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

U.S. Resilience Project

BEST PRACTICES IN CYBER SUPPLY CHAIN RISK MANAGEMENT

Utility Sector
Best Practices for Cyber Security Supply Chain Risk Management

Discussion with Chief Information Officer (CIO)

The Next New Things in Risk Management

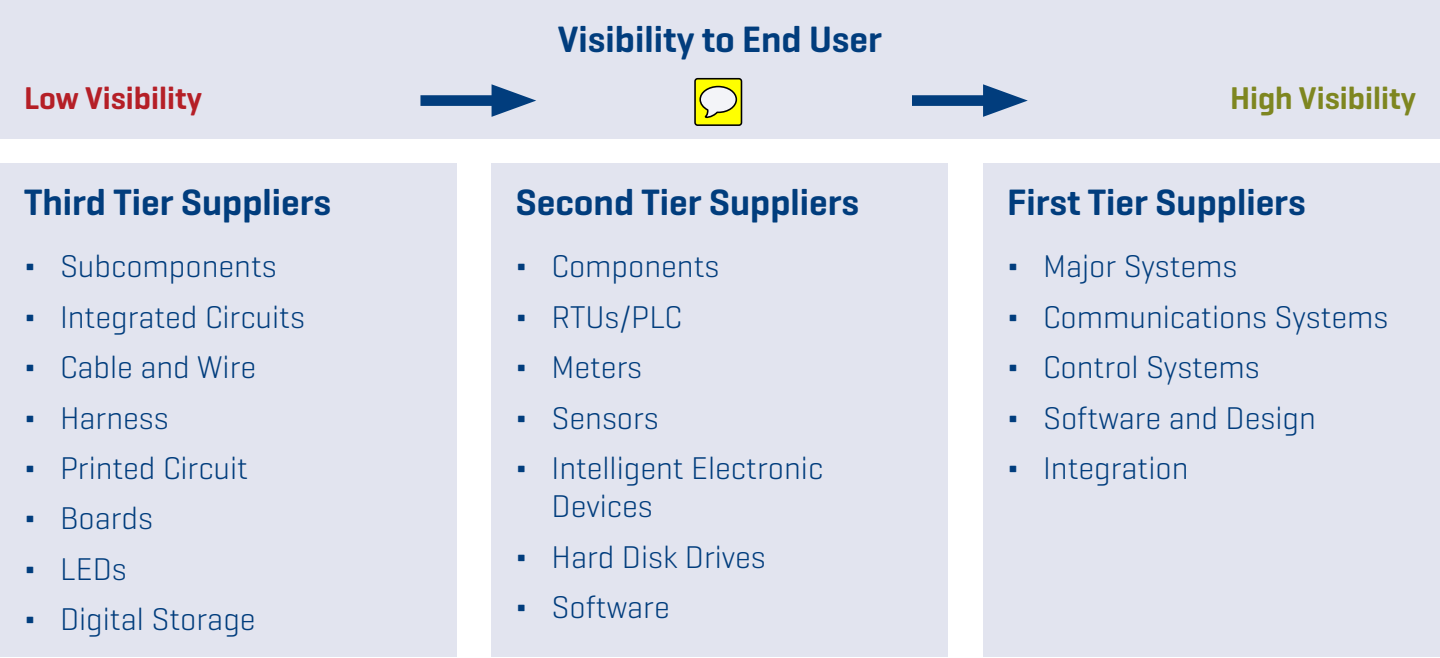
.

Overview

The safety and reliability of critical infrastructure has always been a first priority for the companies that manage these services. When the electric power does not work, neither does almost anything else. Financial, transportation, telecommunications, water and sewer networks all depend on electric power at some point in their product or deliver cycle. Virtually every retail cash register, every gas pump, every cell phone, every computer depends on a hot plug.

In recent years, cybersecurity has emerged as a critical risk to the quality and reliability of the power infrastructure. But, not all cyber challenges come from hacking, phishing over IT and communications systems. Another vector for cyberattack is through the supply chain — compromising the integrity of the critical hardware and software than underpin utility operations. Software or hardware that has been counterfeited, tampered with or otherwise tainted can fail to operate as designed, or worse, contain rogue functionality, unstable configurations or undermined security mechanisms. For example, rogue code could be inserted into software long before the devices are connected in a utility. Kill switches or back doors could be built into the hardware to enable remote access which could either steal data or disable the system. The compromised components could enter the supply chain from lower tiers which have traditionally been less visible to the utilities.

