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

U.S.
Resilience
Project

BEST PRACTICES IN CYBER SUPPLY CHAIN RISK MANAGEMENT

Exelon Corporation
Cybersecurity Supply Chain Risk Management

INTERVIEWS

Spencer Wilcox
Managing Security Strategist and Special Assistant to the Chief Security Officer

Tom Minton
Manager, Security Governance and Risk, Corporate and Information Security Services

The Next New Things in Supply Chain Risk Management:

- Security Exception Protocol that requires formal acceptance of risk from the ranking business unit leader for an authorized deviation from risk policy.
- Integrated information security and risk management organization that manages cyber and physical risks across the enterprise.
- Expanded definition of supplier to include all third parties that touch Exelon's networks, components or information systems, including scrutiny of vendor personnel.
- Establishment of a Security Operation Center and Cybersecurity Operation Center (SOC and CyberSOC) for round-the-clock monitoring of facilities and advanced detection of cyber threats.

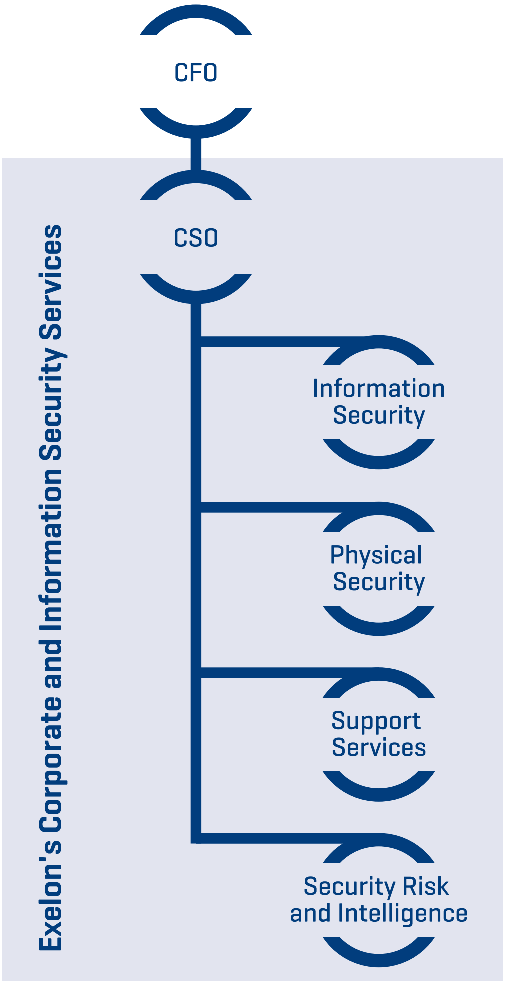
Company Overview

Exelon is the nation's leading competitive energy provider, with more than 32,000 megawatts of owned generating capacity and 7.8 million electric and gas utility customers. With revenues over $27B, $86.8B in assets and almost 30,000 employees, the company's business is vast, complex and dynamic. Nevertheless, it is well regarded for its clean energy solutions and low cost products.[1]

[1] http://www.exeloncorp.com/assets/newsroom/downloads/docs/fact%20sheet_ExelonCorporation%20 2015.pdf.

Organizational Approach to Risk Management

Physical and cybersecurity are always among Exelon's top enterprise risks. To better address the complex and changing risk landscape, in 2012, Exelon established a Chief Security Officer position with four areas of operation in the new Corporate and Information Security Services (CISS) organization.[2] These include physical security, information security, security operations support, and security risk and intelligence.


CFO
CSO
Exelon's Corporate and Information Security Services
Information Security
Physical Security
Support Services
Security Risk and Intelligence

CISS is responsible for preventing, detecting and responding to security incidents across the enterprise, as well as assuring compliance with security-related regulations. In 2013, the CISS group launched the Exelon Security Operation Center (ESOC) and the Cybersecurity Operation Center (CyberSOC). The ESOC enables round-the-clock monitoring of facilities, which allows the security team to remotely control access to sensitive areas, detect events on the ground as they occur to minimize impacts and identify persons responsible, as necessary. The CyberSOC uses advanced detection methods to constantly monitor the state of Exelon's networks.[3]

The Security Risk and Intelligence team, one of the four areas of responsibility within CISS, manages security policy and risk to create a holistic security risk governance framework under which all of the business units operate. This team directly manages vendor and third-party security risk enterprise-wide. Its biggest challenge, according to Spencer Wilcox, Managing Security Strategist, is how to enforce the standards. The team is creating metrics to understand how well the business units are implementing security guidance — and security metrics will eventually be applied to application portfolios as well. This allows the business units and application portfolios to be measured — and ranked — against one another in terms of their readiness to withstand a cyber attack or physical security incident.

