CANADIAN CENTRE FOR CYBER SECURITY

Canadian Produce Marketing Association Convention and Trade Show

June 2022

Communications Security Establishment   Centre de la sécurité des télécommunications

Canada

Who am I?

- Sr. Business Analyst – Partnership team
- MBA, M.Sc., Management of Information System Certificate
- 11 years of experience at Communications Security Establishment
  - 3 years experience - Cyber Centre
  - 8 years experience - SIGINT and Corporate Services
- 20 years experience in the private sector and Crown Corporation

Agenda

I. Canadian Centre for Cyber Security;

II. Risks in the Agriculture / AgriFood Sector;

III. Cyber Threat Landscape;

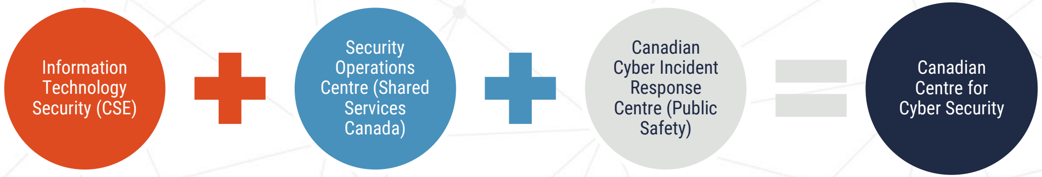
IV. CCCS Services

THE CANADIAN CENTER FOR CYBER SECURITY (CYBER CENTER)

- Business line of the Communications Security Establishment, a Federal Agency
- Located in Ottawa, Ontario
- Created in 2018

CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

The Cyber Centre provides **expert advice, guidance, services and support on cyber security for government, critical infrastructure owners and operations**, the private sector and the Canadian public.


Information Technology Security (CSE)
+
Security Operations Centre (Shared Services Canada)
+
Canadian Cyber Incident Response Centre (Public Safety)
=
Canadian Centre for Cyber Security

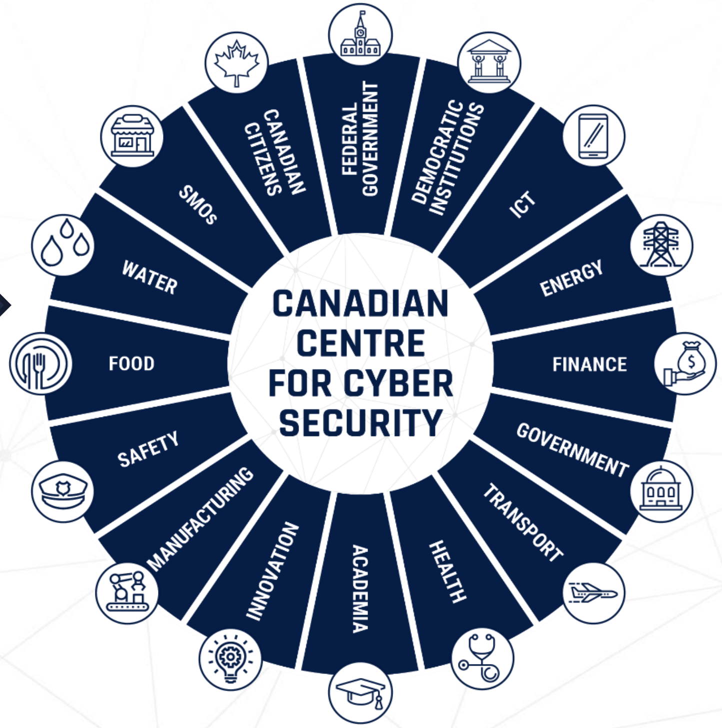
INCREASED CYBER SECURITY SERVICE SCOPE

National Defence Act (NDA)

CSE could provide advice, guidance and services to protect information infrastructures of importance to the GC.

CSE Act

CSE is now authorized to provide more robust cyber defense services by deploying its cyber defence tools to <u>critical non-Government networks</u> designated as being of importance to Canada.



CANADIAN CENTRE FOR CYBER SECURITY

CRITICAL INFRASTRUCTURE SECTORS

- Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders.
- Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence.

FEDERAL GOVERNMENT

ROYAL CANADIAN MOUNTED POLICE (RCMP)

The RCMP works to prevent crime, enforce the law, investigate offences, keep Canadians, and their interests, safe and secure, and assist Canadians in emergency situations/incidents. It operates within three main areas of responsibility:

- Contract and Indigenous Policing
- Federal Policing
- Specialized Policing Services

CANADIAN SECURITY INTELLIGENCE SERVICE (CSIS)

CSIS is at the forefront of Canada's national security system with a role to investigate activities suspected of constituting threats to the security of Canada and to report on these to the Government of Canada.

PUBLIC SAFETY (PS)

PS Canada ensures coordination across all federal departments and agencies responsible for national security and the safety of Canadians. The mandate is to keep Canadians safe from a range of risks such as natural disasters, crime, and terrorism with a mission to build a safe and resilient Canada.

INNOVATION, SCIENCE AND ECONOMIC DEVELOPMENT CANADA (ISED)

ISED works with Canadians in all areas of the economy and in all parts of the country to improve conditions for investment, enhance Canada's innovation performance, increase Canada's share of global trade and build a fair, efficient and competitive marketplace.

*Information provided for each organization comes from their respective web sites.

VICTIM OF CYBERCRIME, FRAUD, OR SCAMS?

Where do I report a cybercrime?

- You should report a cybercrime to your local police department.
- For geographical areas where the RCMP is the police of jurisdiction, report cybercrimes to the local detachment.
- Report cybercrimes to the Cyber Centre's online portal to get support and advice on how to protect your organization from being targeted repeatedly.
- Report fraud to the Canadian Anti-Fraud Centre through their Fraud Reporting System.

Agenda

I. Canadian Centre for Cyber Security;

II. Risks in the Agriculture Sector;

III. Cyber Security landscape;

IV. CCCS Services.

RISKS

- Disruption of grain and corn production could impact commodities trading and stocks
- Disruption of processing with effects cascading down to the farm level
- Disruption of supply chains at critical cycles with cascading impact across multiple business elements
- Pressure and risks of managing perishable commodities

RISKS (cont'd)

- Potential for key commodities or infrastructure to become unavailable
- High number of supply chain and other interdependencies with other critical infrastructure sectors, particularly the transportation sector
- New devices being installed without being able to assess security considerations ahead of time
- Rush to catalog assets
- Personal and professional devices for the home and business needs are on the same network

