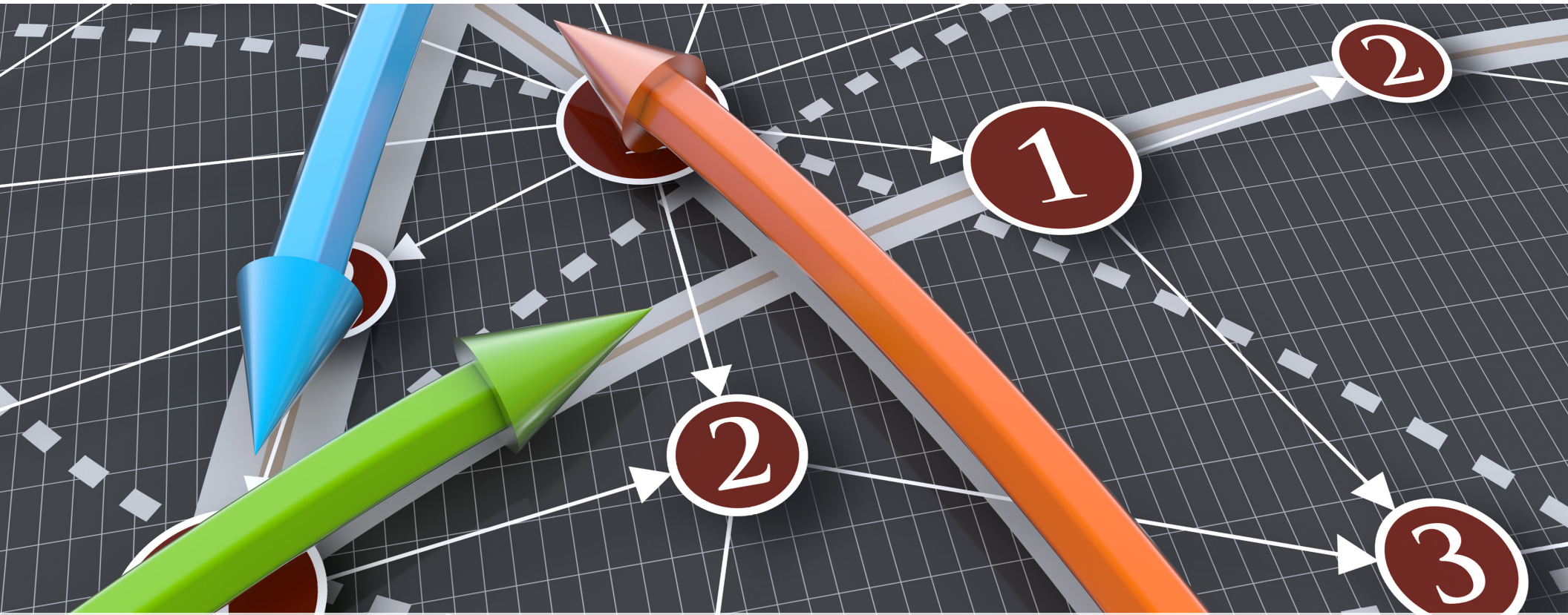
SourceToday

Thought Leadership Series

Issue 07.2017



Managing Supply Chain Security Risks

Security ranks right behind counterfeits in the risk priorities of procurement managers, according to a recent SourceToday survey of OEM procurement managers. It's no wonder, considering digital security attacks are on the rise, and the threats are getting more sophisticated. Following are strategies for protecting systems and minimizing the impact of attacks.

Successfully competing in today's economy increasingly requires that companies share data across digital platforms with companies, organizations, and people with which they share a business interest. According to Gartner's 2017 CIO survey, 79% of top-performing companies, based on IT and enterprise performance, report that they participate in such "digital ecosystems"—as opposed to only 49% and 24% of "typical" and "trailing" performers, respectively.[1] For these leading organizations, Gartner postulates, digital ecosystem adoption offers enhanced market (or consumer/citizen) access and thus promotes more rapid innovation and greater productivity growth.

