Hackers and Extreme Weather: Using a Risk Based Framework to Protect Consumers from Both

BY JACKIE ASHLEY & MICHELLE NOCK

Jackie Ashley is a Senior Regulatory Specialist at the British Columbia Utilities Commission and can be reached at Jackieashley5@gmail.com. **Michelle Nock** is a student at McGill University.

Abstract

Cybersecurity is increasingly being regulated by incorporating a risk-based framework that is a process – not a set of standard or rules. This article describes this framework and proposes that it could also be used for climate related risks, such as extreme cold/heat events and wildfires.

Introduction

The February 2021 severe winter storms crippled the electricity grid in Texas and left millions of people shivering without power, heat and running water for several days. Most tragic of all were the deaths it caused, with some people dying from the cold and others from carbon monoxide poisoning while trying to keep warm.

A key contributor to the Texas outage was inadequately winterized electricity generation and natural gas equipment. This risk was already known – a winter storm in 2011 triggered widespread blackouts and revealed the power grid's vulnerability to cold temperatures. Unfortunately, recommended changes were not made.

What can utility regulators do to ensure that utilities proactively identify and address these types of weather-related risks, such as extreme cold, extreme heat, hurricanes, storms and wildfires?

Currently regulators tend to use input standards (such as planning criteria) or output metrics (such as desired reliability levels) to address reliability concerns. However, given the rapid evolution of the generation resource mix and increased frequency of severe weather events, these approaches on their own may no longer be sufficient to address emerging resilience risks.

This article suggests that utility regulators look to the risk-based framework developed to address cybersecurity risk for inspiration. These risk-based frameworks are a process – not a set of standards or rules – that focus the utility's attention on cybersecurity risks. A similar approach could also be used to ensure that weather related risks receive the attention they deserve.

NIST Cybersecurity Framework

To address cybersecurity risks, in 2014 the National Institute of Standards and Technology (NIST) produced a Cybersecurity Framework that utilized a risk-based approach. It is a voluntary framework developed through collaboration between industry and government. It was designed to be flexible enough so that it can be applied to organizations of any size, any cybersecurity risk level, and any level of cybersecurity preparedness, regardless of the industry or country.

The NIST Framework Core consists of five concurrent and continuous functions – Identify, Protect, Detect, Respond, Recover.

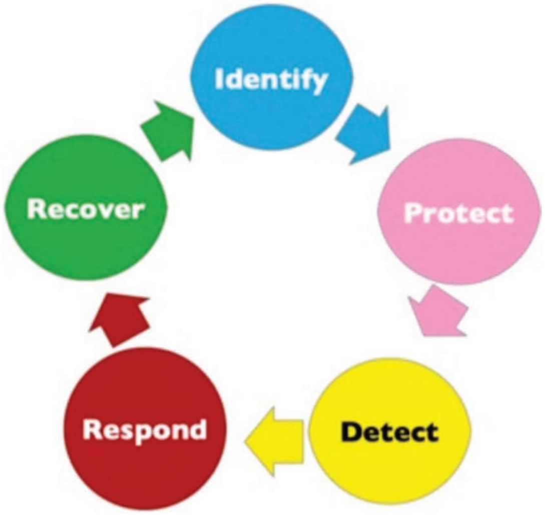


Figure 1: NIST Framework Core Functions (NARUC)

When considered together, these functions provide a strategic view of an organization's management of cybersecurity risk:

- **Identify** – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- **Protect** – Develop and implement appropriate safeguards to ensure delivery of critical services.
- **Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- **Recove**r – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

The framework can be described as a basis for having a discussion or a template to start a conversation. The focus of this approach is therefore not to tell the utility specifically what it should do to manage risks (which could risk regulatory overreach as regulators do not have a mandate to manage the utility), but to ensure that the utility goes through the proper process to arrive at a plan that is in the public interest.

NARUC Cybersecurity 'Questions for Regulators'

The NIST framework has been used as the cornerstone for the development of risk-based cybersecurity approaches by regulators in the US, UK, Canada and Australia. This included development of questions for regulators to ask utilities and tools to evaluate responses.

For example, the National Association of Regulatory Utility Commissioners (NARUC) has developed a comprehensive suite of resources, collectively referred to as the "Cybersecurity Manual," to help public utility commissions gather and evaluate information from utilities to inform their decision making about cybersecurity risk management practices.

This includes "Understanding Cybersecurity Preparedness: Questions for Utilities" which contains a 4-page "Plain English" list of context-sensitive questions that regulators can ask of a utility to gain a detailed understanding of its current cybersecurity risk management program and practices. Regulators do not need to become cyber industry authorities or enforcers, but asking a utility a question can motivate the development of a well-founded answer.

