Cyber Security: Integrated Roles and Responsibilities

Panel Remarks

by

The Honourable Sergio Marchi

President and CEO of the Canadian Electricity Association

CAMPUT Regulatory Key Topics Meeting

February 22, 2016

Opening:

- Let me start by complimenting Ken and CAMPUT for organizing this panel, as it is extremely useful for information sharing, which is at the very heart of our ability to successfully deal with cyber threats.

- While preparing these remarks, I was reminded of a recently-launched website called "cybersquirrel1.com." The site talks of the latest "war operations" perpetrated by squirrels, birds, and other animals against electricity facilities, which were "successful" in causing grid disruptions and outages.

- To date, there have been hundreds of grid disruptions caused by rodents, compared to the miniscule number caused by human directed cyber-attacks, so I'm wondering if we're focusing on the right culprit?!

- On a more serious note, let me touch on 4 items:

1. **First, the current state of risk that utilities face.**

- For CEA, cyber threats constitute a critically high priority.

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

- Canadians cannot enjoy a high standard of living and the Canadian economy cannot function competitively, without a reliable and sustainable supply of electricity.

- As such, electricity is a *strategic asset*.

- And thus, any attempt to cripple our system, must be addressed with seriousness and urgency.

- Simply put, cyber is a top of mind issue for us.

- The grim reality is that cyber attacks have grown exponentially; they are regrettably, a growth industry.

- And the electric utility sector remains a high target.

- Like all businesses, electric utilities face cyber-attacks on their IT systems. But impacts to IT systems do not result in the loss of service to customers, as our Industrial Control Systems, such as SCADA systems, operate on separate, and protected networks.

- However, since the Stuxnet attack on Iran in 2010, for example, there has been interest in and attempts to penetrate the SCADA networks of electric utilities.

- Another illustration of this acute awareness is the annual risk mapping exercise undertaken at NERC, in which experts gather to identify the major evolving risks in our sector, and to prioritize efforts to control and mitigate these risks.

- Unsurprisingly, in the most recent exercise completed in October 2015, cyber security ranked highly in the pyramid of risks - warranting ongoing vigilance and action.

- Last December, the electricity sector crossed a cyber-Rubicon for the first time, when a cyber-attack resulted in the loss of electricity service to 200,000 customers in Ukraine.

- We are working closely with the US, who dispatched a team to help Ukrainian officials to investigate, and are ensuring that our members are provided with recommended mitigation measures coming out of this investigation.

- When we consider the cyber threat, we must address how the Canadian and North American communities share information. And here, the report card is not as good as it needs to be.

- Typically, people's initial reactions mirror the game of poker. They wear a poker face and keep their cards close to their chest. It's understandable. It's not easy to talk about this for fears that it may get out and impact one's company negatively.

- Yet, this approach represents a real risk and vulnerability going forward.

- (Mention on a North American basis……)

- People must confidentially but candidly talk about the threats, share information on what technologies people are employing, how those technologies are working, and exchange best practices.

- By taking such an approach, we would strengthen are defensive capacities.

2. **<u>This brings me to my second point, namely, how does CEA work to address the cyber threat?</u>**

- We have been engaged with key partners in Canada, and on a North-American basis, since we began addressing Cyber issues, back in 1998, in preparation for the Y2K issue.

- On the Canadian front, we work very closely with NRCan on a broad range of issues, including on cyber. They have proven to be a very effective window into what is occurring in the rest of the energy industry, and have undertaken training initiatives specific to cyber security in the energy sector.

- Both RCMP and CSIS are key partners for security and intelligence information sharing. They have effectively provided situational awareness information to our members and for those who are security cleared, they share classified intelligence

- However, our most critical partnership is with Public Safety Canada, on two levels:

    - First, we engage on policy issues, such as in the development and implementation of the Government's National Strategy on Cyber Security

- And secondly, on the operational level, we work through the Canadian Cyber Incident Response Centre, or CCIRC, with whom we entered into a memorandum of understanding on the sharing of information back in 2012.

- Our CEA members principally work through our Security and Infrastructure Protection Committee (or SIP for short).

- It is also mainly through SIP, where we do much of our advocacy work with governments.

- 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 agency reps, including 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 finally, a "pens down" session, where confidential information over sensitive issues, personas, 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.

- On the North American front, 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.

- Through its Electricity Information Sharing and Analysis Center (E-ISAC)," NERC disseminates threat information across the sector.

- Moreover, every two years, NERC conducts a continent-wide simulation – known as "GridEx" – to test utilities' ability to respond to security threats.

    - The most recent was held in November 2015, and I'm pleased to report that Canadian participation was quite high.

- CEA also joins with our American friends in a North American coalition of electric utility associations.

- These associations are also part of a CEO-led body known as the Electricity Subsector Coordinating Council, which engages the highest levels of the U.S. government on cyber and physical security challenges.

- While cyber threats require defense systems created and operated by technicians specializing in the field, a commitment from the top is critical.

- It is important for Utility Chairs, CEO's and senior executives to have a situational awareness of the cyber threat to their operations and customers.

- (*For example, Target CEO dismissed for the cyber attack that resulted in a breach of customer credit card info*)

- This is why our CEA board is engaged on the cyber file. Besides reports from SIP, for the past two years at our board meetings, members had full cyber briefings from officials from Public Safety, and we will continue this effort.

- Leadership also means providing one's security officials with the funding for the appropriate level of specialized human resources, and for acquiring 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 leaders bring to the cyber file.

- Cyber concerns are at the top of their radar screens. 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 spending the needed monies in investing in the leading edge cyber defenses.

