Canadian Electricity Association | Association canadienne de l'électricité

Cybersecurity in Canada's Electricity Industry:
The Need for Unwavering Leadership

Speaking Notes
By
The Honourable Sergio Marchi
President and CEO of the Canadian Electricity Association

Independent Electricity System Operator (IESO)
Executive Briefing on Cybersecurity
Toronto, Ontario
January 19, 2016

Introduction

- Thanks to Bruce for inviting me to join you this morning. I compliment IESO for organizing this briefing, as it is extremely useful for information sharing, which is at the heart of our capacity to deal with cyber threats.

- It is a real pleasure to be with all of you, including a number of representatives from several CEA members, as well as CEA board member Max Cananzi, CEO of Horizon Utilities.

- In preparing my remarks, Bruce and his team asked me to address a number of items, including the status of: 1) government policy; 2) lobbying initiatives; 3) strategic programs within our member companies; 4) key issues constraining organizations to more effectively manage cyber risks; and finally, 5) the role of senior executives in supporting their organization's cybersecurity risk management program.

- For me and CEA, the overarching imperative is that cyber threats must constitute a very high priority for our industry and for governments.

- And that is because electricity is simply indispensable to the life of Canada as we know it.

- Canadian's cannot enjoy a high quality or standard of living without reliable electricity.

- And the Canadian economy cannot function efficiently or competitively without the reliable supply of electricity.

- So, any attack that has the objective of crippling our system and undermining the reliability of electricity, must be addressed with seriousness and urgency.

- This must be the broader framework that we should all adopt, as we try to find the best solutions and practices to the cyber threat.

- So, let me share with you a few of my thoughts along the lines suggested to me, in relation to the pressing matter of cyber security.

1) **<u>First, the importance of getting Government policy right.</u>**

- The federal government policy – a five year action plan from 2010 to 2015 – is now formally over, and requires updating by the new government.
  - While the electricity sector first started focusing on cybersecurity since about 1997, and led the Y2K initiative, the 2010-2015 action plan was the first comprehensive national cybersecurity strategy.
  - Incidentally, given the integration of our grid with our friends to the south, the U.S. implemented a cybersecurity presidential policy directive at roughly the same time.
  - Thanks to continued vigilance, there has never been, to my knowledge, a cyberattack in Canada or the US that has been successful at causing power outages to date. And let's hope we keep it that way going forward. In fact, to date, most hack attempts are aimed at seeking some sort of commercial advantage.
  - However, the outage in Ukraine last December that was tied to a cyber-attack, thought to have originated in Russia, reminds us why we do what we do on the cyber security front, and why we must remain steadfast.
- According to his mandate letter, Ralph Goodale, the new Minister of Public Safety and Emergency Preparedness, has been instructed to conduct "*a review of existing measures to protect Canadians and our critical infrastructure from cyber-threats".*
- And CEA is hoping to be a participant in that review, and make our respective contribution.
- The 2015 Budget had allocated some $36.4 million over five years to protect Canada's vital cyber systems, and also to support promised new legislation that would require operators of vital cyber systems to implement specific cyber security plans, and report cyber security incidents to the Government.
- As well, last July, the previous government announced an additional $142.6 million over five years to beef up cyber security across government agencies and in turn help private companies ward off cyber-attacks.

- This new funding would be expected to double the size of CCIRC, from 45 officials to around 90, by April 2017.

- So, we await the new government's pronouncements on renewing the five year plan, the funding envelope and the prospects for any legislative action.

- With respect to any mandatory reporting of cyber security incidents for federally regulated entities, one critical question is how this will impact the provincially regulated electricity sector, which already reports through NERC?

- To ensure that all levels of government have a consistent plan, and that all sectors operate within the same framework, it is essential that national mandatory reporting standards be clearly articulated.

- While these new rules would apply to federally regulated industries, other levels of governments are waiting for direction from the federal government before implementing their own standards, to ensure policy coherence.

- And that is a positive approach to take because it is vital to have consistency and complementarity, and avoid duplication or contradictory signals.

- Another issue is that new standards will need to take into account and bridge the fact that while nuclear assets are federally regulated, electricity is provincially wired.

- Like Canada, when we consider the state of play in the US, they do not have mandatory reporting. There are a raft of proposal floating around in draft Bills in the House and Senate, but nothing is pending.

