Creating a Farm Business Continuity Plan for Cyber Incidents[1]

Why having a cyber business continuity plan 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 business continuity plan for cyber security incidents (Cyber BCP). This can help minimize risks and downtime in the event of an incident.

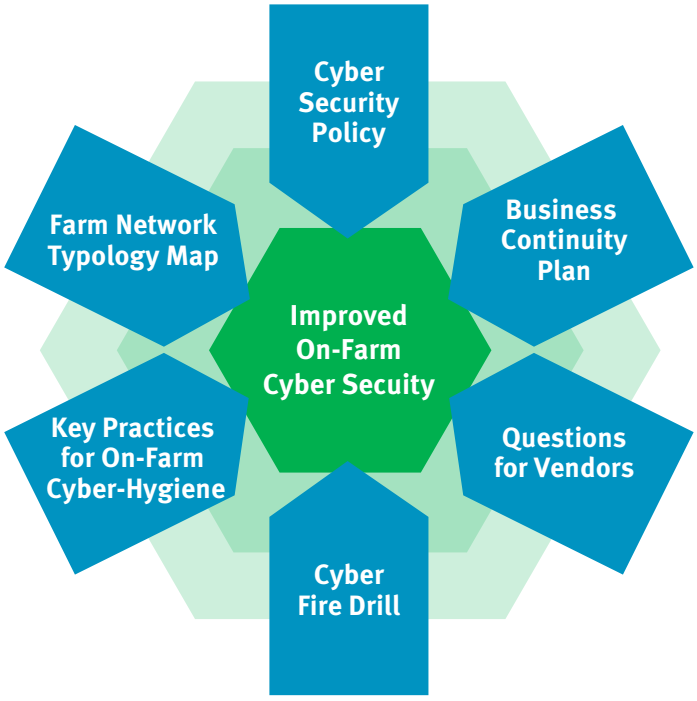
A Cyber BCP is an important part of a farm business's everyday risk management strategy. It can help minimize the impact of cyber attacks, protect important business assets, and ensure that the business can continue operating even during widespread disruptions. A Cyber BCP outlines how a farm business will protect itself from cyber attacks, and what steps it will take to be operational as quickly as possible if an attack or disruption does happen. It can give producers peace-of-mind knowing what they'll do if a disruption does happen.

The goal is that by strengthening your protections and building a resilient business, your farm operations will be able to continue in some fashion, *even if a cyber disruption happens*.

Here is a description of the main objectives of a Cyber BCP:

Prevention	**Protect critical data:** A cyber incident can result in the loss or theft of historical data about livestock or crops, financial information or customer data. A business continuity plan can include steps like creating an inventory of business critical data, making sure sensitive data is encrypted in storage and in transit, regularly backing up data, and keeping up-to-date through training and information sharing.
	Prevent losses: A cyber incident can cause significant financial losses to a farm business, including lost revenue, damage to equipment and infrastructure, livestock losses and service or legal fees. A business continuity plan can help to prevent these losses by identifying potential threats and taking steps to reduce risk, detect an incident that might be happening, and minimize its impacts on your business.
Response	**Comply with regulations or policies:** Businesses that collect or store sensitive data about customers, or to comply with different kinds of reporting requirements, may be required to have certain data security measures in place. The same may go for an insurance policy. A business continuity plan can help to ensure compliance with legal, contractual and regulatory requirements. Best practices can help minimize immediate operational impacts while an incident is underway. They also help avoid potential fines, financial losses or legal action.
Continuity (Recovery)	**Maintain operations:** A cyber incident can disrupt operations, leading to downtime, lost productivity, and unhappy buyers. A business continuity plan can include procedures to maintain operations during and after an attack. Examples are: backup systems, on-call help, and alternative ways of getting resources and managing other aspects of farm operations.

A Cyber BCP can be used together with a cyber security policy, a map of your farm network, 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

How to put together a business continuity plan for cyber security on your farm

Your plan should focus on your most important business assets and operations and the actions that are vital before, during, and after a major disruption.

