CYBER SECURITY RISKS AND RESOURCES:

Safeguarding Canadian agriculture and agri-food

As agricultural and agri-food businesses become more digitized and connected online, the need to safeguard against cybercrime increases. Precision agriculture, automation and smart farming technologies contribute to efficiency and productivity, but without proper safeguards, the door opens to cyber vulnerabilities that can range from disruptive to devastating effects, including paralyzing business and impacting profitability and consumer trust.

In this digital landscape, it's critical to **understand and guard against cyber risks.**

What is cyber security?

Cyber security is the practice of safeguarding computer systems, networks and data from digital disruptions. Examples of cyber incidents affecting the agriculture and agri-food industry include **fraudulent texts, phishing emails that seek to gain private info and access to systems, and ransomware demands**, to name just a few.

What agricultural systems are at risk?

Targets can include production, financial, customer and other data, wireless sensors, automated and robotic machinery, autonomous and semi-autonomous vehicles and equipment, and heating, refrigeration, lighting and ventilation controls and systems.

Quick tips to minimize your risk

- **Have different passwords for each account**, preferably 12 characters-long, including 1 upper and 1 lower case letter, and 1 special character. **Change passwords frequently.**
- **Enable multi-factor authentication** on all your accounts, wherever possible.
- **Back up vital information regularly,** including vendor and client data and information. Store backup information offline or in an external drive.
- **Don't open unknown emails, and don't click on links or attachments** unless you're sure of their origin and legitimacy.
- **Don't save personal or financial data on browsers** if prompted and avoid auto-fill features.
- **Access more tips at agriculture.canada.ca/cyber-security-farming-business.**

Get started today with these tools and resources

Canadian Centre for Cyber Security

A go-to resource for expert advice, guidance, services and support, and to report cyber incidents

cyber.gc.ca

Public Safety Canada

Access the Canadian cyber security tool assessments. Select "National Security" then "Cyber Security".

publicsafety.gc.ca

Community Safety Knowledge Alliance

Access targeted resources to help protect your farming business.

cskacanada.ca/projects/strengthening-the-cyber-security-capacity-of-canadas-agricultural-sector

Agriculture and Agri-Food Canada
Agriculture et Agroalimentaire Canada

Canada

CHECKLIST FOR SMALL AND MEDIUM-SIZED ENTERPRISES

Cyber security and your farming business

You can take **simple** and **effective** steps to **increase your protection** from common cyber security incidents.

Secure your devices and data

□ I have **changed the default passwords of all my devices** that connect to the internet or are GPS-enabled, both on my farm and in my home.

- This includes the passwords of the **routers for Wi-Fi network(s), tractors and other machinery in the field**.

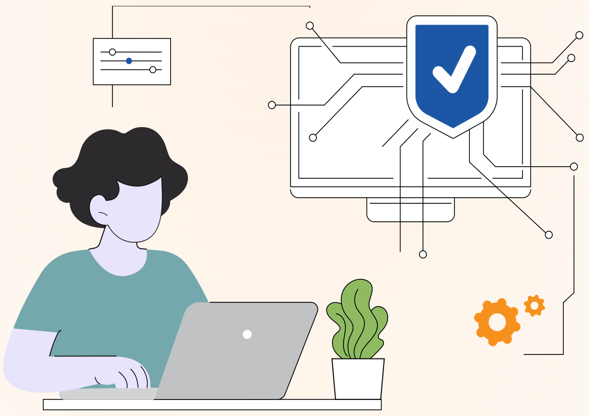
□ I have a **unique and strong password** for each of my accounts.

□ I have a **password policy** for my employees.

- Employees are **reminded to change their passwords every quarter** and they cannot reuse a password.

□ I have **multi-factor authentication (MFA)** enabled on all my accounts.

- MFA adds an **extra layer of security** to accounts and makes it harder for threat actors to gain access.



Stay updated, stay safe

□ I have **downloaded and installed** an anti-virus software from a trusted source.

□ I have **updated the firmware of all systems used** in my business from reputable sources, to minimize the risk of a supply chain attack.

□ I have **enabled automatic software updates** so that I do not miss an important security update.

□ I review the **list of authorized employees that can access the network and our data** every 6 months, and remove permissions where needed.

□ I conduct a **review every 6 months of the applications (apps)** I have downloaded on my devices and uninstall the ones I no longer use.

- Periodically **checking app permissions** ensures they don't access data that is not relevant to their function.
- **Turn off the permission** that allows an app to know your location **when you are not using it**.

□ I back up **valuable data and information on a quarterly basis and store a copy offline** in a place that's separate from my network. If a **security breach** happens, I will be able to access the important files I need to resume operations.

- This includes **key contact information on clients, vendors, partners, and any proprietary agricultural data** collected from agriculture technology devices.

For more information on how to **minimize your cyber security risks**, visit
agriculture.canada.ca/cyber-security-farming-business

For additional resources on how to stay safe online, visit
getcybersafe.gc.ca

Agriculture and Agri-Food Canada
Agriculture et Agroalimentaire Canada
Canada

Cyber security preparedness

Plan to Detect, Respond, Recover

In today's digital age, it's essential to be able to quickly and effectively respond to cyber incidents. Use this guide to establish procedures and documentation that help detect, respond to and recover from cyber incidents, minimizing the impact on your farming business.