These questions are organized by the five NIST core functions (Identify, Protect, Detect, Respond, and Recover) and are further divided into two categories "Policy and Plans," and "Implementation and Operations." Sample questions from this list are provided in Figure 2:

Sample Questions – Cybersecurity

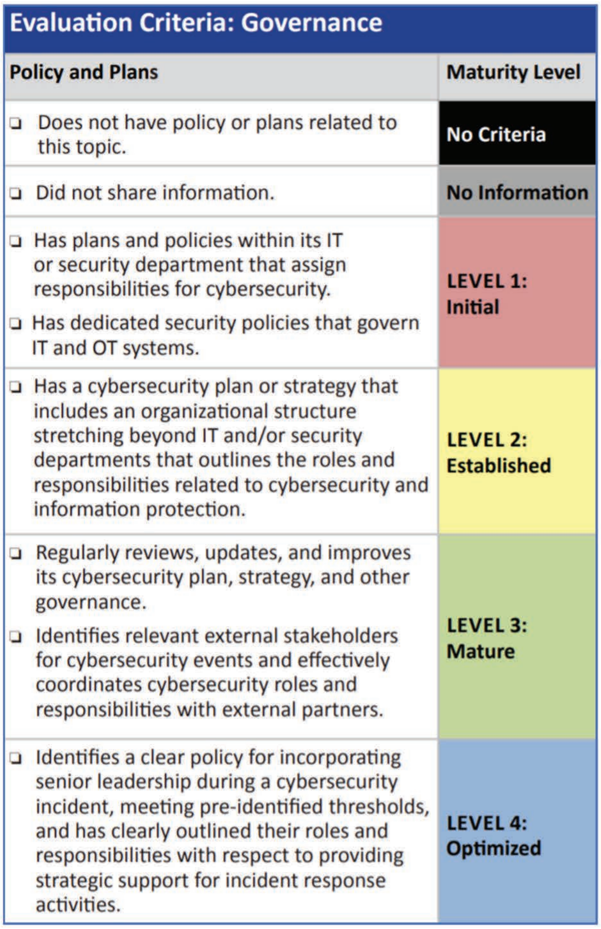
1. Do you have a cyber risk management program? a) If so, who leads the program? b) Is executive leadership actively engaged? c) Are cybersecurity roles and responsibilities defined? d) Have you formed a cross-functional team that spans relevant business units to assess risks to and criticality of business functions? e) Is the program based on a cybersecurity framework (e.g., NIST, NERC CIP)?[1] f) Is the program integrated into overarching enterprise risk management? g) Are criteria for defining and managing cybersecurity risk included? If yes, please explain.
2. Have resources (funding, personnel, technology) been dedicated to meet cybersecurity risk management objectives? a) Are personnel dedicated full time, part-time, or as part of other duties? b) Is funding commensurate with cybersecurity risk management objectives? Are funding levels consistent?
3. Have you developed policies and procedures regarding cybersecurity event detection activities, including roles and responsibilities, oversight, and communications, to rapidly detect and mitigate cybersecurity incidents? If so, please describe a) the classification scheme for identifying and reporting cyber events, including thresholds; b) the system and network monitoring requirements; and c) the frequency of reviews and updates to policies and procedures.
4. Do you have cyber incident response policies and plans in place for minimizing the effects of a cyber incident? a) If yes, are roles and responsibilities for recovery defined? b) Are incident severity thresholds defined? c) Are escalation criteria defined? d) Are mandatory third-party incident notification requirements documented (e.g., to PUC, SEC)?[2] e) Does your response plan include interactions with third-party service providers?
5. Have you identified minimal operational functionality for recovery of critical assets?

NARUC Cybersecurity 'Evaluation Tool'

Just asking questions isn't enough—once the right questions have been asked of utilities, regulators bear the responsibility of understanding the answers to determine whether they represent prudent activities and investments.

To assist in this next step, NARUC have also developed a simple, easy to use "Evaluation Tool" to help regulators evaluate a utility's responses against generally accepted standards, best practices, and the utility's specific needs.

For example, evaluation criteria for the first category of "Questions for Regulators" (Identify – Governance: Policy & Plans) are shown below:



Evaluation Criteria: Governance

Policy and Plans	Maturity Level
❑ Does not have policy or plans related to this topic.	No Criteria
❑ Did not share information.	No Information
❑ Has plans and policies within its IT or security department that assign responsibilities for cybersecurity. ❑ Has dedicated security policies that govern IT and OT systems.	LEVEL 1: Initial
❑ Has a cybersecurity plan or strategy that includes an organizational structure stretching beyond IT and/or security departments that outlines the roles and responsibilities related to cybersecurity and information protection.	LEVEL 2: Established
❑ Regularly reviews, updates, and improves its cybersecurity plan, strategy, and other governance. ❑ Identifies relevant external stakeholders for cybersecurity events and effectively coordinates cybersecurity roles and responsibilities with external partners.	LEVEL 3: Mature
❑ Identifies a clear policy for incorporating senior leadership during a cybersecurity incident, meeting pre-identified thresholds, and has clearly outlined their roles and responsibilities with respect to providing strategic support for incident response activities.	LEVEL 4: Optimized

Figure 2: NARUC Evaluation Tool: Identify (Governance)

The "Evaluation Tool" does not require that utilities use a specific approach, and this flexibility accommodates a wide range of different cybersecurity practices. The specific needs of each utility differ and, as such, each utility would be expected to adopt the cybersecurity practices that best fit its unique circumstances.