Figure 1. Utility Supply Chain



Similarly, counterfeit components, which could make their way into distribution channels, could degrade system performance. Maintenance and repair activities — software upgrades or equipment services, whether done onsite or remotely — also create an opportunity to corrupt or compromise systems. And this has implications far beyond the utility and its customers, affecting the economic and national security of the country.

In many ways, the power industry is best-in-class in dealing with many different kinds of operational risks. Certainly, it has learned to rebuild its infrastructure rapidly, even when its generating plants, substations and transmission lines have been flooded or flattened by hurricanes or tornadoes. And its risk management capabilities are supported by a complex and unique network of mutual aid agreements that stretch across the country — agreements in which utilities mobilize to assist others with personnel, trucks and equipment. But, the industry is still coming to grips with the new risks posed by cybersecurity, particularly through its supply chains.

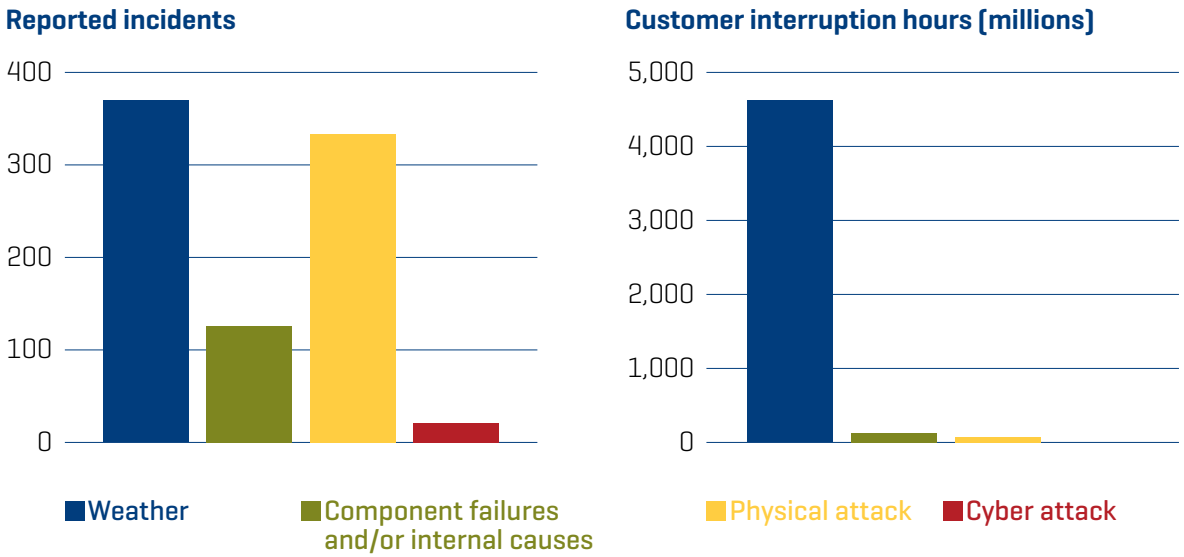
The following provides some insights from a Utility CIO on how the sector can develop standards and best practices to address supply chain cyber risks.

Utility Risk Management Strategies

The business case for risk management in utilities is straightforward — customer satisfaction. As the Business Insider rankings show, customers care about the reliability of their electricity. This is the overarching driver of investments to mitigate financial, reputational and operational risk. However, utilities are constantly balancing risks in order to determine where to best put their resources.

For example, according to the US Energy Policy and Systems Analysis, weather remains the largest threat to operations, although there has been an increase in physical and cyberattacks in recent years.[1]

Figure 2. January 2011 — August 2014 Electricity Disturbances Reported to the Department of Energy



Since utility companies cannot control the weather, they invest heavily in mitigation capabilities to minimize the impact of weather-related interruptions. Although the cybersecurity efforts are largely focused on prevention, the CIO maintains that a focus on recovery is increasingly important for two reasons. First, it is not clear that the best prevention in the world will intercept every attack, so utilities need to design systems with the assumption that a breach is possible. Second, the industry's current continuity plans are designed for site-specific disasters, not a cyber attack scenario that affects multiple sites hundreds of miles apart.

1 http://energy.gov/sites/prod/files/2015/07/f24/ElectricityAppendix.pdf

Organizational and Management Approaches to Cyber Risk

One of the foundational elements of cybersecurity strategy is creating cross-functional collaboration inside the enterprise. The worlds of Operational Technology (OT) and Information Technology (IT) were already converging as control systems began connecting to the Internet — with attendant cyber risks.

Grid modernization is accelerating that the level of risk.