And the growth in data generation and sharing is forecast to spiral. Market intelligence company IDC predicts that by 2025 the global datasphere, buoyed by growth in the Internet of Things (IoT), will reach 163 zettabytes, 10 times the volume of data generated in 2016. By that time, IDC says the typical connected person will interact with web-enabled devices of one sort or another roughly 4,800 times per day—one interaction every 18 seconds.[2]

But while data sharing will help companies boost the efficiency of their supply chains, and improve their consumer and market responsiveness, it will also multiply the number of potential points of exposure and vulnerability to cybercrime. Already a thriving black market has emerged to support hackers' sale of financial information, intellectual property, and personal data stolen from manufacturers, retailers, and others.

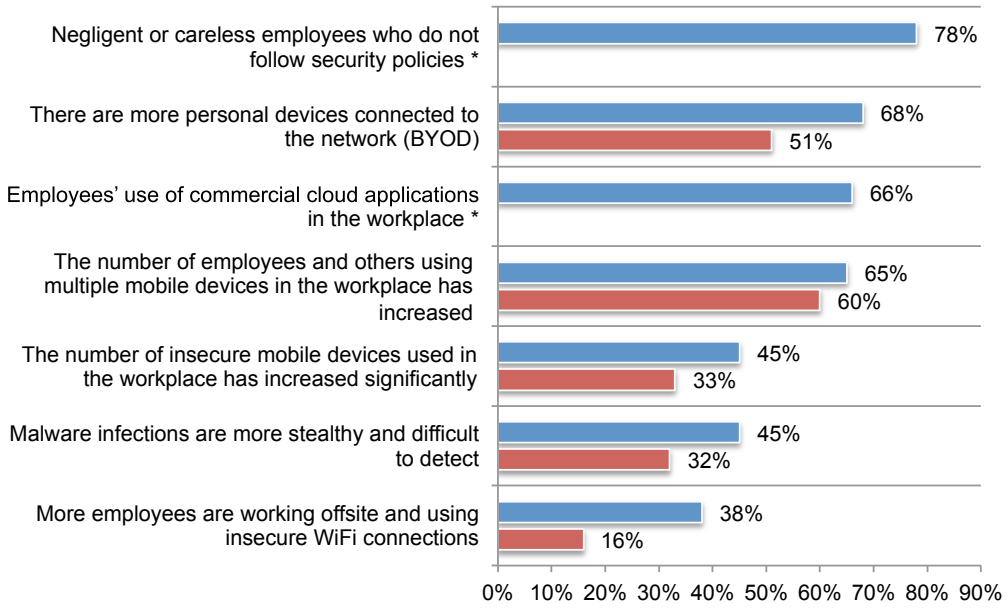
Cyberattacks range widely in form and virulence, from nuisance crimes such as denial-of-service attacks to ransomware, phishing, virus dissemination, webjacking, and more. The damage to a company or organization can be as simple as the temporary shutdown of a website, as extensive as the theft of millions of pieces of private customer or company data—or as life threatening as the takeover of industrial controls at a manufacturing plant.

With money, digital and physical property, lives, and brand reputation all at stake, how can companies protect themselves and their supply chains from cyber threats?

Safety Begins at Home

It is generally agreed that cybersecurity is foremost a "people problem," as employee actions that allow hackers an entry into a company's network—whether by intent or out of ignorance—can override even the most sophisticated security systems. A 2015 Ponemon Institute survey of over 700 IT professionals on endpoint risk in organizations found that negligent or careless employees who do not follow security policies were ranked as the greatest cybersecurity threat (see Figure 1).[3]

Figure 1. What are the biggest threats to endpoint security in your organization?
Five choices permitted



Source: Ponemon Institute

* This response was not available in all fiscal years

"Phishing" is one common method of attack that preys upon this "weak link" in companies' cyber defenses to penetrate company networks. In such schemes, hackers disguise themselves as a trustworthy entity to lure employees, either en masse or individually, into divulging sensitive information such as usernames, passwords, and credit-card details. In 2015, an employee of a subsidiary of healthcare insurance company Anthem Inc. opened a phishing email, unwittingly downloading malware that led to the exposure of 80 million customer health records.

