CANADIAN CENTRE FOR CYBER SECURITY

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Workshop: National Cyber Threat Assessment (NCTA) & Cyber Security Readiness Goals (CRG)

VIPSS – March 2025

Our Role in Cyber Security

- We use our expertise to keep safe the information and systems that Canadians rely on every day.
- We work to protect and defend the country's valuable cyber assets and lead Canada's federal response to cyber security events.
- We raise Canada's cyber security bar so Canadians can live and work online safely and with confidence.

Canada's national cryptologic agency

Canada's technical authority on cyber security

Agenda

National Cyber Threat Assessment (NCTA)

Cyber Security Readiness Goals (CRGs)

Walkthrough scenarios – Threats + Mitigations

Cyber Centre Resources

National Cyber Threat Assessment (NCTA) – Threat overview

NCTA

High-level threat activities

Threats to Critical Infrastructure

NCTA 2025-2026

- NCTA 2025-2026 provides the Canadian public with CSE's current insights on the state and non-state cyber threat actors conducting malicious cyber threat activity against Canada and how we assess the cyber threat landscape evolving in the next 2 years.
- **Structure:**
  - **Section 1** – Cyber Threat from State Adversaries
  - **Section 2** – Cybercrime Threats
  - **Section 3** – Trends Shaping Canada's Cyber Threat Landscape
- **Key narratives:**
  - Canada is confronting an expanding and complex cyber threat landscape with a growing cast of malicious actors.
  - Canada's state adversaries are becoming more aggressive in cyberspace.
  - Cybercrime remains a persistent threat to Canadian individuals, organizations, critical infrastructure, and all levels of government.

Key Judgements

Canada's state adversaries are using cyber operations to disrupt and divide.

The PRC's expansive and aggressive cyber program presents the most sophisticated and active state cyber threat to Canada.

Russia's cyber program furthers Moscow's ambitions to confront and destabilize the West, including Canada.

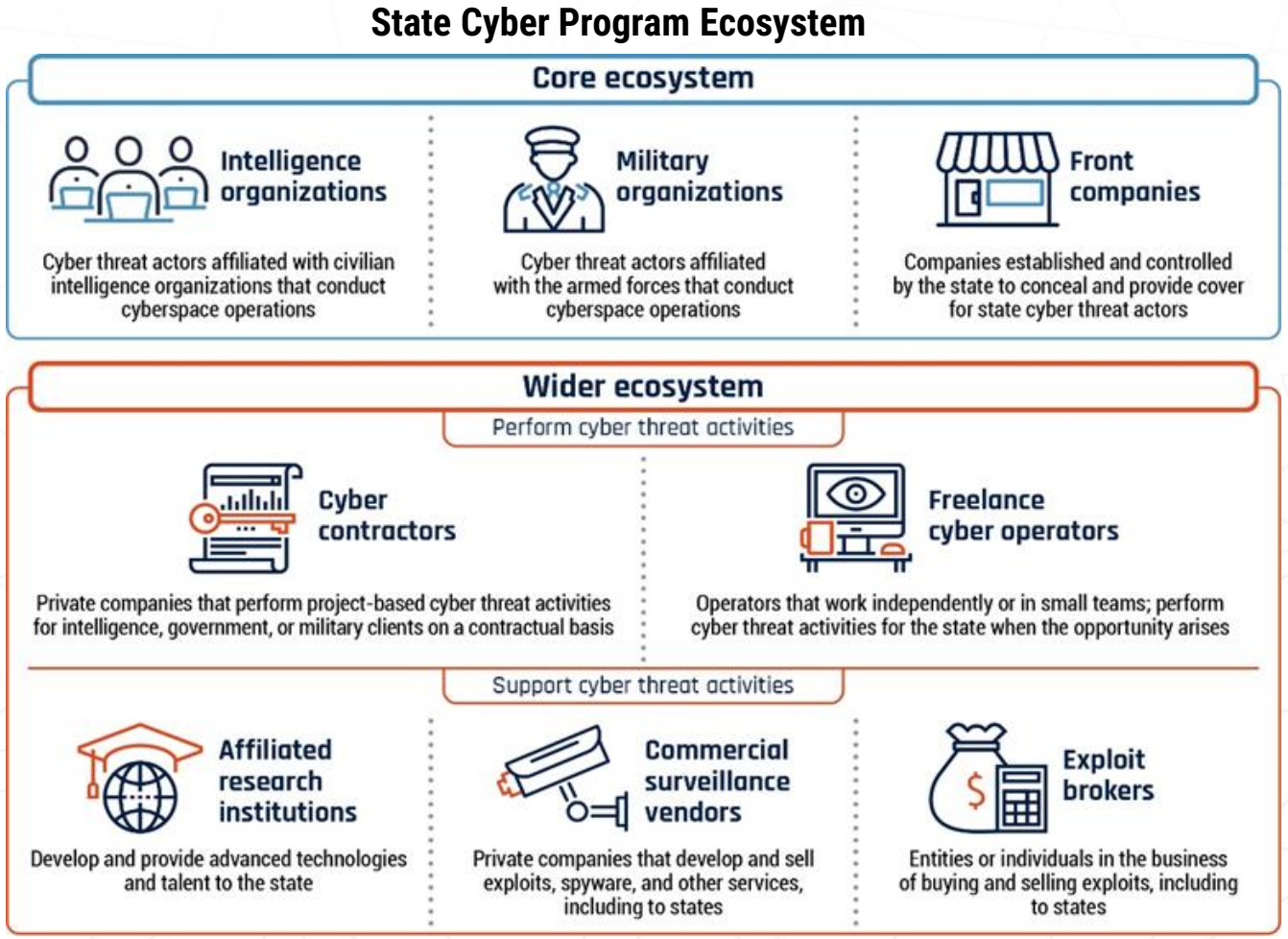
Iran uses its cyber operations to coerce, harass, and repress its opponents, while managing escalation risks.

