

Wendy Young

Cyber Security 101 for Manufacturers

Cyber Security 101 for Manufacturers Round Table

Join us next **Thursday December 3rd at 10am EST**
for a round table discussion on Cyber Security for
Manufacturers.

We'll be discussing several of the strategies from our
presentation today by Wendy Young and the CCCS,
sharing best practices and strategies to ensure the
long-term resilience of manufacturing in Canada.

This will be a facilitated discussion, and is open to
senior manufacturing leaders.

Watch your email for further details, and to register!



Manufacturing is being disrupted around the world

Intense competition

Personalized customer expectations

Stringent regulatory environments

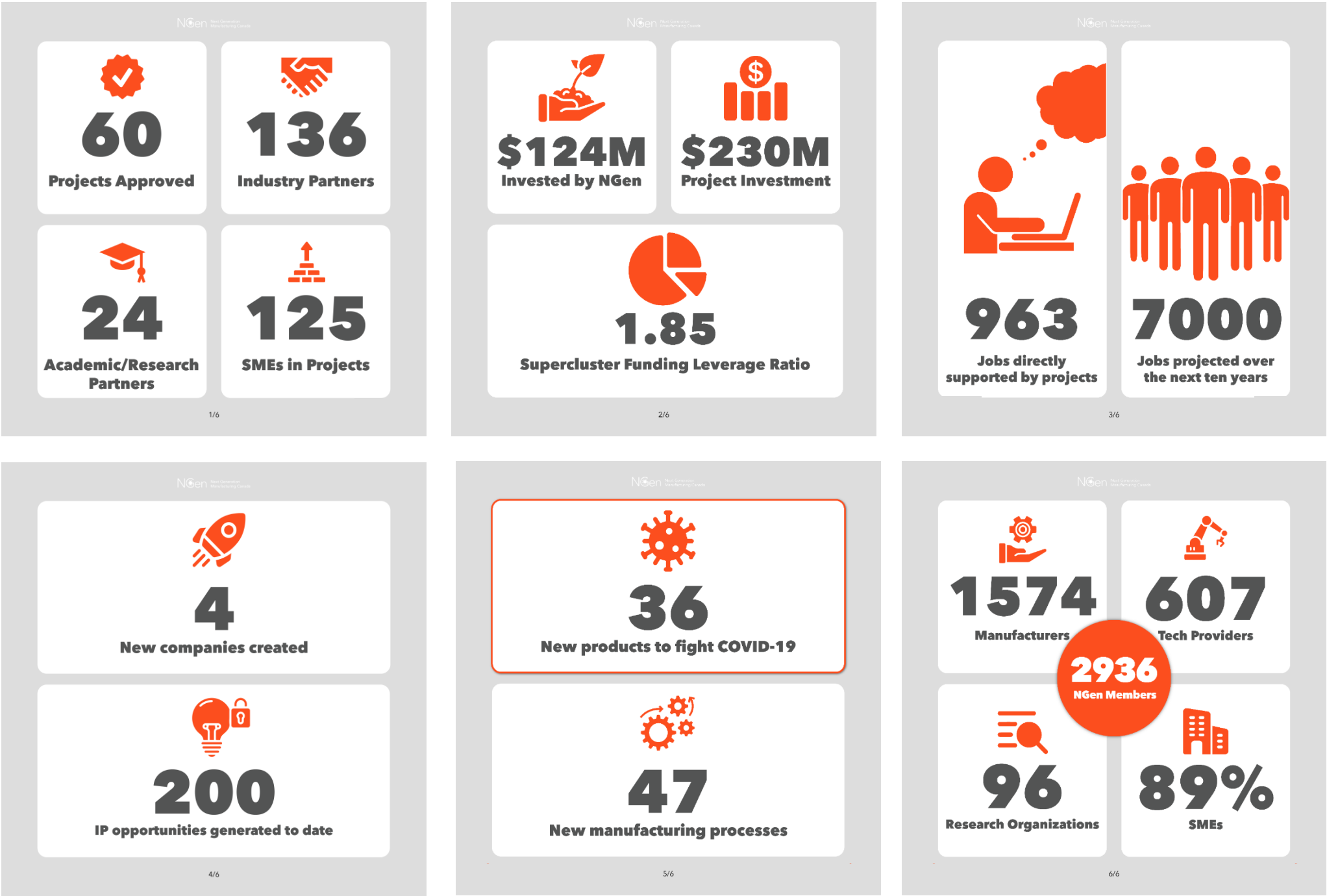
Rapid advances in technology

**Canadian Manufacturing is well-positioned to
take advantage of these new opportunities**

About NGen

- Next Generation Manufacturing Canada (NGen) leads Canada's Advanced Manufacturing Supercluster
- Committed to building world-leading advanced manufacturing capabilities in Canada
- Supporting and strengthening collaboration across Canada's advanced manufacturing ecosystem
- Supporting skills development and advanced manufacturing management capabilities
- Co-investing in collaborative, industry-led projects that have the potential to create unique competitive advantages for Canadian manufacturing

Our Impact



Risks facing Canadian Manufacturers in today's Cyber World

- **Ransomware**
- **Data leakage**
- **Insider threat**
- **Plug-n-play devices with no security standards**

