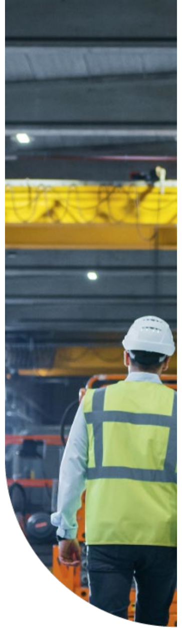


FORTINET

Global OT cybersecurity leader

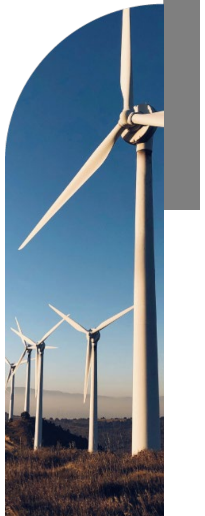
Bill C-26 Protecting Canada's Critical Infrastructure

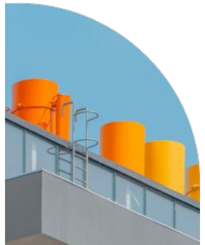
Jeff Brown

Regional Sales Manager - OTCI

Jose “Ze” Barreto

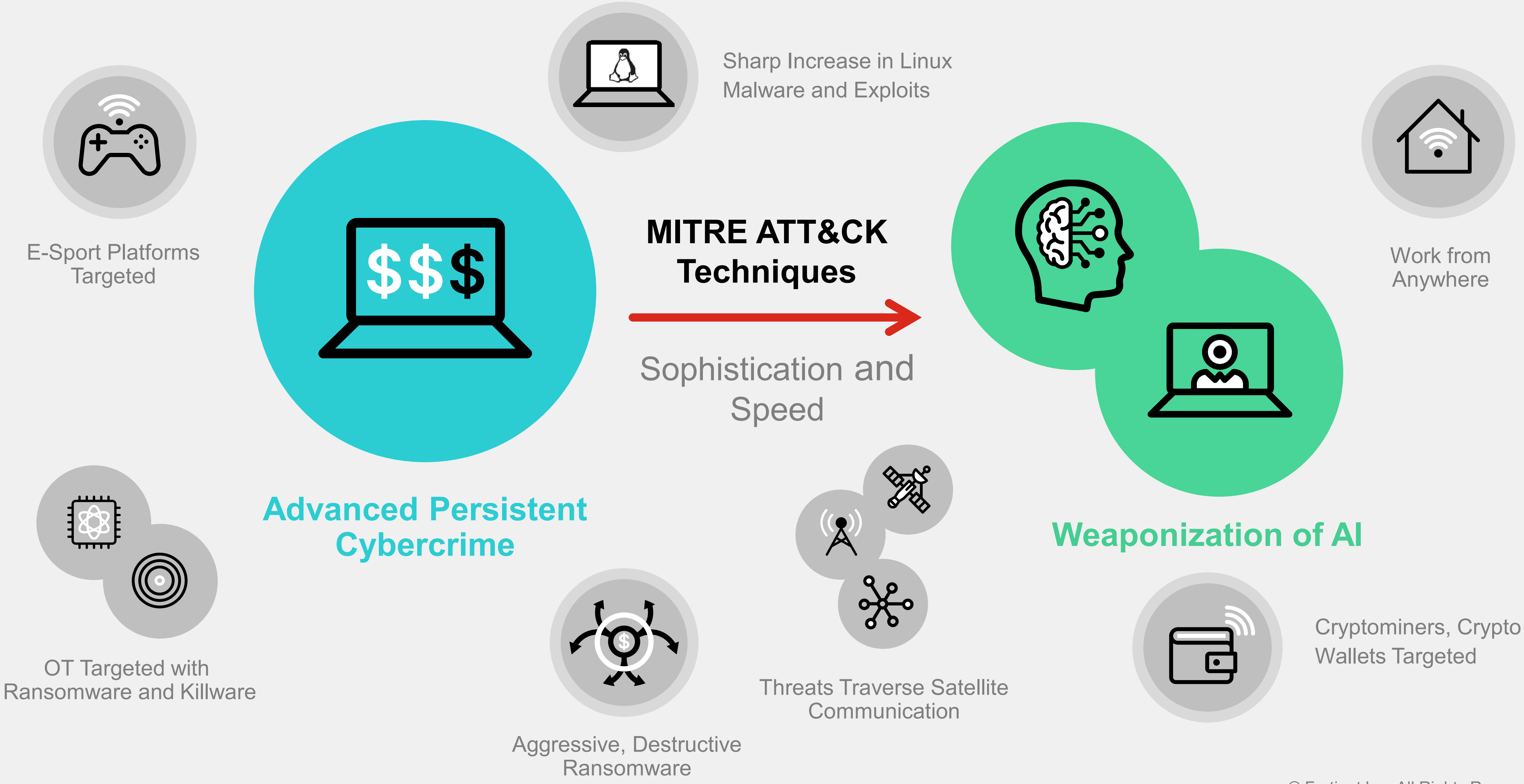
Business Development Engineer - OTCI





Organizations are under attack more than ever

Perforated Attack Surface



E-Sport Platforms Targeted

Sharp Increase in Linux Malware and Exploits

Work from Anywhere

Advanced Persistent Cybercrime

MITRE ATT&CK Techniques

Sophistication and Speed

Weaponization of AI

OT Targeted with Ransomware and Killware

Aggressive, Destructive Ransomware

Threats Traverse Satellite Communication

Cryptominers, Crypto Wallets Targeted

“By 2025, 75% of OT security solutions will be delivered via multifunction platforms interoperable with IT security solutions.”

Gartner

FORTINET

“Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully: **Harm or Kill Humans”**

Organizations Can Reduce Risk by Implementing a Security Control Framework

“In operational environments, security and risk management leaders should be more concerned about real world hazards to humans and the environment, rather than information theft,” said Wam Voster, senior research director at Gartner

STAMFORD, Conn., July 21, 2021

Gartner

2021:In December 2021, the Prime Minister asked Public Safety Minister to develop a new National Cyber Security Strategy.