Agenda

I. Canadian Centre for Cyber Security;

II. Risks in the Agriculture Sector;

III. Cyber Security landscape;

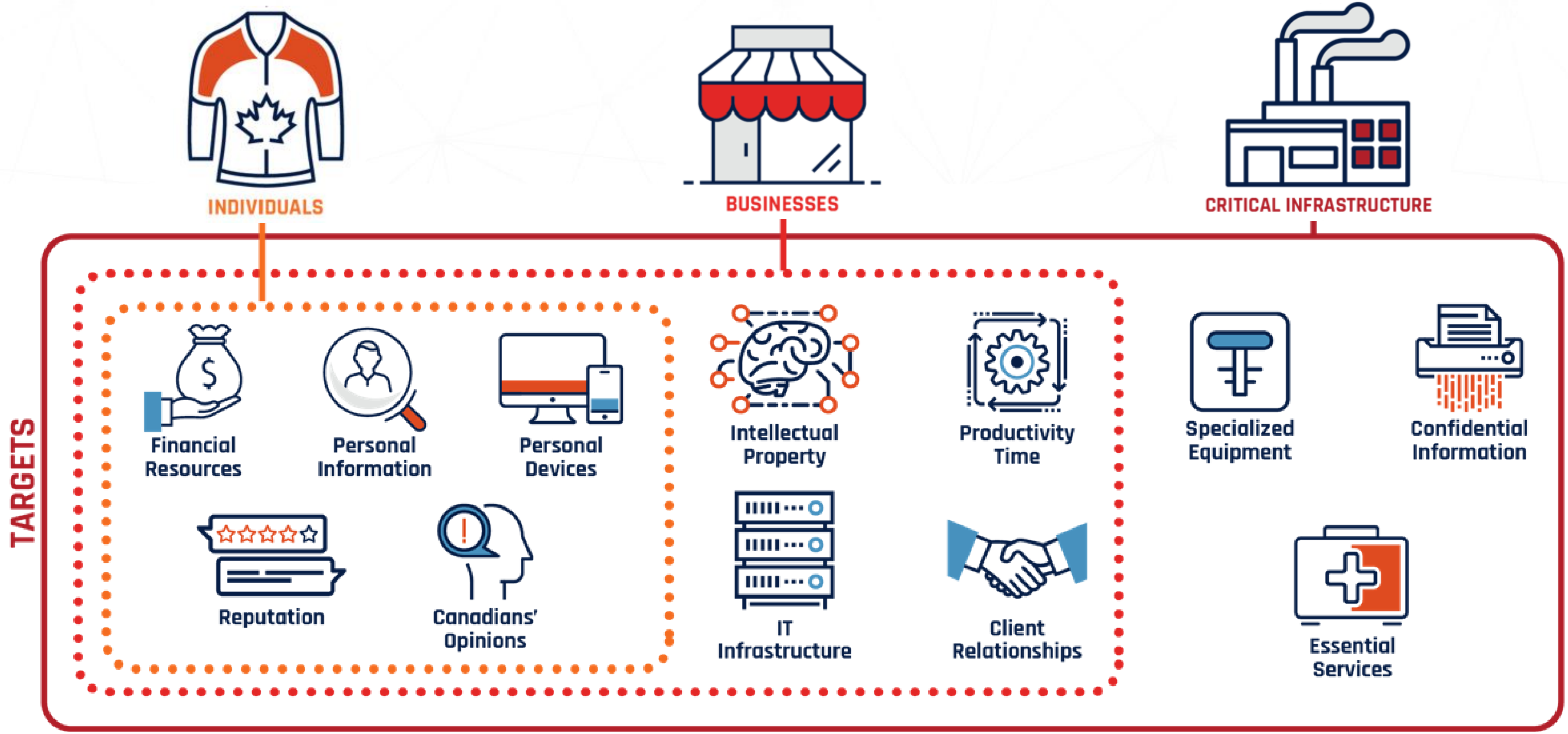
IV. CCCS Services.

THE THREAT LANDSCAPE

National Cyber Threat Assessment – 2020

- **Cybercriminals** represent the most pervasive cyber threat to Canadians
  - Ransomware and Phishing attacks
- **State sponsored** cyber threat actors have most sophisticated capabilities
  - Cyber espionage, IP theft, online influence campaigns, disruptive cyber attacks

THE CANADIAN CYBER THREAT LANDSCAPE



APTs... HOW SCARED SHOULD I BE?

- Advanced Persistent Threats (APTs), like cyber criminals, will use techniques that work

- Most malware variants exploit publicly known vulnerabilities, often for which a patch has been made available from the vendor

THE THREAT LANDSCAPE

The ransomware threat in 2021

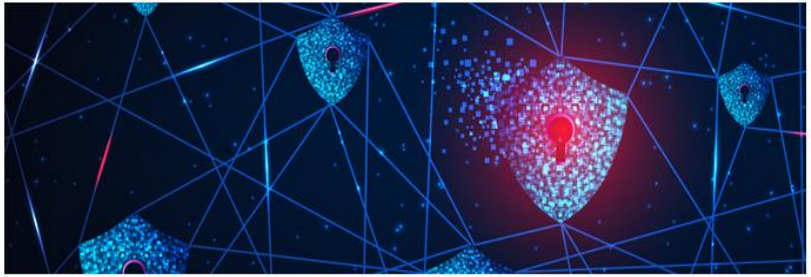
- First half of 2021, global ransomware attacks increased by 151% when compared of the first half of 2020 (fueled by Ransomware-as-a-service)
- 2021 was marked by the highest ransoms and the highest payouts
  - In Canada, average cost of a data breach (includes ransomware) was $6.35M CAD
  - Global average cost of recovery from ransomware incident (paying ransom / remediating compromised network) increased from $970 000 CAD in 2020 to $2.3M CAD in 2021
- Cyber Center is aware of 235 ransomware incidents against Canadian victims from Jan 1 to Nov 16 2021
- Once targeted, ransomware victims are often attacked multiple times

RANSOMWARE

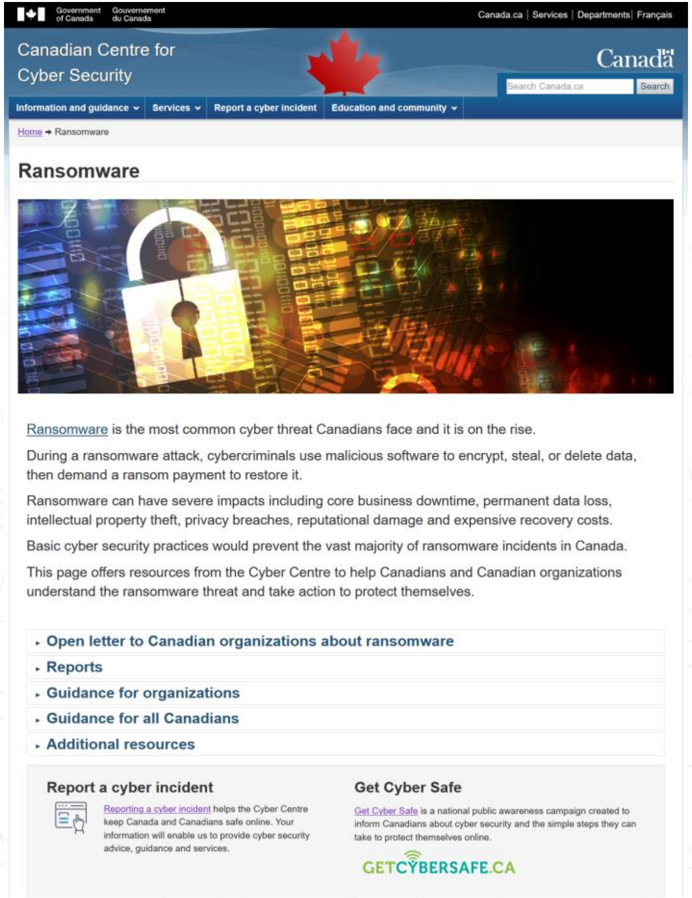
Ransomware playbook ITSM.00.099

https://cyber.gc.ca/en/guidance/ransomware-playbook-itsm00099

Cyber threat bulletin: The ransomware threat in 2021



https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-ransomware-threat-2021



Ransomware

Ransomware is the most common cyber threat Canadians face and it is on the rise.

