A Cyber ‘Fire Drill’[1] How-to for Farmers

When the fire alarm goes off you know exactly what to. You leave behind what isn’t absolutely necessary to your personal health and safety, and you help people who may require assistance. You go outside and you muster in a designated spot. Someone will do a roll call and check to make sure everyone is safe. 911 has been called. Sprinklers and other fire suppression systems probably have gone off, fire doors will have been closed to help prevent the fire from spreading, and many construction materials and furnishing will likely have been made from from retardant materials so they are less combustible. Emergency services show up. Once the all-clear is sounded, people work to resume their regular business activities.

In the event of fire drill, there might be an opportunity to reflect on what happened and how to do better in the future. In the event of a real fire, it could take some time to clean up and resume operations. A business continuity plan may need to be activated. Most organizations have documents that describe policies (what and why) and procedures (how) related to fire drills and business recovery.

A cyber ‘fire drill’ has a similar role – it is a practice exercise that you conduct periodically, to remind you how to act in an emergency, and to identify preparations that could reduce the impacts of a disruption. It helps you feel confident that you’ll know what to do in the event of a cyber incident, so that you can minimize damage (including livestock, crop, information or financial losses) and get your business up and running again, as quickly as possible.

Conducting a cyber fire drill doesn’t have to be complicated – it just needs to be planned, documented, implemented on a regular schedule, and updated every time you learn something new about what will help you be more cyber safe, or add more layers of protection to your operation.

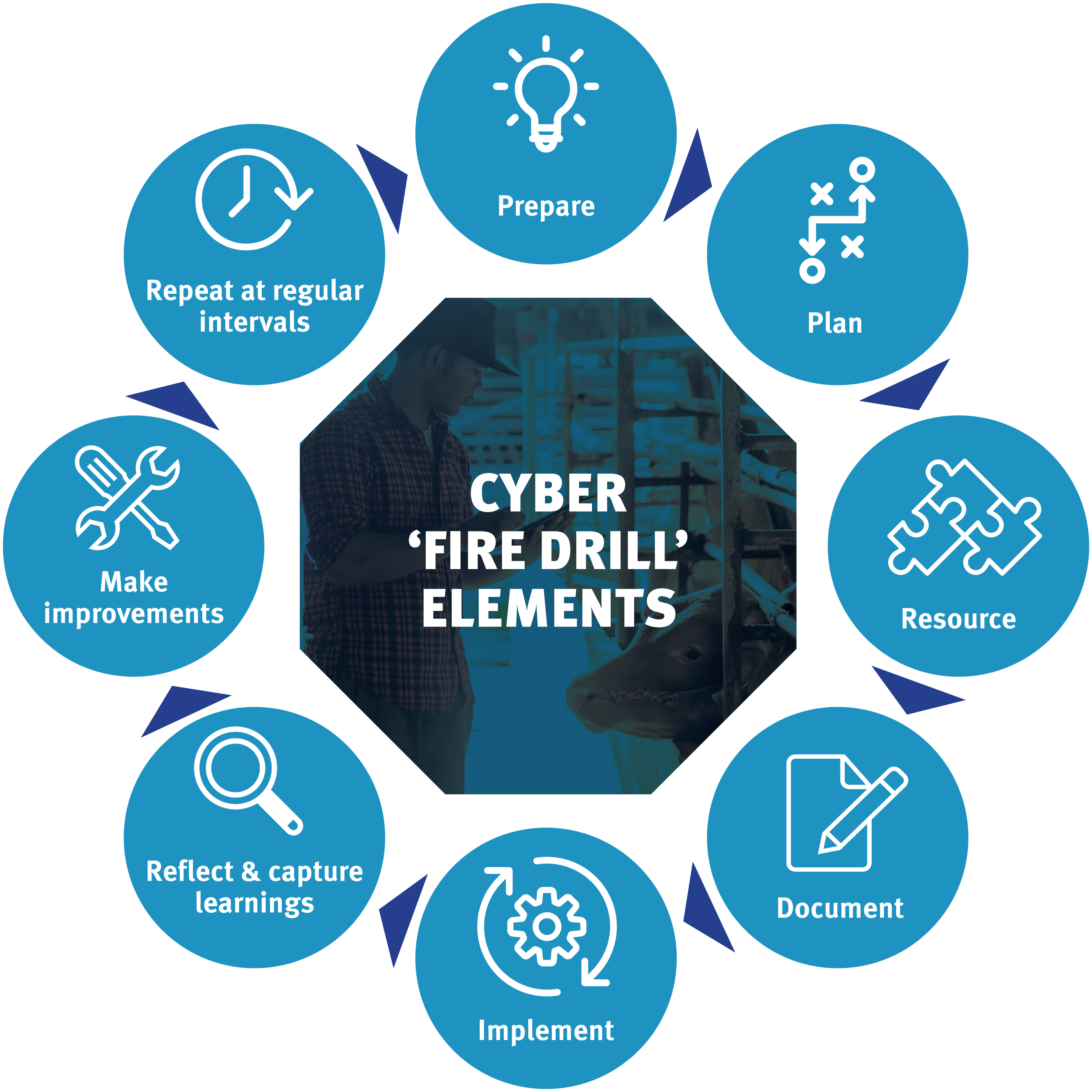
Let’s look at what you can do, by comparing a regular fire drill to a cyber ‘fire drill’. And, while we’re doing this, remember that a real fire can also lead to a cyber incident by disrupting industrial control systems, destroying data, and interfering with e-commerce and supply chains. Your cyber ‘fire drill’ should consider accidental physical disuptions to electronic systems, as much as intentional attacks on data and electronic networks.

