National Institute of Standards and Technology
U.S. Department of Commerce

U.S. Resilience Project

BEST PRACTICES IN CYBER SUPPLY CHAIN RISK MANAGEMENT

Great River Energy
Managing Supply Chain Risks Holistically

INTERVIEWS

Mike McFarland
Director, Enterprise Risk Management

Andy Stewart
Director, Business Operations

The Next New Things in Cyber Security Supply Chain Risk Management

- An umbrella framework to guide its risk management operations, based on the British government's integrated security framework, that balances physical, technical and procedural controls and business needs.
- Tiered security requirements depending on the criticality of the asset.

Company Overview

Great River Energy (GRE) is a generation and transmission cooperative. They manage the power generation and the big transmission lines to the substations where their customers — 28 different rural distribution cooperatives — deliver power to homes and businesses. Conceptually, they run the interstates and the rural cooperative takes care of the city streets.

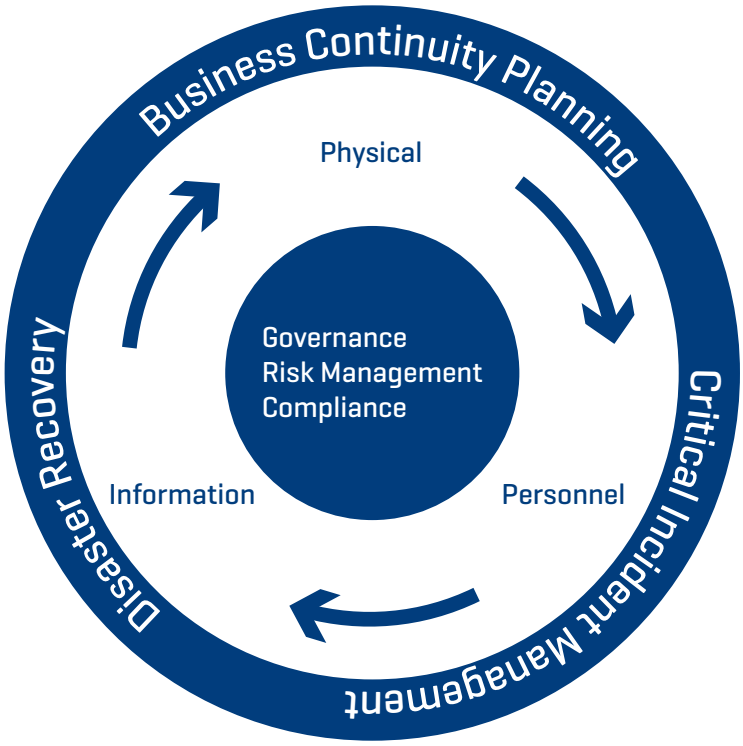
Holistic Risk Management Framework

One challenge the company faced was to develop a broad risk framework to guide risk decision-making for the entire organization. None of the frameworks it researched met the need. They were either too cyber focused, too focused on physical security with a cyber piece bolted on, too prescriptive, or too generic.

Senior managers stumbled on a document that fit their requirements for an integrated risk management framework perfectly: the British government's Security Policy Framework. At the highest level, the framework created:

> "...A risk management process to protect assets (i.e. people, information, infrastructure and facilities) and services appropriately, proportionate to threats and in a way that supports (and does not inhibit) business. Physical, technical and procedural controls need to be balanced to achieve an appropriate security approach that meets the needs and circumstances of an organization. These controls should be supported by effective and resilient business processes to respond to, investigate and recover from any incidents."[1]

Figure 1. Holistic Risk Management Framework



1 http://www.shreddingmachines.co.uk/pdfs/HMG_20Security_20Policy_20Framework_20-_20v8_200_20-_20April_202012.pdf.

One of the flexible aspects of the framework that GRE appreciates is that it is not prescriptive. With regard to governance, for example, it outlines best practices for effective governance, such as annual risk assessments, but does not detail how the organization should be organized. At GRE, supply chain operations and enterprise risk both report to the CFO. The two functions collaborate on risk identification, which range from procurement of critical supplies to power generation and transmission to mitigation activities, such as supplier buffer inventory agreements.