During a ransomware attack, cybercriminals use malicious software to encrypt, steal, or delete data, then demand a ransom payment to restore it.

Ransomware can have severe impacts including core business downtime, permanent data loss, intellectual property theft, privacy breaches, reputational damage and expensive recovery costs.

Basic cyber security practices would prevent the vast majority of ransomware incidents in Canada.

This page offers resources from the Cyber Centre to help Canadians and Canadian organizations understand the ransomware threat and take action to protect themselves.

- Open letter to Canadian organizations about ransomware
- Reports
- Guidance for organizations
- Guidance for all Canadians
- Additional resources

Report a cyber incident

Reporting a cyber incident helps the Cyber Centre keep Canada and Canadians safe online. Your information will enable us to provide cyber security advice, guidance and services.

Get Cyber Safe

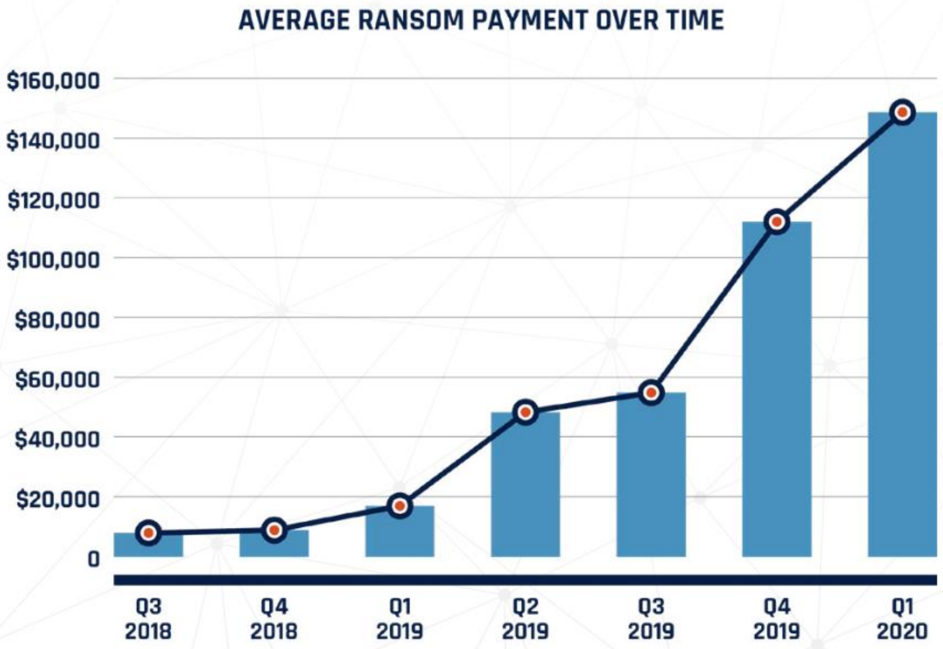
Get Cyber Safe is a national public awareness campaign created to inform Canadians about cyber security and the simple steps they can take to protect themselves online.

RANSOMWARE

Growing popularity of Ransomware

- Ransomware: How to Prevent and Recover
- Combatting Ransomware - RCMP
- Threat Bulletin: Modern Ransomware and Its Evolution
- Cyber Center : Ransomware portal
- CISA: Ransomware Guidance and Resources
- CISA: Reduce the Risk of Ransomware Campaign
- CISA / MS-ISAC: Ransomware Guide
- CISA: Stop Ransomware
- CISA: Ransomware Readiness

Figure 5: Average Ransomware Payments, 2018 to 2020 (data from Coveware converted from USD to CAD)[43]



PRIVATE INDUSTRY - NOTIFICATION

- The Federal Bureau of Investigation (FBI) is informing Food and Agriculture (FA) sector partners that ransomware actors may be more likely to attack agricultural cooperatives during critical planting and harvest seasons, disrupting operations, causing financial loss, and negatively impacting the food supply chain. The FBI noted ransomware attacks during these seasons against six grain cooperatives during the fall 2021 harvest and two attacks in early 2022 that could impact the planting season by disrupting the supply of seeds and fertilizer.

- *This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors.*

VARIOUS CYBER ATTACKS

Articles

FBI warns of 'timed' ransomware attacks on agriculture sector	The FBI's cyber division published a flash alert for the food and agriculture sector stating that "ransomware actors may be more likely to attack agricultural cooperatives during critical planting and harvest seasons" like the fall and early spring."
JBS Paid $11 Million to Resolve Ransomware Attack	JBS USA Holdings Inc. paid an $11 million ransom to cybercriminals who last week temporarily knocked out plants that process roughly one-fifth of the nation's meat supply.

Social Engineering

Phishing…all it takes is just one click

Unfortunately, employees are often the weakest link in the cybersecurity chain. "88% of UK data breaches caused by human error, not cyber-attacks," according to data obtained from the UK's Information Commissioner's Office (ICO).

Reference: https://www.hlb.global/howvulnerableisthefoodsupplychaintoacyber-attack%3f/

PHISHING

- Phishing is the number one delivery vehicle for ransomware.
  - Phishing, SMiSing, Vishing, Quishing
  - Don’t Take the Bait: Recognize and Avoid Phishing Attacks
  - The 7 red flags of Phishing

SOMETHING MAY BE PHISHY IF:

- You don’t recognize the sender’s name, email address, or phone number (e.g. very common for spear phishing)
- You notice a lot of spelling and grammar errors
- The sender requests your personal or confidential information
- The sender makes an urgent request with a deadline
- The offer sounds too good to be true

Phishing…Don’t Take the Bait

- Be wary of phishing. Phishing is an attack where a cyber criminal tries to trick you into clicking a malicious link or sharing information.
- These emails / texts appear legitimate and usually are related to a topic you care about.
- Be careful if you do not know the sender. Contact the sender another way.
- In this case, cyber criminals may take advantage of COVID-19 (panic around the pandemic or vaccination status) and the Olympics (results, information about your event, etc.) to try to lure you into clicking on malicious links
  - Check sender’s email has a valid username and domain name and that you know the sender
  - Check the tone of the email, is it urgent or too good to be true?
  - Look for grammatical error in the body of the text

