Uncovering the Hidden Risks in Your Supply Chain

Across the critical infrastructure community, few issues have garnered more attention in recent years than supply chain risk management. Congressional investigators, regulators, and the media have all highlighted the risk that malicious actors can insert vulnerabilities into hardware and software at virtually any point in a product's lifecycle to steal sensitive information or cause damage or destruction of an organization's information systems. Mitigating these risks is challenging for most organizations, even those with vast resources like the intelligence and defense agencies.

While the focus for many commercial organizations has specifically been on the risks posed by information technology vendors, today's threat actors are increasingly targeting an organization's business associates and contractors to obtain sensitive business information or direct access to the first party's information systems. Electric utilities evaluating cyber risks to their supply chain should develop a program that evaluates all "critical" vendors, to include IT vendors but also those less-obvious vendors who pose hidden risk to the organization due to their access to sensitive business data or the corporate network.

Third-Party Attacks on the Rise

While hardware and software supply chain penetrations have been difficult to observe, cyber attacks targeting third-party business partners have been well publicized.

Last month, U.S. law enforcement officials, along with the Securities and Exchange Commission, announced the indictment of 35 individuals who hacked into PR newswire databases so that they could read the earnings press statements of publicly traded companies prior to their official release. Armed with this insider information, the traders made $100 million in profitable trades before the earnings became public.

The case is a perfect illustration of why corporate executives and government regulators are increasingly concerned about data breaches affecting critical vendors, contractors, and other "non-IT" business associates who have sensitive data or may even have direct network access to first-party organizations. They are the critical vendors who represent hidden, non-obvious risk to the organization.

Cases in which third parties are the source of a data breach are clearly on the rise. Aside from the most recent indictment, there is perhaps no more famous incident than the 2013 Target breach. In that incident, attackers penetrated the network of Target's HVAC contractor, which had a direct connection into Target's network to observe refrigeration units in each of the stores. Gaining access to the HVAC contractor, the attackers rode directly into the Target network and stole millions of credit card numbers. The result was not only a material financial loss for Target, but also the ousting of Target's CEO and CIO and near dismissal of several key board members.

Third-party attacks are a popular method of compromise in the retail industry. Lowe's, Goodwill, and other retailers have also been victimized through third parties. But it's not just retailers. From attacks against the defense industry to key government contractors, adversaries increasingly understand that highly sensitive, valuable data may lie outside of the first-party organization. Attackers are smartly assessing the security of both obvious and lesser-known third parties to gain the access they desire.

Electric utilities are familiar with cyber attacks against third-party vendors, though the most highly publicized third-party attacks have targeted IT vendors. In 2012, Telvent Canada alerted its customers that attackers installed malicious software and stole project files related to one of its SCADA offerings. Though public reports indicated that intellectual property was the target of the attack, Telvent also advised its customers at the time that it was temporarily disconnecting the links between its organization and customers while the data breach was being assessed. In 2014, the Midcontinent Independent System Operator (MISO) reported a vulnerability affecting a third-party server used by MISO's market monitor. MISO was forced to sever connections between that third party's information systems.

By Jacob Olcott

Continued on page 28

Continued from page 27

Why Attack Third Parties?

Attacks against third parties have become commonplace for three main reasons.

First, organizations rely on more third parties for key business functions that used to be performed in-house. With payroll, HR, legal, sales, PR, and even product development functions being outsourced, more third parties have access to more sensitive business information, which presents a great challenge to protect that data.

Second, business environments have become more interconnected, which means that more third parties have been granted direct access to the corporate network to perform essential job functions. This privileged access is great to achieve business objectives, but it also creates greater risk.

Third, as first-party organizations improve their cyber defenses, attackers are increasingly searching for the weakest links. Smaller businesses often have fewer resources to protect their environments and represent easier attack vectors for the bad guys. Given their access to sensitive data or even the broader network itself, third parties represent great targets for the bad guys.

