Ontario Energy Board
Commission de l'énergie de l'Ontario

Protecting Privacy of Personal Information and the Reliable Operation of the Smart Grid in Ontario

Assurance of Cyber Security Capability

Presenter: OEB | Andres Mand
Regulations | Consumer Protection & Industry Performance

Presenter: AESI Inc. | Doug Westlund
Senior Vice President

The Mearie Group - June 23 2017

Outline

1. Expectations
2. Cyber Risks & Security
3. OEB Policy Consultation & Staff Report
4. Engagement Process & Strategic Objectives
5. Cyber Risk Profile Assessment
6. Framework Methodology & Benefits
7. Next Steps
8. Q&A

Expectations

Assurance that distributors address their business in a consistent manner that achieves OEB expectations for reliability, security and privacy.

Increasing Exposure to Cyber Risks

Evolution of Ontario’s Energy Sector:

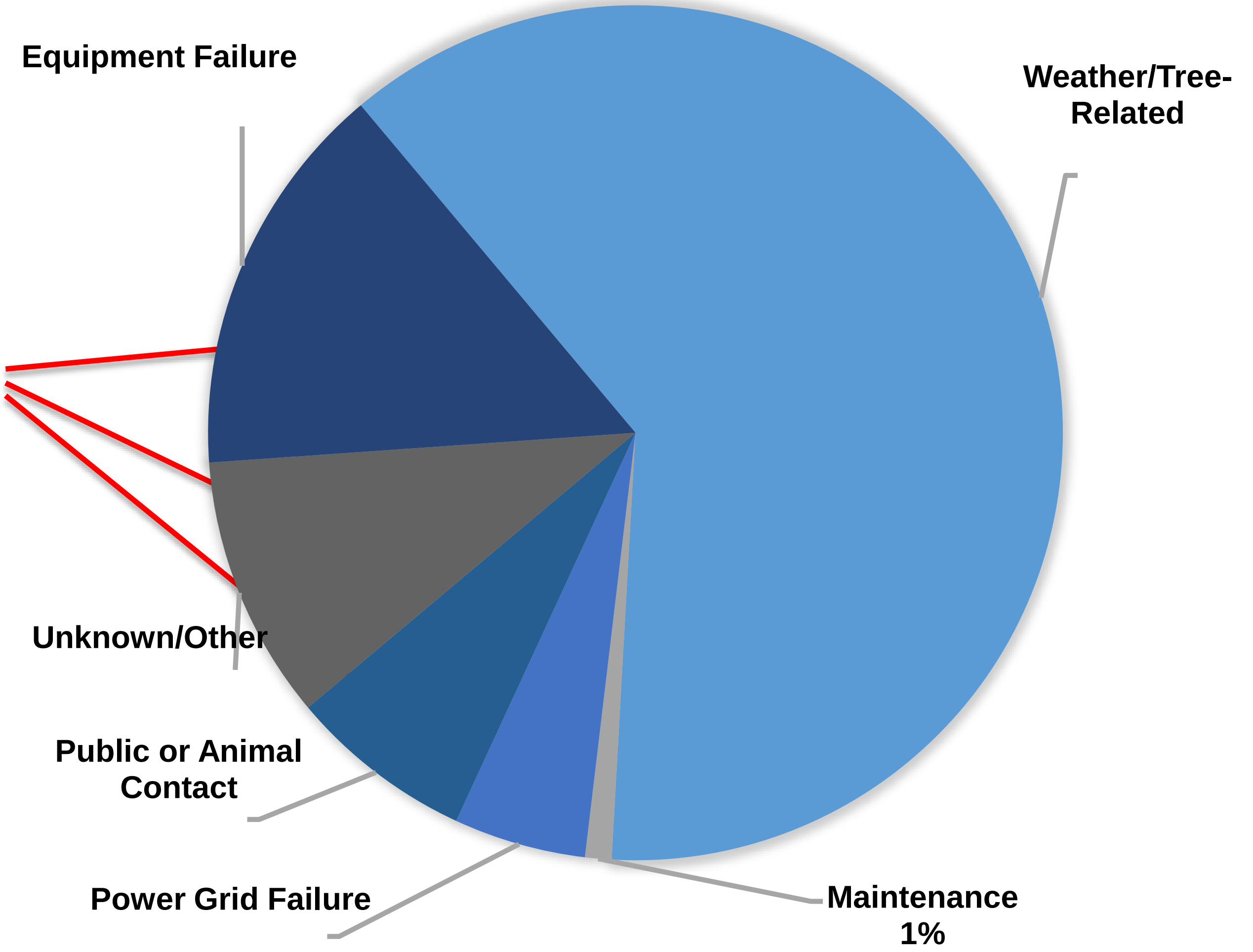
- Growing reliance on new technology and automation
- Increased use of third-party service providers
- External entities interfacing with energy distribution systems

Results in:

- More exposure to cyber risks

Biggest Threats – North American Electrical Service

Cyber is mixed in here somewhere.