The Cybercrime-as-a-Service (CaaS) business model is almost certainly contributing to the continued resilience of cybercrime in Canada and around the world.

Ransomware is the top cybercrime threat facing Canada's critical infrastructure.

Cyber Threat from State Adversaries

- Canada is confronting a complex state cyber ecosystem
  - Strategic Adversaries
  - Emerging Cyber Programs
  - Wider Cyber Ecosystem

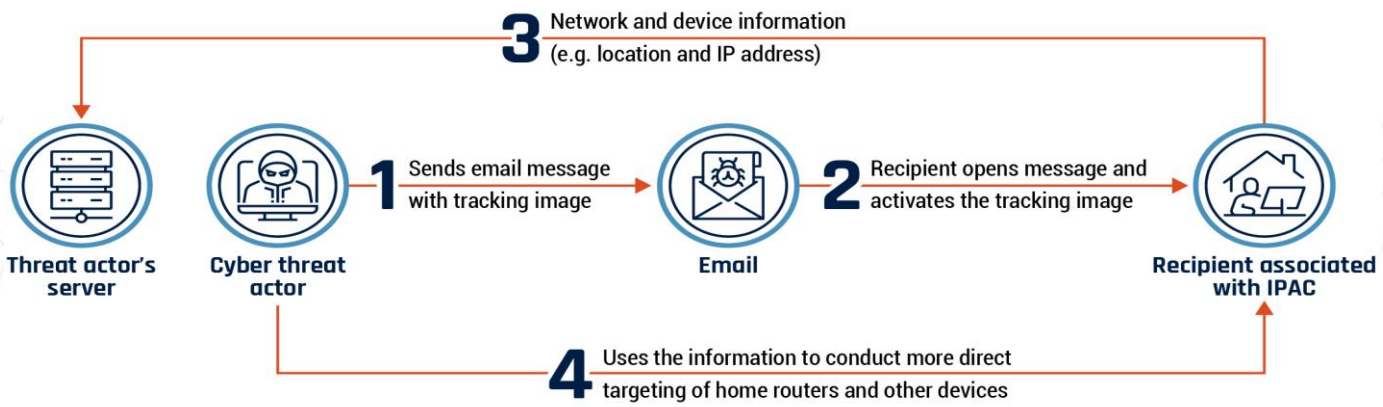


Cyber Threat from State Adversaries

In Focus: People's Republic of China

- PRC cyber actors conduct cyber espionage against all levels of government and public officials in Canada.
- PRC cyber-enabled transnational repression targets individuals in Canada.
- PRC cyber program almost certainly supports China's espionage activities against Canada's private sector and innovation ecosystem for competitive advantage.
- PRC pre-positioning within U.S. critical infrastructure increases risk to Canada.

