The MEARIE Group

The Reciprocal

Managing risk together

Duke Energy – Cyber Risk & Costly Repercussions

The recent news headlines about Duke Energy and the issues they're facing related to North American Electric Reliability Corporation (NERC) regulatory violations could serve as a cautionary tale for utilities here in Ontario.

Duke Energy is one of the largest utility providers in the U.S. with 7.6 million customers across six states. Recently NERC cited Duke Energy for a total of 127 violations. Duke Energy was handed the biggest fine in NERC's history, with an agreed amount of $10,000,000.

The violations cited were caused by:[i]

- Lack of managerial oversight
- Process deficiencies
- Inadequate training of staff
- Lack of internal controls
- Operational silos and a lack of communication between management levels
- A general lack of awareness of the state of security and compliance

In the rules based regulatory environment in the U.S., compliance is key to avoiding hefty fines and lengthy remediation requirements and is best coupled with strong corporate governance.

Although the regulatory landscape differs in Canada, tending towards principles-based guidance, the net exposure is similar and utilities in Ontario face the same challenges in protecting their networks from cyber threats. The recent introduction of the OEB Cybersecurity Framework has also raised awareness for Ontario utilities for potential regulatory recommendations and compliance requirements related to understanding and management of cyber risks.

There are clear parallels between the Duke Energy violations and the intent of recommendations under the OEB cybersecurity framework.

Among the most serious violations cited against Duke Energy were:

- Failure to protect critical cyber asset (CCA) information.
- Failure to maintain annual cybersecurity training for employees with electronic and/or physical access to CCAs.
- Failure to timely revoke former employees' and contractors' electronic access rights.
- Allowing individuals improper access to critical infrastructure protection (CIP)-protected information.
- Failure to monitor electronic security perimeter (ESP) inbound and outbound communications and to restrict inbound electronic access to ESPs. Also, the use of overly broad firewall rulesets which allowed potentially nefarious traffic.
- Firewalls were configured to allow external remote access to sensitive systems without first going through an intermediate system, using encryption or requiring multi-factor authentication.
- Failure to implement physical access controls to limit unescorted access to the physical security perimeter and failing to document all required information in visitor log books.
- Repeated failures to adhere to cybersecurity testing procedures, including deficient testing on software upgrades and failures to implement security patch programs.
- Failing to change passwords on an annual schedule and failing to change factory default passwords for remotely accessible BES cyber assets.

Originally issued February 2019.

The above nine violations could have been avoided with the implementation of a well-developed corporate cybersecurity policy which considers cyber risks on an enterprise wide basis. Effective management controls and oversight can be difficult and require focused effort on a continuing basis. Some important aspects include quality assurance, staff supervision, development and enforcement of corporate policies, and facilitating improvements in practice.[ii]

Duke Energy did not just get hit with a huge fine but had to agree to several measures to materially improve management and oversight of cybersecurity and ensure future compliance with the regulations. As part of the settlement, Duke Energy agreed to:

- Pay $10 million in fines
- Improve their performance by increasing senior leadership involvement and oversight
- Create a centralized critical infrastructure protection (CIP) oversight department
- Restructure roles to focus on standards, enterprise oversight, enterprise CIP tools, compliance metrics, and regulatory interactions.
- Conduct industry surveys and benchmark discussions to develop best practices
- Invest in enterprise-wide tools for assets and configuration management, visitor logging, access management, configuration monitoring, and vulnerability assessment
- Increase training
- Institute annual compliance drills

For utilities, the stakes are high. In addition to privacy regulation, related to the protection of client data, clearly the disruption of the electrical system would have dire consequences – particularly due to remediation costs, potential damage to customers, as well as company reputation and public trust. In 2018, the "Department of Homeland Security reported that over the last year, Russia's military intelligence agency had infiltrated the control rooms of power plants across the United States. In theory, that could enable it to take control of parts of the grid by remote control."[iii]The threat is real and easily transcends borders to Canada as well.

For resources to help in the development of corporate policies related to cyber risk management, MEARIE Members can find more information and useful guidance in the NetDiligence eRiskHub. Log in through www.mearie.ca to access this valuable tool.

NetDiligence® | eRiskHub®

[i] Heidorn Jr. Rich. "NERC Seeks $10M Fine for Duke Energy Security Lapses." https://www.rtoinsider.com/nerc-fine-duke-energy-cip-110308/. Accessed on February 12, 2019

[ii] Gheorghiu Iulia. "Duke fined $10M for cybersecurity lapses since 2015." https://www.utilitydive.com/news/duke-fined-10m-for-cybersecurity-lapses-since-2015/547528/. Accessed February 11, 2019

[iii] Sanger, David E. "Russian Hackers Appear to Shift Focus to U.S. Power Grid." https://www.nytimes.com/2018/07/27/us/politics/russian-hackers-electric-grid-elections-.html Accessed February 12, 2019