Strike a balance between acceptable risk and the cost of mitigation strategies

Top 4 Strategies

Incident Response Plan

Know your assets

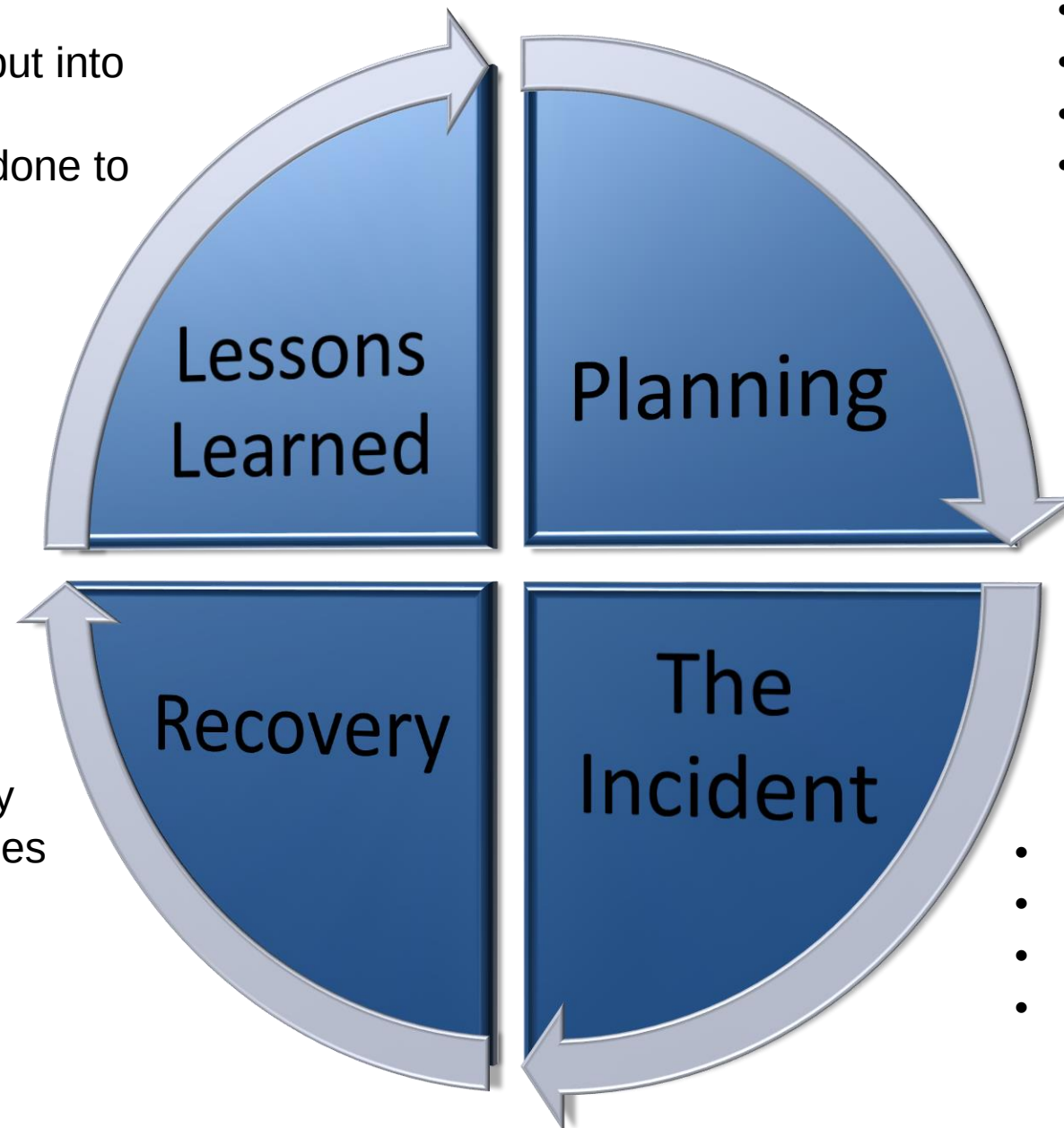
Protect your assets

Train your employees

Implement Incident Management...

- Review the incident
- Have all controls been put into place?
- What could have been done to stop the incident?

- Define your Team
- Conduct a BIA
- BCP plans
- DR plans



- Put BCP plans into play
- Start restoration activities
- Communication to the business critical
- Restore systems

- Triage and investigate
- Contain the exposure
- Know who to contact
- Know what to inform

Know your Assets...



Data

- Intellectual Property
- Customer information
- PII – personal identifiable information

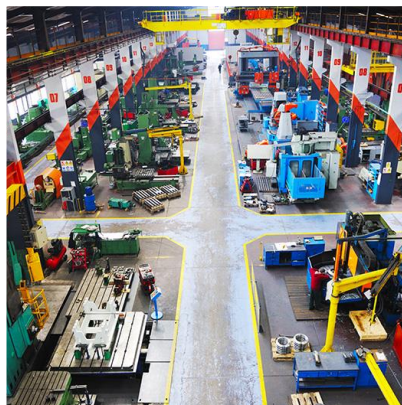
People

- Developed Business Process
- Unique knowledge
- Key players in the organization



Facilities

- Critical Production systems
- Unattended office space



Technology

- VPN
- Shop Floor Reporting
- PLC Programming
- Email & Communications

People

- Third Parties
- Employees
- Customers

Process

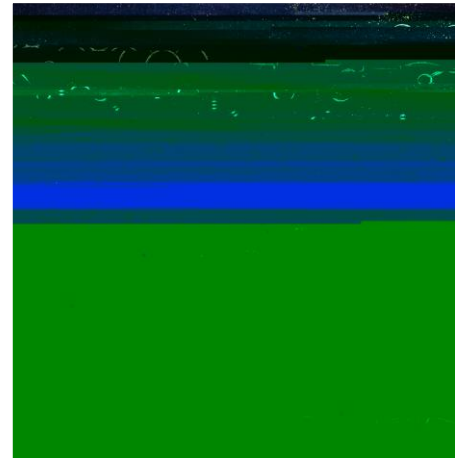
- Supply Chain
- Third Party connected Systems

Protect your assets....