Canadian Companies under Attack

Spikes in Canadian Business Cybercrime

FORTUNE 100

FORTUNE 500

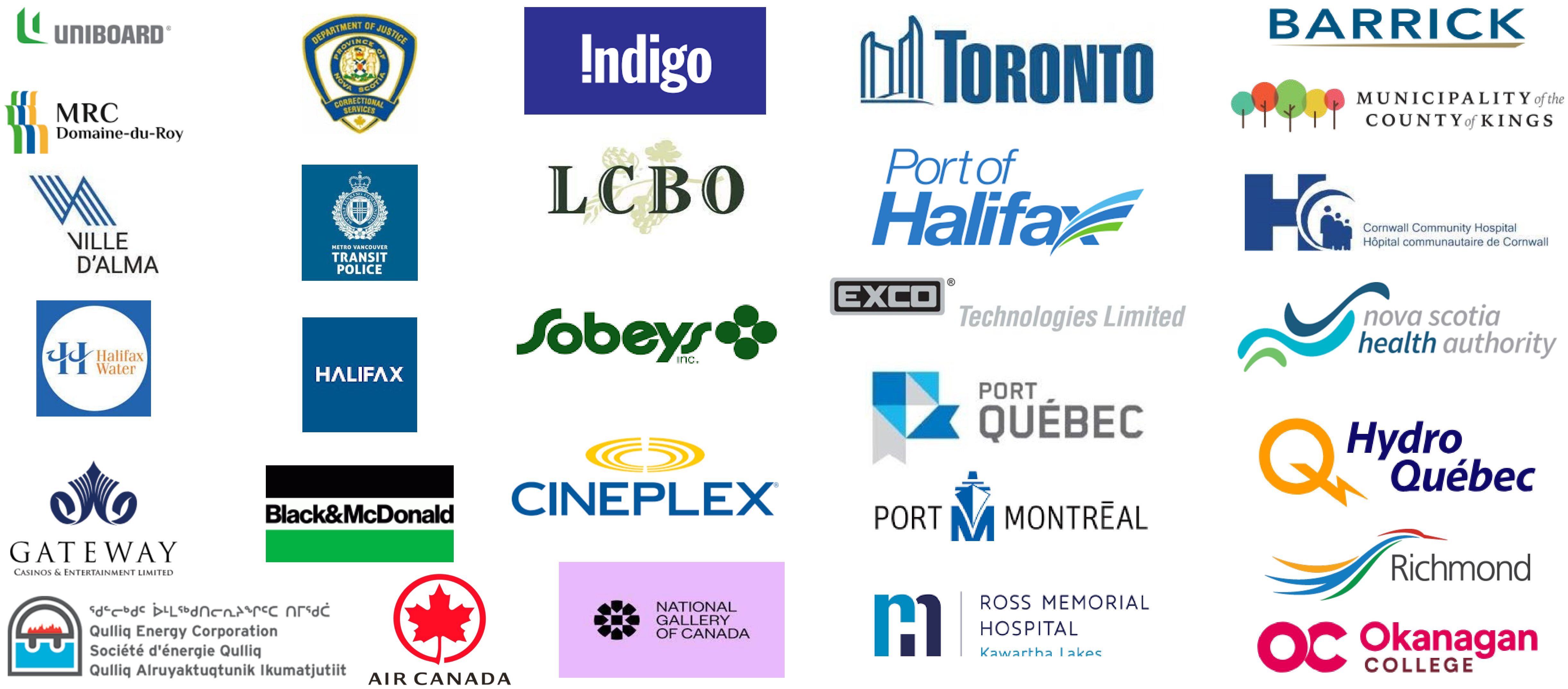
FORTUNE 1000

Since the beginning of 2023, many Canadian Companies have been hit by cyberattacks.

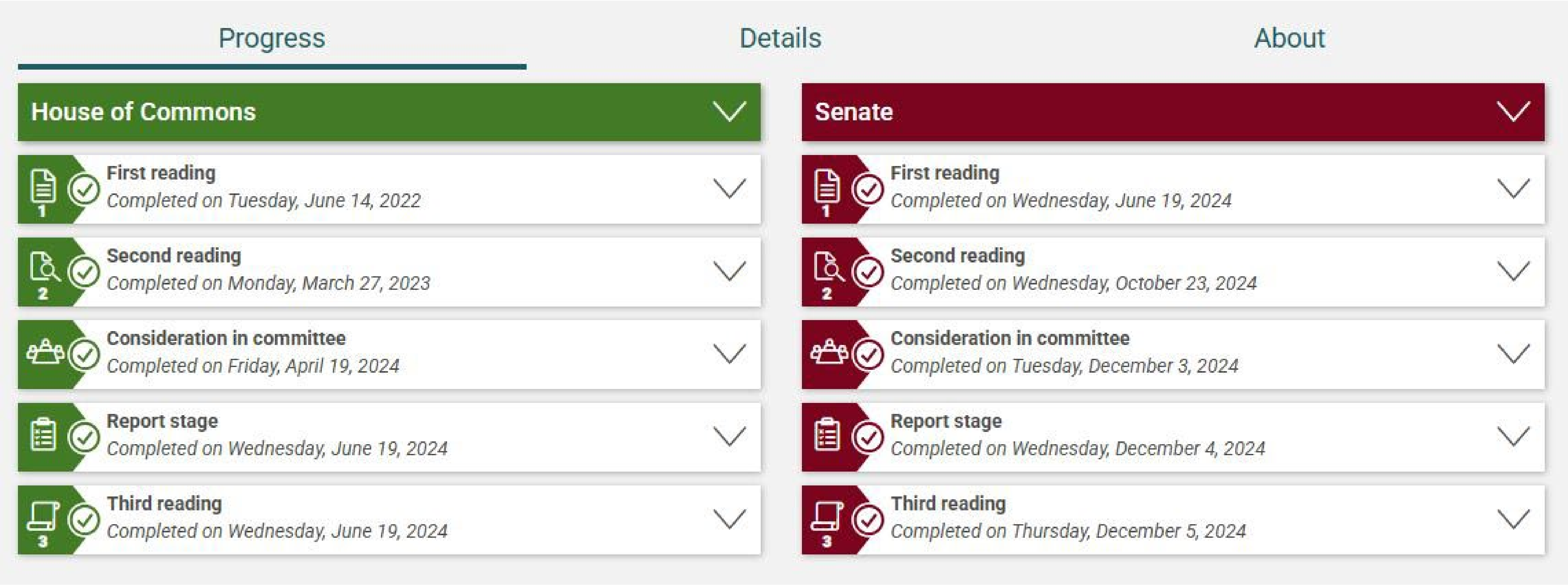
Healthcare
Oil & Gas
Wastewater
Energy
Transportation
Manufacturing

Banking
Retail
Telecom
Food & Agriculture
Government
Dams

Spikes in Canadian Business Cybercrime



Legislation Timing



House of Commons

1 ✓ **First reading**
Completed on Tuesday, June 14, 2022

2 ✓ **Second reading**
Completed on Monday, March 27, 2023

✓ **Consideration in committee**
Completed on Friday, April 19, 2024

✓ **Report stage**
Completed on Wednesday, June 19, 2024

3 ✓ **Third reading**
Completed on Wednesday, June 19, 2024

Senate

1 ✓ **First reading**
Completed on Wednesday, June 19, 2024

2 ✓ **Second reading**
Completed on Wednesday, October 23, 2024

✓ **Consideration in committee**
Completed on Tuesday, December 3, 2024

✓ **Report stage**
Completed on Wednesday, December 4, 2024

3 ✓ **Third reading**
Completed on Thursday, December 5, 2024

Bill C-26 - Timelines

2013: Communications Security Establishment (CSE) established its Security Review Program (SRP)

2016: Conducted public consultations on cyber security (NIS)

2018: Released the National Cyber Security Strategy (NCSS). CSE's Canadian Centre for Cyber Security was established as a key NCSS initiative

2019: Allocated $144.9M through Budget 2019 to develop a Critical Cyber Systems framework

2021:In December 2021, the Prime Minister asked Public Safety Minister to develop a new National Cyber Security Strategy.