The International Organization for Standardization (ISO) offers a widely-used standard for a business continuity management system (ISO 22301:2019 and 22313:2020). The following template is based on the ISO standard, and other best practices. It walks you through a set of practical, basic, steps you can take to improve your farm's cyber security and resilience. Once you've done this, you should be more prepared and better able to sustain – or more quickly recover – your operations, if a cyber disruption occurs. To keep up with new solutions and changing practices, we encourage you to use this as a starting point for conversations with technical service vendors, and your own peers to identify solutions that make sense for your business. This will help you maintain a reasonable and affordable level of preparedness.

A BCP lays out the steps to take during a disruption, and the roles and responsibilities of the individuals involved. By the time you've answered the following questions, you will have a basic Cyber BCP that can help you better manage on-farm cyber security risks, as well as strengthening the sustainability of your farm business.

Once you have a draft of the plan in place, you can use it to help keep all of the people who contribute to running your business on the same page about what to do in the event of a disruption. You may also want to share your plan with a cyber security or IT service provider, as the basis for building an even more secure plan to protect your investments and livelihood. Additional resources that you can add to your toolkit are listed at the end of this CyberAg Infosheet.

Putting together your cyber business continuity plan

Pull together the members of your farm business team (this might be just yourself, or yourself, your spouse and one or more children or employees). Go through and write down answers to each of the following questions. As you think about each question, give some thought to what your answer means, from the standpoints of: the ***people*** involved; the ***processes*** that run your operations; and the ***technologies*** that support the people and processes.

Note: Today's farms are usually a mix of everyday physical things (barns, fences, feed storage, equipment) and digital technologies (also called information communications technology – or ICT), which include things like: computer networks, automated equipment, data, and the command, control and analytic software that make things happen or support business decision-making. More and more, these are blended together into connected-up 'cyber-physical' systems that do things like: regulate the environmental conditions in livestock barns, deliver feed and carry out milking, monitor soil, plant growth or pest conditions, analyze input costs and productivity, handle inventory and billing, and many other functions.

Context

What are the business reasons for the digital agricultural technologies and equipment you use now in your farm's operations?

What were the benefits that made you adopt them (what problems did they help to solve/what opportunities did they help create for you – for example, more economical application of inputs, greater insights into managing production, or more time available to spend with family)? How are these working for you and your farm business?

Are there any big trends or changes in your sector that might make you want add new digital agricultural technologies and equipment to your operation? What opportunities might these provide for your business? Are you aware of any risks that using these technologies might involve for your business – what are these? What safeguards are you aware of? Who do you turn to when you have questions about new trends and new risks?

You may want to look at the CyberAg Infosheet, Top Questions for AgTech Vendors.

Business Impact

What are the parts of your business that will be *most important* to protect and recover?

Identify the digital assets of your farm business that are most critical to your ability to maintain your operations. This could include: databases containing historical production data or financial data; computers and mobile devices; your overall network, including control systems, sensors, and the software that makes everything work. List the assets that are most critical and most sensitive – what are they, where are they located, where data is kept and how it's they kept. Be specific – identify the parts of your business that are critical and describe why they critical – for example, how would a disruption affect different parts of your farm's operations.

You may want to look at the CyberAg Infosheet, Mapping Your Farm Network.

Who are the vendors (field or barn equipment), contractors (including IT, bookkeeping), suppliers and buyers, and other services (like insurance and farm advisors) that you rely on for your farm operations? List these, along with their contact information, the hours they are usually available, emergency contact information, and anything else that you need to remember in a pinch. Details about specific contracts (what, when, quantity), policies, protections and warranties can be included at the back of a tabbed binder, so you can easily get at this information when you need it.

What parts of your farm's operations are most vulnerable to disruptions?

Examples of physical disruptions are: a server cabinet damaged by animals, dust or moisture, a monitoring system damaged by extreme weather, or a livestock containment system vandalized by activists.