Data/Systems

- Automatically patching operating systems and applications
- Ensure Backup and Encryption Services



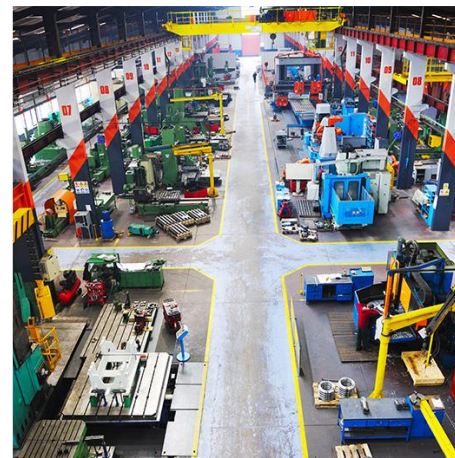
People

- Documented Business Process
- Cyber Security Awareness Training
- Use of strong authentication

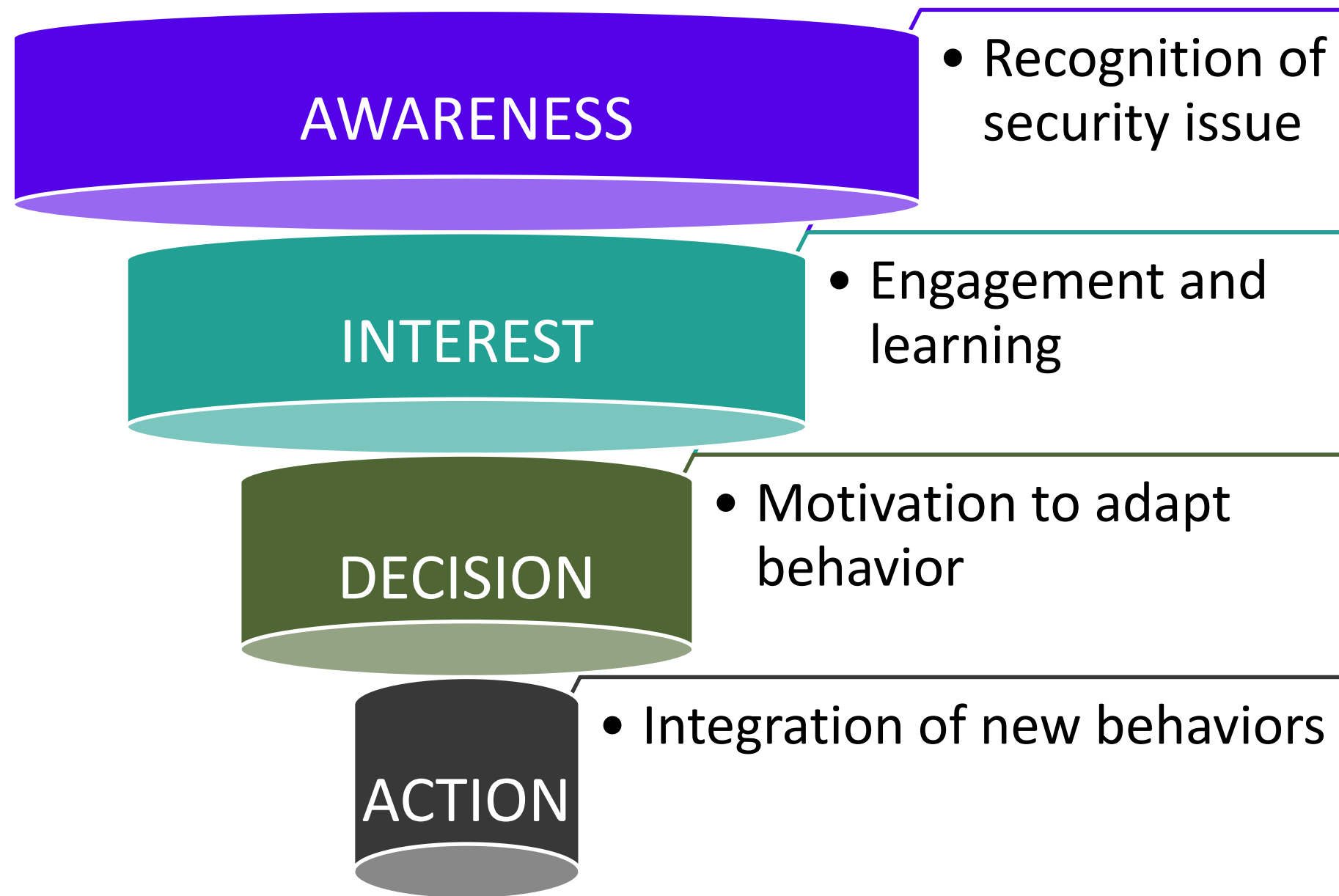


Facilities

- Physical Security-Cameras
- Controlled access-card/biometrics



Training...