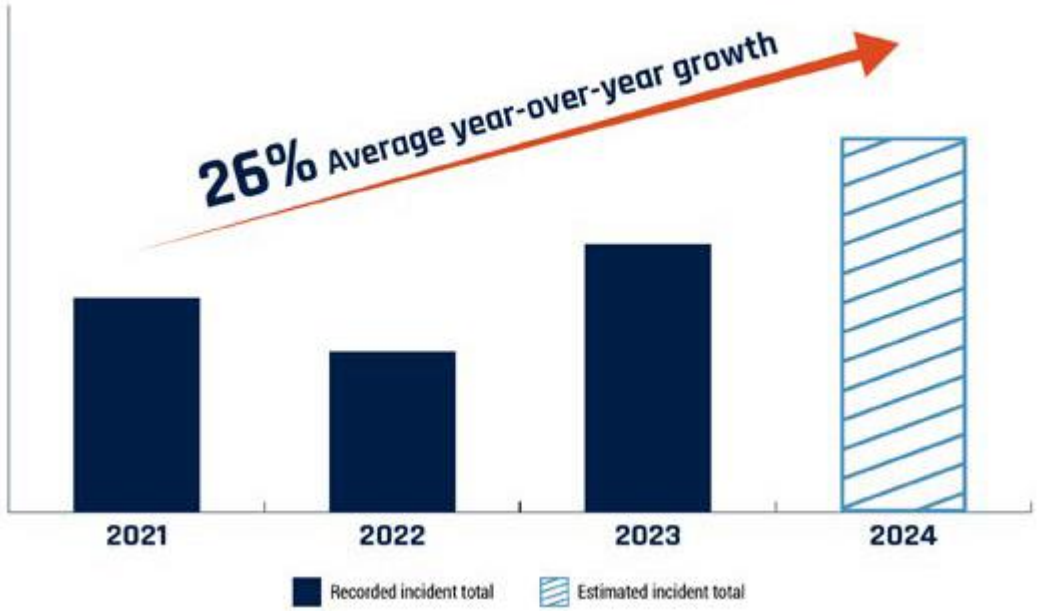
PRC Email Operation Against Members of Inter-Parliamentary Alliance on China



Ransomware: A Growing Threat Impacting CI

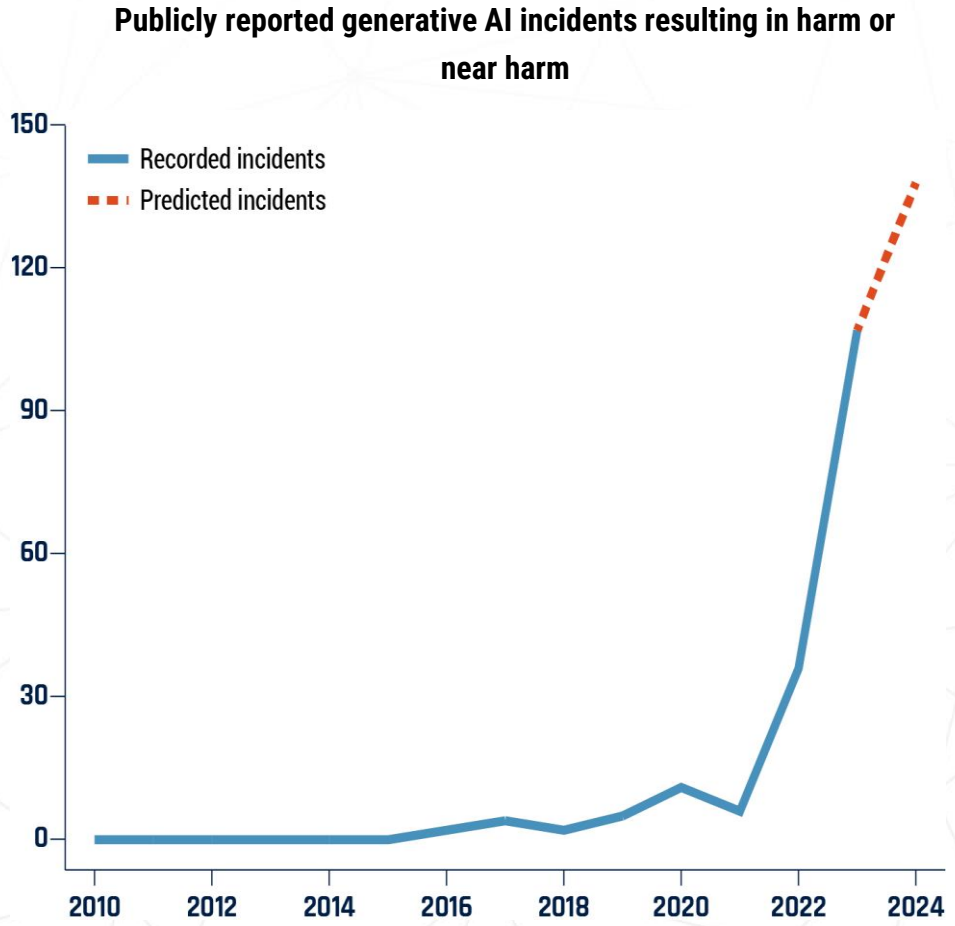
- Ransomware is almost certainly the top cybercrime threat facing Canada's critical infrastructure.
  - Specifically, ransomware incidents impacting healthcare are on the rise.
- Ransomware actors are using "big game hunting" and elevating extortion techniques to extract larger ransom payouts.
- Top threat stems from Ransomware-as-a-Service groups.
- Ransomware actors constantly refine their tactics to maximize profits.

