Creating a Farm Business Cyber Security Policy

Why having a cyber security policy 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.

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 technologies, 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 cyber security policy to help prevent cyber security incidents. A cyber security policy can be used together with a business continuity plan, 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.

A farm cyber security policy is an important part of a farm business's everyday risk management strategy. It can help minimize the chance of cyber attacks, protecting important business assets, so the business can keep operating and stay profitable. A cyber security policy outlines your farm business's approach to managing information security risks, including the things you will and won't do that, together, will protect information and systems from cyber threats.

A cyber security policy is a practical tool that can help you stay on top of the practices that will help your farm business lower the risk of a cyber incident. Having one on file may also help you comply with the expectations of insurers or lenders – that you are taking reasonable steps to minimize the risk of business losses. And, if you hold sensitive data about other people (like credit card data collected by a farm gate store), having an active policy in place could help minimize reputational damage and legal liability in the event of a data breach.

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

Note: To make sure you can get the full benefit of having a policy (including the ability to demonstrate in a court of law that you took all reasonable steps to safeguard your data and your operations), you'll need to review it on a regular basis and write down the steps you took to put the details of your policy into practice (your procedures). Your policy and procedures, and your periodic reviews and updates should be recorded and dated to support any future claims you may need to make. And, remember, the basic policy you will have after completing this worksheet is a starting point – you should eventually review it with a professional who is familiar with your farm business operations, and to make sure it reflects the latest cyber security standards and best practices.

A cyber security policy for your farm

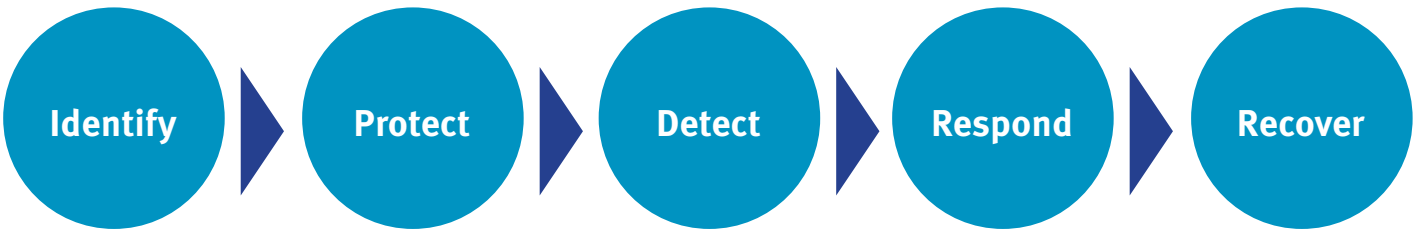
First, some basic definitions. A business policy is a set of statements that describe the way certain kinds of things should be done in specific circumstances. Having a policy can help you stay focused on goals that are important to your farm business. Often, a list of procedures is added to a policy as guidelines for how the policy is supposed to be applied in different situations. A policy can be a formal document or even an informal understanding.

A Simple Example: We know that some cyber attacks are carried out by targeting people during busy, important, times of the year, when they are tired, under pressure and distracted by the need to focus on time-sensitive work, like planting or harvesting. If one of your business goals is to avoid becoming a victim of cyber fraud, you may have a policy that says that, during identified times of the season, no one should answer emails or text messages that ask you to click on an unverified link, without first confirming that the sender and the request are real. This could be as simple as a sticky-note on the side of your computer or the dashboard of your combine that says "Remember: Don't click on email or text message links right away - first check with the sender and one other member of the farm team!".

But, we can do better than a sticky-note on your dashboard.

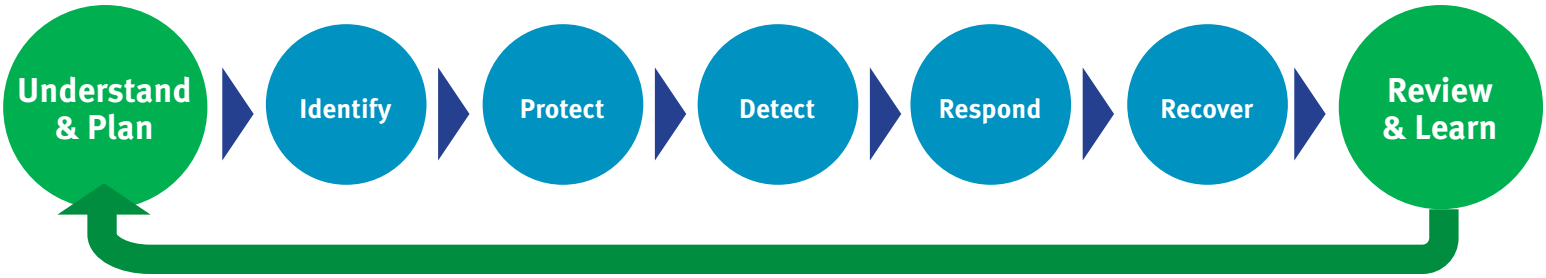
The National Institute for Standards and Technology (NIST) is one widely-used framework for developing a business cyber security policy.[2] The following template is based on NIST and related best practices. It walks you through a set of practical, basic, steps you can take to improve your farm's cyber security and resilience. Once you've done this, you should have a better chance of avoiding a cyber disruption, and to continue or resume operations if one does happen. 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 readiness.