[1] R. Kotak with J. Botschner (2022)

Cyber 'Fire Drills' – The Basics

Like fire drills in large organizations (schools, hospitals, big companies), cyber 'fire drills' can be long, drawn-out exercises, including simulations and table-top exercises. But, they can also be simple and straightforward for smaller organizations, including family farms. Here are the basic elements of a regular fire drill and a cyber 'fire drill'.

You can do develop and implement a plan for your own cyber 'fire drill' OR consider taking a 'cyber barn raising' approach and collaborating with some of your peers to support one another in conducting and learning from your collective experiences. You might be able to achieve an economy of scale by chipping in on the fees for a cyber security consultant. Grouping together to engage your commodity associations, farm sector organizations, levels of government and vendors can also be a way to bring collective attention to the supports you might find helpful.



Elements	Regular Fire Drill	Cyber 'Fire Drill'
Prepare	• Account for the people and the assets that need to be protected • Determine key fire risks to be aware of (these will be different in an office tower than in a manufacturing facility)	• Identify business-critical information and systems • Identify production vulnerabilities (such as industrial control systems supporting livestock feeding, milking and environmental needs, key crop planting and harvesting periods and related equipment, monitoring, control system and input needs) • Inform yourself about existing and potential cyber risks and methods (such as phishing, business email fraud, ransomware) • In some cases, it might be useful to engage a cyber security consultant to help you identify vulnerable aspects of your operation and make a plan for how to make them more resistant to attack
Plan	• Identify evacuation routes and safe mustering locations • Consider evacuation challenges • Develop procedures including emergency notifications and communications about training and drills • Identify goals for drills (such as time to evacuate, time to resume operations) • Identify details of drills and their frequency and level of complexity (such as simple evacuation or more realistic scenarios or simulations)	• Identify options for protecting and recovering your system by focusing on the basics: software and firmware updates and patches; anti-virus/anti-malware measures; firewalls; segregated networks; off-premise back-up; business recovery; insurance (where relevant, available and appropriate to level of risk and affordability) • Identify likely scenarios that will be the basis for your drill (such as interruptions in inputs, disrupted contro systems, data breaches/theft, ransomware attacks, website defacement) • Identify goals for testing your system and response
Resource	• Identify and engage emergency services so that they are aware of your needs and plans and can participate in fire drills • Install necessary fire monitoring, alarm and suppression systems • Verify composition of building materials and furnishings • Ensure presence and operation of fire doors and accessibility of exits (no parking, snow cleared, etc.) • Map and post evacuation routes, exists and procedures • Inform staff, identify and train evacuation teams • Create tools (such as checklists) to account for evacuated employees	• Identify and engage IT services/vendors so that they are aware of your needs and can advise you on what to do in the event of a disruption • Consider and secure other sources of help (family, community members, business consultants, vendors, insurers) • Create a list of critical information/ data assets and a rough diagram of your networked components • Agree on any training other materials that you want to review together, as a family farm business • Create tools, like checklists, activities and timelines to follow

Elements	Regular Fire Drill	Cyber 'Fire Drill'
Document	• Develop and communicate policies and procedures to all relevant employees and business units	• Consolidate everything into at least two copies of a binder and review together
Implement	• Test automated systems • Communicate dates and details of upcoming drill • Conduct fire drill involving organization and emergency services	• Test your back-up systems • Agree on a date for the drill • Conduct the drill (consider having a peer farmer observe and make notes about what happened, then return the favour!)
Reflect & capture learnings	• Review goals for fire drill • Ask what worked, what didn't work, and why	• Review goals for cyber 'fire drill' • Ask what worked, what didn't work, and why
Make improvements	• Identify specific actions that can be verified • Identify responsibilities for implementing actions • Identify required resources	• Identify and write down specific actions that can be verified • Identify responsibilities for implementing actions • Identify required resources
Repeat at regular intervals	• Do it again and continue to learn together	• Do it again and continue to learn together

What can you do tomorrow, next month, and next year, to:

- **Start doing your own cyber 'fire drills'; and to**
- **Build your capacity to learn from them to make your farm operation more resilient and better able to manage business risks related to digital technologies?**

For further information

CSKA Community Safety Knowledge Alliance
Research to Practice to Alignment

www.cskacanada.ca

Partly funded by Canada

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.

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.