Relative growth from 2021 of Canadian ransomware incidents known to the Cyber Centre



Trends Shaping Canada's Cyber Threat Landscape

1. Artificial intelligence technologies are amplifying cyberspace threats
2. Cyber threat actor tradecraft is evolving to evade detection
3. Geopolitically inspired non-state actors are creating unpredictability
4. Vendor concentration is increasing cyber vulnerability
5. Dual-use commercial services are in the digital crossfire.



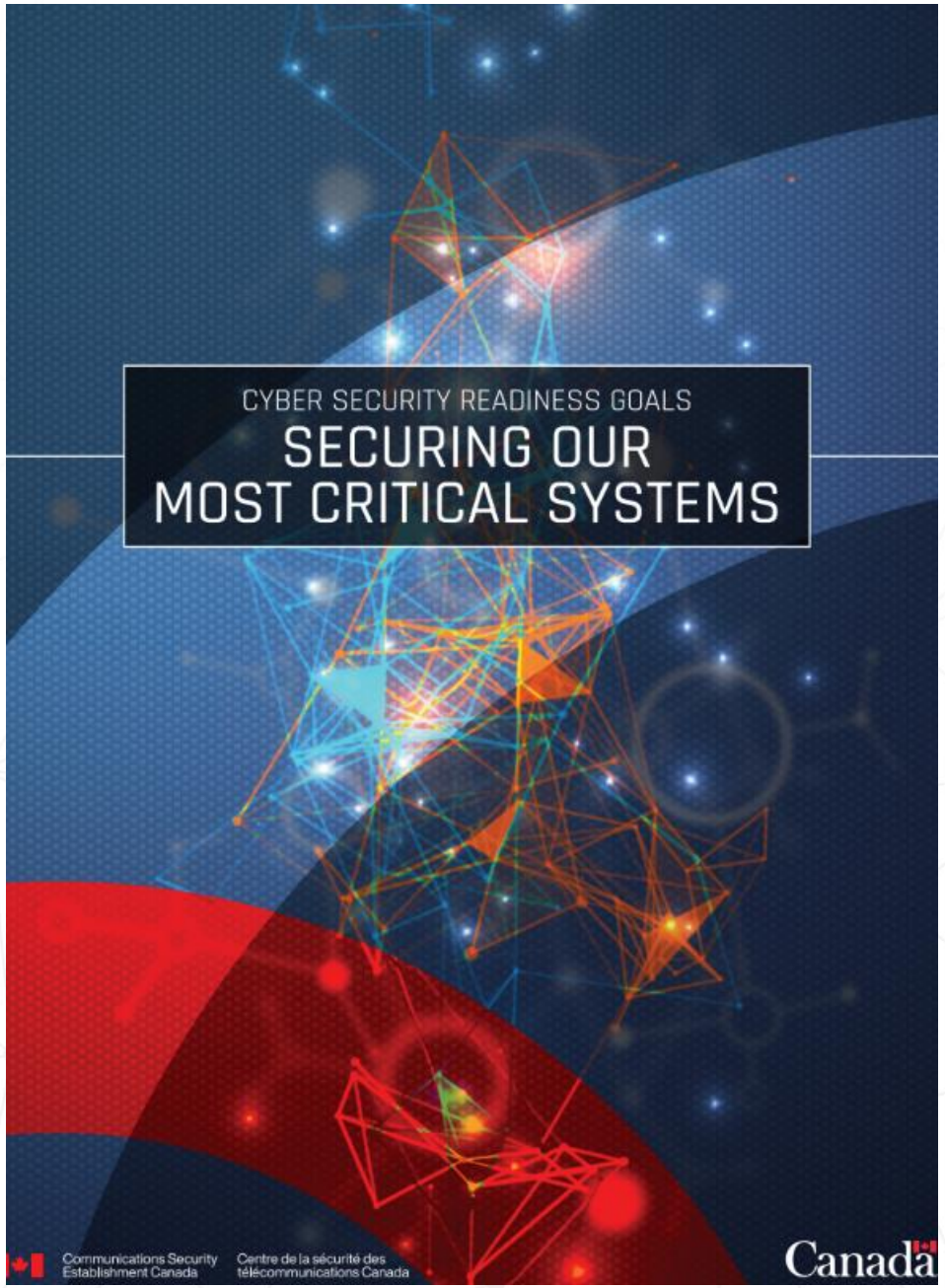
Cyber Security Readiness Goals (CRGs)