2021: Completed an inter-departmental 5G Security Examination, which recommended an updated security framework to safeguard Canada's telecommunications system

2022:Ministry of Public Safety acted to introduce new legislation, Bill C-26 An Act Respecting Cybersecurity. Bill C-26 passed its first step in Parliament in November of 2022

2023: Second reading (March 27th , 2023) – House of Commons

2024; February 4th, Alignment of Departments creation of the Standing Committee

2024:Third reading (June 19th , 2024) House of Commons

Bill C-26 Enacts the *Critical Cyber Systems Protection Act* (“CCSPA”),

The impact of the bill falls into many areas :

- Legal Liability of Cybersecurity now falls on Executives and directors of Governments and Public Companies, Private companies, Corporations .
- New rules will potentially move Cybersecurity Reporting squarely in the laps of Legal and C Suite and pushes organizations to report breaches immediately to the government.
- Monitoring of Cybersecurity in IT/OT Convergence (OT/IT Breaches How do you report)
- Reporting on Cybersecurity as a Framework
- KPI Dashboards of the IT/OT Convergence and the tools give access to this data will play a major role moving forward
- Cybersecurity OT Governance and Compliance will become mandatory as organizations need to provide visibility on their compliances

Bill C-26 Enacts the *Critical Cyber Systems Protection Act* (“CCSPA”),

Penalty

91 The amount that may be fixed under any regulations made under paragraph 135(g) as the penalty for a violation must not be more than

(a) $1,000,000, in the case of an individual; and

(b) $15,000,000, in any other case.

Due diligence available

92 **(1)** Due diligence is a defence in a proceeding in relation to a violation.

Common law principles

(2) Every rule and principle of the common law that renders any circumstance a justification or excuse in relation to a charge for an offence under this Act applies in respect of a violation to the extent that it is not inconsistent with this Act.

Liability of directors or officers

93 If a designated operator commits a violation, any director or officer of the designated operator that directed, authorized, assented to, acquiesced in or participated in the commission of the violation is a party to the violation and is liable to a penalty of an amount to be determined in accordance with this Act and the regulations, whether or not the designated operator has been proceeded against in accordance with this Act.

Continuing violation

94 A violation that is committed or continued on more than one day constitutes a separate violation in respect of each day on which it is committed or continued.

Administrative Monetary Penalties

Penalty

91 The amount that may be fixed under any regulations made under paragraph 135(g) as the penalty for a violation must not be more than

- **(a) $1,000,000, in the case of an individual**; and
- **(b) $15,000,000, in any other case**.

Continuing violation

94 A violation that is committed or continued on more than one day **constitutes a separate violation** in respect of each day on which it is committed or continued.

93: Individuals include any director or officer of the designated operator

CANADIAN CENTRE FOR
CYBER SECURITY

National **Cyber Threat** Assessment

2023
2024

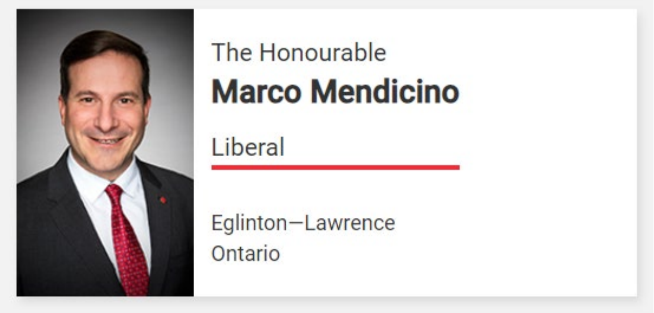
Communications
Security Establishment

Centre de la sécurité
des télécommunications

Canada

76ui

- **Protect your Operational Technology (ITSAP.00.051)**
- **Security considerations for industrial control systems (ITSAP.00.050)**
- **Security considerations for critical infrastructure (ITSAP.10.100)**



The Honourable

Marco Mendicino

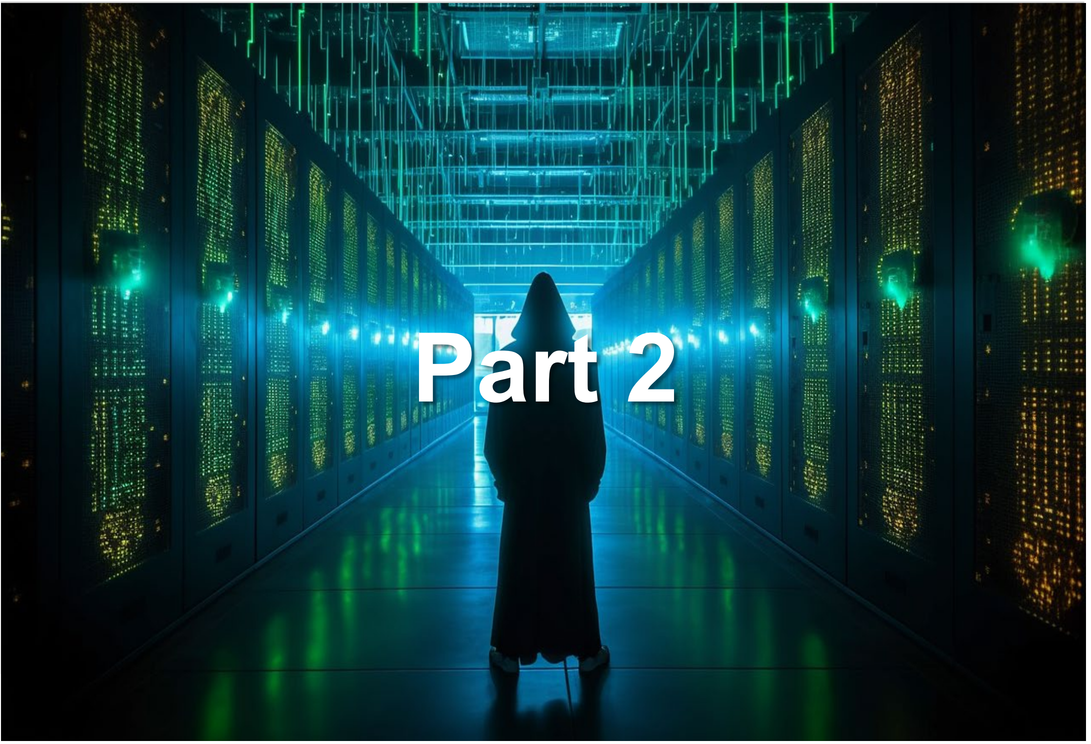
Liberal

Eglinton—Lawrence
Ontario

Bill C-26 Enacts the Critical Cyber Systems Protection Act (“CCSPA”),

On June 14, 2022, the House of Commons of Canada introduced Bill C-26, an Act Respecting Cyber Security (ARCS) proposing new cybersecurity requirements that protect vital systems and services pertinent to Canada's security and public safety.