[2] http://www.exeloncorp.com/assets/newsroom/docs/csr/pdf/EXL_SR_2013_pg87-92.pdf.

[3] http://www.exeloncorp.com/assets/newsroom/docs/csr/pdf/EXL_SR_2013_pg87-92.pdf.

Business Case for Cybersecurity Supply Chain Risk Management

Exelon recognizes that the security of its business and partners is essential to the continuity of service to its customers. For Wilcox, the company is "...literally one of the first lines of defense for critical infrastructure here in the United States."

Guiding Principles of Supply Chain Risk Management

Prioritization: Exelon prioritizes its mitigation efforts through a criticality lens. The most critical real-time risk priorities are often the highly regulated ones, and they are regulated for a reason. Next in importance are systems that Exelon classifies as high; these are business critical systems that could have a significant business impact. The third priority are systems that Exelon classifies as medium; these systems would have less impact on the business than the critical and high systems, but are still very valuable to Exelon. Finally, the systems with the least business value are classified as low. The valuation methodology helps the business to prioritize the criticality of its assets and its risks by addressing the most critical impacts first.

Managing Cyber Risks: Cyber issues cut across all risk priorities. Exelon mitigates the risk of cyber attacks with a range of sophisticated technical tools — network segmentation, segregation of assets, detection capabilities — as well as policy controls. However, the company believes that the ability to recover is a fundamental responsibility for all types of hazards, including cyber risks. According to Wilcox:

> "When people talk about the potential impact of a cyber attack, they often depict a cataclysmic scenario. But, here is the reality: If the attackers are incredibly successful, really resourceful — and they have nation-state capabilities — they may disrupt the grid for a time. But, the worst case scenario — that they will knock us back to the Stone Age — is just not realistic. The more likely worst case scenario is that they knock us back to the 1950's, for a short time. At that point, the nation's power producers will go into manual mode and rebuild the system. Recovery is what the industry does best — and Exelon believes that it is our responsibility to recover quickly from all hazards, regardless of what they may be."

Scrutinizing an Extended Supplier Base: When Exelon addresses supply chain risk management, it adopts an extended definition of supplier, including the entire panoply of vendors and their suppliers, service providers and third parties.

Exelon prioritizes three risks for its extended supply chain.

- First, how well do the vendors vet their personnel? Of particular concern are the personnel in supplier companies that have access to Exelon's data, systems and facilities. Such individuals are a top risk priority because they are trusted insiders, but they have very different loyalties than Exelon employees. Exelon asks the question about every person: Should they be here and should they have that access? This includes requiring background screenings of vendor staff that will have access to Exelon assets.
- Second, how well do the vendors vet their services? Vendors who will work in Exelon facilities or with Exelon assets are required to go through an exhaustive vendor security screening to assess the vendor's ability to protect Exelon, its people, processes and technologies.
- Third, how well do the vendors vet their products? Every piece of technology that comes into the company — every SCADA system, every programmable logic controller, every computer, every piece of software — has the potential to harbor within it the seed of risk. The majority of these technologies are not developed in the United States — and caution needs to be the order of the day.

The stakes are high and Exelon relies on these processes and best practices to narrow the scope of risk.

Vendor Risk Management Processes

Vendor management starts with the supply chain organization, which has primary responsibility for ensuring that contract terms and conditions are designed and met. Although the supply chain group has principal responsibility for the negotiations, it is supported by a cross-functional team including security, legal and IT. This team assesses the terms and conditions to ensure that appropriate contract controls are in place. Its goal: Hold vendors — particularly those that have access to Exelon's networks, components or information systems — to the same standards that the company applies to itself.