What are the CRGs

The CRG Toolkit

What are the Cyber Security Readiness Goals (CRGs)

- The CRGs are
  - realistic, but not exhaustive
  - cross-sector cyber security goals
  - aligned with CISA's CPGs and Canadian requirements.
- The CRGs include
  - a narrative section, background and context
  - **toolkit with 36 goals**.
- Moving forward the CRGs will
  - be regularly updated
  - be aligned to mitigate new and emerging threats
  - evolve with the ever-changing legislative landscape.



How the CRGs came to be

Critical infrastructure (CI) services and systems are increasingly vulnerable due to their reliance on complex networks of interdependent digital services, assets, and facilities.

The GC, through its **National Cyber Security Strategy (NCSS),** is committed to enhancing the security and resilience of critical cyber systems and to exercising leadership in cyber security to foster collaboration.

CI owners and operators in Canada have unique requirements, but also operations that overlap international borders.

Not just another another tool

The CRGs are …

- ☑ actions to help Canadian CI owners and operators enhance their cyber security
- ☑ the minimum benchmark for CI organizations
- ☑ complementary to existing Cyber Centre advice and guidance publications

CRG Toolkit

IDENTIFY [1]

Asset inventory and network topology [1.0]

Outcome Better identify known, unknown, and unmanaged assets, including web-facing assets for the cloud and data assets. Your organization can then more rapidly detect and respond to new vulnerabilities and maintain service continuity.

Recommended Action

Maintain a regularly updated inventory of all assets within the organization's IT (including IPv6) and OT networks (if applicable). Include in the inventory accurate documentation of network topology and identified data assets, in particular sensitive or classified information. Update this inventory on a regular basis for both IT and OT, and immediately log in the existing inventory any new asset that is integrated into the organization's infrastructure.

TTP/Risks

- Hardware Additions (T1200)
- Exploit Public-Facing Applications (T1190, ICS T0819)
- Internet Accessible Device (ICS T0883)

