Cybersecurity & Operational Technology

Reshape. Respond. Recharge

Sami Khoury
Government of Canada Senior Official for Cyber Security
Communications Security Establishment

Overview

- About CSE…
- A Complex Reality
- Threat Landscape & Trends
- Geopolitical Uncertainty
- Incidents Reality
- Lessons Learned
- Reflections
- Q&A
- Resources

Communications Security Establishment

WHO WE ARE…

- CSE is Canada's foreign signals intelligence agency, and technical authority for cyber security and information assurance.
- CSE includes the Canadian Centre for Cyber Security (the Cyber Centre) CCCS, the federal government's operational lead for cyber security.
- CSE's mandate has 5 aspects:
  - Foreign signals intelligence;
  - Cyber security;
  - Active cyber operations;
  - Defensive cyber operations;
  - Technical and operational assistance to federal partners.

CSE Act: One Mandate with Five Aspects

S.16 - FOREIGN INTELLIGENCE

COLLECT FOREIGN INTELLIGENCE

Use advanced techniques to access foreign networks to collect intelligence in support of government priorities

S.17 - CYBERSECURITY AND INFORMATION ASSURANCE

DEFEND GOVERNMENT OF CANADA NETWORKS

DEFEND DESIGNATED NON-FEDERAL SYSTEMS

Provide advice, guidance, and services that include deployment of CSE's cybersecurity tools on Government of Canada systems and other designated systems of importance

S.20 - TECHNICAL AND OPERATIONAL ASSISTANCE

ASSIST FEDERAL LAW ENFORCEMENT, SECURITY AGENCIES AND DND/CAF

Provide technical and operational assistance while operating under requesting department/agency's authorities

S.18-19 - FOREIGN CYBER OPERATIONS

DEFENSIVE CYBER OPERATIONS

Counter foreign cyber threats targeting federal systems and systems of importance

ACTIVE CYBER OPERATIONS

Counter foreign entities that engage Canada's international affairs, defence, and security interests

MANDATE (S.15): National signals intelligence agency for foreign intelligence and technical authority for cybersecurity and information assurance

A Complex Reality

Setting the Scene

- Security shocks now move faster, farther, and across more boundaries
- Domestic and international security are increasingly intertwined
- The leadership test is coherence under uncertainty

- The new operating model

Incomplete Information… compressed timelines… high consequences

A Sector in Motion

- Energy sector is “in motion”, facing new challenges and expectations
- Cyber is no longer IT → it is core business risk for utilities

Electricity is now as much a digital service as it is a physical one—and that changes everything

- Utilities are now prime targets
  - Critical infrastructure = high impact

- Expanding attack surface:
  - OT + IT convergence
  - Smart grid / telemetry

Threat Landscape & Trends

Themes & Judgments

- The threat landscape is expanding and getting more complex
- A growing cast of malicious actors and some new unpredictable players
- Aggressive cyber activities including disruptive effects
- Cybercrime remains a persistent, widespread and disruptive threat
  - Financially motivated and opportunistic
  - Proven resilience (MaaS, RaaS, AaaS, PaaS)
- Ransomware is the top cybercrime threat to Canada's Critical Infrastructure
- AI is amplifying cyber threats
- Dual-use commercial services are part of the cyber battlefield
- State adversaries are using cyber operations to disrupt & divide and extend beyond espionage

Worrisome Trends

- Every indicator is pointing **up**
  - 3Vs: Volume Velocity, Variety, Sophistication
- Triple extorsion in Ransomware
- Credential theft driving more intrusions
- Supply chain compromises (open-source software)
- AI contributing to attacker scale and speed
- Critical Infrastructure
  - IT/OT/IOT
- Social engineering as a leverage
- Q-Day is coming