Whatever way it's laid out, a cyber security policy usually covers the following steps to safeguard your business:



2 The Center for Internet Security (CIS) and the Multi-State Information Sharing and Analysis Center (MS-ISAC) created a tool for developing an organizational cyber security policy based on the NIST Cybersecurity Framework (www.NIST-Cybersecurity-Framework-Policy-Template-Guide-v2111Online-2.pdf). There are many resources that describe the NIST framwork in simple terms. One is: C.J. Brooks, C. Grow, P. Craig & D. Short (2018). Cybersecurity Essentials. Sybex/John Wiley and Sons. We have adapted the NIST baseline template for use by family-owned farm businesses, as the basis for this Work Sheet. The suggestions offered here are not a substitute for professional technical advice tailored to an individual business. Once you complete this Work Sheet, print out the Policy Template Guide developed by CIS and MS-ISAC, and share these with an IT or cyber security provider when you're ready to take the next step. These will give you a great starting point to continue to improve your farm business cyber security.

These steps aren't exactly a straight sequence. They should be looked at as things that build on one another and that provide learnings to help you get better at managing cyber risks. For example, if an incident does occur, the process of responding and recovering can show you where you can improve your cyber security position for the future. So, we could another piece – Review and Learn. This can connect back to the others through another piece called, Understand & Plan:



Even though we're talking here about digital technologies, some of the same ideas can apply to the ordinary physical systems you rely on to keep information (like filing cabinets of historical records) or that control critical systems (like the room that contains the control panel for a livestock barn). These need to be protected from physical threats like fire, flood, animals, dust, or vandalism and theft. That's why a cyber security strategy for an organization can also tie into other areas like information security (being careful to protect sensitive information or not over-sharing information that could be used to target your business), physical security (to prevent things like vandalism or equipment theft) and biosecurity (to prevent unauthorized access of people to your fields or barns or contact between wildlife and livestock).

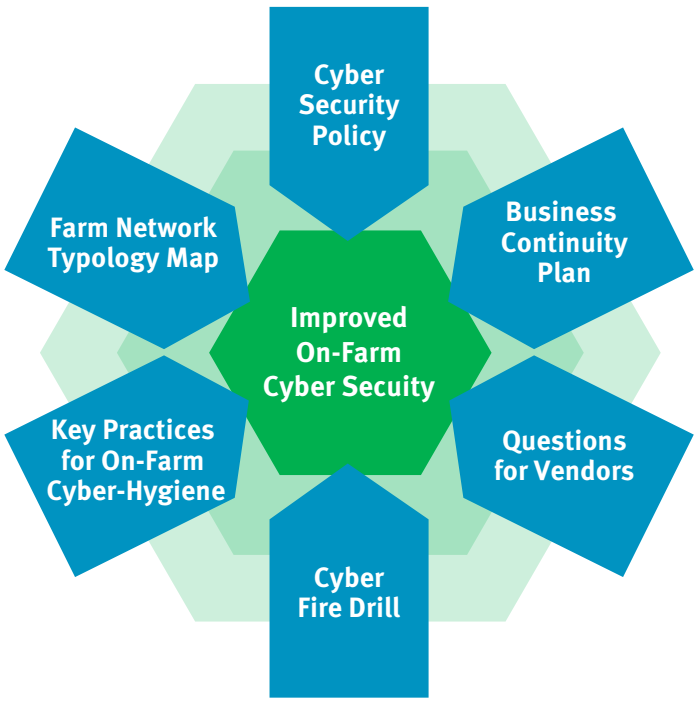
Many of these are things you probably already do every day. Creating and using a cyber security policy involves similar kinds of ideas, and can draw from your own experience managing farm business risks.

Putting together your farm cyber security policy

A cyber security policy 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.



Understand and Plan

Like developing a Cyber Business Continuity Plan, your Farm Cyber Security Policy should focus on your most important business assets and operations.