References

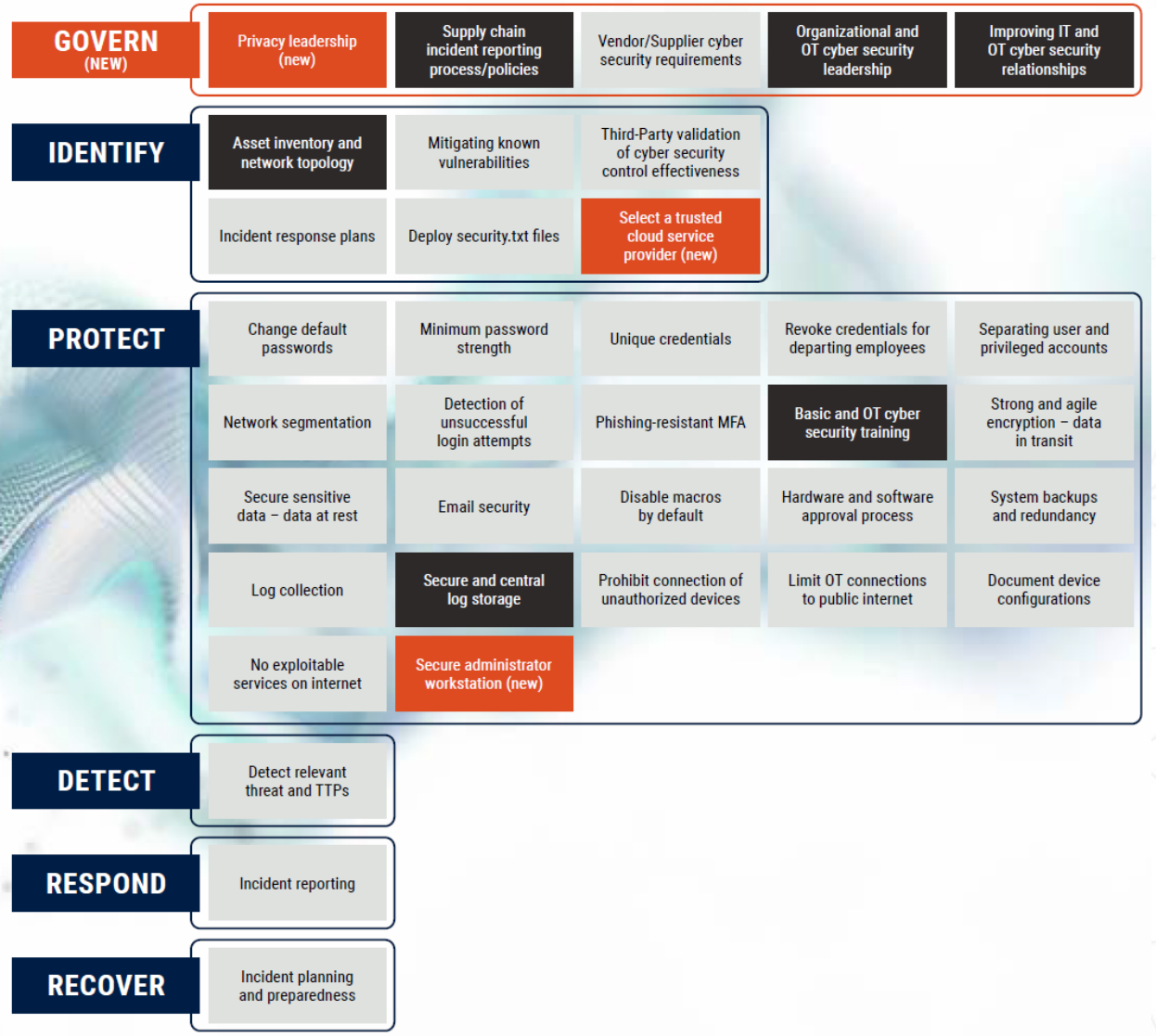
ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, DE.CM-01

Using information technology asset management (ITAM) to enhance cyber security (ITSM.10.004) (https://www.cyber.gc.ca/en/guidance/using-information-technology-asset-management-itam-enhance-cyber-security-itsm10004)

Assessment

- ○ Not Started Date: _____
- ○ Scoped Date: _____
- ○ In Progress Date: _____
- ○ Implemented Date: _____

Notes



Goal profile : Asset inventory and network topology [CRG 1.0]

Asset inventory and network topology [1.0]

Outcome

Better identify known, unknown, and unmanaged assets, including web-facing assets for the cloud and data assets. Your organization can then more rapidly detect and respond to new vulnerabilities and maintain service continuity.

Recommended Action

Maintain a regularly updated inventory of all assets within the organization's IT (including IPv6) and OT networks (if applicable). Include in the inventory accurate documentation of network topology and identified data assets, in particular sensitive or classified information. Update this inventory on a regular basis for both IT and OT, and immediately log in the existing inventory any new asset that is integrated into the organization's infrastructure.

TTP/Risks

Hardware Additions (T1200)

Exploit Public-Facing Applications (T1190, ICS T0819)

Internet Accessible Device (ICS T0883)

References

ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, DE.CM-01

Using information technology asset management (ITAM) to enhance cyber security (ITSM.10.004) (https://www.cyber.gc.ca/en/guidance/using-information-technology-asset-management-itam-enhance-cyber-security-itsm10004)

Goal profile : Phishing-resistant multi-factor authentication [CRG 2.7]

Phishing-resistant multi-factor authentication [2.7]

Outcome Add a critical, additional layer of security to protect asset accounts whose credentials have been compromised.

Recommended Action

Implement MFA for access to assets using the strongest available method for that asset (see below for scope).

MFA options ranked by strength, from high to low, are as follows:

1. Hardware-based, phishing-resistant MFA (for example, FIDO/WebAuthn or public key infrastructure (PKI) based).
2. If such hardware-based MFA is not available, then use mobile app-based soft tokens (preferably push notification with number matching) or emerging technology such as FIDO passkeys.
3. Only use MFA via SMS or voice when no other options are possible.

Ensure all IT accounts leverage MFA to access organizational resources. Prioritize accounts with highest risk, such as privileged administrative accounts for key IT systems.

Within OT environments, enable MFA on all accounts and systems that can be accessed remotely, including vendors/maintenance accounts, remotely accessible user and engineering workstations, and remotely accessible human-machine interfaces.