Vendor Ratings: Exelon queries its vendors on acceptable use standards and policies and other cybersecurity governance issues. Vendors answer approximately 109 questions that span nine domains:

1. Business continuity/disaster management
2. Personnel security
3. System development
4. Application security
5. Overall system security
6. Network security
7. Data security
8. Access control (physical and cyber)
9. Vulnerability management

The answers determine the risk ratings. Risks are rated as low, medium or high depending on the vendor security posture, policies and what they do for Exelon.

The questionnaire is in the process of being streamlined and automated. As Wilcox notes: "When you send vendors 109 questions, some in essay form, they have a tendency to get a little testy." The security team has started working on a new idea — a Choose Your Own Adventure online or in-booklet format. In this new format, the questions would not be linear. Answers to certain questions might conclude the response — or open up a dialogue box with other questions.

Security Exception Process: If there is a business reason to take on more vendor risk than the rating would justify, Exelon requires that a security exception be approved. Tom Minton, Manager, Security Governance and Risk, Corporate and Information Security Services, explains:

> "Prior to adopting the Security Exception Protocol, Security would bear the responsibility for an authorized risk that deviated from the guidelines. Today, risk is transferred to the responsible business unit. If a security policy exception is requested, Security will analyze the threat, identify the potential impact to the business, assess the mitigation measures the business unit is taking, and propose additional remediation measures as necessary. Before the exception request is approved, an authorized person in that business unit must acknowledge the risk and accept responsibility for any adverse impact to the company, based upon the intentional deviation from policy.

> Although there are still exception cases every day, the pace at which they come in has slowed — and the risk remediation steps are made by the business unit very promptly. This translates into supply chain risks as well. If a Supply Chain risk is rated as high, the business unit might not necessarily want to accept the risk as is, so there is a greater motivation to remediate third party shortcomings. If a vendor wants to do business with Exelon, it's far more likely today that the vendor will be asked to remediate the risk first."

Audit Processes: The security language to test third-party risk has long been in place. Like most successful companies, Exelon has an audit clause in its contracts, but it was not always effectively exercised. Just prior to the Constellation-Exelon merger in 2012, the company began exercising its audit clauses to great effect — recovering a couple of million dollars' worth of contract monies. Exelon is considering relying on the company's internal auditors to perform external audits of supplier compliance.

Breach Notification: Many vendors are required contractually to notify Exelon of any security breach. One vendor reciprocated, asking Exelon to agree to a breach notification clause. After the initial shock, the security team saw this as an opportunity to strengthen risk management. They are considering instituting tabletop exercises to build mutual assistance agreements between the vendor community and the company in the event of a security incident on either side. A tabletop exercise would help clarify what the response would be, whether Exelon is the vector for a cyber attack into the supplier company or whether the supplier company is the vector into Exelon.

Vendor Risk Management Challenges

Exelon has identified a number of areas for improvement in vendor risk management.

Vendor Patch Controls: Historically, the business model for utility supply chain was that vendors sold a product designed to last for 50 years in the rain, wind, snow and sleet without failing. And that model worked well for a long time. Today, however, products designed to last for decades also have embedded software systems that are not readily remediable — and that can increase their risk to cyber attack.

The problem for a utility is that if it unilaterally makes a change to the product — for example, by patching back end software — it voids the maintenance contract. According to Wilcox:

> "Our vendors will provide the machine, the operating system, the software, the backend databases that run the software, and the logic that goes into the programmable logic controllers. However, every single one of those components is subject to vulnerabilities because they are purchased from a third party, with the original equipment manufacturer (OEM) assembling the system. Let's say one of those third party vendors releases a software patch. The OEM has to certify that patch before Exelon can use it. If the OEM is running behind on certifying patches — or it only drops a patch from a third party when it updates its own software — it is possible that a company like ours may not get a patch for a critical security vulnerability for some time. And it cannot address that vulnerability without jeopardizing its service contract."