Top 4 Strategies

Incident Response Plan

Know your assets

Protect your assets

Train your employees

CANADIAN CENTRE^{FOR} **CYBER** SECURITY

Cyber Center Services Briefing
November 2020

© Government of Canada

This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.



Canadian networks need to be **secured** from adversaries and personal information of Canadians must be **protected**.

Securing these systems is not simply a matter of operational efficiency; it is a matter of **national security**, **sovereignty** and **privacy protection**.

CSE'S ROLE IN CYBER SECURITY



CYBER SECURITY
LEAD IN CANADA



ACCESS TO UNIQUE
FOREIGN INTELLIGENCE



AHEAD OF
EMERGING THREATS



MONITOR GC SYSTEMS
24/7 FOR CYBER THREATS



SAFEGUARDS CANADA'S
MOST IMPORTANT INFORMATION



CANADIAN CENTRE FOR
CYBER SECURITY | CENTRE CANADIEN POUR LA
CYBERSÉCURITÉ

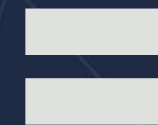
Information
Technology
Security (CSE)



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 critical non-Government networks designated as being of importance to Canada.

CYBERSECURITY AND INFORMATION ASSURANCE



DEFEND IMPORTANT NON-GOVERNMENT OF CANADA NETWORKS

Upon request, deploy CSE's cybersecurity tools on non-government systems

Remove legal barriers to sharing cyber threat information and mitigation advice

WHO WE SERVE

We welcome partnerships that help build a stronger, more resilient cyber space in Canada. We hold unclassified, multi-purpose spaces for the joint use of government, private industry and academia.

We are the centralized voice and resource for senior leadership in government on cyber security operational matters.

We are the primary federal government point of contact on cyber security operational matters for external partners, including incident response and coordination.

We are the single authoritative source of technical cyber security expertise to support lead agencies in their policing, security and intelligence work.

We inform, communicate, and educate Canadians about cyber security issues by providing clear, practical advice backed up by unique expertise and insight.

THE CYBER CENTRE VISION AND MISSION

VISION - *OUR PURPOSE*

A SECURE DIGITAL CANADA

MISSION - *OUR PROMISE*

PROTECT

Safeguard
Canada with
advanced cyber
security
capabilities.



INFORM

Provide trusted
and authoritative
cyber security
advice and
guidance for
Canada.



EMPOWER

Strengthen
Canada's cyber
security capacity
through
collaboration,
innovation, and
partnerships.



The COVID-19 crisis has provided new opportunities for cyber attacks.

Cybercrime will continue to target many sectors, jeopardizing R&D efforts

State sponsored cyber espionage directed at Canada will continue to attempt to steal Canadian intellectual property and disrupt progress



CYBER THREAT ACTIVITY IN A HIGHLY DISTRACTED WORLD

UNCLASSIFIED // TLP AMBER



COVID-19-Themed Lures (expected to rise)

Communications with COVID-19 as a theme and/or as an attachment or impersonating government (Canadian Emergency Response Benefit, etc) or institutions (Health Canada or World Health Organization)



Ransomware Targeting of Healthcare and Medical Research Facilities

Compromising of operations, equipment supply, research and healthcare data (leaking of victim documentation when ransom demands not met)



COVID-19 Online Influence Campaigns

Spreading falsehoods and fomenting greater skepticism of official figures and statements regarding the COVID-19 pandemic

What this means is that where you would have seen your Inbox filled with phishing attempts disguised as a bank deposits or tax returns, you are now seeing phishing attempts related to fraudulent Emergency Relief Benefits Payments or PPE availability

Our Services

1. Leverage our Advice and Guidance
2. Complete the Canadian Cyber Security Tool
3. Subscribe to Cyber Alerts
4. Leverage Cyber Center Defense Tools
5. Join our Community Calls

1. Leverage CCCS Advice and Guidance: Publications



Cyber Threats

- National Cyber Threat Assessment
- Cyber Threat Bulletin: Impact of COVID-19 on Cyber Threat Activity

VISIT: cyber.gc.ca

for more publications

Implementing Cyber Security

- Baseline security Controls for Small Medium Organizations
- Rethink your Password Habits to Protect your Accounts from Hackers
- Secure Your Accounts and Devices with Multi-Factor Authentication
- Cyber Security Best Practices: Contracting With Managed Service Providers
- Ransomware: How to Prevent and Recover
- Protect Your Organization from Malware
- Don't take the bait: Recognize and avoid phishing attacks

COVID-19 Related

- Focused Cyber Security Advice and Guidance During COVID-19
- Cyber Hygiene for COVID-19
- Cyber Threat Bulletin: Impact of COVID-19 on Cyber Threat Activity
- Security Tips for Organizations With Remote Workers

FOCUSED CYBER SECURITY

ADVICE AND GUIDANCE DURING COVID-19

SEPTEMBER 2020 | ITSAP.00.150



The COVID-19 pandemic has proven to be an extremely disruptive event, affecting all components of society. The IT world is not immune. The pandemic has forced both public and private sectors to rethink how, when, and where work is performed. Traditional models of office versus home-based work environments have been completely inverted; in many cases, most employees are now working remotely. This inversion has caused IT management, implementers, and clients to scramble to adapt to a new way of working. Unfortunately, this rapid transformation presents both new and unique opportunities for threat actors to take advantage of. The entire IT hierarchy, from management to client, must be made explicitly aware of this fact and take every precaution possible.