The AI Inflection Point

- AI as a threat accelerator: AI is lowering barriers to entry, improving the quality and scale of malicious cyber activity.
- Speed, scale, precision & plausibility: Faster content production, greater realism (deepfakes, voice clones, robo-calls), more targeted and personalised influence campaigns, and better amplification across platforms.
  - Smart phishing
  - Deepfake executives
- AI in the attack life cycle: Content creation for social engineering → malicious code generation → vulnerability research → data identification → scaling and automation. Specialised LLMs on the darkweb and "Jailbreaking-as-a-Service" (JaaS) are emerging.
- (semi)-autonomous campaigns driven by AI -> scale & speed

Geopolitical Uncertainty

- States use cyber operations to project power below the threshold of armed conflict
  - → Moving beyond espionage to disruption, coercion, and influence.
- Critical infrastructure is a strategic pressure point
  - → Cyber incidents now translate into economic, safety, and confidence impacts.
- Pre-positioning inside networks increases national risk
  - → Access today enables disruption during future crises.
- Cyber + Information Operations are increasingly combined
  - → Aiming to sow division and undermine trust in institutions, markets, and society.
- Non-state actors add volatility during global flashpoints
  - → Hacktivism and proxy activity spike with little warning.
- Convergence of Cyber + Kinetic Operations

Cyber Incidents **WILL** Happen

AI incidents*

- Mar 2025 – **Deepfake** CEO video scam (Singapore, corporate/financial operations)AI-generated video and voice impersonation used to deceive a finance director into authorising a high-value transfer.
- 2025-08-27 — ZipLine targeted US manufacturers using AI-related **social engineering** pretexts
- Sep 2025 – State-linked **autonomous** AI cyber-espionage campaign (global) A nation-state actor used a **jailbroken AI** model to conduct largely autonomous intrusions.
- Dec 2025–Feb 2026 – Mexican government **AI-assisted mass data breach** (“Operation Tortuga”, Mexico) Attackers used generative AI tools to scale exploitation and data analysis.
- Mar 2026 – **AI software supply-chain compromise** (LiteLLM ecosystem, global) A widely used AI/ML library was maliciously modified, enabling credential theft and backdoor access in downstream organisations.
- May 2026 – AI-Assisted **ICS** Attack on a municipal water utility in Monterrey, Mexico

*Courtesy of RecordedFuture

OT / Cyber-Physical Incidents in Recent Years

- **Jaguar Land Rover** (2025): Cyberattack shut down manufacturing operations, the costliest production shutdown in almost a decade. (UK GDP impact)

- **Polish Energy Sector** / DER Attack (2025): Russian attackers compromised more than 30 Polish wind and solar sites and disrupted automation devices in a major near miss.
- **Ukraine Power Grid** (2024–2025): Repeated cyberattacks disrupted power distribution and underscored the vulnerability of energy infrastructure in conflict zones.
- **U.S. Water & Wastewater** Exploitation (2024): Threat actors used basic tactics to exploit weaknesses in critical water infrastructure.
- **Colonial Pipeline** (2021): A compromised VPN account without MFA contributed to ransomware impact and an OT shutdown.
- **Oldsmar Water** (2021): Attackers used shared remote-access credentials to reach an OT HMI and attempt to alter chemical dosing.
- **Norsk Hydro** (2019): Ransomware spread through Active Directory and forced manual operations when OT systems became inaccessible.
- **Ukraine Power Grid** (2015–2016): Attackers pivoted from IT into OT, remotely opened breakers, and later deployed destructive firmware.
- **STUXNET** (2010): A highly targeted worm that sabotaged Iranian nuclear enrichment operations by manipulating Siemens industrial control systems while feeding false normal readings to operators

Sample of Incidents in the Utilities Sector*

- City of Greenville / **Greenville Electric Utility System** (2025-08-26), Cyberattack, likely ransomware — customer-facing disruption
- **Nova Scotia Power** (2025-Q2), Cyberattack / customer data theft.
- **Norwegian dam operator** (2025-Q2), Unauthorized access / OT-related security incident, potential physical impact
- **Halifax Water** (2026-03-06), Unauthorized access to customer portal. possible exposure of customer information
- Unnamed **Canadian water treatment facility** (2025-10-29), Industrial control systems compromise / hacktivist intrusion, temporary service disruptions and unsafe conditions.