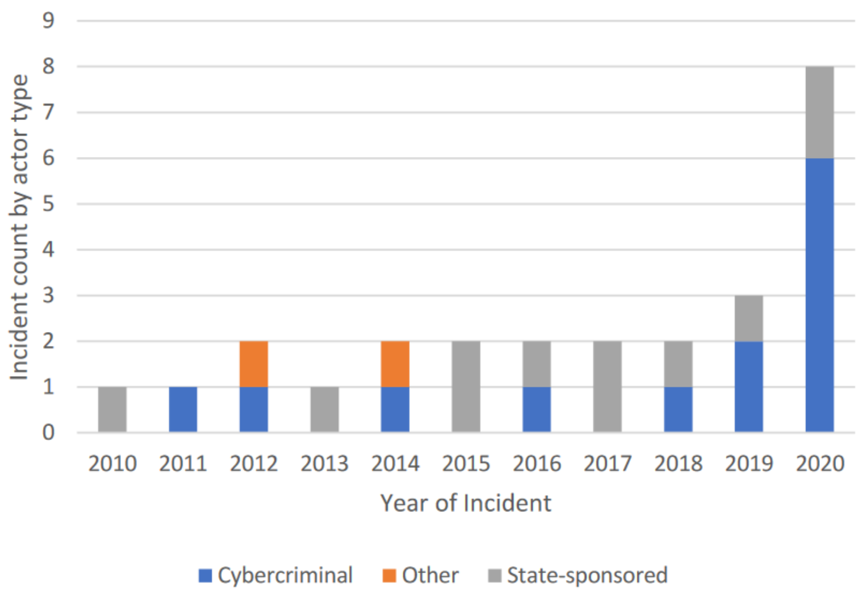
Don’t Take the Bait: Recognize and Avoid Phishing Attacks
Protecting Yourself from Identity Theft Online (ITSAP.00.033)
Best Practices for Passphrases and Passwords (ITSAP.30.032)

THE THREAT LANDSCAPE

Cyber threat to operational technology

- Operational Technology (OT) plays an essential role in the management of Canada's CI
- Digital transformation of OT is providing cyber threat actors new opportunities to access and disrupt OT systems
- 2020 saw a spike in cyber threat activity against OT systems around the world

Figure 1. Publicly-reported cyber incidents targeting OT, by actor type.



THREATS POSED BY IT AND OT CONVERGENCE

- Threat actors can now reach OT systems through increased exposure

- Vulnerabilities in ICS systems that were previously not accessible given the air gap traditionally in place can now be actively exploited

IOT USE CASES IN AGRICULTURE

- Smart irrigation systems
- Drones
- Weather sensors and other Internet of Things (IoT) monitoring tools in which aggregated data is provided for convenience:
  - Monitoring of climate conditions
  - Greenhouse automation
  - Crop management
  - Cattle monitoring and management
  - Precision farming
  - Agricultural drones
  - Predictive analytics for smart farming
  - End-to-end farm management systems

THE THREAT LANDSCAPE

Russian-backed cyber threat activity

- Given the Ukraine crisis, Russia will very likely attack the CI of perceived adversaries
- Be prepared to isolate CI components and services from the Internet
- Increase monitoring of your networks
- Enhance security posture (patch systems, enable logging, etc.)

SUPPLY CHAIN CYBER THREATS

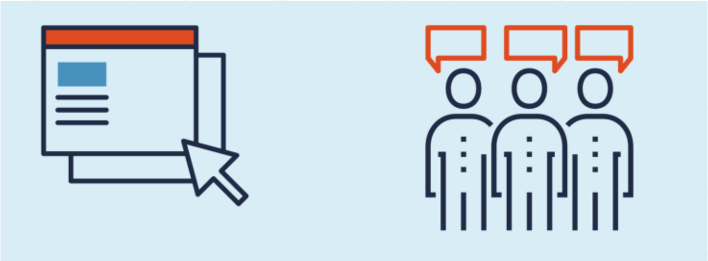
- Sophisticated cyber threat actors can target the supply chain of goods and service providers in order to gain information on and access to their ultimate targets.
- We assess that indirect targeting through the supply chain is almost certainly an active, increasing threat to agriculture and agri/food sector.
- We assess the energy sector is almost certainly a top target for cyber actors.
  - Transportation of goods is highly vulnerable to disruptions in the supply of energy.

WORKING FROM HOME VULNERABILITIES

- What are the additional vulnerabilities?
  - Members of staff working from home on personal unsecured devices
  - Remote worksites: quickly deployed using default configurations and unpatched applications
  - Increased use of vulnerable VPNs, remote desktop services, cloud services
  - Rapid adoption of relatively untested applications (Zoom!)

MISINFORMATION, DISINFORMATION AND MALINFORMATION

- **Misinformation:** False information that is not intended to cause harm.
- **Disinformation:** False information that is intended to manipulate, cause damage, or guide people, organizations, and countries in the wrong direction.
- **Malinformation:** Information that stems from the truth but is often exaggerated in a way that misleads and causes potential harm



CONSEQUENCES OF CYBER ATTACKS

- **Safety:** Malfunctioning IoT devices
- **Ethical:** Privacy breaches
- **Legal:** Civil action, lawsuits, regulatory investigations
- **Operational:** Service interruptions
- **Financial:** Expenses for investigation, remediation, settlement costs
- **Reputational:** Loss of public trust due to mis-information
- **Loss of IP:** Stolen research data or tampering

RECENT TRENDS

- Comparison of the first half of 2021 with the second half of 2020.
  - **Website defacements**: Website defacements were up 8%↑and primarily impacted small and medium-sized enterprises.
  - **Phishing**: Unique phishing URLs, with a large number of malicious links being associated with WhatsApp, is up by 56%.↑
  - **Ransomware**: Reports of ransomware cases increased 17%.↑ Small-medium enterprises from the manufacturing and IT industries were affected the most.
  - **Botnet drones**: The number of botnet drones observed daily on unique and locally hosted C&C servers rose 146%.↑

Agenda

I. Canadian Centre for Cyber Security;

II. Risks in the Agriculture Sector;

III. Cyber Security landscape;

IV. CCCS Services.

THE ROLE OF THE CYBER CENTRE

For Free Cyber Center Services: contact@cyber.gc.ca

INCIDENT HANDLING SUPPORT

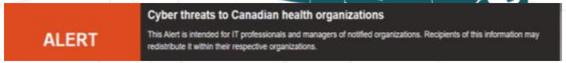
24/7 SUPPORT

contact@cyber.gc.ca

THREAT INTELLIGENCE

ACCESS TO ACTIONABLE CYBER THREAT INTELLIGENCE

Alerts, Advisories



ALERT

Cyber threats to Canadian health organizations

This Alert is intended for IT professionals and managers of notified organizations. Recipients of this information may redistribute it within their respective organizations.

COMMUNITY BUILDING

FURTHER CYBER SECURITY TOGETHER

ADVICE & GUIDANCE

LEVERAGE THE CYBER CENTRE'S EXPERTISE

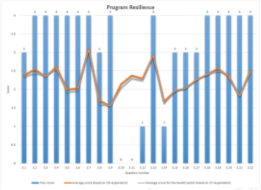
Publications

YOUR SOFTWARE IS
SO LAST YEAR
We got it – there's nothing more annoying than stopping what you're doing for a software update. But trust us, it has its benefits.
REGULARLY UPDATE YOUR
PC and mobile OS
antivirus software
web browser
apps and games

CYBER DEFENCE SERVICES

STRENGTHEN YOUR DEFENCE CAPABILITIES

Assessments, Vulnerability Notifications, Sharing IoCs, etc.