Detect

Monitor your systems and data and proactively plan for any cyber security incidents.

- ✓ Assign a **cyber security lead** to monitor your systems and data.
- ✓ Make sure your **employees know how to report** security issues or unusual activity.
- ✓ Make an asset inventory list, including those that are required to **maintain your operations**.
- ✓ Identify **key contacts, both internal and external**, to notify during an incident.
- ✓ Maintain a list of reputable **professional services** that you could contact in the event of a cyber incident.
- ✓ Develop a **communications plan** to inform customers and the public if operations are affected.
- ✓ Run **anti-virus and anti-malware** software on all devices

Cyber security lead

Monitors systems and data, and is the employee point of contact.
Use the space below to record names and contact info.

Cyber security lead: ____________________

____

____

Alternate contact: ____________________

____

____

Other key contacts and service providers

In an incident, the cyber security lead informs all key contacts and liaises with professional service providers. Use the space below to record names and contact info.

Communications lead: ____________________

____

Legal lead: ____________________

____

Key suppliers: ____________________

____

Key clients: ____________________

____

Investors: ____________________

____

Professional services providers: ____________________

____

Respond

Take immediate actions to contain and mitigate the impact of the attack.

- ✓ **Disconnect all devices** from the network immediately.
- ✓ **Suspend employee access** temporarily, to prevent further incidents.
- ✓ **Seek professional cyber security services** if needed.
- ✓ **Change affected passwords** and enable multi-factor authentication (MFA).
- ✓ **Notify your financial institution** if financial information was compromised.
- ✓ **Communicate the incident** to your key contacts and the public, as needed.
- ✓ **Report the incident** to local police, the Canadian Anti-Fraud Centre and Canadian Centre for Cyber Security.

Recover

Restore systems and data, update security measures, and learn from the incident.

- ✓ **Restore systems** and data from backups.
- ✓ **Update all software**, including your anti-virus software, firewalls and firmware.
- ✓ **Run anti-virus and anti-malware software** on all devices.
- ✓ **Identify and address** any security flaws.
- ✓ **Patch and update** any security vulnerabilities.
- ✓ **Analyze the incident** and your response, and conduct a lessons learned exercise with all key contacts.

Validate

Test and refine your cyber security preparedness.

- → Regularly review each step of your preparedness plan to ensure all systems and assets are included.
- → Conduct walk-throughs of your plan, using specific incidents, to identify any vulnerabilities.
- → Perform simulations with your team to practice responding to a cyber attack.
- → Test your backup systems to be sure of business continuity during an incident.

For more information on how to **minimize your cyber security risks**, visit **agriculture.canada.ca/cyber-security-farming-business**

For additional resources on how to stay safe online, visit **getcybersafe.gc.ca**

QUESTIONS TO ASK BEFORE MAKING YOUR NEXT AGTECH PURCHASE

Help protect your farming business from cyber security risks

As your **farming business** becomes more digitized and connected online, it's critical to **guard against cyber security risks**. These **questions** can help guide your conversation with agriculture technology vendors so you can make **informed decisions** about who you are trusting to **protect** your business from cyber security risks and **safeguard** your data and operations.

Does the vendor have a good reputation?

- How long has the vendor been in business?
- Is the vendor known to you?

Does the vendor work with other companies in your sector?

- Do they know your line of business or commodity?
- Are they expanding their reach in your sector, or are they a new entrant?
- Do they have a good reputation?
- Will the vendor provide contact information for customers you can speak to for feedback (known as reference customers)?

Can the vendor explain your contract in plain language?

- Can they explain the clauses in your contract in a way that's easy to understand?
- Can they tell you where your information is stored, who has access to it, and how it is protected?

What steps will the vendor take if there is a data breach that impacts data they have stored about you and your business?

- Have there been previous data breaches? If so, what happened?
- Can they explain simply how your data is stored and protected?
- Do they have an emergency response plan they can share with you?

This isn't a full list of questions, but it's a good starting point for talking with a new vendor.

For more information on how to **minimize your cyber security risks**, visit
agriculture.canada.ca/cyber-security-farming-business

For additional resources on how to stay safe online, visit
getcybersafe.gc.ca

Agriculture and Agri-Food Canada
Agriculture et Agroalimentaire Canada

Canada

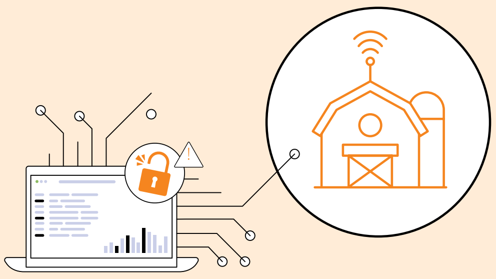
CYBER SECURITY: A CASE STUDY IN THE DAIRY SECTOR

Agri-businesses of all sizes are vulnerable to cyber incidents. Here's one example of how a phishing attack could impact your business and what you can do to protect it.