*Courtesy of RecordedFuture

How Cyber Becomes Physical

- **Operational** disruption
  - systems unavailable, processes delayed, facilities degraded
- **Safety** implications
  - degraded monitoring, delayed response, unsafe fail states
- **Security** gaps
  - badge/access anomalies, surveillance blind spots, alarm interruptions
- **Reputational** and business impact
  - downtime, public concern, leadership pressure

Anatomy of a Cyber Event

Building Resilience

Recovery

Incident

Identify Protect Detect Respond Recover

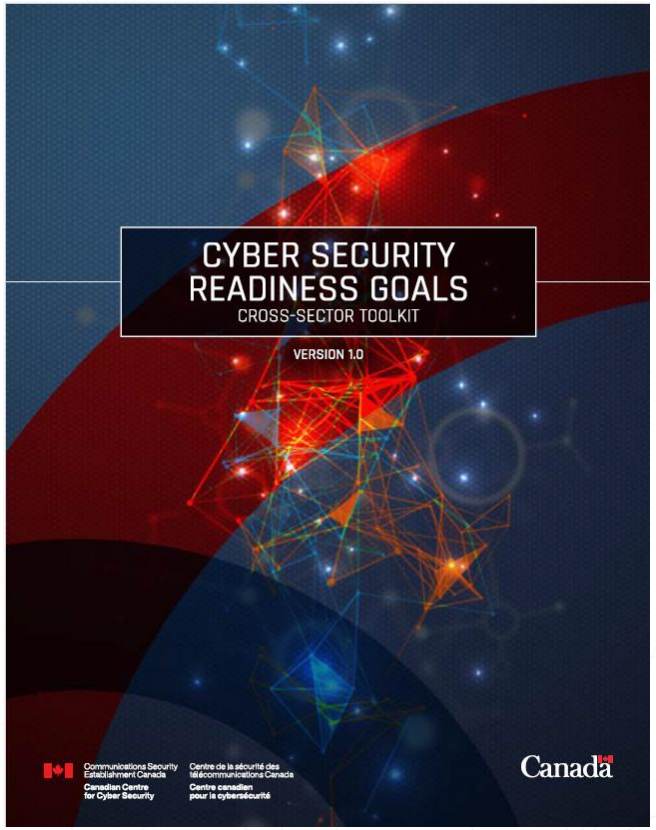
NIST CSF 2.0

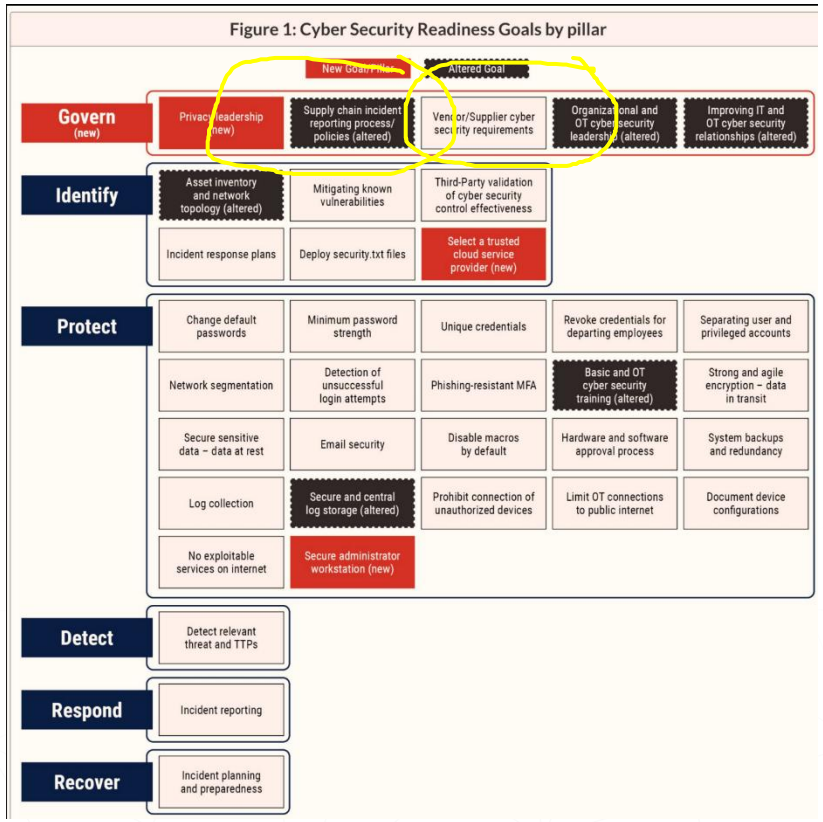
Govern

Cyber Security Readiness Goals

"The Cross-Sector Cyber Security Readiness Goals Toolkit outlines 36 CRGs to support Canadian CI owners and operators, from any sector, in prioritizing investments in cyber security and to elevate their cyber security posture."

Cyber supply chain security for small and medium-sized organizations (ITSAP.00.070)





Lessons Learned

Practical Risk Patterns

- **IT/OT boundary is the soft underbelly**
  - Flat networks or weak segmentation between enterprise IT and OT/building systems
- IT-to-OT pivoting occurs through
  - compromised engineering workstations,
  - shared credentials, and
  - exploitation of remote-access solutions
- Internet-exposed OT and building systems
- Unsupported or legacy controllers
- Inadequate logging/monitoring
- Poor asset inventory: not knowing what is connected
- Vendor-managed systems with unclear accountability