The Canadian Centre for Cyber Security (Cyber Centre) has created a valuable collection of advice and guidance products, many of which are now more relevant than ever. To assist you during this disruptive time, we curated a selection of our products and organized them by area of interest. We hope this helps, and, as always, we are here to assist you whenever possible. **You may find our complete list of guidance products at: cyber.gc.ca/**

IT MANAGEMENT GUIDANCE

- [Top 10 IT Security Actions: #6 Provide Tailored Cyber Security Training \(ITSM.10.093\)](#)
- [Cloud Security Risk Management \(ITSM.50.062\)](#)
- [Top 10 IT Security Actions to Protect Internet-Connected Networks and Information \(ITSM.10.189\)](#)



IT IMPLEMENTER GUIDANCE

- [Implementation Guidance: Email Domain Protection \(ITSP.40.065\)](#)
- [Cyber Centre Data Centre Virtualization Report: Best Practices for Data Centre Virtualization \(ITSP.70.010\)](#)
- [Steps to Address Data Spillage in the Cloud \(ITSAP.50.112\)](#)
- [Security Tips for Organizations with Remote Workers \(ITSAP.10.016\)](#)
- [Using Virtual Desktop At-Home and In-Office \(ITSAP.70.111\)](#)
- [Security Considerations for Mobile Device Deployments \(ITSAP.70.002\)](#)
- [Protecting Your Organization Against Denial of Service Attacks \(ITSAP.80.100\)](#)



CLIENT AWARENESS

- [Don't Take the Bait: Recognize and Avoid Phishing Attacks](#)
- [Cyber Hygiene for COVID-19](#)
- [Video Teleconferencing ITSAP.10.216](#)
- [How Updates Secure Your Device \(ITSAP.10.096\)](#)
- [Secure Your Accounts and Devices with Multi-Factor Authentication \(ITSAP.30.030\)](#)
- [Protect Your Organization From Malware \(ITSAP.00.057\)](#)
- [Virtual Private Networks \(ITSAP.80.101\)](#)
- [Ransomware: How to Prevent and Recover \(ITSAP.00.099\)](#)
- [Rethink Your Password Habits to Protect Your Accounts from Hackers \(ITSAP.30.036\)](#)
- [Best Practices for Passphrases and Passwords \(ITSAP.30.032\)](#)
- [Using Bluetooth Technology \(ITSAP.00.011\)](#)
- [Spotting Malicious Email Messages \(ITSAP.00.100\)](#)



ADDITIONAL INFORMATION

- [RSS feed](#)
- [Alerts and Advisories](#)
- [Contracting with Managed Service Providers](#)
- [Canadian Shield—Sharing the Cyber Centre's Threat Intelligence to Protect Canadians During the COVID-19 Pandemic](#)



Traditional models of office vs. home-based work environments have been completely inverted.

Need help or have questions? Want to stay up to date and find out more on all things cyber security? Visit the Cyber Centre website at cyber.gc.ca

2. Canadian Cyber Security Tool



2. Canadian Cyber Security Tool (CCST)

What is it:

On-line, 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 serve organization with appropriate guidance, services and support

Tool reports

Advice and guidance related to each of 6 cyber domains
Entity specific score and peer based comparisons



