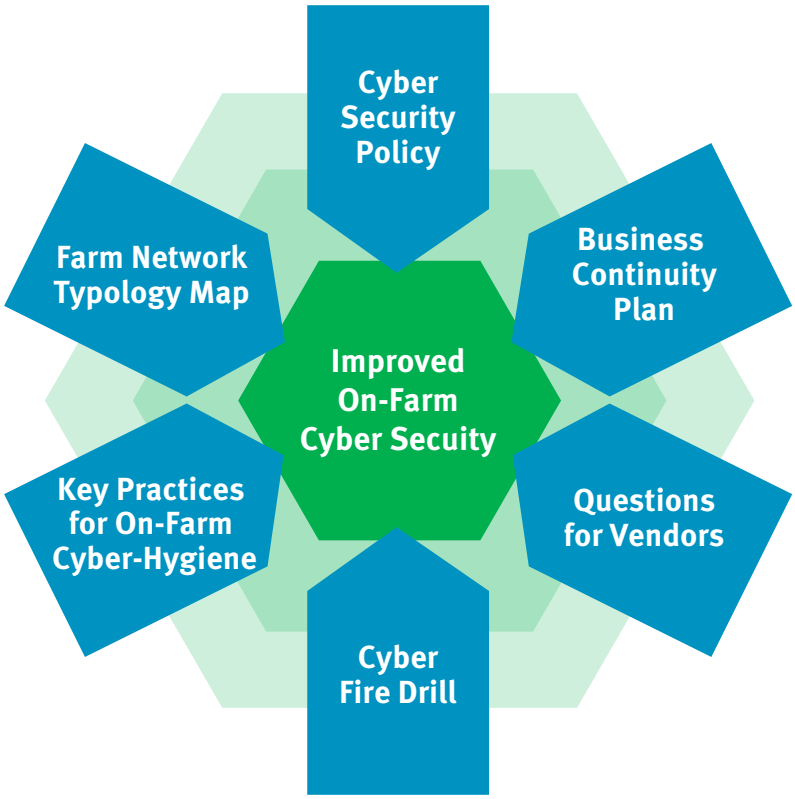
The Community Safety Knowledge Alliance (CSKA) is a non-profit corporation that supports governments, organizations, communities and others in developing, implementing and assessing new approaches to improving community safety and well-being outcomes.

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 Cyber Security in Canadian Agriculture project created a package of free tools for producers who want to take some of these important next steps.



These tools will walk you through things you can start doing today, and will help you be more informed when you're talking to vendors of equipment, supplies and services. Together, they can be thought of as an additional set of best management practices to improve farm business risk management and farm business development.

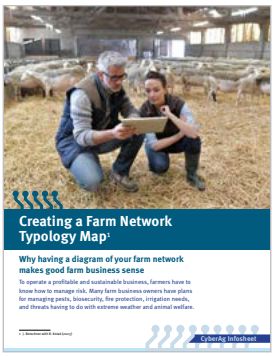
Tools for farm businesses

scan the QR codes below to view PDFs of these tools

Top Questions for Ag Tech Vendors

Farm Business Cyber Security Policy

Farm Cyber Business Continuity Plan



Farm Network Typology Map

Cyber Fire Drill

To access a free online introductory learning module* about on-farm cybersecurity that ties all of these tools together, scan the QR code and go to **Module 6 Cybersecurity**

*Developed by CSKA's Cyber Security in Canadian Agriculture initiative in collaboration with Enterprise Machine Intelligence Learning Initiative (EMILI).

Including basic cybersecurity as a best management practice in agriculture can make a big difference for the cyber preparedness of a farm business. But producers should never have to go it alone. There's a role for every player across the agri-food sector to contribute to the cybersecurity of our food system. This starts and ends with conversation and collaboration. We call this Cyber Barn Raising.

For more information, scan this QR code:

Additional resources

Agriculture and Agri-Food Canada's Cyber Security and Your Farming Business webpage: Which provides information about how to minimize the risk of cyber disruptions that can affect agricultural and agri-food businesses, along with links to additional resources. https://agriculture.canada.ca/en/programs/tools-manage-farm-risk-and-finance/cyber-security-and-your-farming-business

EMILI Data Initiative's Fundamentals of Farm Data Program: A data literacy training program designed to equip farmers with foundational knowledge and data governance skills related to agriculture data. Module 6, which was based on tools created by CSKA's Cyber Security in Canadian Agriculture initiative, focuses on cybersecurity. https://data.emilicanada.com/data-literacy

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

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

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.