- Lack of tabletop exercises for cyber-physical incidents

Final Thoughts

The Leadership Imperative

- At its core, cyber security is about **trust** — in systems, data, and institutions

- We still move too slowly;
  - Adversaries iterate faster than decision processes
  - We still underinvest in fundamentals
  - We still operate in silos

- Resilience **isn't** about preventing a breach
  - It is about detection speed **&** operational continuity

- Cyber risk is persistent, not episodic
    - Plan for continuous pressure not the exception

Reshape. Respond. Recharge…

- Daily management decisions shape cyber risk,
  - Technology doesn't fail alone—people and decisions matter most
- Cybersecurity Is a Team Sport: you are **not** alone
- A Common Failure Pattern
  - Delegation **+** Pressure **+** Shortcuts **=** Accumulated Risk
- What Governance Really Means
  - Clarity on who decides what, when.

Reshape. Respond. Recharge

- Continuous adaptation: reshaping risk strategies, responding with governance, and recharging capabilities.

Questions ?

Thank You

Connecting & Reporting

To report a cyber incident:
Canadian Centre for Cyber Security
1-833-CYBER88
https://cyber.gc.ca

To report fraud:
Canadian Anti-Fraud Centre
1-888-495-8501
www.antifraudcentre-centreantifraude.ca


@cse_cst


contact@cyber.gc.ca

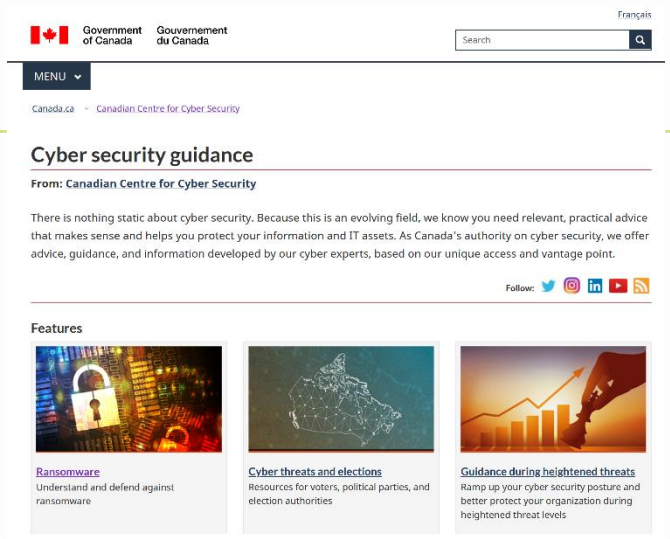

www.cyber.gc.ca


@cybercentre_ca

To report a cybercrime:
Local police or
Royal Canadian Mounted Police
www.rcmp-grc.gc.ca