Power, Telco, Water & Gas have analogous, but different, risks.

OEB Policy Consultation

Cyber security policy consultation initiated by the OEB:

- To facilitate the development of an industry led framework leveraging distributor best practices and international frameworks
  - Distributors already responsible for managing cyber security and privacy
  - Currently a lack of consistent criteria to demonstrate an appropriate level of cyber resiliency to the OEB
  - Objective is to ensure that electricity and gas distributors are taking actions to meet security, reliability and privacy obligations
  - Provides a methodology and tools to assess risk, set benchmarks and measure progress

Staff Report

Staff Report and proposed cyber security framework:

- Provides a methodology and a tool set to assess risks, set benchmarks and measure progress
- Issued by OEB staff to the Board on June 1, 2017 for comment

Engagement Process

A large number of industry stakeholders - electricity distributors, electricity transmitter, IESO and Natural Gas distributors participated:

- *Cyber Security Steering Committee* comprising Electricity Distributors Association (EDA), electricity distributors' senior leadership, Independent Electricity System Operator (IESO), academics, gas distributor – providing strategic direction
- *Cyber Security Working Group* comprising significant number of electricity distributors, Ministry of Energy, EDA, a natural gas distributor, IESO and the Electrical Safety Authority (ESA)
- *Industry Experts* – AESI, DLA Piper and Richter

Strategic Objectives of the Framework

Cyber Security Steering Committee directed the working groups to:

- Leverage an existing, flexible framework already in use by other critical infrastructure sectors
- Apply distribution business criteria to this existing framework
- Minimize rework for distributors which already have advanced cyber security
- Establish self-assessment and auditing measures
- Ensure cyber security objectives are outcome based
- Ensure framework is scalable

Working group combined three authoritative methodologies: US National Institute of Standards and Technology (NIST); Cyber-security Capability Maturity Model (C2M2) Program; and Ontario's Privacy by Design (PbD) program