Telecommunication	Critical Cyber Systems Protection Act (CCSPA)



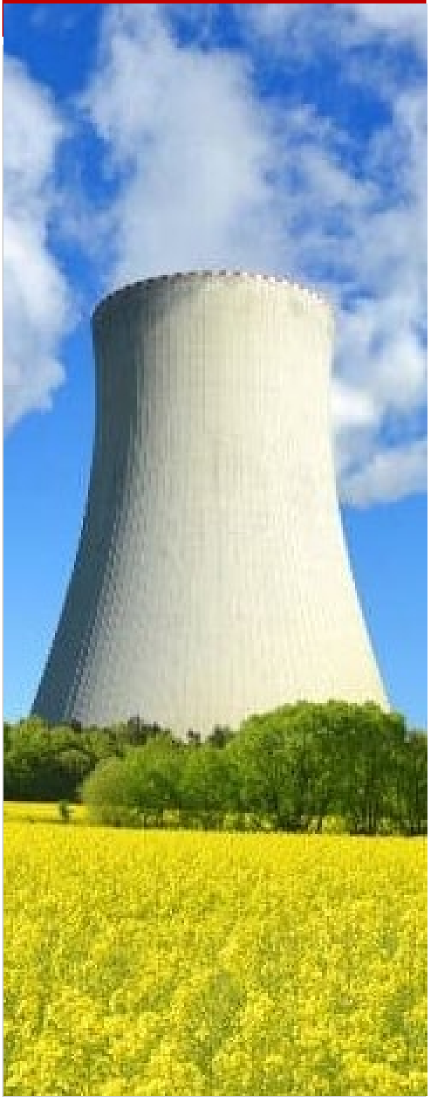
CCSPA – Target Sectors Vital to National Security/Public Safety

Telecom Services

Transportation

Power & Pipelines

Nuclear Energy



Banking Systems

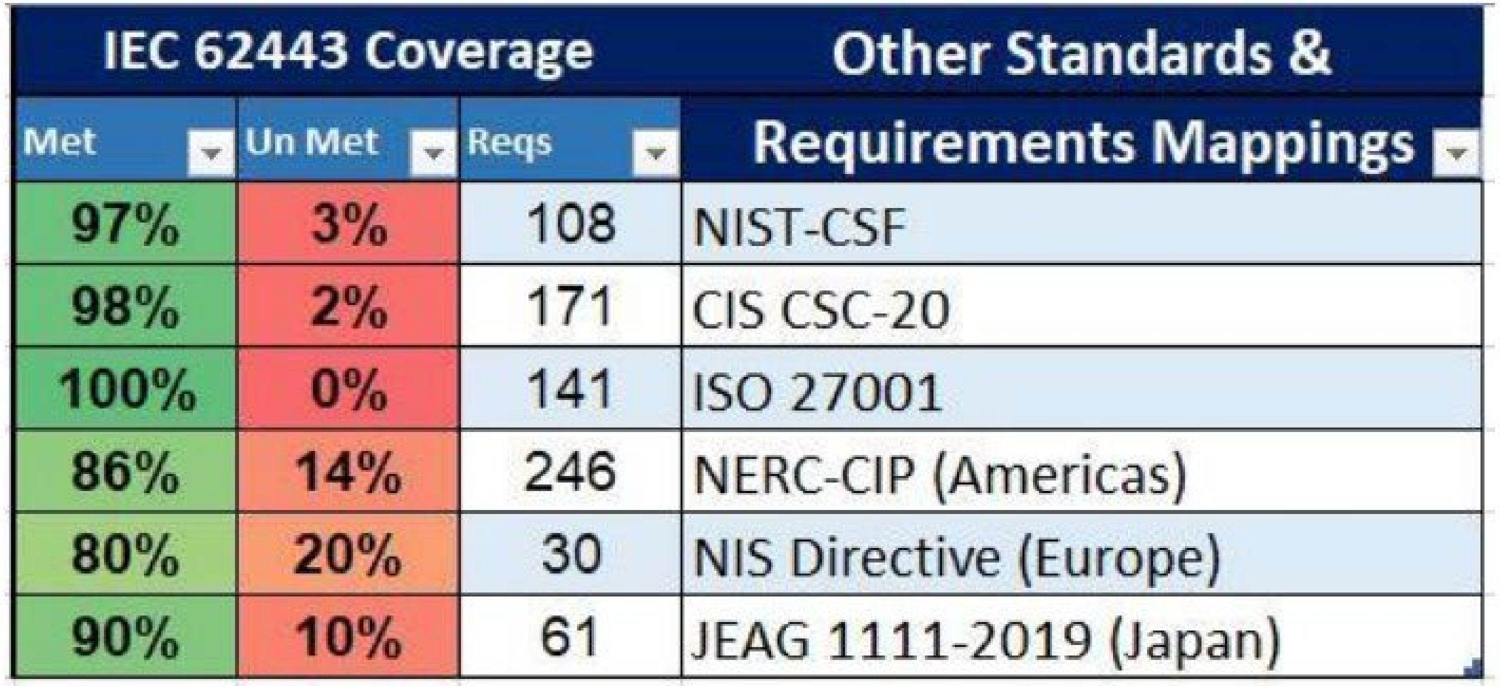
Clearing Systems

Schedule 1: Vital Services and Vital Systems

Vital Services and Vital Systems	Regulator
Telecommunications services	Minister of Industry
Interprovincial or international pipeline and power line systems	Canadian Energy Regulator
Nuclear energy systems	Canadian Nuclear Safety Commission
Transportation Systems that are within the legislative authority of Parliament	Minister of Transport
Banking systems	Office of the Superintendent of Financial Institutions
Clearing and settlement systems	Bank of Canada

