The Legal Intelligencer
THE OLDEST LAW JOURNAL IN THE UNITED STATES 1843-2017
PHILADELPHIA, TUESDAY, JUNE 6, 2017 VOL 255 • NO. 108 An ALM Publication

CYBERSECURITY

Company Cyberinsurance—The Supply Chain Dilemma

BY NICHOLAS A. PASCIULLO
Special to the Legal

A company's supply chain is an integral and sometimes complicated part of its business. As companies optimize their supply chains using interconnected technology, the cyberrisk of disruption and lost business multiplies. Where a third-party supplier is connected to a company's systems, a compromise at the supplier can disrupt the company's business or allow a direct attack on the company. Cyber underwriters are especially concerned about recognizing and assessing the risk of disruption of supply chains after recent catastrophes, such as the 2011 tsunami in Japan and flooding in Thailand hit major manufacturing sectors that were single-source suppliers to major manufacturing and electronics companies.

Current risk-assessment practices, and cyberinsurance, focus on potential vulnerabilities of supply chain systems and the systems in place to prevent and detect cyberattacks. This is a nearly impossible task given the complexity and autonomy in supply chains as well as the constant change of technology affecting a company's system and the constant adaptation of cybercriminals probing vulnerabilities. As discussed below, a more practical means of risk assessment is to evaluate a company's ability to respond to a disruption in its supply chain. In other words, evaluate its robustness and responsiveness.

NICHOLAS A. PASCIULLO, *a partner at Weber Gallagher Simpson Stapleton Fires & Newby in the firm's Pittsburgh office, represents underwriters in property, energy and engineered risks insurance matters. He also counsels clients on cybersecurity risk. Contact him at npasciullo@wglaw.com.*

Since the olden days of 2011, the goal of developing an internet of things (IoT) has become a reality and smart technology is allowing for greater and more autonomous interconnectivity. Wireless sensor and controller technologies now allow greater connectedness and autonomy in machines and robots, inventory and ordering, transportation and distribution, ground and aerial vehicles, medical devices and building and home security. Cyberphysical systems comprised of "smart devices" that collect data and control actions are in place in companies and entities involved with power, manufacturing, health care, banking, transportation, municipal and home products and services, to name only a few. Yet experts have demonstrated that many devices and protocols employed in these systems are vulnerable to outside manipulation when they are accessed. More often, a company's system is accessed through an attack on an entity in its supply chain.

Recent cyberincidents in 2013 at Target and 2014 at Home Depot demonstrated how a compromise at a smaller third-party vendor allowed thieves to steal millions of customer's data, including payment cards. While those events involved theft of data, the risk to physical assets is growing. As an example, in 2015, an attack at a German steel company using stolen login details allowed outside access to the controls of a blast furnace. The intruders caused an unscheduled shut-down damaging the furnace. This year, cyberthieves exploited a flaw in a telecommunications company's protocols to bypass 2-Factor authentication and emptied a number of accounts at a German bank.

Current underwriting practices are unlikely to identify and evaluate risks to a company's supply chain accurately as they rely on a company's knowledge of its connectivity, location and access to data and vendor protocols and its efforts to secure its business activities. Even where a company can identify all of its

suppliers and the extent of its connectivity to its system, it is unlikely that it can evaluate the risk at each stage. Few companies drill down for information on their supply chain from end to end or are aware of the various smart components, communications protocols or insider training at a supplier.

Current risk assessment practices can develop an overall snapshot, including identifying a company's most important vendors in its supply chain, how reliant a company's income generation is on vendor operations and how much access a vendor has to the company's cyber-physical system. Entities, such as NIST, identify additional checklist items for interconnected relationships, including the extent of:

- Vendor access to a company's cyberphysical system;
- Network segmentation, so that a breach cannot expand to critical assets or processes;
- Vendor selection, guidelines, standards and controls, including contract language requiring reports, audits and validation of performance;
- Password and monitoring safeguards, policies and practices;
- Insider threat training, including both intentional and unintentional insider threat; and
- Audit programs to monitor security protocols within the company and at supply chain vendors.

This snapshot is affected by time and complacency. Research demonstrates that a lack of successful cyber intrusions leads to complacency and lax security practices. A culture of "it worked before" or "it hasn't happened" typically leads to an under-appreciation or a biased assessment of risk. For example, a company employee is contacted by a long-standing vendor to "troubleshoot" communications. The employee may interact with that contact without first verifying that it is in fact the vendor, that there is in fact a communications issue and that the employee is authorized to give out company information. Or, more commonly, an employee accesses social media at work and, having opened photos, ads or "click-bait" many times before, introduces malware into a company's system.

"Risk assessment that focuses on a company's ability to respond to a cyberevent impacting its supply chain provides more practical and accurate information.

With cybercriminals constantly attempting to introduce malware, deny service or access a company's system, researchers assert that it may not be a question of "if" a company's cyberphysical system will be impacted by outsiders, but "when." Different attacks are discovered almost daily with alerts arriving in my email about commercial or social media vulnerability.

I have reviewed information from many underwriters providing various types of cyberinsurance as well as information from insurance industry studies. This information focuses on preparedness for and actions to prevent an attack, all of which are important for risk assessment. However, of the many recommendations for assessing the risk of a cyberevent that could disrupt a company through a supply chain and cause a physical or business loss, one of the least emphasized is how thoroughly and quickly a company can react.

While an underwriter may not be able to accurately assess the strength and vulnerability of a company's supply chain, it may be able to accurately assess its robustness and responsiveness. Using the German bank's 2-factor authentication as an example, the bank appreciates that its business is based upon authorized access. An underwriter can examine whether the bank has a separate system of authentication that it can quickly switch users to when the 2-factor authentication system is shut down due to vulnerability at the third-party telecommunications company. Where the bank is robust and agile, an underwriter can determine whether an attack on a central system will result in a major loss.

Similarly in manufacturing, such as the German steel company or similarly situated power companies where the process controls are network-segregated, when a major event such as a shut-down is triggered, an underwriter can examine whether there are systems in place that automatically alert personnel to the directive before the shut-down process begins and require a manual response in order to proceed.

Risk assessment that focuses on a company's ability to respond to a cyberevent impacting its supply chain provides more practical and accurate information. It tracks the supply chain functions necessary for a company's profitability and measures its plans to maintain these functions where one of its vendors is disrupted. Rather than gamble on "if" or "when" a disruption will occur, by examining robustness, i.e., alternative or distributed systems and responsiveness, i.e., agility to switch systems or vendors, an underwriter can assess the extent of damage such a disruption may cause. ●