CSAC and the Ontario Cyber Security Framework

Dan Gaudette

Chair, CSAC
Information Systems Manager
Synergy North

Craig Makela, CISSP

Co-vice chair, past Chair, CSAC
Manager of Information Security & Technology
GSU

Agenda

- What is the CSAC?
- The premise and overview of the Ontario Cyber Security Framework
- OEB Requirements: What's new
- OSCF Version 2
- Pressing Cyber Risks

The Cyber Security Advisory Committee (CSAC)

- industry-led group comprising representatives from Ontario's electricity utilities and other interested parties
- collaborates with the OEB to evolve the OCSF in response to emerging threats and industry best practices
- Started in 2016

Ontario Cyber Security Framework (OCSF)

- a structured approach developed by CSAC and published by the Ontario Energy Board (OEB)
- help electricity distributors assess and enhance their cybersecurity capabilities
- aims to ensure the reliability, security, and privacy of Ontario's electricity system
- Version 1 released 2017

OCSF (continued…)

- based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework
- incorporates the U.S. Department of Energy's Cybersecurity Capability Maturity Model (C2M2)
- integrates privacy principles from Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)

Cybersecurity Capability Maturity Model (C2M2) Maturity Indicator Levels (MILs)

- evaluates the implementation and effectiveness of cybersecurity controls across five core functions: Identify, Protect, Detect, Respond, and Recover
- MIL0 – not performed
- MIL1 – Initial practices are performed, but may be ad hoc
- MIL2 – Practices are documented; adequate resources provided
  - current target for mandated controls
- MIL3 – guided by policy; personnel have skills and knowledge; responsibility, accountability, and authority for practices are assigned to personnel; effectiveness is tracked

Ontario Cyber Security Framework Inherent Risk Profile

- Utilities assess their inherent cybersecurity risk using a tailored Inherent Risk Profile Tool
  - 46 questions over 7 Risk Areas with Weighted scores

- Risk Score determines the appropriate security controls that should be completed

Risk Level	Control Objectives
Low	61
Medium	90
High	120

Cybersecurity Capability Maturity Model (C2M2) Maturity Indicator Levels (MILs)

- Released in December 2023
- 3rd party supply chain risk
- Provides illustrative examples based on C2M2 version 2.1 to enhance the evaluation and sustainment of cybersecurity programs

OSCF Version 1.1(Current version)

ID.SC-1: Cyber supply chain risk management processes are identified, established assessed, managed and agreed to by organizational stakeholders

ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process

ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan

ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results or other forms of evaluation to confirm they are meeting their contractual obligations

ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers

PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions

PR.AC-7: Users, devices and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)

PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity

PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations

RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers)

OEB Requirements: What's new

- **OEB issues Ontario Cyber Security Standard v1.1:** Issued in December 2023, this standard mandates utilities to implement specific control objectives and participate in independent assessments, reinforcing the OCSF's role in enhancing cybersecurity readiness
- **Independent Assessments:** Starting January 30, 2026, utilities are required to undergo periodic independent cybersecurity assessments conducted by qualified third-party assessors. These assessments evaluate utilities' cybersecurity maturity and inform their action plans

OSCF Version 2.0 - What's coming

- NIST Cybersecurity Framework 2.0
- Govern added to existing 5 functions
  - informs what an organization may do to achieve and prioritize the outcomes of the other five functions.
- Reorganized subcategories for improved clarity and mapping to other frameworks.
- Many subcategories combined and moved into Govern from other functions
- Release date TBD
  - Target release 2026

Risk in OCSF 2.0

More emphasis on Risk Management Strategy and Supply Chain Risk Management

OCSF will include additional subcategories that focus on risk governance and management

Highlight the importance of cybersecurity risk in organization governance and decision-making

Why do we need the OCSF?

- Previously no standard or framework for distributors
- Provides a common base framework
- Address the increasing threats against Industrial Control Systems (ICS) such as SCADA (Supervisory Control And Data Acquisition)
- Addresses the need for privacy controls
- Encourages information sharing amongst distributors, regulator, system operators

Why do we need the **next** version of OCSF?

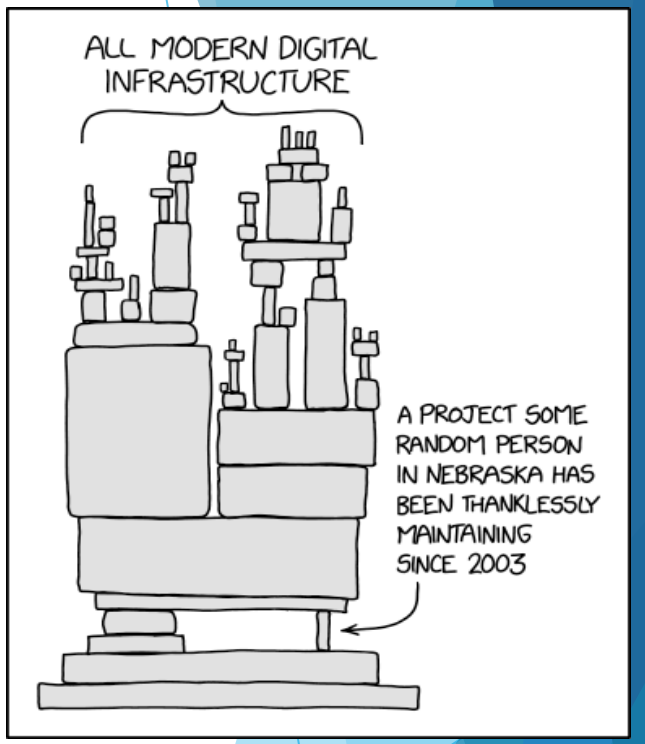
- Evolving threat landscape
- Current challenges

