Wanted: Innovative Responses to a New Security Threat

By Jim Rice

Jim Rice is deputy director at the MIT Center for Transportation & Logistics (MIT CTL). He can be reached at jrice@mit.edu.

The recent cyber attacks and security breaches at Target and Home Depot drew executives' attention to the vulnerability of their companies to this type of crime. The incidents exposed some 40 million and 56 million credit cards respectively, and in the case of Home Depot, occurred despite the company's best efforts to protect the firm.

What has this to do with supply chain management, and in the context of this column, supply chain innovation (SCI)? The answer is a great deal. As I have argued on these pages, one of the main types of SCI entails challenging the dominant design. In this case, that means challenging the prevailing method for supply chain security in response to the cyber security threat. The SCI will become a reality when firms develop the robust responses that are required.

Edge of the Precipice

High-profile breaches such as the ones cited above have spotlighted cyber security, but awareness of the actual risks involved is still relatively limited.

This is especially true with regard to the flow of information that parallels the flow of materials, and powers all supply chains. These information streams include product details, logistics data, and customer information, as well as facts and figures on factory and retail operations and financial management. On the factory and warehouse floor, automated equipment and machines are increasingly assigned an IP address, creating additional access points that serve as openings for intrusions.

In terms of protecting this information from cyber attacks, I believe it is as if we are doing business in a pre-9/11 period, where a disaster that will expose our cyber weaknesses is imminent.

The signs are there if we look at recent incidents and imagine the potential implications for supply chains. Here are three examples to consider.

- After being dismissed by his employer, a wastewater plant employee in Australia remotely hacked into the organization's plant operations and altered fluid flows resulting in a sewage release into the public waterways.
- Just a few months ago the Zombie-Zero malware attack was discovered in several logistics and robotics firms. It had been active inside the organizations for more than a year, and was being used to observe and track conveyances on their logistics journey. The malware was found in scanners that were used by each of the firms, and was apparently embedded in a Chinese supplier's facility. Sadly, software updates provided by the manufacturer failed to rectify the vulnerability.
- A study on ocean-going vessels showed that clever adversaries have already figured out how to take control of a vessel using its GPS system.

These examples show how attackers are capable of gaining access to internal systems to not only steal operational information that drives the supply chain, but also to control the targeted operations.

Redefining Dominant Designs

Current defenses against attacks like these are based on dominant designs for security systems. What are these models?

The dominant design for protection in the supply chain domain involves physical site security for material flows and/or conveyances. But, physical measures are of little use where cyber crimes are involved. Many of the IT systems that underpin information flows are protected by password systems, but invariably these are not very robust

There is also a dominant design for responding to supply chain security breaches. This often entails a lengthy process that starts with chartering a committee to investigate, develop, and implement a solution. The process tends to proceed relatively slowly, however. For example, Home Depot responded speedily after learning of the Target breach, but its efforts to inspect,

detect, and protect were not fast enough to outpace the attackers. Companies often lack the in-house tools and resources to properly evaluate their vulnerabilities, much less respond quickly.

There are also some perceptual barriers to more effective responses. Most supply chain organizations view cyber security as an IT concern. The assumption makes sense given supply chain's traditional focus: efficiency and effectiveness in sourcing, producing, and delivering to demand, while collaborating with upstream and downstream partners.

Ironically, it is these activities—enabled by integrated IT systems—that make the supply chain prone to cyber attacks. But companies have not yet learned that the threat to our systems through IT is as great as any other potential disruption.

The Need to Learn Fast

Why is the threat so different now? Today, cyber adversaries not only destroy information, they can also commandeer systems and use them to distribute weapons and contraband. They can engage in human trafficking or turn your business into a conduit for malware and further cyber attacks. And they are in the business of aiding and abetting the theft of cargo and competitive intelligence, and of doing damage by altering information on customers and shipments.

Cyber criminals include professional gangs, business competitors, "hacktivists," and nationalists intent on disrupting commerce for profit and political gain. Moreover, for every $1 that a hacker spends attempting to break into your system, your firm must spend $100 to defend itself. As a result, most firms have already lost or are losing the battle to prevent illicit access to their systems; the bad guys are already inside.

What Can a Firm Do?

In general, companies should focus on detecting infiltrators and limiting their ability to remove data and exert control over operations.

To begin with, a firm should conduct an assessment on the presence of adversaries, the quality of the software, and the validity of the data sources used. It is also advisable to identify every potential network access point including suppliers, maintenance third parties, 3PLs, and contractors.

The outcome of the assessment will likely require investing in skilled human resources to detect and protect the firm's supply chain and cyber systems. Another possible recommendation is to change the way systems are accessed to include two-factor authentication, and perhaps a "100 percent reliable" information supply chain. This level of assurance and security is necessary for nuclear weapons testing but may be cost-prohibitive for logistics and supply chain applications.

An ongoing monitoring system is required to identify atypical data movements and access within the firm. Keep in mind that an adversary already inside the system will likely traverse from its entry point to other systems, attempting to laterally move data to its access point. As a result, companies should look for atypical lateral movements of data and access.

And once an intrusion has been detected, the firm will need an Incident Response Team (IRT) that can respond quickly—in minutes, not weeks or months.

The firm must also invest in resilience measures to deal with the inevitable breaches, designing the operations to limit the impact of an intrusion. In addition to traditional measures, firms need to adopt some innovative counter-measures such as kill-switches that enable them to reclaim control of vital systems. There could be parallel control systems that can be disconnected from the internet and other internal systems, and allow for local/manual operation only. This gets challenging when considering control for the entire network of upstream and downstream supply chain partners.

Companies often lack the in-house tools and resources to properly evaluate their vulnerabilities, much less respond quickly.

The concept of a kill-switch is a new idea gaining credibility. A recent *Wall Street Journal* piece "Unleash the Repo-Drones," advocated for the use of remotely-controlled kill-switches to disable military equipment stolen by ISIS fighters; something the U.S. military wishes it had now.

These are not the only challenges. Supply chains are traditionally focused on efficiency, and are run by logisticians and engineers—not IT. Supply chain, IT, and security departments have to work shoulder-to-shoulder in new ways in order to effectively deal with cyber threats.

An Emerging Innovation

The dominant design for supply chain security decision-making and response must change if organizations are to have a chance of keeping pace with the cyber security threat.

Companies are not alone. Two documents, GAO-13-652T and NIST 800-161, are especially useful resources. These guidelines help companies to map their responses and can serve as a starting point.

But the primary challenge is developing a new dominant design for supply chain security that integrates the elements described in this article in new ways. In effect, we are laying the groundwork for a new form of resilience that is specific to cyber attacks, perhaps called "cyber resilience." Whatever name it takes, it will be an important innovation that enables supply chains today and in the future.