Air, rail, road, and sea

Bill C26 is not re inventing the wheel



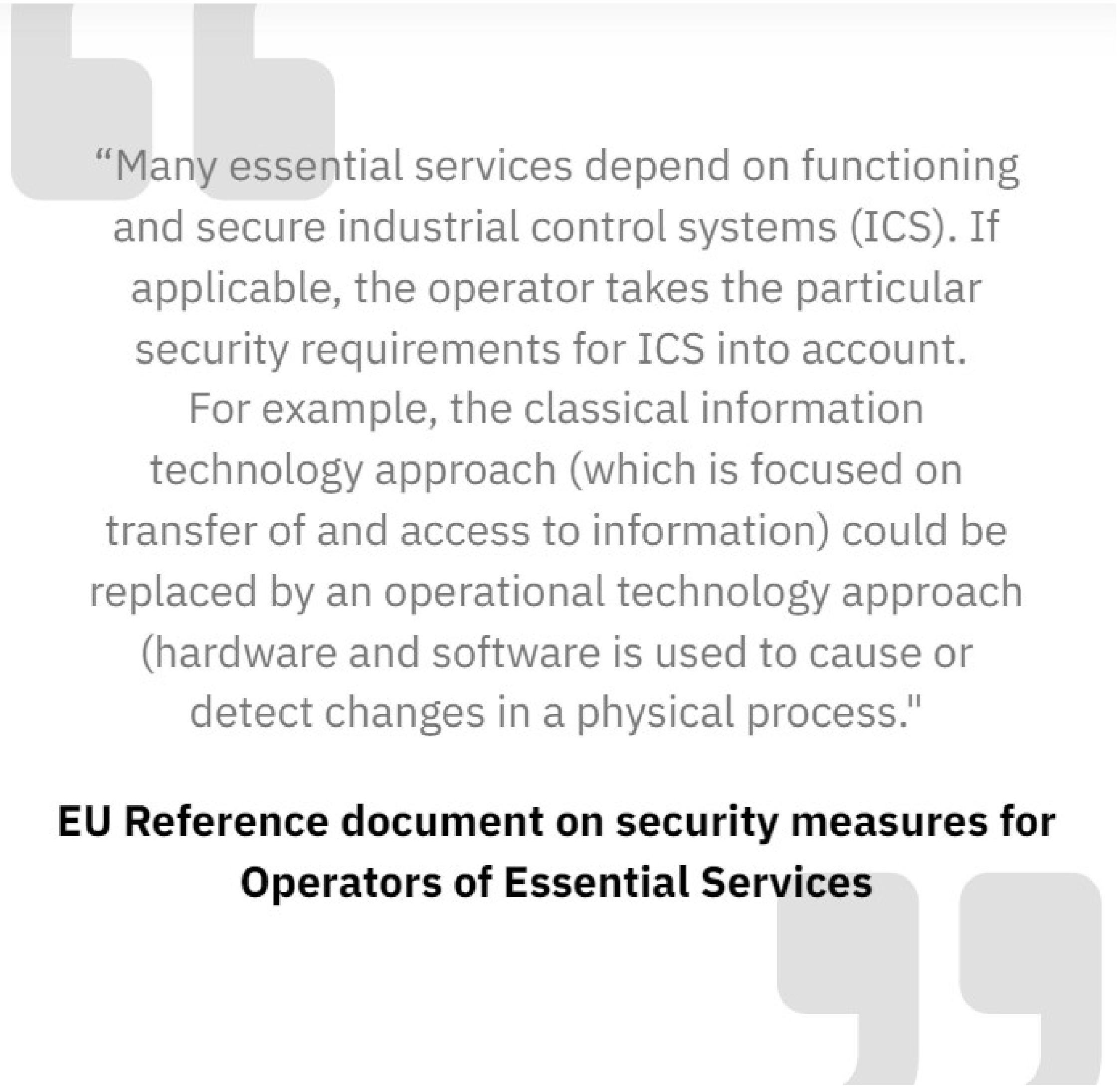
IEC 62443 Coverage			Other Standards &
Met	Un Met	Reqs	Requirements Mappings
97%	3%	108	NIST-CSF
98%	2%	171	CIS CSC-20
100%	0%	141	ISO 27001
86%	14%	246	NERC-CIP (Americas)
80%	20%	30	NIS Directive (Europe)
90%	10%	61	JEAG 1111-2019 (Japan)

Table 1: IEC 62443 coverage of requirements in major international standards used for OT and IT security of distributed renewable energy assets

ISO 27001 is an international standard to improve an organization's information security management systems, while NIST CSF helps manage and reduce cybersecurity risks to their networks and data. Both ISO 27001 and NIST CSF effectively contribute to a stronger security posture

NIS 2 OT Guidance

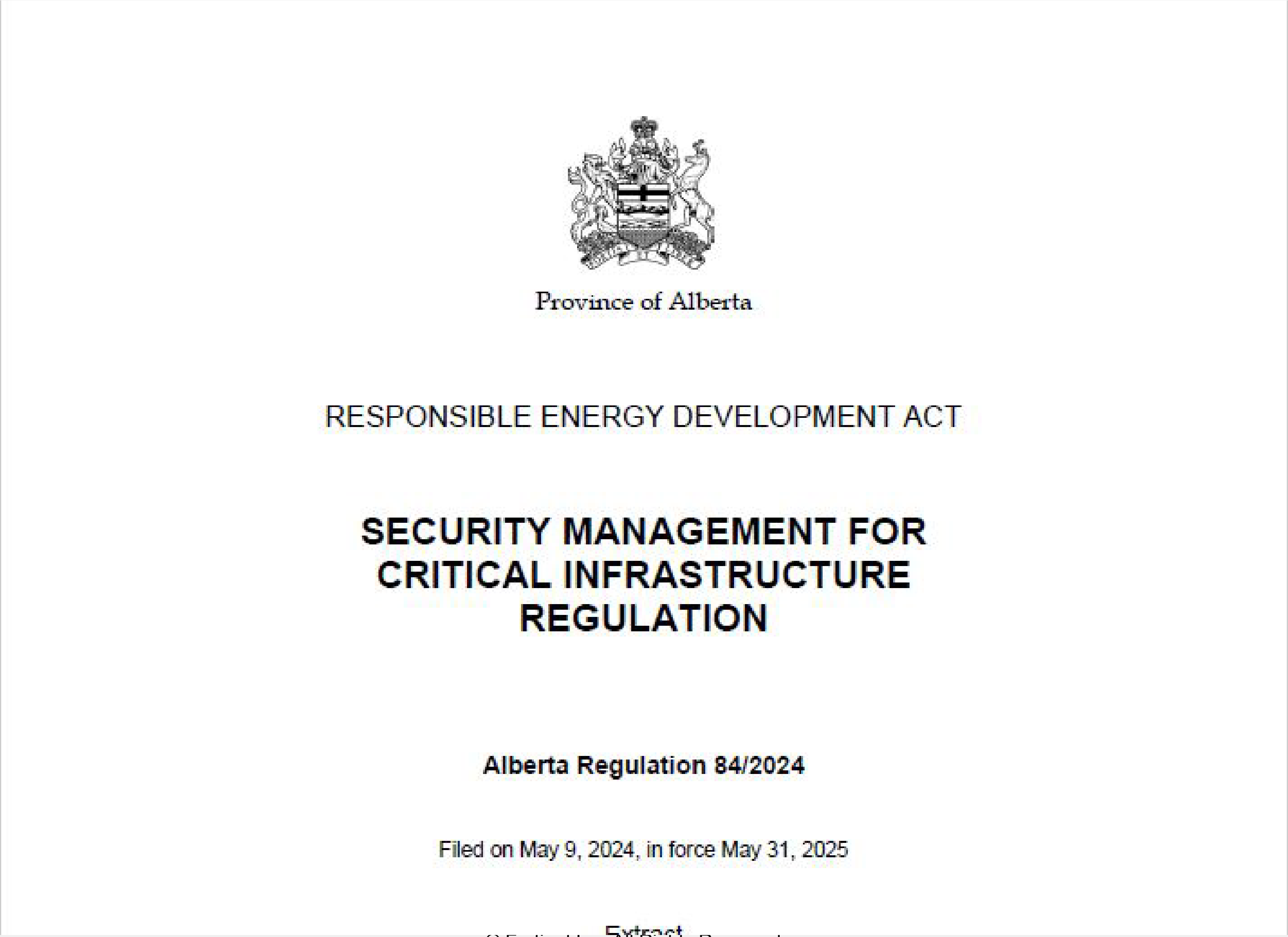
EU guidance includes specific provisions that address the cybersecurity of industrial control systems (ICS) and operational technology (OT), recognizing their critical importance to the functioning of essential services.