IT Supply Chain Risk: Physical

- Hardware Sourcing and Manufacturing
  - Dependency on foreign manufacturing
  - Logistics and Transportation
- Compromised Hardware
  - Critical infrastructure
  - Undocumented Communication Devices in Solar Inverters and Batteries

IT Supply Chain Risk: Software

- Third-Party Dependencies
  - Vulnerabilities in open-source or proprietary libraries
- Inadequate insight into sub-tier suppliers
  - Vendor may not list what packages are included
- Threat actors inserting malicious code into build processes
  - Software could be compromised through an update



Someday ImageMagick will finally break for good and we'll have a long period of scrambling as we try to reassemble civilization from the rubble.
Credit https://xkcd.com/2347/

AI and OSCF

- Many benefits to AI
  - Increased productivity
  - cybersecurity response
    - Accuracy
    - Efficiency
    - Behavioral
- Is the OSCF ready for AI?

AI Governance Risks: Leadership Without Oversight

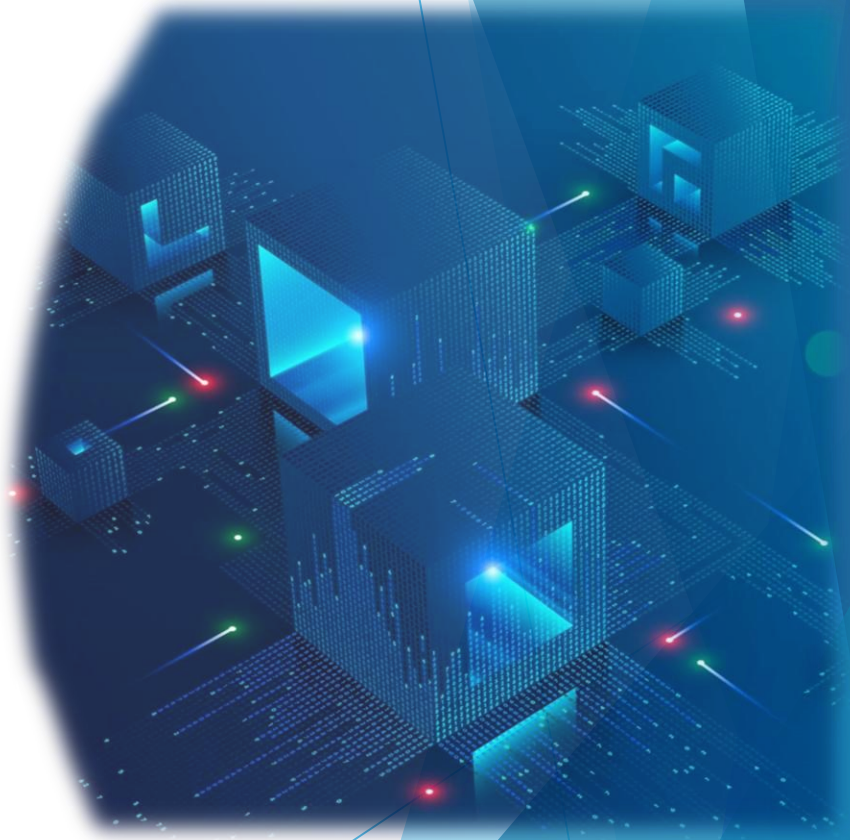
- Opaque decision-making
- Regulatory compliance or misalignment
- Unclear ownership/responsibility
- Accountability gaps

AI Privacy Risks: Sensitive Data

- Exposure of sensitive customer / employee data
- Lack of user consent
- Data overcollection
- Re-identification risks
- Surveillance concerns

AI Security Risks: New Attacks

- Model manipulation (adversarial attacks)
- Automated vulnerabilities
- Breakout time dropping significantly
- Voice phishing (vishing) up 442%
- GenAI in cyberattack campaigns



AI Operational Risks: Pitfalls in Deployment

- Over-dependance on AI recommendations
- Model drift
- System dependencies
- Resistance from staff to adopt AI tools
- Data poisoning

AI Ethical Risks: Reputational and Social Harm

- Unintended consequences or unfair treatment of customers
- Lack of human oversight
- Dehumanization
- Bias and discrimination
- Manipulation

CSAC Next Steps

- Cybersecurity is still evolving very fast
- Continue to develop and evolve the OSCF, and incorporate other frameworks
- Spend time upfront on security and privacy

Questions

Dan Gaudette

Chair, CSAC
Information Systems Manager
Synergy North
dgaudette@synergynorth.ca

Craig Makela, CISSP

Co-vice chair, past Chair, CSAC
Manager of Information Security & Technology
GSU
craig.makela@gsuinc.ca