3. **<u>Third, a renewed look at the role of our federal government</u>.**

- 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".

- CEA is hoping to be a participant in that review, and make our respective contribution.

- Likewise, I believe this pending federal review provides a key opportunity for CAMPUT members to further enhance their understanding of existing cyber policy, and to explore opportunities for effective partnerships – all with an eye towards protecting customers.

- 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.

- On top of this, last July, an additional $142.6 million over five years was announced, to beef up cyber security across government agencies and in turn help private companies ward off cyber-attacks.

- The new funding levels would have been expected to double the size of CCIRC, from some 45 officials to around 90, by April 2017.

- While the agency is growing in size, it's critical that financial resources grow in lockstep, so as to adequately build sufficient capacity to meet the growing cyber threats;

- The 5 year national cyber plan expired at the end of last year.

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

- In fact, last Tuesday, I appeared before the Finance Parliamentary Committee re our Budget asks, and the cyber imperative was on my list.

- Some observers expect that a key area of discussion in this federal review will be whether mandatory reporting of cyber security incidents should be required for federally-regulated entities and critical infrastructure sectors.

- 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 any new such 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.

- For us, one crucial question is, how any new reporting standards would impact the provincially regulated electricity sector, which already reports through NERC?

- 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.

- CEA will also be encouraging the federal government to introduce a more aggressive tabletop exercise program to more frequently test our readiness, similar to the semi-annual GridEx initiative led by NERC, and do so across interdependent critical infrastructure sectors and governments.

- We need high thresholds for the **three Ps** *prior* to events: Prepare, Predict, and Prevent.

- And equally for the **three Rs** *after* events: Respond, Recover, and Restore.

4. Finally, where does CAMPUT go from here?

- While the regulator's role in cyber-security is not operational in nature, CEA nevertheless believes there are several opportunities for CAMPUT to enhance its engagement in this space and provide a value-added contribution to the larger effort of mitigating risks:

    - The first of these involves strengthening participation in existing forums which are essential for policy and regulatory dialogue and action.

    - For instance, NERC hosts quarterly meetings of its Board and major stakeholder representatives committee, the latter of which has seats for Canadian provincial and federal government representatives.

    - CAMPUT has been very ably represented to date by your colleagues Ken Quesnelle and Murray Doehler. Respectfully, CEA would invite CAMPUT members to collectively consider whether these seats at the table are being fully leveraged, or whether an enhanced presence and voice may be feasible?

    - Likewise, the August quarterly NERC Board meeting is always held in a Canadian venue. On the margins of last year's meeting, NERC held an event for the specific purpose of facilitating dialogue between Canadian regulators and NERC leadership on cyber security issues.

    - In fact, that's where I met Ken. There was good attendance at this event, and we hope that efforts will be undertaken to build upon the momentum and successes of these forum to yield greater fruit in the future.

- Similarly, CEA is aware that individual CAMPUT members engage regularly with their U.S. counterparts, in a variety of ways.

- This includes liaising with NERC and FERC staff through the existing Federal-Provincial-Territorial (FPT) Electricity Working Group; participating in FERC's annual Technical Conference on electric reliability policy issues; meeting with NARUC peers on a yearly basis; and inviting NERC, FERC, and NARUC leaders to your AGM, as is planned for this year's event in May.

- CEA sincerely commends these efforts and encourages CAMPUT to explore ways to maximize the frequency and effectiveness of these activities.

- For example, the FPT Group arguably stands to benefit from more fulsome participation by each province.

- Furthermore, a rotation of CAMPUT participants at FERC conferences would likely enhance the collective Canadian effort and voice.

- And perhaps engagement with NARUC could involve more focused attention and action, when it comes to learning about and adopting best practices that NARUC has developed.

- In this regard, an excellent example is NARUC's cyber security guide for state regulators. Released in 2013, this is a valuable primer on the issue – particularly from a distribution-level perspective – and includes sample questions for regulators to ask utilities.

- It might also be valuable, as I already intimated to Ken, for your May conference in Montreal to have a cyber security panel, where you can build on the efforts of today's session.

- In addition, more and stronger bridges between sectors are required, and we must 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 shared security interests.
- More specifically for our sector, because we rely heavily on the telecommunications, transportation, and water and waste water communities, it is important that those sectors subscribe to high cyber security platforms.
- And finally, given that the cyber threat is relatively a more recent phenomenon, compared to the other issues that we have had to grapple with, and that it is becoming increasingly more sophisticated, we need to reflect on how best to approach this emerging challenge?
- We know that cyber threats will not go away. They will unfortunately only increase, as a new E- theatre of "war" replaces or complements the old, traditional one.
- Thus, projecting into the future, as our utilities increase their vigilance and their expenditures on cyber security technologies, how do we ensure that regulators and the public have a full appreciation of the threats we are encountering?
- That you have a solid situational awareness of the magnitude of the cyber problem?
- In this regard for example, at present, regulators don't have access to classified information. Should they? Some would argue no, since you do not have an operational role in this domain.
- And if you did have access, given that the information is strictly confidential, how would you reflect this in your final decisions which are public?

- Another related matter is, how 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?

- In other words, how do we build public confidence levels around this growing threat, with the right measure of proportionality?

- As we craft policies and protocols for dealing with the cyber reality, we will need to address these and other issues on an ongoing and evolving basis.

- And that's why today's forum is so useful, because it provides an opportunity to share information, to educate one another, and to raise the relevant questions.

- And this is the first step towards coming up with the right answers.

- In closing, I hope my remarks were helpful to this cause, and I look forward to your feedback and our open discussion.

- Thanks for your attention.