COMMUNITY BUILDING
CYBER THREAT BRIEF

Purpose is to share Relevant Cyber Information

- Updates on Cyber Incidents
- Updates on Cyber Security Threat

Bi-weekly on Wednesday

Walk-The-Talk Virtual Seminar Series

WHAT IS WALK-THE-TALK?

The Walk-the-Talk series of presentations are live virtual sessions featuring a subject matter expert providing in-depth information about a topic, tool or service, as well as answering questions from attendees.

Topics covered at recent talks include:

- Setting up and optimizing DMARC
- Supply Chain Risk and Inquiry
- Partner experiences dealing with incidents
- Guided introduction to malware.cyber.gc.ca

WHY USE THIS SERVICE?

The cyber threats faced by Canadian organizations evolve constantly. The goal of the Walk-the-Talk sessions is for the Cyber Centre to provide specific, actionable information to help partners improve their cyber security.

Similarly, the Partner Experience talks within the series aim to share specific tactics or solutions that a Cyber Centre partner has come across, with the goal of helping other organizations to tackle similar situations or prevent a similar incident.

AT A GLANCE

Walk-the-Talk is a Cyber Centre-hosted series of virtual presentations each covering one cyber security topic. The goal of these sessions is to collaboratively discuss cyber security so that the community of Cyber Centre partners can learn more about various aspects of cyber security from the Canadian community.

Subject matter experts present their topic and field any questions from attendees. These talks range from 30 to 90 minutes, and provide actionable information, or an introduction to a new Cyber Centre tool, service or capability.

Many of the Walk-the-Talk presentations are offered by subject matter experts from the Cyber Center. The **Partner Experience talks** within the series open to floor to Cyber Centre partners to share details about a particular security challenge, open-sourced investigative findings, or dark web insights, while still allowing time for questions and discussion.

SIGNING UP FOR SERVICE

Existing Cyber Centre partners should contact their cyber engagement lead for an invitation to this seminar series.

Prospective partners should contact contact@cyber.gc.ca for more information.

RELATED CYBER CENTRE PRODUCTS AND SERVICES

Partners who attend the Walk-the-Talk sessions might also be interested in our Alerts and Cyber Flash notifications. These provide time-sensitive information relating to a high-impact cyber issue.

In addition, most sectors also hold regular calls where they share threat briefings, as well as sector-relevant updates.

Please speak with your Cyber Centre engagement lead about these and other services your organization would like to receive from the Cyber Centre, or if you would like to present at a Partner Experience talk.

CYBER CENTRE

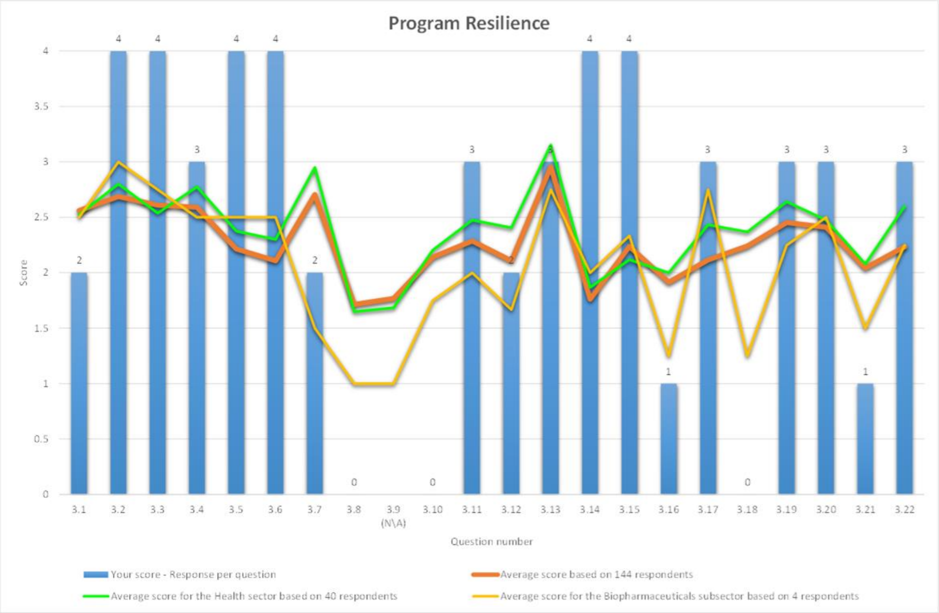
CANADIAN CYBER SECURITY TOOL (CCST)

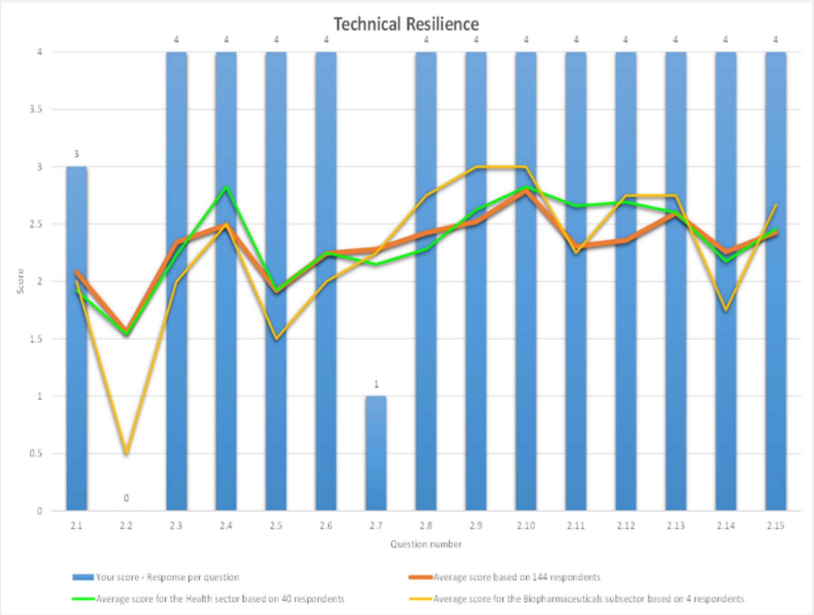
- What is it:
  - Online self-assessment tool designed to be completed in under 60 mins
  - Relevant for entities with a wide range of cyber postures
- The Goal:
  - Understand the RISK you are facing in order to better protect organization with implementation of appropriate controls
- Tool reports
  - Advice and guidance on **technical resilience and programmatic resilience**
  - Entity specific score and peer-based comparisons

Canadian Cyber Security Tool

BUILDING A **SAFE** AND **RESILIENT CANADA**

PROGRAM AND TECHNICAL RESILIENCE RESULTS

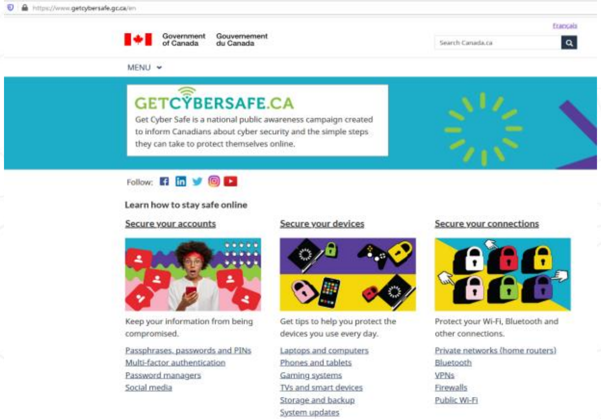




Indicator Level	Status	Description
MIL - 0	Incomplete	Practices are not being performed
MIL - 1	Performed	All practices are being performed
MIL - 2	Planned	Practices are supported by planning and guidelines
MIL - 3	Managed	Practices are organized and managed
MIL - 4	Measured	Practices are monitored and controlled
MIL - 5	Defined	Practices are uniform across an organization

TRAINING AND AWARENESS

- Get Cyber Safe Campaign https://www.getcybersafe.gc.ca/en
- Learning Hub https://cyber.gc.ca/en/learning-hub
- Publications https://cyber.gc.ca/en/publications



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.