- In fact, electricity is the only sector that has mandatory reporting through NERC.

- But when we contrast our two countries, we in Canada are more fortunate, because ours is a much smaller community of utilities, and we have far fewer government security agencies and protocols.

- Moreover, we are a far less litigious society which, combined with the smaller utility and security/intelligence community, makes for a more collegial environment in Canada. It also makes decisions and policy development generally more nimble.

- As the new federal government prepares to renew the action plan, CEA would encourage the Minster to consider a number of issues:
  - Consider a funding increase for CCIRC. While the agency is growing in size, its financial resources must also grow in lockstep, so as to adequately build sufficient capacity to meet the growing cyber threats;
  - Foster more systemic information sharing between different sectors;
  - Implement mandatory reporting standards for federally-regulated sectors, which would include the telecommunications sector – because that is a sector that electricity is most heavily dependent upon; and
  - Introduce a more aggressive tabletop exercise program to more frequently test our readiness, similar to the semi-annual initiative led by NERC, and across interdependent critical infrastructure sectors and governments
  - Address vigorously and establish high thresholds for the **three Ps** *prior* to events: Prepare, Predict, and Prevent.
  - And finally, equally apply and/or simulate, standards relating to the **three Rs** *after* events: Respond, Recover, and Restore.

2. Secondly, we need to ensure effective government advocacy of our needs and concerns as a national strategic industry

- Besides my ongoing meetings and those of my staff with appropriate federal government officials on cyber and physical security matters, CEA and its members make a coordinated and concerted lobbying effort principally through our Security and Infrastructure Protection Committee (or SIP for short).
- SIP was launched in 2000, and meets four times a year, for a day and a half. And all meetings consist of 3 components;
  - a full discussion with security agencies reps such as Public Safety, CCIRC, CSIS, RCMP, NRCAN, NEB and NERC,
  - a business component that focuses on reviewing best practices, developing guidelines, and coordinating member efforts across the country; and

    - a “pens down” session where confidential information over sensitive issues and/or events is shared.

- SIP has become a very valuable forum for our members, and has served to strengthen our relationship with the different arms of government as it relates to cyber security.

- As alluded to earlier, SIP presses government to undertake consistent consultations and reporting regionally, nationally and internationally, the latter through NERC.

- By doing so, critical information in turn cascades to other levels of government and fosters consistency and complementarity.

- As well, considering we are already reporting through NERC, the same model and criteria could be implemented for other sectors and other levels of governments

Thirdly, vigilance naturally starts at home, with each Member’s commitment and focused program.

- It is fair to say that each of our members fully understands that the cyber threat has regrettably become a growth industry, and that this therefore requires a dedicated and ongoing strategy to combat this menace, in an effort to ensure the integrity of our systems.

- This commitment fundamentally recognizes that an indispensable line of defence is in the sharing of information and in closely collaborating with other members.

- But on this, frankly, the report card on a North American basis leaves room for much improvement. This comment is not aimed as a criticism, as much as it is identifying opportunities for growth.

- By applying such a discipline, members can then coherently and holistically engage with outside government agencies, and other critical sectors and stakeholders.

- In all of this, regional collaboration is imperative, and in this regard, CEA consistently cites IESO’s Cyber Security Forum as a best practice to emulate across the country.

- Nationally, we work closely with federal officials on policy and programming, and have an information sharing Memorandum of Understanding with CCIRC.

    - The core mission of this agreement is to quickly and regularly exchange information, experiences, and solutions.

    - As you know, CCIRC is not a regulatory body. It focuses on operations. It provides real, hands-on assistance.

- CEA and our members with security clearances also meet with CCIRC, RCMP and CSIS twice a year for classified briefings.

- On a North American basis, CEA collaborates well with NERC, where our members are active in developing the standards that underpin the security of our shared North American electricity system.

- We also partner with the International Electricity Infrastructure Assurance (IEIA) Forum for information and intelligence sharing among the five “eyes”, as they are referred to --- comprising of Canada, US, UK, Australia, and New Zealand.

    - The group meets annually, has an independent secretariat, and the meeting includes both industry and government representatives.

Fourthly what are some of the constraints we need to strategically overcome?

- Two longstanding ones stand out specifically, and one that I would refer to as “new and emerging.”