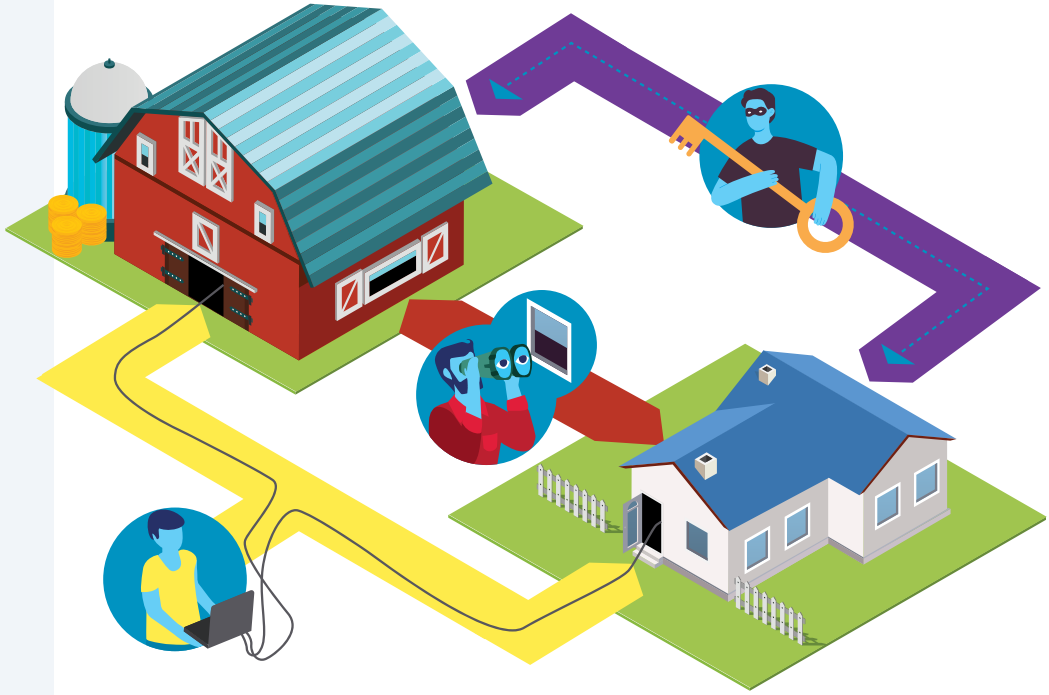
Examples of cyber disruptions are: credit card data stolen by a disgruntled former employee to commit fraud, a criminal ransomware historical data 'locked up' by a ransomware attack done through a fraudulent email.

Farm network vulnerabilities

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)*



What operational data, financial data or other information about your farm – like historical data on pesticide application, animal feeding, disease management, or productivity – do you hold that is vital to your ability to manage your business? What would happen if this was lost, stolen, disrupted or made public?

Threats and Risks

What are the potential threats to your farm's operations, assets, and information that you are aware of? How likely are these? How damaging they would be? You may want to look at trade magazines, sector-serving news sites you commonly visit, or other information you may have received from your associations and insureres to see where and how certain threats might show up in your farm business.

Here are some examples: an attack targeting field crops might focus on seeding or harvesting equipment and come from a hack into part of the manufacturer's technology; an attack affecting an animal producer/finishing/processing supply chain could focus on interrupting key pinch-points like food and watering systems at feedlots or technologies used in processing plants; an exploit targeting dairy might lock up and steal key proprietary data, hold it for ransom, then sell it to a third party; and an attack on a large greenhouse operation or a poultry or swine operation could involve the takeover of environmental controls regulating temperature, humidity and ventilation. The likelihood of each of these will depend on the context of the sector, the nature of cybercrime at that moment, and of Canada's relations to the wider world. In other words, the likelihood is going to change over time. But, the impact could vary from minor to catastrophic, depending on what safeguards you have in place to make it less likely that an attack will succeed, and more likely that you can recover your operations without significant losses if one does happen. Impact will also depend on how much time you have to get things back up and running, being able to get the help you may need, and what would happen to your business if you failed (for example, loss of part or all of a year's harvest or livestock).

Cyber threats[1]

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

Regulatory and Compliance

You may also have certain reporting or security requirements that you have to comply with, and which involves storing, sending or receiving sensitive data. For example, if you operate a farm gate store, you may have customer information (name, credit card numbers) on file that you are expected to safeguard. If you are a pig producer, there are regulations in place around identification and traceability (related to controlling disease outbreaks and identifying food safety issues) that depend on data outputs from your operation. **What data expectations and regulations are relevant to your farm business? What resposibilities to you have for safeguarding and reporting the data you create and hold? What about data that your vendors and service providers may hold about your operation? How is that safeguarded? What should you be able to expect from them if a data breach happens?**

Strategies

What are you already doing to address the highest priority vulnerabilities and risks you know about?