Learn how to stay safe online

Secure your accounts

Keep your information from being compromised.

- Passphrases, passwords and PINs
- Multi-factor authentication
- Password managers
- Social media

Secure your devices

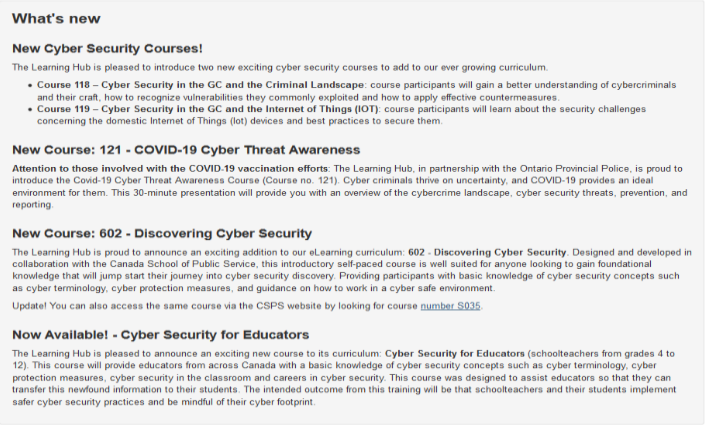
Get tips to help you protect the devices you use every day.

- Laptops and computers
- Phones and tablets
- Gaming systems
- TVs and smart devices
- Storage and backup
- System updates

Secure your connections

Protect your Wi-Fi, Bluetooth and other connections.

- Private networks (home routers)
- Bluetooth
- VPNs
- Firewalls
- Public Wi-Fi



What's new

New Cyber Security Courses!

The Learning Hub is pleased to introduce two new exciting cyber security courses to add to our ever growing curriculum.

- **Course 118 – Cyber Security in the GC and the Criminal Landscape**: course participants will gain a better understanding of cybercriminals and their craft, how to recognize vulnerabilities they commonly exploited and how to apply effective countermeasures.
- **Course 119 – Cyber Security in the GC and the Internet of Things (IOT)**: course participants will learn about the security challenges concerning the domestic Internet of Things (Iot) devices and best practices to secure them.

New Course: 121 - COVID-19 Cyber Threat Awareness

Attention to those involved with the COVID-19 vaccination efforts: The Learning Hub, in partnership with the Ontario Provincial Police, is proud to introduce the Covid-19 Cyber Threat Awareness Course (Course no. 121). Cyber criminals thrive on uncertainty, and COVID-19 provides an ideal environment for them. This 30-minute presentation will provide you with an overview of the cybercrime landscape, cyber security threats, prevention, and reporting.

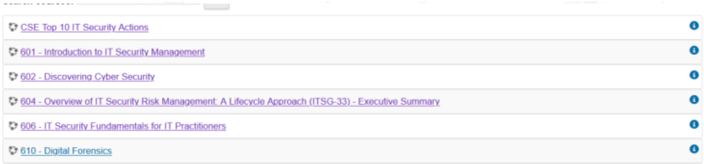
New Course: 602 - Discovering Cyber Security

The Learning Hub is proud to announce an exciting addition to our eLearning curriculum: **602 - Discovering Cyber Security**. Designed and developed in collaboration with the Canada School of Public Service, this introductory self-paced course is well suited for anyone looking to gain foundational knowledge that will jump start their journey into cyber security discovery. Providing participants with basic knowledge of cyber security concepts such as cyber terminology, cyber protection measures, and guidance on how to work in a cyber safe environment.

Update! You can also access the same course via the CSPS website by looking for course number S035.

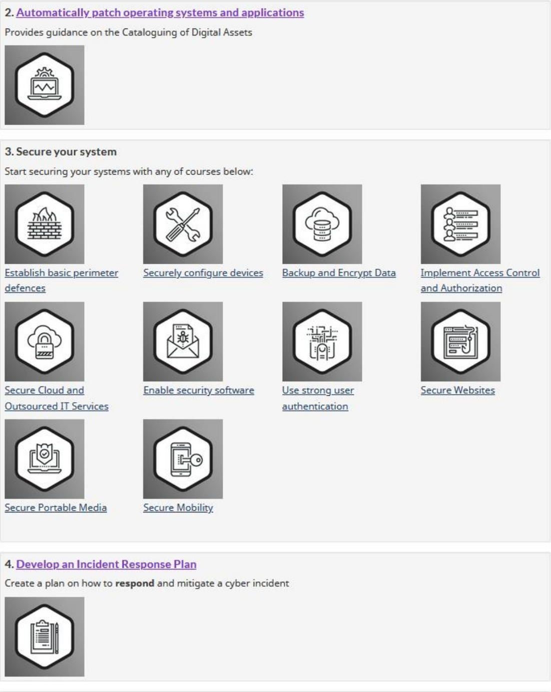
Now Available! - Cyber Security for Educators

The Learning Hub is pleased to announce an exciting new course to its curriculum: **Cyber Security for Educators** (schoolteachers from grades 4 to 12). This course will provide educators from across Canada with a basic knowledge of cyber security concepts such as cyber terminology, cyber protection measures, cyber security in the classroom and careers in cyber security. This course was designed to assist educators so that they can transfer this newfound information to their students. The intended outcome from this training will be that schoolteachers and their students implement safer cyber security practices and be mindful of their cyber footprint.



- CSE Top 10 IT Security Actions
- 601 - Introduction to IT Security Management
- 602 - Discovering Cyber Security
- 604 - Overview of IT Security Risk Management: A Lifecycle Approach (ITSG-33) - Executive Summary
- 606 - IT Security Fundamentals for IT Practitioners
- 610 - Digital Forensics

ISED Cyber Secure Program



2. Automatically patch operating systems and applications

Provides guidance on the Cataloguing of Digital Assets

3. Secure your system

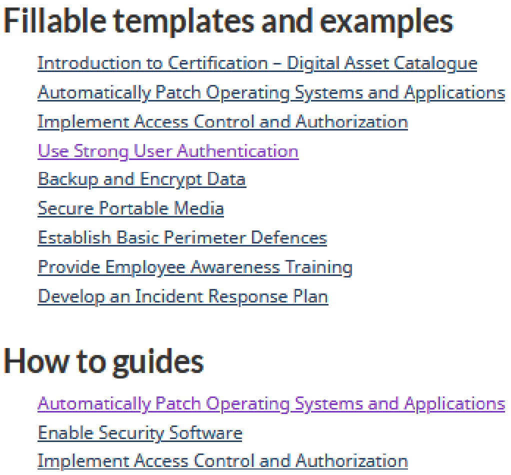
Start securing your systems with any of courses below:

- Establish basic perimeter defences
- Securely configure devices
- Backup and Encrypt Data
- Implement Access Control and Authorization
- Secure Cloud and Outsourced IT Services
- Enable security software
- Use strong user authentication
- Secure Websites
- Secure Portable Media
- Secure Mobility

4. Develop an Incident Response Plan

Create a plan on how to **respond** and mitigate a cyber incident

https://www.ic.gc.ca/eic/site/137.nsf/eng/h_00017.html



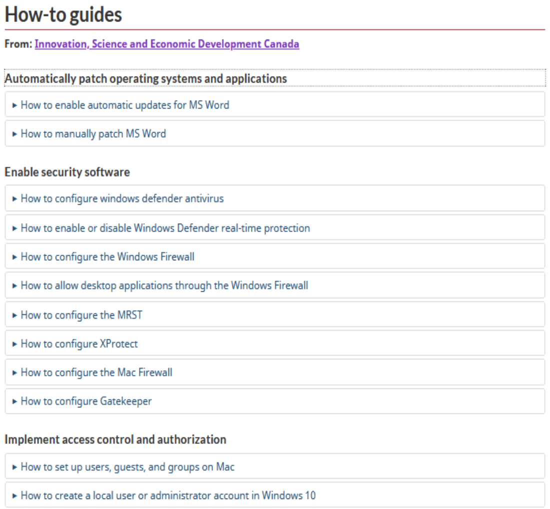
Fillable templates and examples

- Introduction to Certification – Digital Asset Catalogue
- Automatically Patch Operating Systems and Applications
- Implement Access Control and Authorization
- Use Strong User Authentication
- Backup and Encrypt Data
- Secure Portable Media
- Establish Basic Perimeter Defences
- Provide Employee Awareness Training
- Develop an Incident Response Plan

How to guides

- Automatically Patch Operating Systems and Applications
- Enable Security Software
- Implement Access Control and Authorization

https://www.ic.gc.ca/eic/site/137.nsf/eng/h_00040.html



How-to guides

From: Innovation, Science and Economic Development Canada

Automatically patch operating systems and applications

- ▸ How to enable automatic updates for MS Word
- ▸ How to manually patch MS Word

Enable security software

- ▸ How to configure windows defender antivirus
- ▸ How to enable or disable Windows Defender real-time protection
- ▸ How to configure the Windows Firewall
- ▸ How to allow desktop applications through the Windows Firewall
- ▸ How to configure the MRST
- ▸ How to configure XProtect
- ▸ How to configure the Mac Firewall
- ▸ How to configure Gatekeeper

Implement access control and authorization

- ▸ How to set up users, guests, and groups on Mac
- ▸ How to create a local user or administrator account in Windows 10

https://www.ic.gc.ca/eic/site/137.nsf/eng/00042.html#1

A FEW EXAMPLES OF OUR PUBLICATIONS

Cloud:

- Guidance on using tokenization for cloud-based services (ITSP.50.108)
- Guidance on the Security Categorization of Cloud-Based Services
- Guidance on defence in depth for cloud-based services
- Cloud computing
- Guidance on cloud security assessment and authorization
- Guidance on cloud service cryptography

Ransomware:

- Cyber Threat Bulletin: Modern Ransomware and Its Evolution
- Ransomware: How to recover and get back on track
- Ransomware: How to Prevent and Recover

Supply Chain (MSP):

- Supply chain security for small and medium-sized organizations
- Cyber Security Considerations For Consumers of Managed Services

Digital World:

- Best practices for passphrases and passwords (ITSAP.30.032)
- Cyber security at home and in the office: Secure your devices, computers, and networks (ITSAP.00.007)
- Cyber security tips for remote work (ITSAP.10.116)
- Digital footprint (ITSAP.00.133)
- Don’t take the bait: Recognize and avoid phishing attacks (ITSAP.00.101)
- Have you been hacked? (ITSAP.00.015)
- How to protect your organization from malicious macros (ITSAP.00.200)
- How Updates Secure Your Device (ITSAP.10.096)
- How to identify misinformation, disinformation, and malinformation (ITSAP.00.300)
- Password Managers-Security (ITSAP.30.025)
- Protect your organization from malware (ITSAP.00.057)
- Protecting Your Organization While Using WI-FI (ITSAP.80.009)
- Protecting Yourself From Identity Theft Online (ITSAP.00.033)
- Security considerations for QR codes ITSAP.00.141
- Security considerations when using social media in your organization ITSM.10.066
- Spotting malicious email messages (ITSAP.00.100)
- Virtual Private Networks (ITSAP.80.101)

INSIDER THREAT

- An individual can expose sensitive or personal information after gaining access to your network.
- Guidance:
  - Cyber Centre: Protecting against Insider Threat
  - Public Safety: Insider Risk Checklist
  - CISA Insider Risk Mitigation Self-Assessment Tool

8 Recommended Security Actions

1. Establish a Culture of Security
2. Develop Clear Security Policies and Procedures
3. Reduce Risks from Partners and Third Party Providers
4. Implement a Personnel Screening Life-Cycle
5. Provide Training, Raise Awareness and Conduct Exercises
6. Identify Critical Assets and Protect Them
7. Monitor, Respond to, and Mitigate Unusual Behaviour
8. Protect Your Data

HOW CAN I PROTECT MY ORGANIZATION?