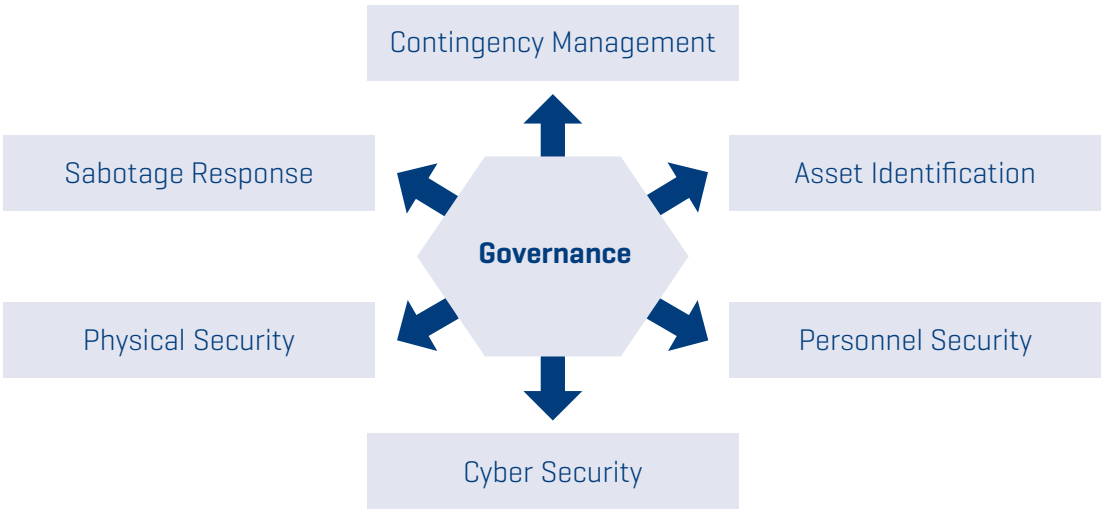
Another core principle in the framework that fits GRE's priorities is that it places responsibility for the protection of assets and people and continuity of business on the leaders of the departments and divisions that manage those assets, not on the IT, security or supply chain groups.

The integrated framework identifies seven priority areas for risk management:

1. Governance
2. Asset Identification
3. Personnel Security
4. Cyber Security
5. Physical Security
6. Sabotage (or terrorism for the UK government)
7. Contingency Requirements

Figure 2 identifies key requirements in each of the seven areas.

Figure 2. Integrated Framework



Key Requirements included in the GRE Risk Management Framework

Governance

- Asset owners have primary responsibility for ensuring implementation and performance of security controls.
- All staff have a responsibility to follow policy, including making contractors, vendors suppliers aware of these responsibilities.
- Asset owners will be trained in security responsibilities; security will be built into staff inductions and training programs.
- Asset owners shall provide updates on areas not in compliance with security policies. Exceptions must be documented and include a description of risks, existing or planned mitigations, justification and business impact.
- An annual report will be submitted to the security team that includes: all significant security incidents, declaration of compliance with mandatory requirements and summary of exceptions.
- Security requirements must be specified in supplier contracts and referenced in business documents.
- Reviews of security arrangements will be carried out as necessary, including internal/external compliance audits.
- Security team will annually review and where necessary update the Security Policy Framework.

Asset Identification

- Leadership will identify cyber, physical and information assets that require security protection and assign an Asset Owner to ensure implementation of security controls.
- Asset owners shall classify their protected physical and information assets and conduct a risk assessment and gap analysis to ensure appropriate levels of protection.
- Asset owners shall provide security team with list of protected assets, classification levels, risk levels and compliance gaps- reviewed annually.
- Asset owners shall identify different levels of information security and label such information to the appropriate level of restricted access.
- Security team, in coordination with the Information Asset Owner, shall define a set of breach management protocols that provide for coordinate response and communications.

Personnel Security

- All individuals granted access to protected information, assets or facilities will complete background screening commensurate to their level of access. Periodic rescreening as appropriate or required.
- All employees will compete general security training. Non-employees with authorized access to protected information, assets or facilities must receive orientation of security policies and their responsibilities under those policies.

Cyber Security

Asset Owners shall:

- Maintain inventories of — and implement practices to detect — unauthorized devices or software.
- Develop and implement secure configuration standards, vulnerability management, remediation practices, and technical or procedural controls to prevent the introduction of malicious software for protected cyber assets, commensurate with the security associated with the identified risk level.
- Utilize secure coding practices for internally developed software and review third party software prior to purchase to ensure compliance with security requirements.
- Implement only IT-approved wireless networking devices.

Cyber Asset Owners should:

- Implement a plan to back up all information including operating system, application, software and data
- Utilize secure practices for remote access to protected cyber assets.
- Identify and store log events related to security
- Develop and implement account management controls to limit access to information and prevent unauthorized use of access credentials
- Develop and implement a vulnerability assessment program

Physical Security

Assets owners must:

- Have a physical Security Plan for each physical location and facility
- Integrate security in to the process of planning, selecting, designing or modifying their facilities
- Conduct a physical security assessment to understand threats and vulnerabilities
- Monitor and control access to their locations, facilities; maintain records of access; and ensure that access control policies are made available to staff.
- Develop plans and procedures to deal with unauthorized visitors or intruders.
- Conduct periodic testing of physical security controls for each location, facility and key asset.

Asset Owners must adopt a layered approach to physical security that is integrated with a layered cyber security approach.

Sabotage Response

Asset owners shall provide guidance and response action for suspected sabotage incidents and procedures for communicating applicable information.

Contingency Requirements

Asset Owners must:

- Provide operating personnel with cyber and physical incident response procedures that include defined roles and responsibilities and detailed response actions.
- Ensure development and implement of a Crisis Management Plan.
- Develop and Implement detailed Business Continuity and IT-Disaster Recovery Plans with designated recovery time objectives.
- Ensure incident and recovery plans are tested periodically
- Provide quarterly incident reports to security team, including results of exercises or plan testing.