The integration of information and communications is revolutionizing the way electric power can be delivered and used. The more agile and adaptive grid is able to sense and pre-empt potential disturbances, give customers more ability to respond to markets, and make it easier to integrate renewable sources of power into the system. But those capabilities, which are built on two-way connections between devices and utility control systems — which communicate over the Internet — also create new sets of risks.

Managing these risks holistically has been a challenge. Cyber risks cut across three traditionally separate groups within utilities:

- Operational Technologies (OT), which oversees plant operations and control equipment, is vulnerable to cyberattacks like Stuxnet or malware/low quality counterfeits in key components.
- Information Technology (IT), which include the security of all information technology systems and software.
- Supply Chain, which oversees providers of components, systems, software suppliers and services.

Utility cyber experts argue that utilities should be implementing new governance models that enable collaboration among key groups inside the organization and raise awareness of the need for standardized risk management approaches for sourcing, procurement and vendor management, and integrate IT and physical security considerations. Some best practice governance structures include:

- Combining the traditional IT Architectural Review and Operational Design Review Groups with purview over risk management in both IT and Operational Technology — working closely with procurement and supply chain.
- A cross-functional and cross-disciplinary Security Steering Committee to drive awareness of cyber security issues, encourage employees to include security risks in all decision-making.

The challenge for siloed organizations is that risk cannot be separated by group or business. Cyber risks, in particular, cut across every major function and business line. Best practice involves collaboration between IT, engineering, supply chain, operations, legal, finance and others to manage risk on an enterprise-wide basis.

Risk Management Strategies for Supply Chain Cybersecurity

There are already a number of mandatory standards and requirements for supply chain integrity, led by both vendor and government organizations (NIST, ISO, Common Criteria, OTTF). But, according to one CIO, the standards development in this area is still immature, with significant overlap and a lack of third-party certification or accreditation processes. Some standards are economically infeasible; others do not fully address the risk of adverse functionality introduced by malicious or compromised insiders.

Although the responsibility for assuring supply chain integrity falls mainly on the cyber asset manufacturers, utilities have key responsibilities in four key areas:

1. Standards
2. Procurement
3. Manufacturing
4. Assurance

1. Prioritizing Security Standards

This includes functional and technical requirements on cyber assets that enable critical business processes. Utilities should consider the following high-level principles and guidelines to guide standards:

- **Disclose all features, disable what is not required**
  This would include: disabling unnecessary system services, programs, and capabilities as well as known or guest accounts and changing default passwords; ensuring that system passwords are not hard coded and sufficiently complex; fully disclosing the specifications of all communication capabilities; and addressing know security vulnerabilities in the software/ firmware (e.g. buffer overflow).
- **Limit user capabilities**
  System permissions should be restricted with limited elevated privileges and role-based access controls.

- **Block unauthorized access**
  Connections to or communications between networks/devices should be limited through firewalls. Protocols and best practices should be secure enough to prevent unauthorized access. Control system devices should be separated from enterprise IT systems or the Internet by firewalls or air gaps, and physical security should prevent unauthorized access to systems. End devices (e.g. intelligent electronic devices (IEDs), remote terminal units (RTUs) or programmable logic controllers (PLCs) should have adequate physical and cyber security.
- **Secure the data traffic**
  All communications devices should be secured — and where possible with authentication and encryption. Any traffic over unsecured infrastructure should be done through a Virtual Private Network (VPN) with adequate physical and cyber security (access control, event and communication logging, monitoring and alarming).
- **Enable ongoing monitoring, alarming and logging**
  Monitoring should be in place to detect unauthorized system access or abnormal network traffic. Account auditing and logging should be enabled to facilitate detection, forensic analysis and anomaly detection. No authorized logging devices should be installed, and monitoring should include partners, third-party solution providers and support vendors.
- **Ensure update capability**
  Processes should be in place for authenticating firmware/software updates and security patches, for reporting and remediating flaws and detecting malware.
- **Action Steps for Utilities**
  - Establish and document technical standards for systems that enable critical business processes with emphasis on security of hardware and software.
  - Appoint a technical review board for cyber asset decision-making, with emphasis on repeatable governance processes that drives adherence to these standards.
  - Ensure that vendors are aware of these standards and the implication of non-conformance.

2. Managing Procurement Risks

The procurement needs to build in security considerations from vendor selection through the terms and conditions in the contracts.

Key principles for a risk-based approach to procurement include:

1. Procurement processes should be developed jointly with representatives from sourcing and legal as well as technical and functional subject matter experts from IT, security, engineering and operations.
2. Security standards and security terms and conditions should be included in all RFPs and contracts, specifically addressing confidentiality, integrity and availability.
3. Vendors which do not or cannot meet these standards should be excluded from consideration.
4. Utilities should have audit rights to assess vendor adherence to contractual commitments.