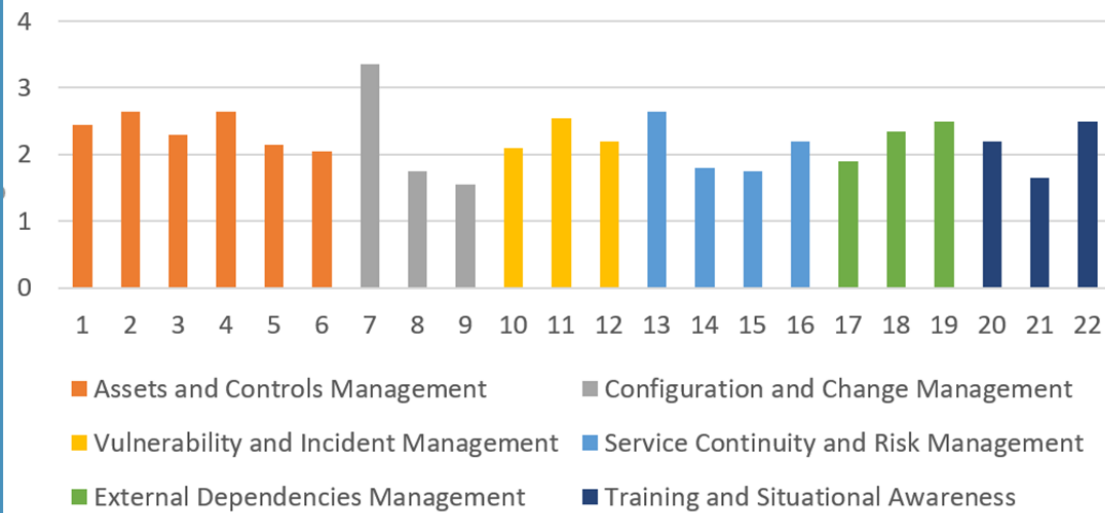
Canadian Cyber Security Tool

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

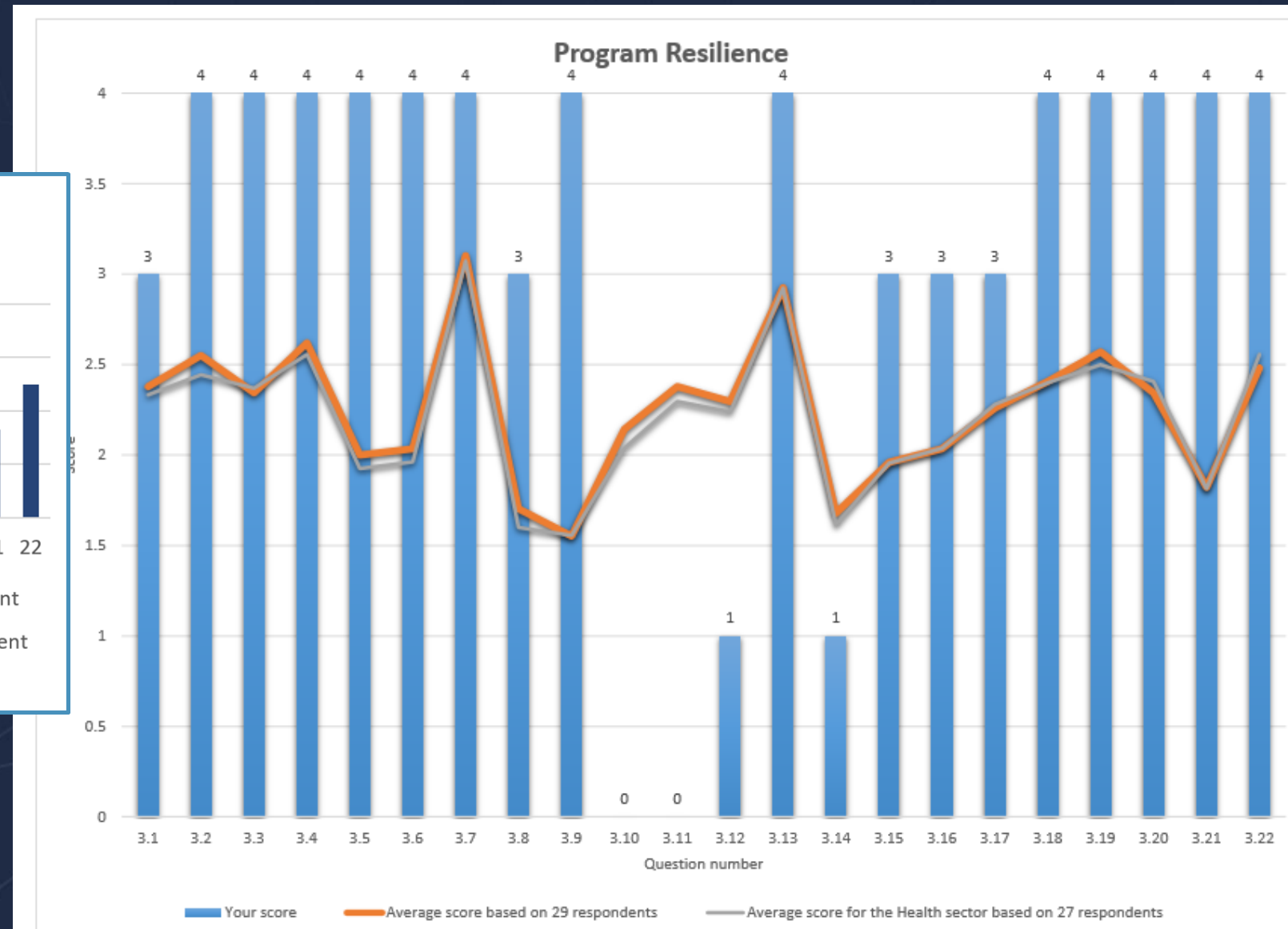
2. Canadian Cyber Security Tool (CCST)

Ability to compare to peers

Health Sector maturity - average answer per question & domain (CCST 2020)



To participate: email
alexandre.perusse@cyber.gc.ca



3. Subscribe to Cyber Alerts

Alerts, Flashes WTR



ALERTS

Pro-active Notifications on New Cyber Threats

ALERTS

Microsoft Security Advisory



Number: AV20-308

Date: 21 August 2020

On 19 August 2020 Microsoft released an out-of-band security update to address vulnerabilities in the following versions of Windows:

- Windows 8.1
- Windows RT 8.1
- Windows Server 2012 R2

<https://support.microsoft.com/en-ca/help/4578013/security-update-for-windows-8-1-rt-8-1-and-server-2012-r2>

An actor with execution rights on affected systems could exploit a memory handling flaw in Windows Remote Access to escalate privileges.

The Cyber Centre encourages users and administrators to review the provided web link and apply the necessary updates as soon as possible.



Email Alerts



Cyber Centre
Website

<https://www.cyber.gc.ca/en/alerts-advisories>

CYBER FLASH

Urgent Notifications on Active Security Issues

Actionable information sent to describe an immediate security issue.

TITLE

Active exploitation leading to PoisonPlug / ShadowPad malware

SUMMARY

The Cyber Centre has become aware of...

DETAILS

SUGGESTED ACTIONS

INDICATORS OF COMPROMISE



Email Alerts

WEEKLY TECHNICAL REPORTS

Reports on activities and incidents

Weekly summaries of cyber activities, incidents and indicators of compromise (IOCs) related to the GoC and Critical Infrastructure.



