ICS/OT Cybersecurity
Executives & Board Members perspectives

AIEQ – February 2022

Gaétan Houle PEng., MBA
Executive Director, ICS Cyber Security Strategy and Governance

WSP Canada Inc.

Disrupting forces are coming your way

- Increasing cyber threats targeting ICS/OT systems for critical infrastructures
- Climate change
- Pandemic

  → Supply chain disruption
- Prosumers (bidirectional flow of Energy and Data/Information)
- Coexistence of legacy and new technologies within the same environment
- Disruptive technology (IIOT, cloud, mobility, etc.) → Need for a new security framework
- Increasing complexity of regulatory compliance requirements
- Shortage of skilled workforce
- IT/OT convergence and integration

The digital transformation will only bring new opportunities to organizations that can secure it

What does it means for Executives & Board Members ?

- Contrary to issues related to IT security, top executives have very limited to no visibility on the risk exposures and vulnerabilities related to their ICS/OT environment, and a poor understanding of the related threats
- Although IT and OT technologies are converging, the organizational structure, at the governance level, will need to be adapted to support this trend
- Decision makers from power utilities need to realize that if not managed and secured properly, the digital transformation and hyperconnectivity could considerably increase risk exposures to their ICS/OT systems (i.e., their main source of revenues)
- ICS/OT air gaps are no longer sustainable; everything is being interconnected either directly or indirectly. A new strategy & approach to address this risk is needed

"

More than 30 countries are developing offensive cyber attack capabilities.

James Clapper
US director of national intelligence
June 2017

Strategic Considerations

Governance & Strategy for Executives & Board Members

- Executives are ultimately accountable. Accordingly, they need to better understand the ICS/OT security vulnerabilities and potential impacts on their business and operations (potential revenues lost & services failure)
- As it is done for IT security, they must appoint an individual accountable for ICS/OT security, who will brief senior management on a regular basis (every 3 months or as required)
- They must develop and maintain a company-wide culture of security through regular communications and training
- They need to establish the top risks (3-4) that the organization is facing and do follow-ups on a regular basis
- They must ensure that the recent threats towards their industry have been addressed by the security team through consequence-driven scenarios most likely to impact their most valuable assets (i.e., business impact analysis)
- They must have a plan and budget to address all known security vulnerabilities by starting with the most critical sites/infrastructure (based on revenues streams and/or the criticality of the services provided)
- They should ensure that the effectiveness of the ICS/OT cyber security program is reviewed and evaluated on a yearly basis (in addition to NERC CIP compliance)

> We have a culture of compliance when we should really have a culture of security.

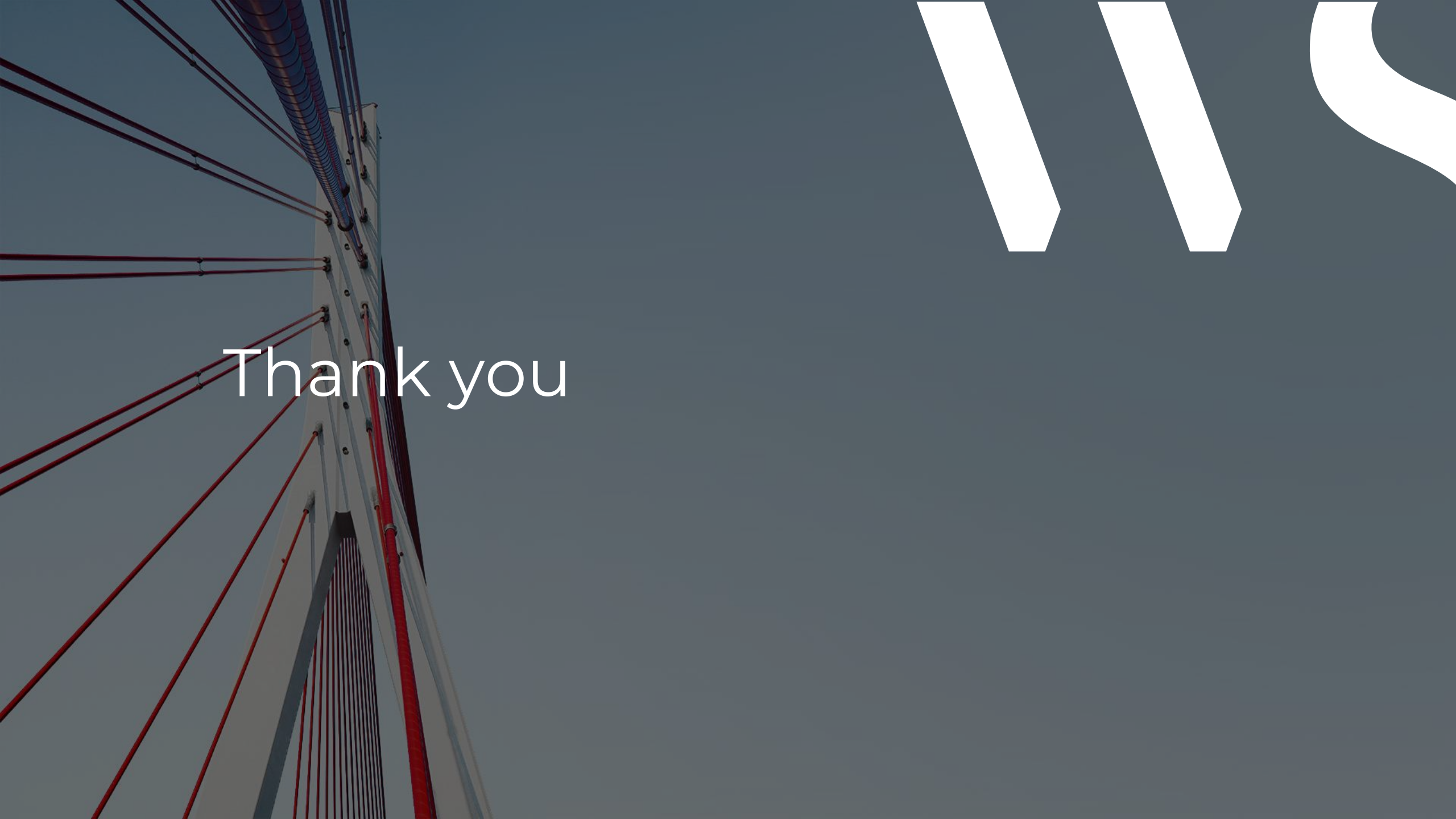
Timothy E. Roxey
VP and Chief E-ISAC Operations Officer at NERC

Governance & Strategy – Standardize where possible!

- Standardize and limit the number of systems/technologies that need to be secured to increase efficiency & interoperability
- Standardize processes and technologies to facilitate the integration of newly acquired utilities and/or companies (M&A)
- Standardize to reduce the number of suppliers you need to deal with. This should reduce the complexity of the security operations, support and compliancy processes
- Standardize to reduce training costs
- Standardize to reduce systems & spare parts inventory

People – your most critical assets (internal & external)

- People being the weakest link in security, a comprehensive security training program must be implemented and performed on a regular basis for:
  - All employees involved in the digital transformation
  - All users at all level of the organization to develop a sense of awareness and a good security culture
- Where needed, partners and consultants should be leveraged to bridge internal knowledge and specific expertise gaps
- Day-to-day operations should be centralized where possible to reduce the number of expert resources needed
- Where possible, non-core, or highly specialized functions should be outsourced to reliable third parties (ex., 24/7 monitoring, SaaS)


Thank you