TTP/Risks

Brute Force (T1110)

Remote Services : Remote Desktop Protocol (T1021.001)

Remote Services SSH (T1021.004)

Valid Accounts (T1078, ICS T0859)

External Remote Services (ICS T0822)

References

PR.AA-01, PR.AA-03, PR.AA-05

Steps for effectively deploying multi-factor authentication (MFA) (ITSAP.00.105) (https://www.cyber.gc.ca/en/guidance/steps-effectively-deploying-multi-factor-authentication-mfa-itsap00105)

Secure your accounts and devices with multi-factor authentication (ITSAP.30.030) (https://www.cyber.gc.ca/en/guidance/secure-your-accounts-and-devices-multi-factor-authentication-itsap30030)

Walkthrough Scenarios

Threats + Mitigations

Group discussion

Visit the Cyber Centre website for links to the CRGs and the Toolkit:

Cyber Security Readiness - Canadian Centre for Cyber Security

Scenario : Hospital network compromised by ransomware incident

The staff at your hospital suddenly cannot access patient records, medical reports, or manage appointments. After seeking assistance from third party cyber security experts, you discover that the hospital has been compromised by a ransomware incident, and ransomware actors stole a database of medical information belonging to over 200,000 of your hospital's patients. Analysis of the incident reveals that threat actors purchased credentials obtained via infostealer* attacks from a cybercrime marketplace. This information was used to perform a password spray attack against the hospital's single factor and unpatched remote desktop protocol (RDP) services. From there, the actors were able to move laterally through the hospital network, access a server hosting sensitive patient data, and deploy their ransomware payload to encrypt and exfiltrate that data. The actors threatened to post the stolen data on their dedicated leak site (DLS) for other cybercriminals to purchase. As of now, 300 sensitive patient records have been published on the DLS.

** Infostealers are a type of malware that can exfiltrate sensitive information from a victim's systems, such as login credentials, payment data, cookies, or autofill data*

CRGs - 36 foundational goals

Scenario : Hospital network compromised by ransomware incident

Recommended mitigations

- Asset inventory and network topology [1.0]
- Mitigating known vulnerabilities [1.1]
- Unique credentials [2.2]
- Network segmentation [2.5]
- Phishing-resistant multi-factor authentication [2.7]
- Secure sensitive data: data at rest [2.10]
- System backups and redundancy [2.14]
- Detect relevant threat and TTPs [3.0]
- Incident planning and preparedness [5.0]

Scenario : State-sponsored cyber attack on wastewater facility

A state-sponsored cyber threat group using the persona "CyberR3sistance45" targeted and compromised Internet-connected programmable logic controllers (PLCs) with human machine interfaces (HMI) used in water and wastewater facilities across North America and Europe. The victims included a municipal wastewater facility that you manage. The state-sponsored cyber threat group used brute force tactics to compromise PLCs with default passwords and defaced the HMIs with the message, *"You have been hacked. Your government is bad. You are CyberR3sistance45 legal target!"*. Your facility was named in social media posts by the threat actor boasting about the attack and making exaggerated claims about its impact. At this time, it is unknown to what extent the cyber threat actors compromised the wastewater facility's network(s) and whether they intend to conduct follow-on disruptive cyber threat activity.

CRGs - 36 foundational goals

Scenario : State-sponsored cyber attack on wastewater facility

Recommended mitigations

- Incident response plan [1.3]
- Change default passwords [2.0]
- Network segmentation [2.5]
- Phishing-resistant multi-factor authentication [2.7]
- Basic and OT cyber security training [2.8]
- Limit OT connections to public Internet [2.18]
- Secure Administrator Workstation [2.21]
- Detect relevant threat and TTPs [3.0]

Scenario : State-sponsored compromised enterprise email service

In October 2024, a cloud service provider (CSP) discovered that a state-sponsored cyber threat actor had compromised its enterprise email service and had access to the cloud-based email accounts of a range of customers in Canada and elsewhere. On October 29, 2024, the CSP notified your organization, a large financial institution customer of the CSP, that you were a victim and that the threat actor had access to employee mailboxes. In the notification, the CSP stated that the state-sponsored cyber threat actor was using a stolen signing key* that the CSP had created to issue tokens that allowed access to virtually any enterprise email account. The CSP believes that the compromise may have started as early as March 2024.