The rule of thumb for managing supply chain cybersecurity is that: "If it touches the network, it is in scope" for risk management.

3. Mitigating Vendor Risks

For decades, supply chain functions in utilities were largely logistical — making sure that purchased components arrived on time and in the right quantities and at the right price. What has changed in the utility supply chain world is the advent of a global supply chain base and the integration of electronic components throughout the system. The new suppliers may lack familiarity with the performance and reliability requirement of systems with 30-year life spans. Like many other industries, supply chain managers often lack visibility into their supply chain beyond the first tier — where many types of cyber, continuity and quality risks emerge. And even at the first tier, vendors will not disclose manufacturing processes they deem to be a trade secret and/or competitive advantage.

These changes are forcing a transformation in the role of utility supply chain managers from purchasing and cost optimization to an integral part of the risk management team — with greater responsibility for assessing cyber risks throughout the life-cycle of the purchased products, as well as the risk management practices of the suppliers and distributors in those supply chains.

Given the lack of third-party certification/accreditation processes, many utilities are relying on vendor self-disclosure to ensure that there is no malicious functionality embedded in their products and software. At this stage, according to one utility CIO, what is required is a tougher interview to understand how utility vendors mitigate cyber risks in their own production processes and in their own supply chains. He maintains that research shows that certain types of questions result in better decisions. Some of those questions could include:

- Is the design process documented? Repeatable? Measurable?
- Is the mitigation of known vulnerabilities factored into product design (through product architecture, run-time protection techniques, code review)?
- How does the vendor stay current on emerging vulnerabilities? What are vendor capabilities to address new "zero day" vulnerabilities?
- What controls are in place to manage and monitor production processes?
- How is configuration management performed? Quality assurance? How is it tested for code quality or vulnerabilities?
- What levels of malware protection and detection are performed?
- What steps are taken to "tamper proof" products? Are backdoors closed?
- What physical security measures are in place? Documented? Audited?
- What access controls, both cyber and physical are in place? How are they documented and audited?
- What type of employee background checks are conducted and how frequently?
- What security practice expectations are set for upstream suppliers? How is adherence to these standards assessed?
- How secure is the distribution process?
- Have approved and authorized distribution channels been clearly documented?
- What is the component disposal risk and mitigation strategy?
- How does the vendor assure security through product life-cycle?

These kinds of questions allow utilities to drill down into the technical aspects of issues to make sure vendors fully can meet cybersecurity requirements. This CIO considers "the power of conversation" to be an important part of risk management. And a corollary benefit is that such a detailed interview requires utilities to become better informed and trained themselves so that they can properly enforce these requirements on their vendors.

Finally, utilities should exercise the audit clauses in their supplier contracts by conducting assessments of vendor security practices, based on asset risk and criticality.

Assurance: Security as a Mindset

What distinguishes supply chain cyber risks from other types of tampering is that they extend well beyond the point of sale and delivery. Security is an ongoing journey — and some of the stops on that trip should include:

- Pre-installation inspection and review
- Strong change management controls
- Specialized threat detection (anomaly-based detection rather than signature-based detection)
- Controls on all service providers — physical access controls as well as limitations on remote VPN connections for system maintenance and upgrade.

Next Steps

Raising Awareness and Training

No amount of technology and best practice will be sufficient if employees are not committed to the program. According to the CIO, awareness helps drive better decision making and enables employees to know where to get help on critical issues. His company is striving to help its workforce understand that security spans the "full array of business activities."

But, such efforts are already underway and could be expanded. With regard to employee preparedness, some companies offer or require awareness raising programs or training programs on mandatory industry standards, including the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) requirements. IT Departments have gotten creative, posting cybersecurity messages on computer splash screens (security messages appear as the system is booted up). In some companies, fake phishing scams are launched — and employees who fall for them are required to take additional training. Some utilities develop programs for vendors to educate them on cyber security requirements or new standards. While this may take time and resources, it is ultimately a better investment than either replacing the vendor or suffering a breach.

Exercising Industry Market Clout

In the supply chain arena, the utilities will have to step up, rather than waiting for government to step in, according to the CIO. Utilities should work together to create the market clout to influence their common vendors to adopt security practices that are appropriate for critical infrastructures. When utility companies work together to set industry-wide requirements, security will become a competitive advantage for vendors rather than a compliance requirement. The CIO likens this to the "Volvo moment" when the carmaker introduced three-point seatbelts and waived its rights to patent in order to improve safety for the industry as a whole.[2]

2 http://www.volvocars.com/intl/about/our-company/heritage/innovations