- It's no secret that a leading challenge, if not *the* leading one, is that organizations are reluctant to share cyber information, for fear that this information will somehow leak into the public domain. Or, they are concerned that access to this information could help attackers identify vulnerabilities and plan future cyberattacks.

- Therefore, the knee jerk reaction is to adopt the rules of poker --- put on a poker face and keep your cards close to your vest.

- That is understandable, but in the long run, the lack of reasonable, systematic, and ongoing transparency represents a significant risk.

- Security personnel must have the confidence to talk to colleagues about their problems, about best practises, about which technologies are being employed and with what success rates, etc.

- It is through greater information sharing and collaboration that individual companies and sectors can improve and further build up their defence mechanisms.

- On this issue, if we are to be successful individually and on a North American basis, it will take a “village.”

- Secondly, we have to build more and stronger bridges between sectors, and elevate our efforts to higher and similar standards and thresholds.

- It’s not rocket science, right? A weak link in the chain will weaken and threaten the entire chain. We therefore need to respect our interdependencies and our ultimate shared security interests.

- As we consider the level of standards, it is generally recognized that the banking fraternity is at the top of the class, followed by the electricity sector.

- More specifically for our sector, because we rely heavily on the telecommunications, transportation, and water and waste water communities, it is important for our interests that those sectors subscribe to high cyber security platforms.

- And the third area is relatively new and emerging. As we increase our vigilance and our expenditures on cyber security technologies, how do we ensure that regulators have a full appreciation of the threats we are encountering, especially since they do not have access to classified briefings? And even if they did, they would not be able to refer to this classified information in their public decisions. So, how would they account for this reality, in a transparent fashion, to consumers?

- Also, how do we explain to consumers and our public the urgency of cyber issues and rationalize our efforts and expenditures, without alarming them or causing undo concerns? How do we build their confidence levels around this growing threat?

- We need to give some careful thought to these new policy dimensions.

5. Finally, leadership from senior executives is crucial.

- While cyber threats require defence systems created and operated by technicians specializing in the field, a commitment from the top is critical. Utility Chairs, Presidents and CEO's need to have a situational awareness of the cyber threat to their operations and their customers.

- They also need to have an appreciation for the constantly evolving nature of the cybersecurity environment, as well as of the broad policy framework that industry and governments have created.

- This is why our CEA board is engaged on the cyber file, as Max will know. At our June board meeting last year, members had a full cyber briefing from an official of Public Safety, and will continue this effort.

- And of course, leadership also means providing your security officials with the funding to have the appropriate level of human resources, and for them to acquire the technological tools they require to get the job done well.

- In this regard, last year, CEA led a cyber mission to Israel, as that country is recognized as a leader in the field of cyber security.

- The Canadian delegation came away thoroughly impressed with the uncompromising leadership that their political and corporate class brings to the cyber file.

- It is a top of mind issue. And they spare nothing, when it comes to their efforts of prevention, mitigation and preparedness, as well as to response and recovery measures.

- The other takeaway was that they are heavily investing in leading edge cyber defences. They are spending the needed monies.

- Because cyber-attacks know no borders, and move quickly and without warning, we would be well advised to learn from that calibre of leadership.

Conclusion

- In closing, the advent of the internet has created a phenomenal value-added amount of private and public good across the globe.

- It was a genius invention that has given us the capacity to do things that only a few short years ago were thought to be simply unimaginable. And we know that new, vast, and exciting frontiers lie ahead of us.

- Yet, like most technologies, man's darker side has also ensured that this invention be manipulated for devious and dangerous motivations.

- And it is this thinking which constitutes a new threat at the heart of our society, and which specifically makes a strategic sector like ours vulnerable to attacks.

- And so, we must respond in kind.

- We must be able to consistently build the better mouse trap, and stay one step ahead, so that our systems remain safe, and provide the reliability that Canadians and Canadian industry demand, and have come to expect from their national electricity industry.

- I remain confident that we can collectively and successfully respond to these threats, as our Western community has done before through the long march of history.

- But it will demand hard work on our part, and on the part of corresponding government agencies.

- The effort will require a resolve and a leadership that is unwavering; an ability to build our defences on the pillar of shared information and collaboration; and forging a private-public partnership model that works efficiently and one that is adequately funded.

- Thanks for your attention.