Cyber Security Advice & Guidance

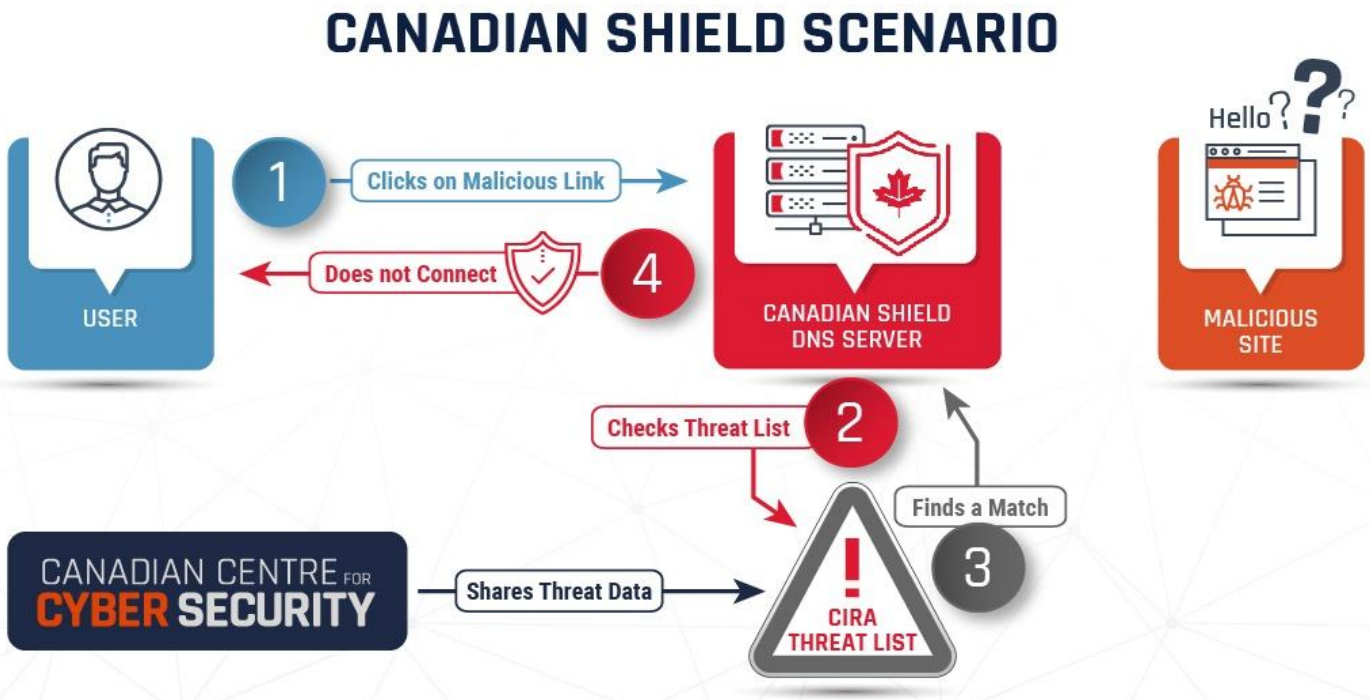
Visit: cyber.gc.ca



GETCYBERSAFE.CA

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.

Threat Intelligence Sharing and Canadian Shield



For the year ending Oct 2025

2.81M Users
2.15T DNS queries
816M DNS blocks

Protecting Canadians from Phishing

Forward your smishing text to **7726**

- Cyber Centre partners share suspected malicious websites for analysis
- Cyber Centre partners share suspected malicious SMS links (smishing)
- Since Mar. 2020, CCCS has worked with partners to take down over 15, 279 spoofed/malicious sites