Managing Key Risks

Supply Chain: Within the risk framework fall supply chain and cyber risks. GRE has identified four primary supply chain risks:

- Access to ancillary chemicals, such as lime for the scrubbers
- Access to fuel — either coal or natural gas — to operate their plants
- Access to critical parts and material for maintenance and repair of the transmission lines

Given its location in the Midwest, weather is a major risk for supply chain continuity. Although the transmission system is resilient, extreme winter weather, such as ice storms, can cause widespread damage and outages. Similarly, heavy snows can prevent trains from getting through.

Lime supply, in particular, is a prime risk factor. GRE's largest plant is located at the mouth of a coal mine. So, while fuel is not an issue, the continuous supply of lime, which must travel long distances, can be problematic. (Lime is used to extract sulfur dioxide from hot flue gases exiting the boiler. Without it, under EPA guidelines, the plant would not be able to operate). The company maintains a 10-day to 2-week supply to manage short-term disruptions. But, an extended rail disruption, or a lime mine disruption, could force GRE to buy power in the spot market at much higher costs — and those higher prices are passed to GRE's rural cooperative customers and their customers.

The criticality of this risk has triggered an internal audit to look at the resiliency and diversity of GRE's lime suppliers. GRE has agreements with its vendors to maintain excess inventory. But, the audit review will look more closely into the business continuity preparations of suppliers and the availability of alternative suppliers in the event of a disruption.

For non-mine-mouth plants, access to fuel is becoming an issue. Increased demand for rail shipments, congestion and constrained capacity out of the Bakken oil field resulted in delays in coal shipments. GRE is working closely with the rail companies to ensure the timeliness of their coal shipments. GRE is mitigating this risk through close relationships with its rail partners and by maintaining contingency plans for coal transportation by truck.

Skilled Workers: Probably the company's top overall risk is access to skilled workers to do maintenance and repair on its generation and transmission systems. According to Michael McFarland, Director of Enterprise Risk Management:

> "The people side is getting more and more attention. The average age of the workforce is over 50 — and 52 percent of skilled engineers and technicians will have to be replaced over the next 5-10 years. The industry is facing huge talent shortages — and there aren't enough young people entering the industry to keep pace with retirements."

Cyber Security: GRE complies with the NERC CIP standard and requires its suppliers to do the same. GRE believes its biggest cyber security risks stem from penetration of its control systems, which could affect power generation or transmission. GRE maintains several varied access controls to its systems and provides restricted access to these systems to its vendors so they can troubleshoot remotely. That flow of information going back and forth could potentially create a vulnerability.

Per NERC mandate, both physical and cyber access to critical systems is strictly limited. GRE controls who can log into their systems or even have terminal access — and those with access must be background checked and drug screened. In addition to limiting vendor access to their systems, GRE has anti-virus protection in place and tracks and evaluates malware incidents as a preventative step. GRE also voluntarily participates in the NERC CRISP program that monitors the critical infrastructure networks in real time for suspicious activities, including communications on a country-by-country basis, and will notify GRE if there is enough suspicious activity of a certain type.[2]

The Cybersecurity Risk Information Sharing Program (CRISP) is designed to detect signs of cyber activity that could impact the national electric grid or specific locations on the grid. CRISP fosters collaboration with private electric partners to facilitate the timely sharing of unclassified and classified threat information. CRISP begins with an information sharing device at the utility which allows DOE lab experts at Pacific Northwest National Laboratory to determine whether suspicious activity can be identified. Once the data is received, parallel analysis efforts begin — one focused on cyber security risks to the utility and a second using government-based information to discover potential threats to the U.S. electric grid.

2 http://www.nerc.com/gov/bot/FINANCE/2015nercbsnsplnbgt/NERC%202015%20BPB%20CRISP%20Background%20Material%20and%20Budget%20Impact%20Analysis.pdf.

From a procurement perspective, GRE manages cyber risks by requiring its vendors to meet the latest NERC, IEEE and other relevant standards. Given the structure of the industry, GRE's suppliers are, by definition, high integrity suppliers. There are few, if any, fly-by-night vendors able to manufacture high performance turbines and generators. Vendors for its critical systems are well-known and respected — and GRE depends on them to manage the cybersecurity risks in the components and software they produce.

Security Controls: Site security and system access is managed very carefully. Although the NERC CIP guidance details specific processes and security procedures, these only apply to critical systems. Under its Risk Management Framework, GRE has extended security scrutiny to all of its facilities, locations and assets — both physical and cyber. It assigns a risk priority to each asset, and that risk rating determines the appropriate level of security and controls.

Final Thoughts

According to Mike McFarland:

> "The Security Risk Framework was designed to look across the enterprise and manage risks holistically. Discussions about the right level of security can sometimes become contentious, but this holistic risk framework was embraced equally by those in the company who wanted more security and those who were concerned about the bureaucracy of too much security. It avoided prescriptive how-to procedures, while clearly specifying roles and responsibilities, which fostered cooperative dialogue between the assets owners and the company's cross-functional security team. The Framework provides a roadmap for our ongoing risk management journey. In today's environment, security threats and vulnerabilities continually change and evolve, and we need a dynamic framework that enables us to adapt flexibly to changing risks."