Hydroelectric Cybersecurity Regulatory 101

Darsh Singh
Northwest Hydroelectric Association
February 20, 2020
Hydroelectric Cybersecurity Making Headlines

• **January 2020** – DHS Warns Escalated Tension with Iran Heightens Cybersecurity Threat to US Critical Infrastructure

• **November 2019** – FERC Staff’s “Key Cybersecurity Program Priorities”
  • New security-focused group within Dam Safety and Inspections
  • Realignment of the functions of the Office of Electric Reliability

• **March 2016** – Iranian cyberattack on U.S. Dam
There is no overarching comprehensive cybersecurity legislation.
NERC Critical Infrastructure Protection (“CIP”) Standards – *Looking Ahead*

- **April 2020** - CIP-003-8 (Security Management Controls)
- **July 2020** –
  - CIP-005-6 (Electronic Security Perimeters)
  - CIP-010-3 (Configuration Change Management and Vulnerability Assessments).
- **January 2021** - CIP-008-6 (Incident Reporting and Response Planning)
Cybersecurity Continuum

Business Impacts

Left of BOOM

- Build Multi-disciplinary Team
- Understand Your Assets and Information
- Understand Interdependency (Supply Chain)
- Review Cyber Insurance Terms
- Create an Incident Response Plan
- Test and Revise Response Plan as necessary

BOOM
(aka Cyber Incident)

- Investigate and Contain Breach
- Execute Notification Strategy
- Regulator Enforcement
  - (State and Federal)
- Class Action Suits
- SEC Disclosures
- Mitigate Adverse Consequences to Business Reputation
- Contact Local Law Enforcement/FBI

Right of BOOM

PROACTIVE MEASURES

REACTIVE MEASURES
Cyber Investigations
Adopt an Utility-Wide Approach

CEO/COO

Risk Management

Physical Security

CSO, CISO, CIO, CPO
Coordination: Investigation, Containment & Recovery

Finance/Contracts

IT Security

Invest in Reasonable Security Measures

Human Resources

Comms & Gov’t Relations

Employee Training Proactive & Reactive

Legal

Notify Law Enforcement, Outside Counsel, Consultants

Review/Understand Insurance Coverage

INCIEND RESPONSE PLAN
- TEST -
- REVISE -
- REPEAT -

Notifications to Consumers, Public, Regulators, Congress
The Cost of Cyber

- Cyber breaches are costly
  - Global average cost of data breach is up 6.4% to $3.86M.
  - Average cost for each lost or stolen record containing sensitive information increased by 4.8% to $148k; Denial of Service Attack can cost $10-50K per hour in lost revenue not to mention reputational harm
  - Reputational Harm

- An ounce of prevention is worth a pound of cure
  - Consider drafting an incident response plan to make investigations run smoother.
  - If a plan already exists, review and update it at necessary.
  - The key is to have an “actionable plan” that recognizes industry standards.

Source: (See IBM’s 13th Annual Cost of Date Breach Study by Ponemon Institute)
Thank you! For more information:

Darsh Singh
202-298-3736
dxs@vnf.com