Alex, a **small dairy farmer**, receives an **email supposedly from the bank** while working on a business computer.

The email says that **Alex's bank account has been blocked**. Wanting to reactivate it, **Alex clicks on the link**.

Unfortunately, the **email and link are fraudulent**. Instead of leading to the bank's website, it **downloads ransomware onto Alex's computer**.



Alex's laptop is **connected to the farm's entire network**. The ransomware **quickly spreads**, encrypting all the farm's data.

This attack has severe consequences

Autonomous milking machines

The ransomware **stops** the autonomous milking machines, **disrupting** the milking schedule and **impacting** the cows' health and milk production.

Supply chain disruption

All supply-chain **contacts** and **communications** are encrypted, halting ordering and distribution.

- Alex can't place orders for feed, vet supplies, equipment, and can't receive updates on deliveries.
- The distribution process is crippled. Milk shipments are halted, inventory and order statuses are impacted.

Operational shutdown

Critical farm management software and records are **inaccessible**, impacting the farm's operations.

- The farm can't communicate with partners or manage logistics, leading to delays, missed deadlines, and potential reputational damage.
- Alex can't access email to reach customers.
- Many orders are delayed, shipments are missed, and trust with partners is eroded.

Alex's farm **does not have an IT team or cyber insurance**. Without incident restoration services, Alex **feels forced to pay the ransom to decrypt data and resume operations**. The financial loss and operational disruption are devastating.

Alex's situation could have been mitigated

- **Cyber security training** for Alex and employees could have helped them recognize phishing emails and avoid clicking suspicious links.
- **Antivirus and anti-malware software** could have detected and blocked the ransomware before it spread.
- **Network segmentation** can prevent malware from spreading.
- **Regular backups** to an isolated, off-network location would have made it easier for Alex to restore systems. Backing up data creates copies of important information, and storing back-ups separately from the main system, such as on an external hard drive or a secure cloud service, adds a layer of security.
- **Cyber insurance** can provide financial support and access to professional incident response services.
- **Incident response planning** ensures that all employees know how to respond to a cyber incident.

Stay vigilant to protect your business

Visit our **website** for more information

agriculture.canada.ca/cyber-security-farming-business

Agriculture and Agri-Food Canada   Agriculture et Agroalimentaire Canada

Canada

CYBER SECURITY GLOSSARY

Anti-virus/anti-malware software: a program used to prevent, identify, and remove viruses and other malicious software from your computer.

Business continuity: an organization's ability to continue with essential functions during a disruption, such as a cyber incident or natural disaster. A business continuity plan or BCP outlines the protocol and processes an organization follows to ensure that operations continue with as little disruption as possible.

Cyber incident: attempt by threat actors to cause harm, destroy, or gain unauthorized access to sensitive information in a networked computerized system.

Cyber safeguards: measures taken to protect data, networks and computer systems from unauthorized access, theft, or damage.

Downtime: not being able to access a system due to the failure of the system, application, or the entire network of a company. Downtime can occur due to maintenance activities, power cuts, or unexpected technical failures from cyber incidents. Consequences can include loss of revenue, decreased productivity, costs to recover systems and reputational damage.

External drive: a storage device that connects to your computer, often via USB (Universal Serial Bus), FireWire or Thunderbolt connection.

Incident response plan: a written document, formally approved by the senior leadership team, which helps your organization before, during and after a confirmed or suspected cyber security incident.

Internet of Things (IoT): a network of physical devices that transfer data to one another without human intervention. IoT are not limited to computers and can include anything with a sensor, software, and network connection.

Malware: abbreviation for 'malicious software'. Malware is designed to disrupt or harm computer systems.

Multi-factor authentication (MFA): the use of two or more authentication methods to log into a system. For example, you are required to enter a code from an authenticator app after entering your password to log in. MFA prevents threat actors from gaining access with just one exploited password.

Network breach: when a threat actor finds a way to bypass your security to get inside your network. Once they have access to the system, they can gain unauthorized access to data, applications, and devices.

Phishing: a form of fraud that involves contacting victims through email, telephone, or text to trick them into sharing personal information. Phishing scams often aim to persuade victims to transfer money, reveal financial information, or share system credentials such as passwords.

Ransomware: a type of malicious software designed to block access to a computer system until a sum of money is paid.

Security patch: a software update that helps address vulnerabilities, bugs and resolves inconsistencies in a software.

Spam: unsolicited communication sent in bulk. Spam can be sent via email, phone, text messages (SMS) and social media.

Threat actor(s): an individual or group who tries to access data they aren't authorized to access or cause harm to digital systems. Often referred to as a "hacker" or "cyber criminal".

Virtual Private Network (VPN): an encrypted internet connection that aims to provide a secure, private network connection for safe data transmission to and from networked devices.

For more information on how to **minimize your cyber security risks**, visit **agriculture.canada.ca/cyber-security-farming-business**

For additional resources on how to stay safe online, visit **getcybersafe.gc.ca**

Agriculture and Agri-Food Canada
Agriculture et Agroalimentaire Canada
Canada