"Many essential services depend on functioning and secure industrial control systems (ICS). If applicable, the operator takes the particular security requirements for ICS into account. For example, the classical information technology approach (which is focused on transfer of and access to information) could be replaced by an operational technology approach (hardware and software is used to cause or detect changes in a physical process."

EU Reference document on security measures for Operators of Essential Services

What about Closer to Home?



Province of Alberta

RESPONSIBLE ENERGY DEVELOPMENT ACT

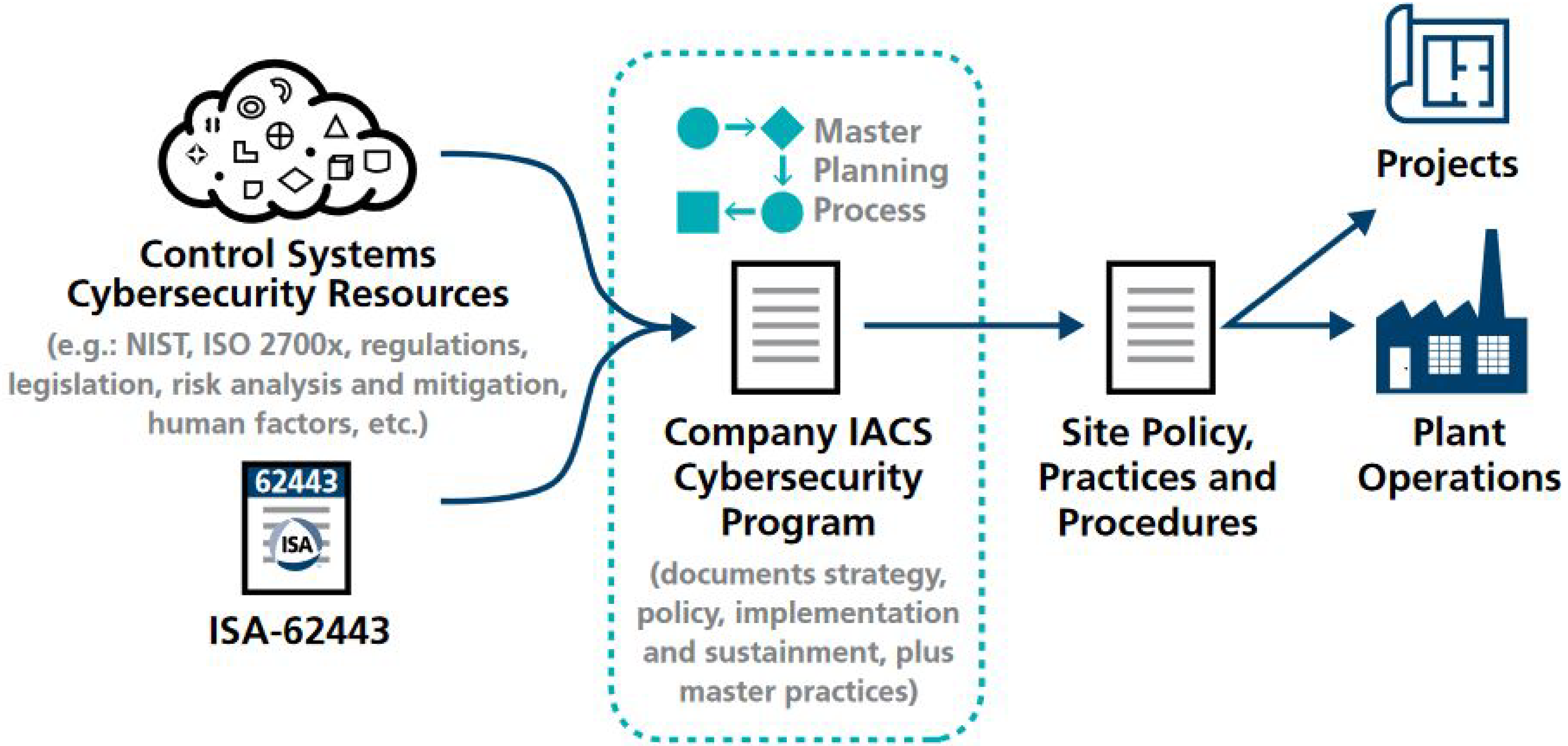
SECURITY MANAGEMENT FOR CRITICAL INFRASTRUCTURE REGULATION

Alberta Regulation 84/2024

Filed on May 9, 2024, in force May 31, 2025

Extract

Rockwell Automation
Allen-Bradley
by ROCKWELL AUTOMATION
Honeywell
EMERSON
GE
ABB
Schneider Electric
SIEMENS
YOKOGAWA
PHŒNIX CONTACT



Control Systems Cybersecurity Resources
(e.g.: NIST, ISO 2700x, regulations, legislation, risk analysis and mitigation, human factors, etc.)
62443
ISA
ISA-62443
Master Planning Process
Company IACS Cybersecurity Program
(documents strategy, policy, implementation and sustainment, plus master practices)
Site Policy, Practices and Procedures
Projects
Plant Operations