Wilcox says that vendors must do or comply with the following:

1. Understand all of the components and attendant vulnerabilities that make up the package that they are selling.
2. Stay current on the patches for all the equipment and software that they are reselling. This, of course, requires the vendor to know and understand all the components of the systems it is selling.
3. Ensure that their software works quickly, and they will be responsive to their customers if the patches are not applicable. Exelon is starting to transition these recommendations into contract requirements by getting security a seat at the negotiation table for vendor contracts. Ultimately, the goal is to hold vendors to the same standards to which the company holds itself, particularly vendors with access to its network and information systems.

By the same token, businesses need to recognize that equipment designed to solve yesterday's problems may not be sufficient for the security needs of today. Today, businesses must ensure that there is a risk management process around the acquisition of every new piece of hardware and software.

Cloud Security: Cloud services pose a different challenge from hardware and software. Exelon uses a series of security controls to monitor inputs and outputs of its network and recognizes the importance of good solid vendor monitoring capabilities in this area. But, as the network or supply chain expands with cloud adoption and clouds services, Wilcox acknowledges the definition of network is becoming very flexible. Exelon is pushing for increased monitoring services during contract negotiations even as some vendors resist it.

Quality Due Diligence: While many vendor companies enjoy an excellent reputation for quality products, many do not permit Exelon to independently verify their quality assurance testing data or share information about potential vulnerabilities in their products or systems. While "obscurity" can be a self-defense tactic for producers, Exelon's security manager believes that the lack of information-sharing is not in the best interest of customers who may be impacted by that vulnerability.

Metrics

One of the key challenges is verifying conformance with security requirements. Another is assessing how effective business units have been in enforcing security conformance.

Exelon uses five key metrics and is continuing to build out the metrics portfolio:

1. **Detection occurrence:** Measures the number of cyber incidents.
2. **Physical vulnerability:** Tracks physical vulnerability site assessments and how well identified vulnerabilities are being remediated.
3. **Business Continuity Planning:** Uses a business continuity scorecard to assess the current state of its business continuity plans, and to ensure that they are sufficient to keep the business running, in the event of an emergency.
4. **Industrial control systems:** Measures the number of industrial control system advisories, how they impact the business, and the remediation of those vulnerabilities. Additionally, Exelon's CyberSOC measures the number of alerts, blocks, occurrences of detection and actual incidents.
5. **Data loss prevention:** Evaluates how many events were experienced that met one of the triggers for data loss [e.g. personally identifiable information (PII)]? Advanced detection capabilities can identify loss of PII by email, smartphone or printer. Sometimes there is a totally innocent reason for the alert. For example, there was an enormous spike in data loss alerts in the February-March 2015 period which caused alarm — until the security unit figured out that employees were emailing home or printing out their W-2s that they received electronically. Though not an actual threat, the system worked precisely as intended.

Standards

Exelon's utilities have many industry specific health, safety and hazard standards in place. In addition to power related regulations, Exelon currently follows the NIST Cybersecurity Framework as well as hybridized ISO 27000.1 and 2 standards. The industry as a whole is still developing and integrating sufficient cybersecurity supply chain standards in their operations. The Federal Energy Regulatory Commission recently announced that it would be developing revisions to critical infrastructure protection Reliability Standards to improve cybersecurity in the electricity industry, including "...supply chain management security controls to protect the bulk electric system from security vulnerabilities and malware threats."[4]

Exelon supports robust standards, but according to Wilcox, there is a critical path beyond standards. "Compliance with regulations is an important baseline, but security requires that we go beyond the status quo to keep pace with the threat," he said.

Exelon works to influence the industry, and through information sharing, helps itself and other companies develop the necessary capabilities to stay abreast of current security threats. Exelon participates in the NERC Advisory Council as well as other forums, such as the Electric Sector Information Sharing and Analysis Center, Edison Electronic Institute's Security Committee, and the US Chamber of Commerce Cyber Coalition. In fact, according to its Sustainability Report:

> In recognition of Exelon's innovative programs and leadership efforts, the Corporate and Information Security Services organization was honored by Security Magazine as the top security organization in the power, electric, gas, nuclear and hydro utilities sector in 2012, 2013, 2014.[5]

[4] https://www.ferc.gov/media/news-releases/2015/2015-3/07-16-15-E-1.asp#.VbV8YcZVhBc.

[5] http://www.exeloncorp.com/assets/newsroom/docs/csr/pdf/EXL_SR_2013_pg87-92.pdf.