** Signing keys, used for secure authentication into remote systems, are the cryptographic equivalent of crown jewels for any cloud service provider. A cyber threat actor in possession of a valid signing key can grant itself permission to access any information or systems within that key's domain. A single key's reach can be enormous and provide the threat actor with extraordinary power.*

CRGs - 36 foundational goals

Scenario : State-sponsored compromised enterprise email service

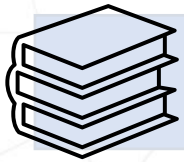
Recommended mitigations

- Mitigating known vulnerabilities [1.1]
- Incident response plan [1.3]
- Change default passwords [2.0]
- Unique credentials [2.2]
- Separating user and privileged accounts [2.4]
- Detection of unsuccessful (automated) login attempts [2.6]
- Phishing-resistant multi-factor authentication [2.7]
- Log collection [2.15]
- Detect relevant threat and TTPs [3.0]

Cyber Centre Resources

Sector-Specific Cyber Security Readiness Goals (SSGs)

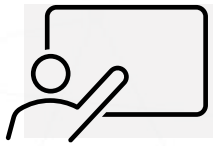
Focused cyber security guidance to assist with implementation of CRGs in critical sectors, based on the specific needs of each sector.



Cyber Centre Publications

- Security considerations for critical infrastructure (ITSAP.10.100)
- Security considerations for industrial control systems (ITSAP.00.050)
- Protect your operational technology (ITSAP.00.051)

Check out other advice and guidance :
www.cyber.gc.ca/en/guidance



Learning Hub Training

- Course 119: Cyber security for IoT devices
- Course 531: Cyber Security Event Management - Table Top Exercise
- Course 625: Cyber Security for Small and Medium Organizations
- Course CYB117C: Cyber Security for Users of Generative Artificial Intelligence
- Course 910: IT security risk management boot camp

Check out our other courses :
www.cyber.gc.ca/en/education-community/learning-hub/courses

Cyber Centre Tools and Services

- Assemblyline – malware detection and analysis tool
- Howler – triaged platform to assist Security Operations Centre (SOC) teams in streamlining their workflow and enhancing their ability to handle alerts
- Aventail - a platform for real-time sharing of Indicators of Compromises (IoCs) that may indicate potential intrusions on a host system or network
- Community building - a suite of information sessions including bi-weekly threat briefs and Walk-the-Talk

WHO TO CONTACT AND WHEN | QUI CONTACTER ET QUAND

CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

→ Reporting cyber incidents | Signaler des cyber-incidents

cybertip!ca®

→ Child exploitation, trafficking of child porn, child sextortion, etc. | Exploitation des enfants, trafic de pornographie enfantine, extorsion d'enfants, etc.

Royal Canadian Mounted Police | Gendarmerie royale du Canada

→ Cybercrime: Ransomware, Money Laundering, Identity Theft, Cyberbullying, etc. | Cybercriminalité: rancongiciels, blanchiment d'argent, vol d'identité, cyberintimidation, etc.

Canadian Anti-fraud Centre
Centre antifraude du Canada

www.antifraudcentre-centreantifraude.ca

→ If you receive personal phishing email, telemarketing, tax scam | Si vous recevez un courriel personnel de phishing, du télémarketing, une escroquerie fiscale, etc.

CONNECT WITH US


contact@cyber.gc.ca


www.cyber.gc.ca


@cybercentre_ca

Scenario : Ransomware variant used to steal sensitive employee info

Your organization – a large shoe store retailer – is taken offline by a cyber security incident. Clients are unable to access your organization's website, and online and in-person debit and credit card payments cannot be accepted. When you try to access your systems, a note from a ransomware group appears, stating that if your organization does not pay the demanded ransom, the sensitive employee data stolen would be leaked on their DLS. The sensitive information stolen included employee emails, home addresses, social insurance numbers, and bank account details. No customer data appears to have been stolen. After consulting third party experts, you discover ransomware actors gained access to your network through a phishing attack where ransomware actors tricked employees into downloading what they believed was a mandatory software update. The ransomware actors then deployed their ransomware variant in your organization's systems, allowing them to encrypt and steal sensitive data. As of two weeks after the attack, your company has continually refused to pay the ransom and none of the sensitive information stolen appears to have been leaked.

CRGs - 36 foundational goals

Scenario : Ransomware variant used to steal sensitive employee info

Recommended mitigations

- Asset inventory and network topology [1.0]
- Separating user and privileged accounts [2.4]
- Network segmentation [2.5]
- Secure sensitive data: data at rest [2.10]
- System backups and redundancy [2.14]
- Secure Administrator Workstation [2.21]
- Detect relevant threat and TTPs [3.0]
- Incident planning and preparedness [5.0]