Figure 1. IACS Cybersecurity Program Workflow

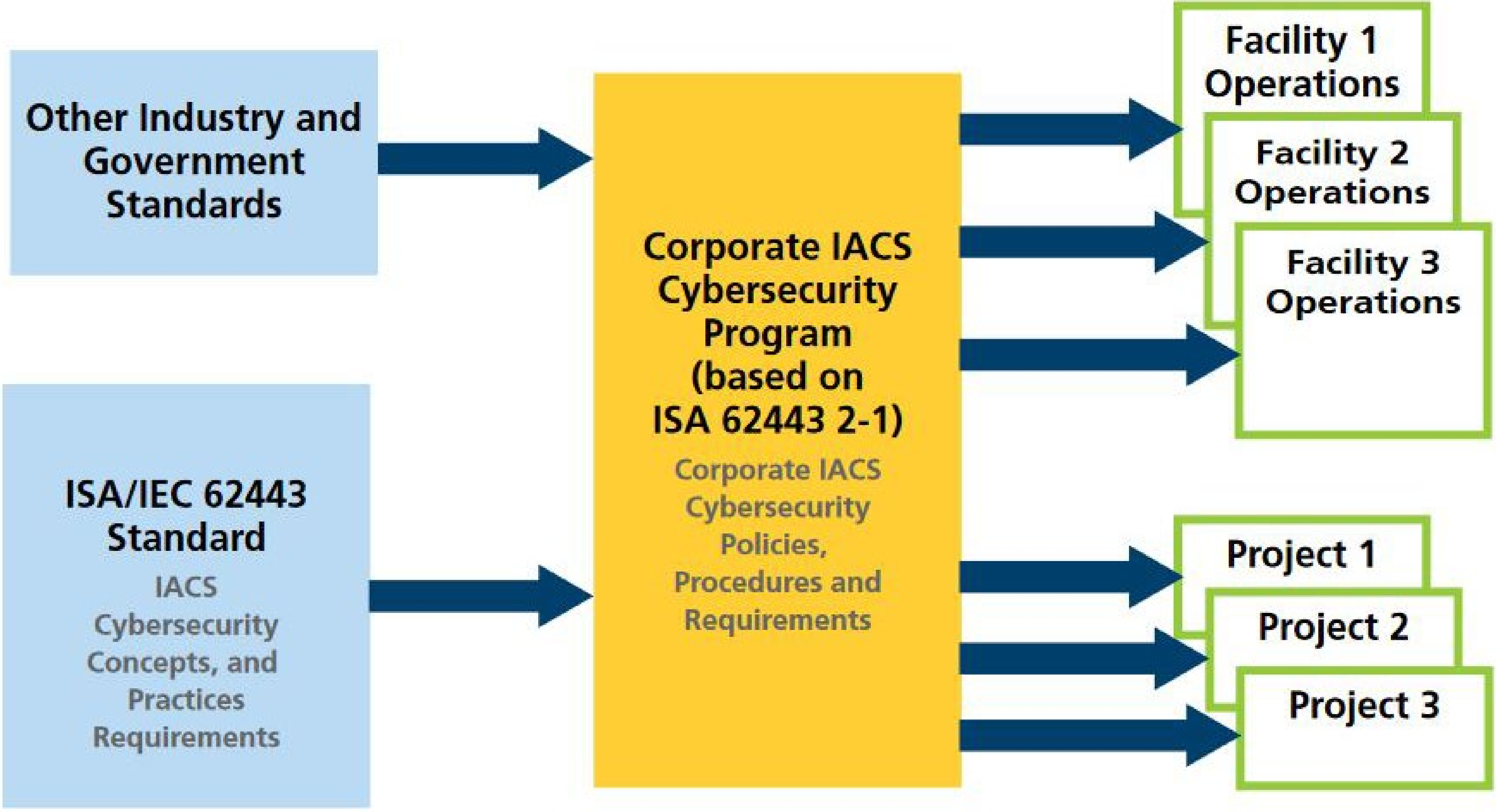

Other Industry and Government Standards
ISA/IEC 62443 Standard
IACS Cybersecurity Concepts, and Practices Requirements
Corporate IACS Cybersecurity Program (based on ISA 62443 2-1)
Corporate IACS Cybersecurity Policies, Procedures and Requirements
Facility 1 Operations
Facility 2 Operations
Facility 3 Operations
Project 1
Project 2
Project 3