Used together, the "Questions for Utilities" and "Evaluation Tool" provide a holistic view of a utility's cybersecurity risk management program that can complement compliance-based approaches already in place.

Application to Extreme Weather Risks & Wildfires

The NARUC cybersecurity "Questions for Utilities" and "Evaluation Tool" could provide a useful starting point in developing a similar risk-based approach to address other emerging and rapidly evolving threats and vulnerabilities, such as the extreme weather events seen in Texas.

This risk-based approach could help regulators identify gaps, spur utilities' adoption of additional mitigation strategies, and encourage improvements over time. It would allow regulators to assess the maturity of a utility's program to address extreme weather-related events (such as extreme cold, extreme heat, and wildfires), gauge improvements to the program year over year, and evaluate utility decisions and their approaches to planning for and making resiliency-focused investment.

To illustrate this approach, the 5 sample questions from NARUC's cybersecurity "Questions for Utilities" shown previously have been reworded to replace "cybersecurity" with "extreme cold":

Sample Questions – Extreme Cold

1. Do you have an ***extreme cold*** risk management program? a) If so, who leads the program? b) Is executive leadership actively engaged? c) Are ***extreme cold*** roles and responsibilities defined? d) Have you formed a cross-functional team that spans relevant business units to assess risks to and criticality of business functions? e) Is the program based on a cybersecurity framework (e.g., NIST, NERC CIP)? f) Is the program integrated into overarching enterprise risk management? g) Are criteria for defining and managing ***extreme cold*** included? If yes, please explain.
2. Have resources (funding, personnel, technology) been dedicated to meet ***extreme cold*** risk management objectives? a) Are personnel dedicated full time, part-time, or as part of other duties? b) Is funding commensurate with ***extreme cold*** risk management objectives? Are funding levels consistent?
3. Have you developed policies and procedures regarding ***extreme cold*** event detection activities, including roles and responsibilities, oversight, and communications, to rapidly detect and mitigate ***extreme cold*** incidents? If so, please describe a) the classification scheme for identifying and reporting **extreme cold** events, including thresholds; b) the system and network monitoring requirements; and c) the frequency of reviews and updates to policies and procedures.
4. Do you have ***extreme cold*** incident response policies and plans in place for minimizing the effects of an ***extreme cold*** incident? a) If yes, are roles and responsibilities for recovery defined? b) Are incident severity thresholds defined? c) Are escalation criteria defined? d) Are mandatory third-party incident notification requirements documented (e.g., to PUC, SEC)? e) Does your response plan include interactions with third-party service providers?
5. Have you identified minimal operational functionality for recovery of critical assets?

In reviewing these reworded questions, readers are asked to consider whether adoption of this risk-based approach after the Texas 2011 storms could have better focused utility management's attention on the severe cold problem, and so mitigated the significant negative impacts to customers of the Texas winter storms a decade later.

The above 5 questions are a sample only. Readers are encouraged to review the full 4-page list of questions included in NARUC's "Questions for Utilities" and the accompanying 9-page NARUC "Evaluation Tool."

In addition, NARUC have developed a complementary resource – "Smart Grid: Questions for Utilities" – for utilities with a high penetrations of distributed energy resources

Conclusion

Managing extreme weather impacts during a time of energy market transformation can be a highly complex undertaking, requiring significant coordination among widely diverse policymakers and stakeholders.

This article recommends that regulators look to the easy to use and innovative risk-based frameworks developed to address cybersecurity risks and consider repurposing them to address other risks, such as extreme cold, extreme heat, hurricanes, storms and wildfires.

Working together we will be able to provide good solutions and great pathways going forward.

Disclaimer

This article does not represent the views or opinions of the British Columbia Utilities Commission (BCUC), nor does it express, or intend to express, any opinion on pending or future matters before the BCUC. This article was developed personally by the author and not in a professional capacity as a BCUC employee.

References

Australian Energy Sector Cyber Security Framework – Framework Overview (2021), Australian Energy Market Operator.

Costantini, L. et al. (2019) "Understanding Cybersecurity Preparedness: Questions for Utilities," NARUC.

Costantini, L. (2020) "Understanding Cybersecurity for the Smart Grid: Questions for Utilities," NARUC.

Hesmondhalgh, S. et al. (2014) “Approaches to setting Electric Distribution Reliability Standards and Outcomes,” The Brattle Group.

Keogh, M. et al. (2017) “Cybersecurity – A Primer for State Regulators,” NARUC.

NARUC Cybersecurity Preparedness Evaluation Tool (2019), The Cadmus Group LLC.

Robb, J. (2021) “Reliability, Resiliency, and Affordability of Electric Service in the United States,” Testimony before the Committee on Energy and Natural Resources.

RIIO-2 Cyber Resilience Guidelines (2020), Office of Gas and Electricity Markets (Ofgem), Great Britain.

Staff Report to the Board of a Proposed Cyber Security Framework (2017), Ontario Energy Board.

Understanding Cybersecurity Maturity Models with the Context of Energy Regulation (2020), NARUC.

Footnotes

[1] North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)

[2] Public Utilities Commission (PUC); Securities and Exchange Commission (SEC)