Regularly back up your data and store off-line. LINK

Use strong and unique passwords, implement MFA. LINK

Update and patch systems. LINK

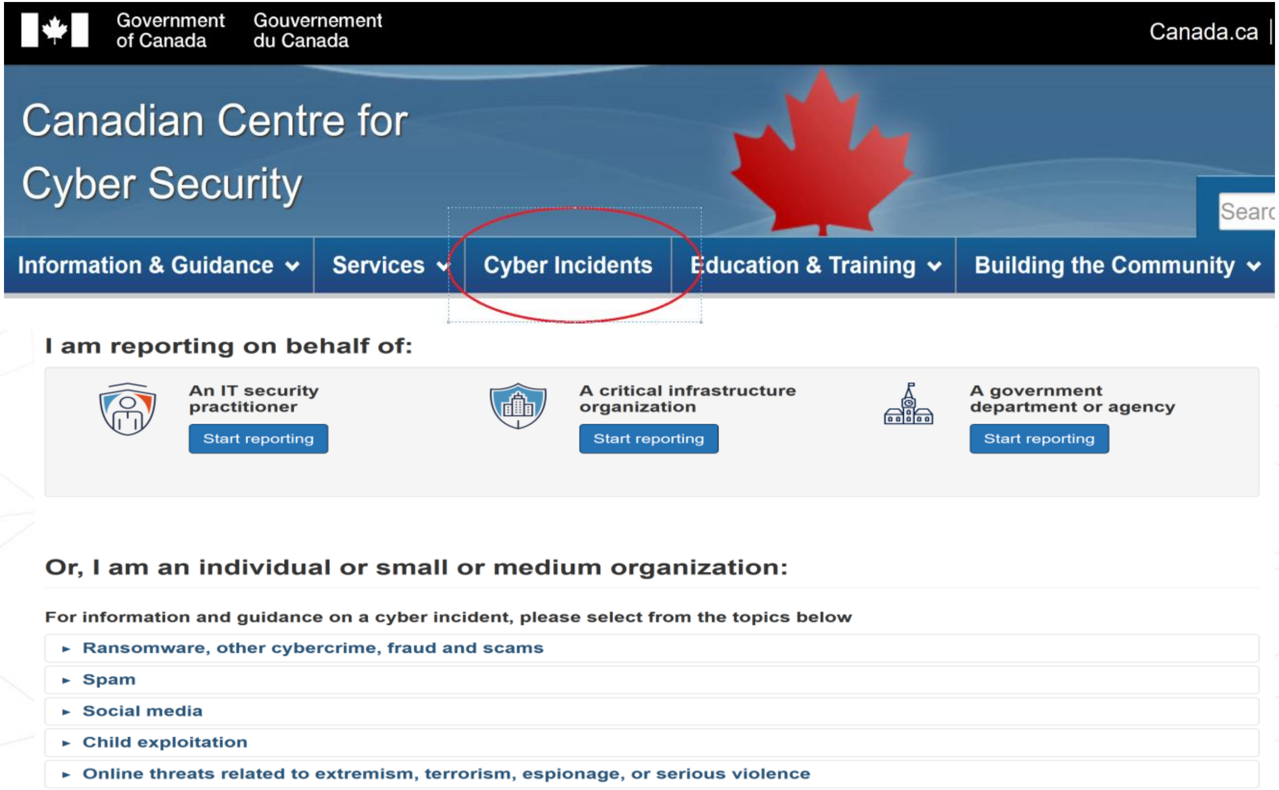
Have an Incident Response Plan (and test it!) LINK

Use security tools. LINK

Cyber Center's **Baseline Cyber Security Controls for SMO**
ISED's **CyberSecure Canada** eLearning

INCIDENT HANDLING PORTAL

Urgency: contact@cyber.gc.ca



I am reporting on behalf of:

An IT security practitioner

Start reporting

A critical infrastructure organization

Start reporting

A government department or agency

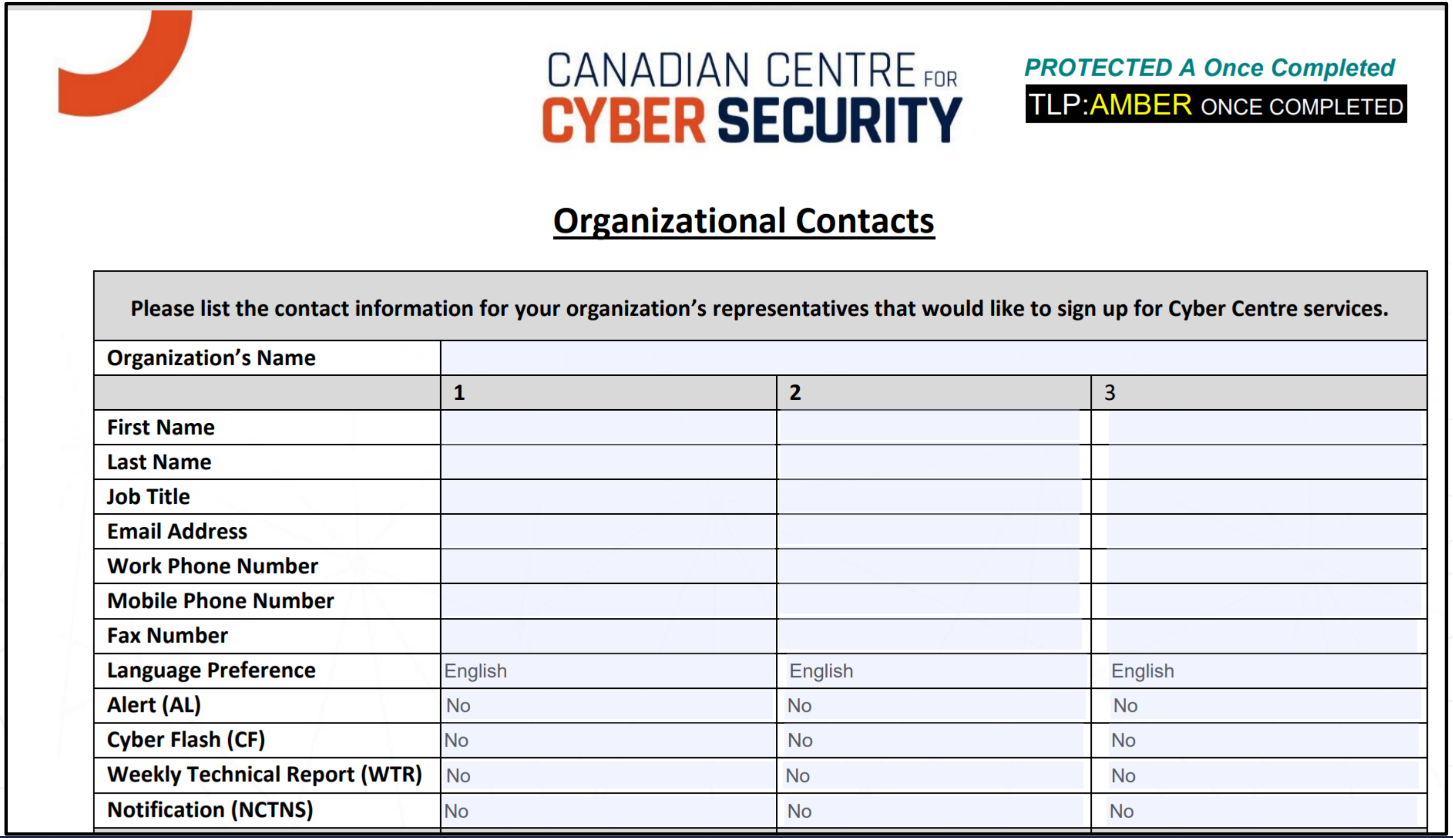
Start reporting

Or, I am an individual or small or medium organization:

For information and guidance on a cyber incident, please select from the topics below

- ► Ransomware, other cybercrime, fraud and scams
- ► Spam
- ► Social media
- ► Child exploitation
- ► Online threats related to extremism, terrorism, espionage, or serious violence

IN SUMMARY: SERVICE ONBOARDING FORM



CANADIAN CENTRE FOR CYBER SECURITY

PROTECTED A Once Completed

TLP:AMBER ONCE COMPLETED

Organizational Contacts

Please list the contact information for your organization's representatives that would like to sign up for Cyber Centre services.

Organization's Name			
	1	**2**	3
First Name			
Last Name			
Job Title			
Email Address			
Work Phone Number			
Mobile Phone Number			
Fax Number			
Language Preference	English	English	English
Alert (AL)	No	No	No
Cyber Flash (CF)	No	No	No
Weekly Technical Report (WTR)	No	No	No
Notification (NCTNS)	No	No	No

CONNECT WITH US
SUIVEZ-NOUS

✉ contact@cyber.gc.ca

🌐 www.cyber.gc.ca

@cybercentre_ca

DISCUSSION