The planning stage is where you think about what makes sense for you and your farm business. Taking time with this will help you go faster when you tackle the other pieces. Talk to those who are most important to running your farm. This could include family members, key employees, advisors, IT providers, and insurers.

What are the digital technologies you use in your farm business? Why are these important to the success of your operation?

What are the business goals that you want this policy to serve? Some of these might be to: maintain insights into how your operations are working; safeguard animal welfare; sustain crop yield; avoid supply chain disruptions; ensure profitability; reduce worry; onboard new employees; maintain consistent practices; build your ability to make decisions about new technology adoption; or reduce liability.

What are some of the ways that you currently manage risk on your farm? How could a farm cybersecurity policy help?

What compliance expectations, regulations, or requirements might a cyber security policy help you address?

What equipment and data safeguards have your vendors and service providers put in place to protect you? See Work Sheet, Questions for Vendors.

Identify

Take some time to understand and describe the main features of your farm's information network. **What are the pieces of hardware that are connected to each other and to the Internet (what people call the 'physical structure')?**

Where and how does data flow between these different parts (what's called the 'logical structure')? You can use the Work Sheets, Map of Your Farm Network and Cyber Business Continuity Plan to help you record your most important digital assets and make a basic picture of how your farm network is laid out.

How do you and your employees, as well as vendors, suppliers and service providers, connect to your digital assets? For example, if you have an app that lets people monitor and control the environment of a livestock barn using a handheld device, like an Android or iPhone, ask yourself: who can access the app and under what circumstances; is it password-protected; who is authorized to have a password?

The same goes for access to portals that connect you to financial or advisory services or equipment vendors. An important idea in cyber security is that only those people who absolutely need to be able to use a system should be authorized to have access to it. Passwords specific to individual people and the systems they access (this allows each time a system is accessed by a particular person or source to be logged – which can help to detect a potential intrusion, or show that one occurred, after the fact). Passwords should be strong and not shared with those who shouldn't know what they are. You can also add extra protection using multi-factor authentication. This is like the PIN code you use to access an ATM with your bank card – your financial institution will tell you that you should never share this with anyone. It's a similar situation when it comes to your social insurance number: there is a limited number of situations when it's okay to share that. In most cases, it should never be shared, and it should be kept in a secure location. **Do you have any access controls in place? What are they? Who has access to what systems and equipment?**

Protect

Identify what you're currently doing to protect the cyber systems (digital technologies, network and data) of your farm business, and what you want to do to improve your position. These steps are your practices and procedures. They include steps that: prevent people from breaking into your systems, like firewalls, anti-malware applications, configuring your systems according to manufacturers' recommendations, regularly update your software allowing it to be 'patched', and access controls. They also include other controls that help you ensure your most important databases and data flows are safe. This could involve things like regular data back-ups and off-site storage, and using things like encryption and multi-factor authentication to protect data in transit (emails, transmission to service providers). Using a VPN (virtual private network) app when you're communicating between business systems and providers can make it harder for unauthorized people to see what you're doing and interfere with, or steal, valuable information. See the Work Sheet, Key Practices for On-Farm Cyber-Hygiene.

Detect

These are things that work like intrusion alarms to tell you if someone who isn't an authorized user is trying to get into your systems. These could be used to detect potential intrusions from either remote users or insiders who might want to steal from you or harm your business. **Are you aware of any detection systems your farm network or equipment have in place?** This is something your IT provider or equipment vendor may be able to tell you about. There are different kinds of software available that provide a window into data flows and that log access by authorized or unauthorized users. More sophisticated organizations often have areas of their systems that fool unauthorized users into thinking they've entered the real system and then record information that could help an investigation.

Respond and Recover

How would you handle a potential problem that is detected?

What would you do if an actual attack occurred?

The aim is to minimize the damage that a cyber incident causes to your operations, so that you can minimize disruptions and losses. This ties into a Cyber Business Continuity Plan.

Review and Learn

Policies should not be snapped into a binder and left on a shelf. **Review your cyber security policy regularly** (perhaps at the end of the harvest season, or once a year, between delivery of quotas. Make sure everyone who needs to know understands what is expected and how these expectations should be met. In the event that a cyber incident does occur, you should review your policy, as soon as possible, after the event to: identify anything you've learned and what you would do differently in the future, and what resources you might need to take care of these things. Then, update your policy to help you keep track of your new commitments. Don't forget to date any changes you make, and to keep all of your key personnel informed, along the way.

Final thoughts:

By the time you've answered the following questions, you will have a basic Farm Business Cyber Security Policy that can help you reduce on-farm cyber security risks, as well as strengthening the sustainability of your farm business.

Once you have a draft of the policy 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. 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.

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.

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.

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

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