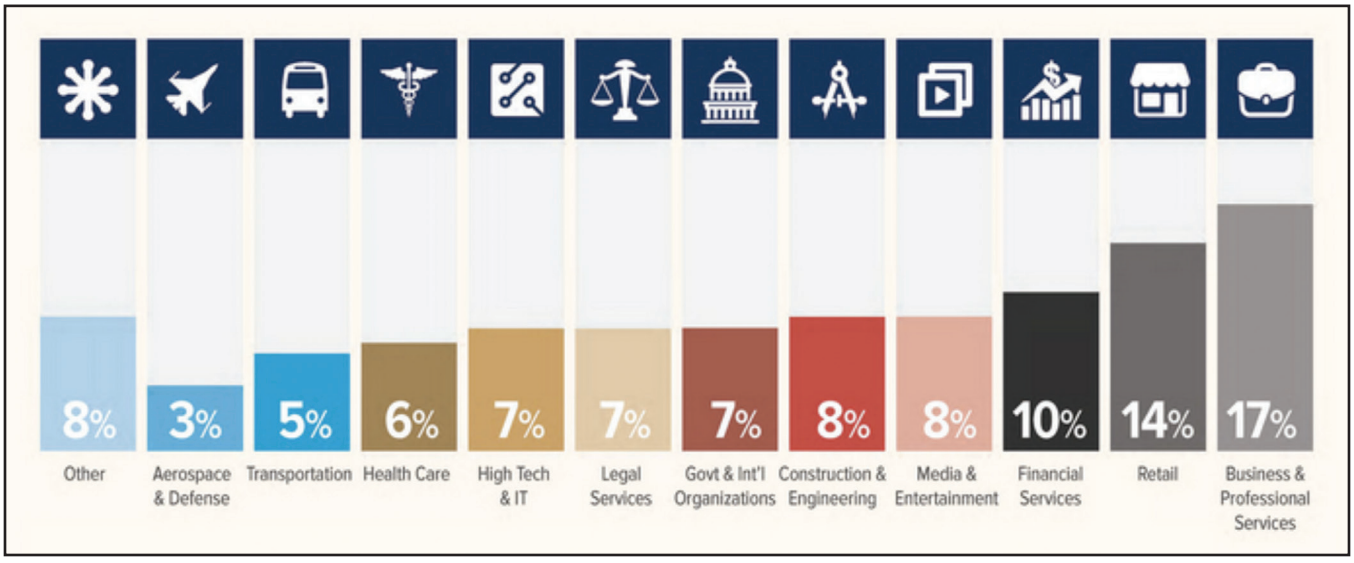
Examples of "Hidden" Third-Party Cyber Risk

So what are some examples of "hidden" third-party organizations, outside of the traditional IT environment, that the electric sector should focus on? Let's start with the industry sectors that have experienced the highest number of cybersecurity intrusions. According to Mandiant, a security consulting services organization, while "high-tech and IT" are approximately 7 percent of its overall cases, the "business and professional services" sector represents the highest percentage of investigated industries.

BitSight analyzed the security of four sectors—Law, Benefits, Accounting, and PR—within the business services industry using the company's proprietary Security Ratings. These ratings range from 250 to 900, with higher ratings indicating better security performance. BitSight analyzes terabytes of security data to gather, process, and assign this information. As the chart below indicates, BitSight observed that some business sectors have objectively greater ability to respond to and mitigate cybersecurity incidents than others. If these types of organizations hold sensitive data about your company or have access to your company's network, additional security precautions should be considered.

Developing a Robust Supply Chain Program

Managing third-party cyber risk does not necessarily mean bringing those functions back inside your organization. Decisions to outsource certain business functions were likely made for cost savings and efficiency, and reversing the trends of outsourcing is difficult, if not impossible.



A number of sophisticated organizations are realizing that the answer lies in better managing these third-party risks through a combination of contract, diligence, and monitoring.

First, organizations are reexamining their contracts to make sure their third parties are meeting an agreed-upon level of cybersecurity. Organizations typically begin with the third parties that present the greatest risk. For electric utilities, that focus must obviously be on the ICT, ICS, and IT vendors that are present in IT, OT, and physical security environments, but also on other third-party organizations that have network access or access to sensitive data. Contracts can require that third parties meet a specific standard for cybersecurity (e.g., ISO 27001, NIST 800-53, NIST Framework). It is not advised to simply require a "generic" level of security; in other words, don't tell your third party that "adequate cybersecurity" is good enough for you!

Second, organizations are performing better cyber diligence for their third parties. Before entering into a contract or signing a renewal, they are asking for and receiving information about their third party's cyber risk management efforts through questionnaires, audit reviews, and technical assessments like penetration testing or vulnerability scans. They are also establishing greater restrictions on third-party access to prevent an untrusted third party from running rampant throughout the corporate network.

While these initiatives are important, they only represent a snapshot in time. That's why organizations are increasingly using continuous monitoring capabilities to monitor their vendors' cybersecurity in real-time. Receiving real-time alerts when a third party's network security is impacted is a critical way to reduce your third-party cyber risk.

Continued on page 30

Continued from page 29

A Note on the FERC Supply Chain Order

The Federal Energy Regulatory Commission (FERC) recently proposed revisions to the CIP Reliability Standards to address the development of standards for supply chain management. FERC specifically mentions its concern about malware injected into hardware or software components by the hardware, software, or maintenance vendor prior to delivery.

FERC's order recognizes the criticality of supply chain; however, the scope of these rules will be limited only to risks that are related to the bulk electric system assets. Electric utilities should consider broader risks to their organization that third parties pose. Again, a focus on risk management will require utilities to assess third-party risk beyond ICT, ICS, and IT providers and include those hidden, non-obvious third parties who present a risk to data or infrastructure.

Concluding Thoughts

Many complicated issues are involved in managing cyber supply chain risk. Organizations would be best suited to begin their supply chain risk management programs by focusing on organizational risk. While ICT, ICS, and IT providers may clearly represent significant and material risk to the electric utility, non-obvious business associations and other third-party relationships should also be examined. These third parties may have direct access to your organization or your organization's sensitive data. Make sure they're protecting themselves as well as you protect yourself.

Jacob Olcott is VP of Business Development at BitSight Technologies. He served as cybersecurity legal advisor to the Senate Commerce Committee and the House of Representatives Homeland Security Committee. He is an adjunct professor at Georgetown University.