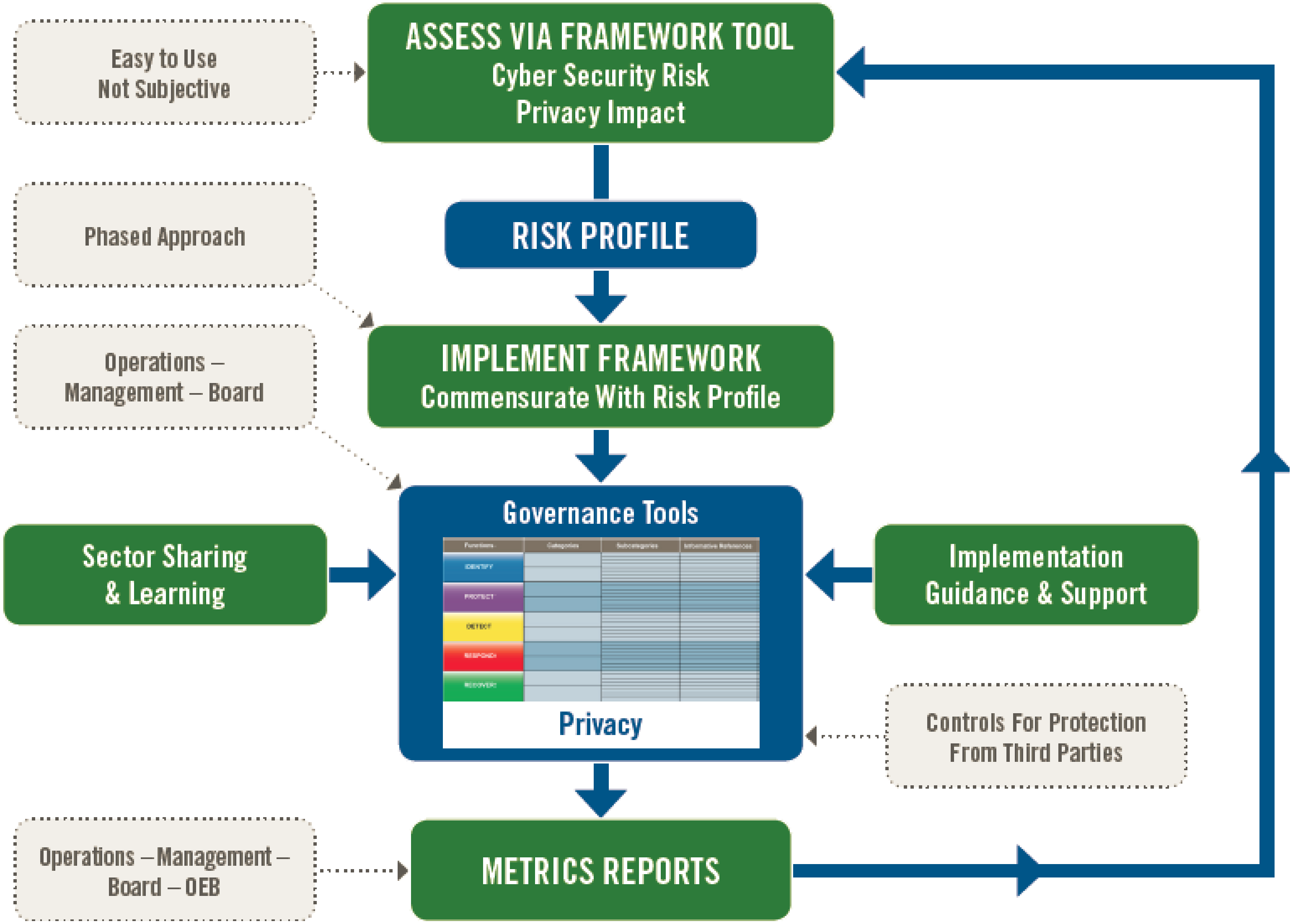
Assessing Cyber Risk Profile

First task in framework is to assess an energy distributor's risk profile:

- Framework begins with a set of tailored questions re: distributor risk
- Distributor self-assesses to define their current state and security gaps
- Forms the basis for the plan to address security threats and to certify cyber security readiness

OEB staff confirm the framework provides an approach supporting consistent assessment and reporting of cyber security readiness

Framework Methodology



ASSESS VIA FRAMEWORK TOOL
Cyber Security Risk
Privacy Impact

Easy to Use
Not Subjective

RISK PROFILE

Phased Approach

IMPLEMENT FRAMEWORK
Commensurate With Risk Profile

Operations – Management – Board

Governance Tools

Privacy

Sector Sharing & Learning

Implementation Guidance & Support

Controls For Protection From Third Parties

METRICS REPORTS

Operations – Management – Board – OEB

Industry and Consumer Benefits

Once the new framework is implemented and evolving:

- Distributors can employ the framework and supporting toolset to advance and report their levels of cyber security
- The OEB and energy consumers will be assured that the industry is taking appropriate actions with respect to security, reliability and privacy

Next Steps

Comment period for the OEB Staff Report and proposed industry-developed framework ends on July 15, 2017

- Framework now being finalized by the working group
- Progress reporting recommended within 3 months of final framework being issued; with annual security certifications following
- Final step is development and implementation of supporting regulatory changes

Sharing Forum Recommended

OEB Staff propose a *Cyber Security Information Sharing Forum* (CSIF) to encourage:

- energy sector collaboration
- awareness and training
- establishment of an industry-led advisory committee (CSAC) for ongoing management and evolution of the framework

Reflective of the high degree of engagement and leadership of the energy distributors to date in developing the framework

FRAMEWORK ELEMENTS

Expectations - Near Term

Incorporate cyber security into your enterprise risk management process

- Review and assess current cyber security posture
- Don’t wait
- Take actions to address gaps

Regulatory Requirements; after coming into force

- Assessment Reporting **(3 months)**
- Be prepared to Certify Posture **(1 year)**

*Reporting is expected to be in force by end of 2017; until finally issued they are not in force.

For more information

Please visit:

Protecting Privacy of Personal Information and the Reliable Operation of the Smart Grid in Ontario

Questions?

Your questions are welcome