Take care of the basics, like managing who has access to your systems and critical information, using commercial-grade (not consumer-grade) equipment, ensuring essential software is up-to-date and any vulnerabilities have been 'patched', and having the right security certificates in place if you have a website. (see CyberAg Infosheet, On-farm Cyber-Hygiene Practices)

What more could you be doing to protect your operations? What would this involve? In the event of a disruption, what are the specific things you will do to keep critical farm operations going? Who has responsibility for these things?

A common mistake people make is to use easily guessed passwords or to share passwords across devices and applications, or with people who don't have a need to know them. Another is not taking advantage of multi-factor authentication (MFA) when it's available. It's also important to keep your software updated and patched (don't use really old outdated systems) and, whenever its affordable, use enterprise-grade instead of consumer-grade technology and software from reputable sources. Enterprise-grade technology generally (e.g., sensors, drones, cameras, alarms, control systems) has more safeguards built-in and is more likely to push out updates to devices connected to the internet. If technology isn't configured properly to ensure security, you could be more exposed than you think (it's a good idea to read the manuals and follow recommendations for changing default settings and for restricting access to only those who need it). If you (or a vendor or service provider) use a website or portal for communications, web communications should be encrypted (for example, does the website have a security certificate, such as SSL or TLS ? It's also a good practice to limit access to your systems and equipment to only those who absolutely need to use them. Other strategies include relocating parts of your operations to a different site, or bringing in additional people or other resources.

If an incident occurs, how will you know? Who needs to know? What will each person do (think about: actions that would be necessary, right away, to safeguard your livestock or crops; as well as steps to repair/restore the operation of your digital systems and data)? Who is available for back-up if certain people are not available right away? How, when and under what circumstances will you communicate to one another, to suppliers, buyers and customers and others about what has happened? Who would you contact for different kinds of assistance (equipment, data, financial, insurance, legal, other)? Do you have back-up information or systems?

If those who are responsible for your farm's operations take some time, now again, to keep informed and trained in ways to understand cyber risks and take care of the cyber security of operations, you'll be halfway there.

Continuity Management

How will you record this information (electronic and paper binder)? Where will you keep copies of this document? How and who will access this plan in the event of a disruption? Is everyone who needs to manage a disruption to your farm business aware of how to access the document and who is responsible for doing what – including back-up, in the event that key people are not there at the time? What is your communication plan to make sure your Cyber BCP can be put in motion immediately?

This can be included with your Farm Cyber Security Policy. Review this binder regularly with the people who are involved in making sure your farm operations are safe, secure and recoverable.

Testing

Try out your Cyber BCP to make sure it works and to identify any problems that need to be fixed.

You can incorporate this into a regular Cyber Fire Drill.

What did you notice about how prepared you were, and how quickly you were able to act? Was anything missing or really hard to do? What could help make this quicker and easier? What will you do in the next six months to improve your preparedness?

Maintenance and Compliance

Keep the plan up-to-date and make changes as needed based on new risks your sector or region is facing, changes in your business, or other factors. How often will you review your Cyber BCP? Is there anyone new you will bring into the conversation? Why? Who will be involved in making revisions to the plan (for example, after each cyber fire drill)? Where will copies of your plan be kept? Who will get a copy of this plan? Record the date of the plan and add new dates whenever it is revised.

A final point to keep in mind:

There are lots of things individual producers can do to improve their cyber preparedness, but they can't – and shouldn't – have to go it alone. Producer and commodity associations, private sector vendors and services, as well as levels of government, have critical roles to play in sharing information, providing incentives and support, and intervening (where appropriate) in the event that a major threat is detected or a large-scale incident happens. For more information, please see our document, Cyber Barn Raising, which describes a framework for building networked support across the food system.

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.

Appendix: Glossary of Common Terms in Cybersecurity[1]

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:[2] 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.

1 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

2 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.[3]

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[4] 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.

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

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.

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
Research to Practice to Alignment

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