Figure 2. IACS Cybersecurity Program Concept

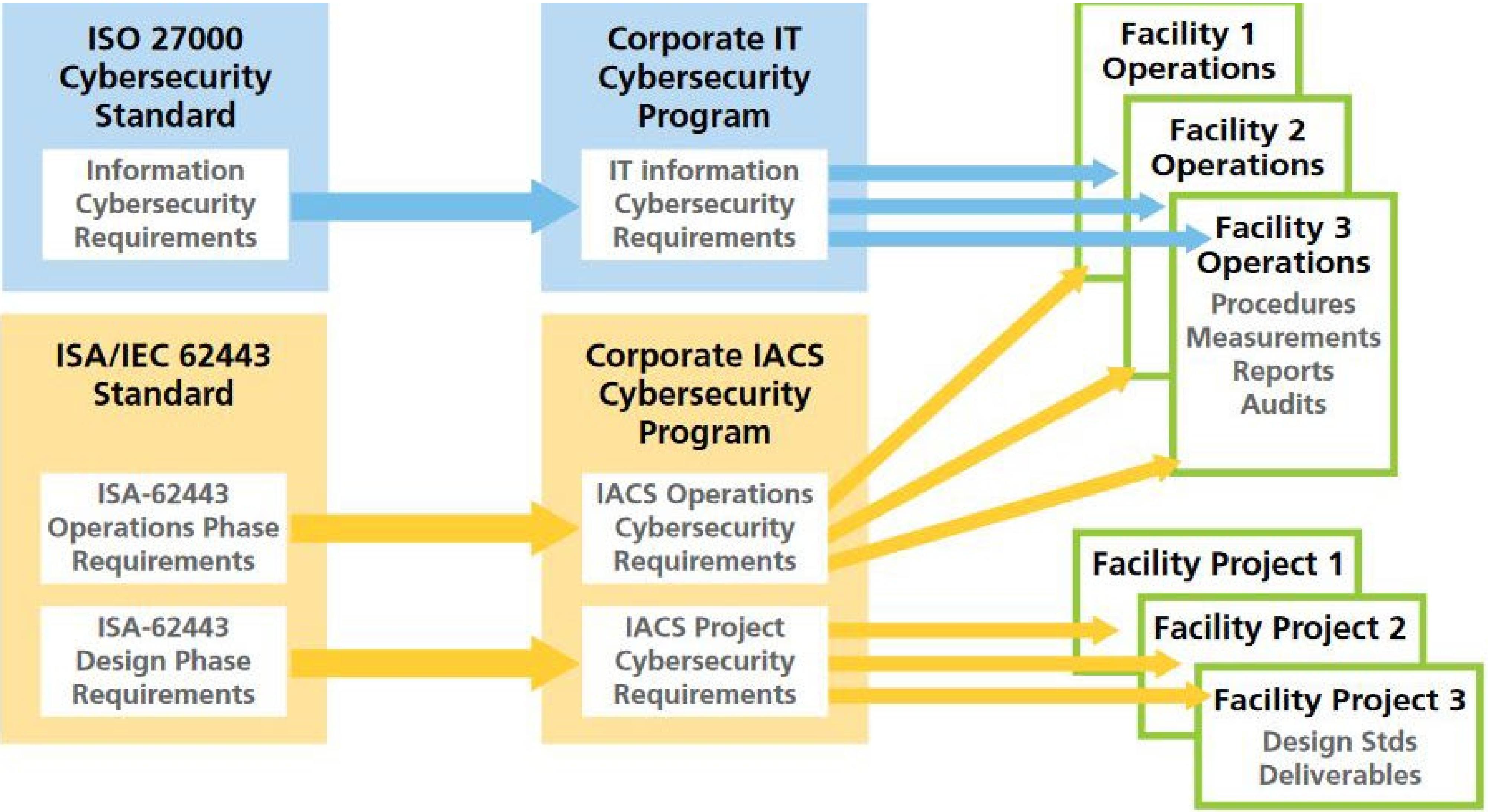

ISO 27000 Cybersecurity Standard
Information Cybersecurity Requirements
Corporate IT Cybersecurity Program
IT information Cybersecurity Requirements
ISA/IEC 62443 Standard
ISA-62443 Operations Phase Requirements
ISA-62443 Design Phase Requirements
Corporate IACS Cybersecurity Program
IACS Operations Cybersecurity Requirements
IACS Project Cybersecurity Requirements
Facility 1 Operations
Facility 2 Operations
Facility 3 Operations
Procedures
Measurements
Reports
Audits
Facility Project 1
Facility Project 2
Facility Project 3
Design Stds
Deliverables

Figure 5. Mapping of Cybersecurity Requirements

What controls are essential to secure OT environments? (IEC62443)

Zones and Conduits	Segmentation protects OT from mistakes and bad actors.	Are your OT assets segmented from the IT side? How flat is your OT network in reality?
Secure Remote Connectivity	Enable secure access for employees and third-parties who connect to your OT environment.	Who requires access to your OT network? How do you enable that securely today?
Deep OT Visibility	You can’t protect what you can’t see.	How well do you understand what’s in your industrial control system?
Role-based Access Control	Limit access to only those who need it.	Do you know who can access what in your OT environment? When was the last time you checked?
Endpoint Security	Apply endpoint security protection to the servers at and near the secure perimeter.	Do you have older servers in your OT environment that are no longer supported?
NOC / SOC	Synergistic benefits of managing everything in one place.	How much money could you save by managing the network security of your OT and IT in the same place?
Advanced Persistent Threat	Advanced Persistent Threats (APT) require advanced solutions.	Have you considered leveraging sandboxing, deception, or AI to up-level your OT security strategy?

OT Network Segmentation: Your 5-Step Guide

1. Build an IT/OT Team
2. Map Your Network
3. Design Your Segmentation Plan
4. Deploy your Plan
5. Enhance, Maintain & Train

Secure Remote Access Best Practices

1

Implement Zero Trust

2

Update Remote Access Tools

3

Continuous Monitoring & Network Visibility

4

Strong Security Policies & Procedures

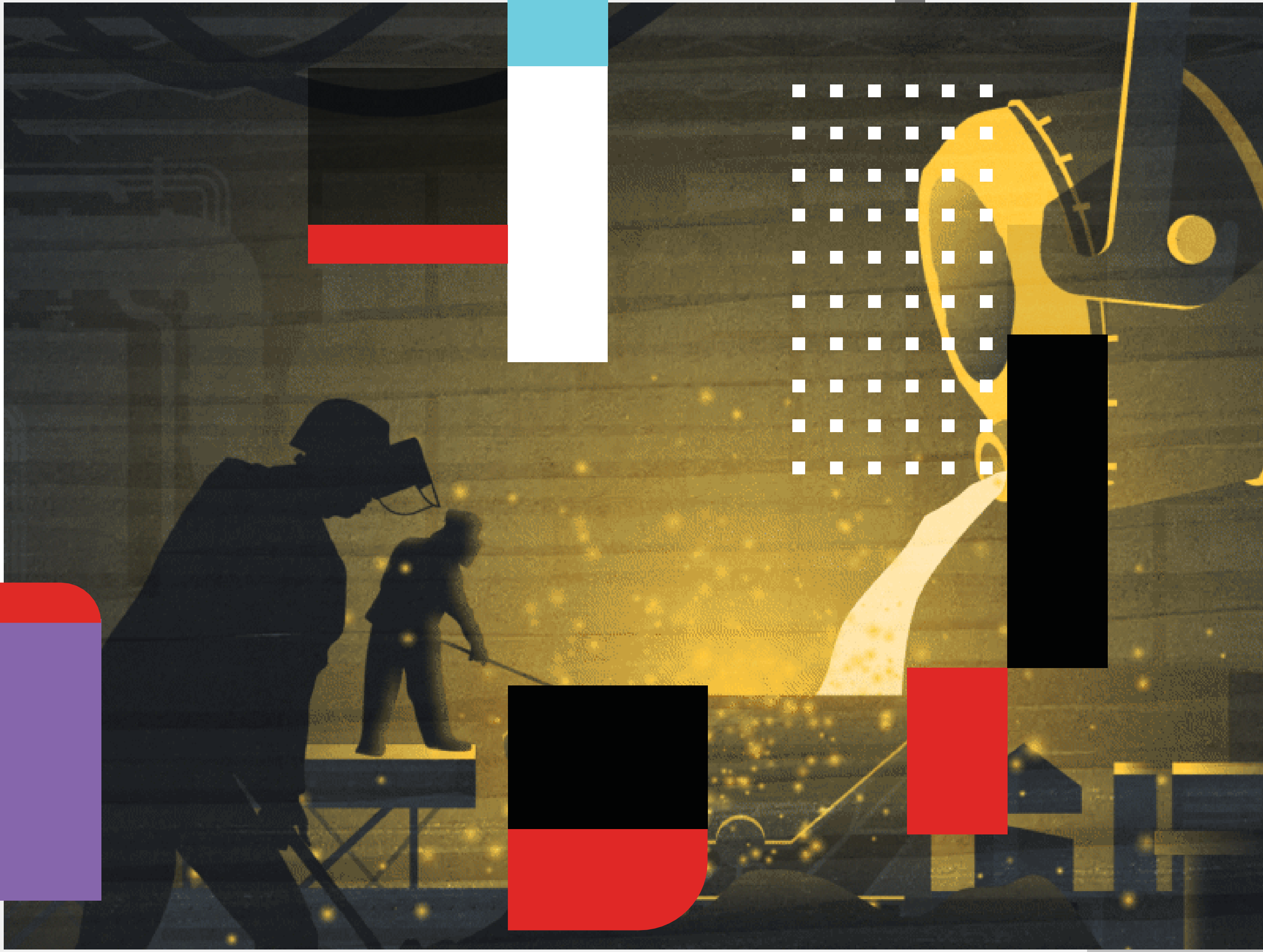
5

Enhance User Awareness & Training

FORTINET®

Global OT cybersecurity leader

Q&A



Let’s Keep the Conversation Going

OT.Canada@fortinet.com

FORTINET®