4. Leverage Cyber Defence Tools

NCTNS, AVENTAIL

NCTNS NOTIFICATIONS

Cyber Threats Seen on Your IP Space

*Sent to you when a **sign of compromise** or a vulnerable service is seen on **your IP space** to notice cyber threats faster and **better protect your organization**.*

Vetted data to ensure quality and a low percentage of false positive

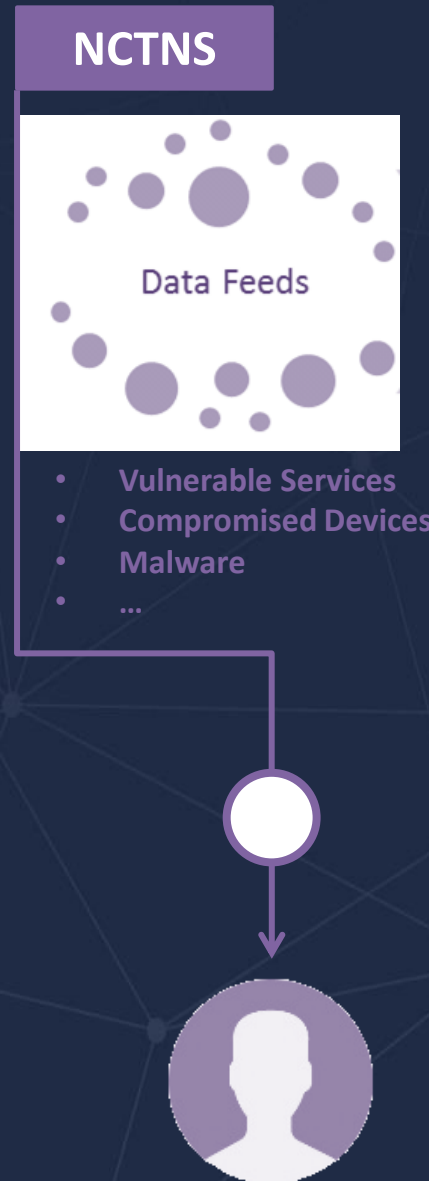


Email Notifications



API
(In development)

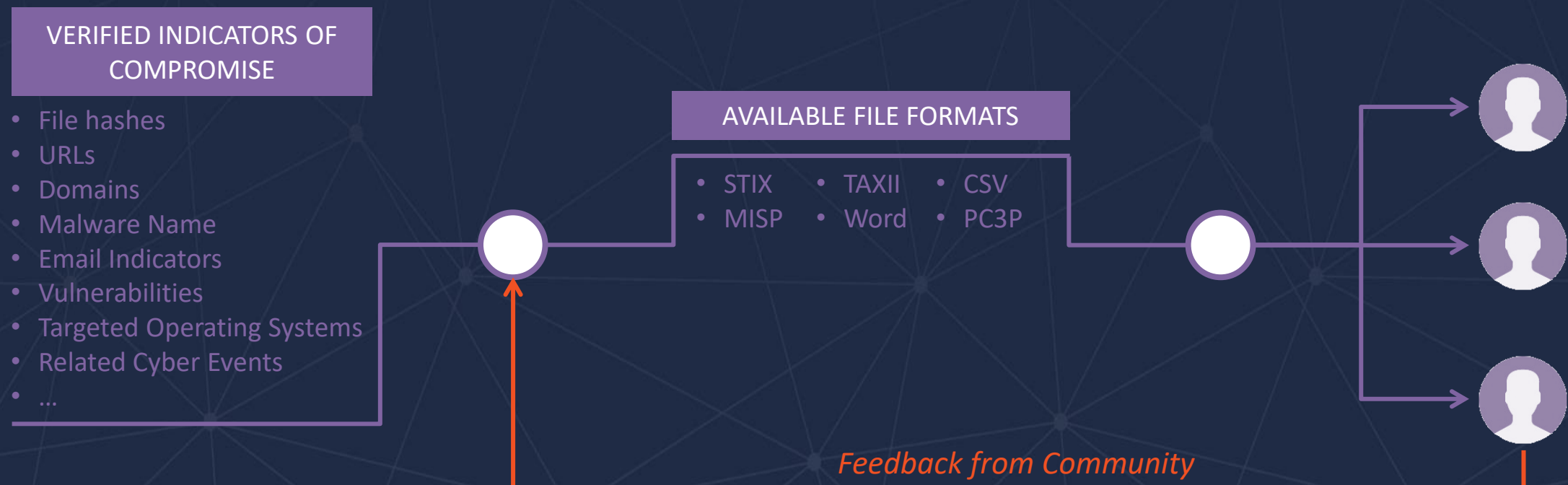
- Accept the Terms of Use
- Provide contact information for the person who will be receiving and using the notifications
- Share the IP range specific to your organization



AVENTAIL

Real-time IOC sharing

*Sharing relevant and **verified information** on Indicators of Compromises (IoCs) at **machine speed***



- Accept the Terms of Use or sign a Non-Disclosure Agreement

Community Calls

...coming soon for the Manufacturing Sector!



5. SECTOR COMMUNITY CALL

Purpose Is To Share Sector Relevant Cyber Expertise

Build Community of Trust

Provide Situational Awareness

Offer at Regular Cadence (early 2021)



To participate: email alexandre.perusse@cyber.gc.ca

Other Services and Products



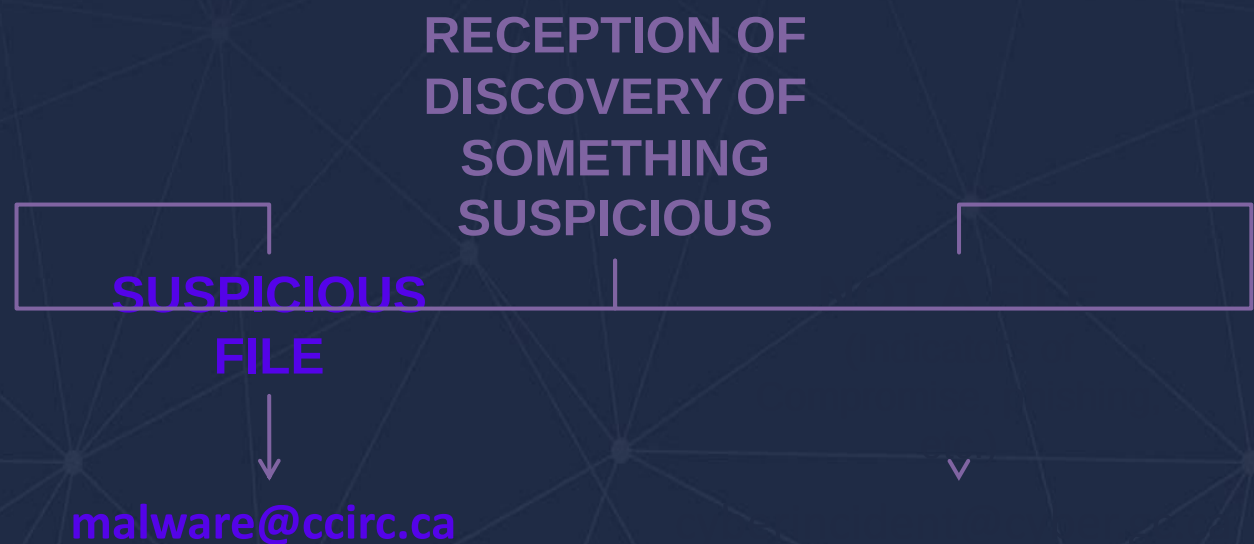
MALWARE INTAKE

To Email Suspicious Files to the Cyber Center for Analysis

Cyber Centre *malware analysts* and *automated systems* assess whether files are malicious or not



Results of analysis
sent by email



- Files will be detonated on the Internet
- Unless otherwise specified, resulting IoCs will be shared with the community without attribution
- Files have to be UNCLASSIFIED (NO PB or

WORKING FROM HOME – WHAT YOU CAN DO...

UNCLASSIFIED // TLP AMBER

Use corporate devices assigned to you by your employer for work whenever possible

If you use personal devices or accounts:

Secure Your Accounts and Devices with Multi-Factor Authentication

Keep your devices in sight when you're working in a public location and report a lost or stolen device immediately

Lock your computer when you take breaks and leave your computer

Updated your devices regularly and when asked by your system administrator

Use secure network connections, avoid public Wi-Fi



WHAT ORGANIZATIONS CAN DO TO PROTECT THEMSELVES?



WHAT TO LOOK AT NEXT FOR YOUR ORGANIZATION

Internal Governance

Is cyber security a maintained priority?

Investment

How much are you focusing resources on cyber security?

Resilience

How prepared are you for a cyber attack?

Supply Chain

Do all components of your supply chain have adequate cyber protection?

Collaboration

Work with commercial cyber experts and leverage GC advice and guidance

WHO TO CONTACT AND WHEN

CANADIAN CENTRE FOR
CYBER SECURITY



Reporting cyber incidents
contact@cyber.gc.ca

cybertip!ca®



Child exploitation, trafficking of child porn, child sextortion, etc.



Royal Canadian Mounted Police

Gendarmerie royale du Canada



Cybercrime: Ransomware, Money Laundering, Identity Theft, Cyberbullying, etc.



If you receive personal phishing email, telemarketing, tax scam

CONNECT WITH US

 contact@cyber.gc.ca

 www.cyber.gc.ca

 [@cybercentre_ca](https://twitter.com/cybercentre_ca)

Cyber Centre Publications :

<https://cyber.gc.ca/en/publications>

Cyber Center Alert & Advisories:

<https://cyber.gc.ca/en/alerts-advisories>

To report fraud:

Canadian Anti-Fraud Centre

1-888-495-8501

www.antifraudcentre-centreantifraude.ca

To report a cybercrime:

Local police or

Royal Canadian Mounted Police

www.rcmp-grc.gc.ca

To report a cyber incident

Canadian Center for Cyber Security

 cyberincident@cyber.gc.ca

Q & A

What Cybersecurity topics would you like to see in the future

What's Next Thought Leadership → December 10th Event

Join us **Thursday December 10th at 11am EST** for our next *What's Next Through Leadership* series event.

**Topic: Building World Class Supply Chains Through
Operational Excellence**

We'll be joined Jay Davis, Supply Chain Excellence Leader for NGen to discuss strategies to build stronger and more resilient Supply Chains.

Watch your email for further details, and to register!





Today's presentation will be made available on our site. Visit us @ NGen.ca.

Thank You

**Join Canada's Advanced Manufacturing
Supercluster**

Membership is free

Join as an Organizations or Individuals

Become a member today

www.ngen.ca/join