In other cases, employees may steal or compromise company data intentionally—whether for profit or in retaliation prior to leaving a company. A 2016 survey of enterprise security professionals by Accenture and HfS Research identified "corporate insiders" as key players in the theft of both corporate and personal data, with 69% of respondents reporting attempted or successful data theft or corruption by such actors during the prior 12 months.[4]

Rule number one in protecting companies from cyber threats is to limit employees' access to data and systems to that which they require to perform their jobs. Employees should be given a unique user ID for access to company systems that will allow any activity to be traced back to a specific individual. Authentication should require use of biometrics, a security token, or a strong passcode that is updated regularly.

Staff need to be instructed as to their responsibilities in helping thwart cyberattacks. That means instituting rules around leaving a computer unattended without logging off or leaving the company premises with corporate information copied to a smartphone, personal tablet, or USB device. Limitations against downloading software, applications, and music—as well as visiting social networking and peer-to-peer file-sharing sites—while on the corporate network will reduce the company's exposure to malware and botnets. Training of employees to help them identify and avoid fraudulent emails will assist in preventing them from unintendedly passing sensitive data or intellectual property to cybercriminals. *(Continued on page 5)*

Case Study: Blockchain—Securing Tomorrow's Digital Supply Chain?

Among the most vexing of challenges companies face today is establishing the provenance of all parts and systems across their supply chains. Manufacturers want assurance that all components used in their fabricating processes are genuine and traceable as such—and that products that they may supply to downstream users similarly will not be tampered with.

Blockchain is an emerging technology that offers the potential for establishing an "unhackable" record of a part or material's provenance at each stage of the sourcing and manufacturing processes. The technology uses an open cryptographic network to produce a digital time-stamp of all transactions—date and location of mining or manufacture, parties involved in the item's production, cost of transportation, etc.—so as to increase transparency into the supply chain.

Once a transaction has been logged—i.e., once a "block" has been formed—it is added to a chain of existing blocks. A record can be altered or removed only via the agreement of a majority of those holding the other blocks—making the system all but tamper-proof. The digital ledger isn't owned by any entity or stored in any one place, but rather is distributed across thousands of systems worldwide.

Unlike RFID technology, blockchain does not require affixing tags to pallets or reading hardware—making it efficient and inexpensive enough to be used to record even the smallest of transactions. That makes it potentially useful to serve as a digital record for the billions of transactions that the IoT is expected to generate across supply chains in the near future.

IBM has launched a service that allows companies to test the technology's use to track items across their supply chains. London-based Everledger has used the service to verify that diamonds sourced from parts of Africa are not supplied from conflict regions.

In December 2016, Everledger became the first company to secure a bottle of wine's provenance using blockchain.[5] The bottle, a 2001 Margaux, was certified and secured on the Chai Wine Vault—a joint solution introduced by Everledger and fine wine expert Maureen Downey to permit provenance tracking of fine wines.

In the fine wine industry, in which an estimated 20% of international sales are of counterfeit wine, problems with document tampering and fraudulent activity affect the supply chain pipeline from grape to glass. "Blockchain enables us to secure the identity of an asset in a way we haven't been able to before," says Leoni Runge, Everledger's head of fine wine. "For the fine wine industry, this means the opportunity to add a layer of transparency to every stage of a bottle's journey across the supply chain."

The Chai Wine Vault issues certification to bottles authenticated through Downey's Chai Method, in which more than 90 data points are collected, in addition to high-resolution photography and records of a bottle's ownership and storage. Everledger uses this information to create a permanent, digital incarnation of the bottle that is written permanently into the blockchain.

This digital proof travels with the wine as it moves among different stakeholders in the supply chain, with ownership and storage records updated as the bottle changes hands. Licensed retailers, warehouses, auction houses, and other sale platforms can link to the bottle's digital identity to verify its provenance. ■

"Employees," in this context, includes executive managers—who by virtue of their supervisory roles may represent choice targets for hackers. Business email compromise schemes, for example, typically use email addresses spoofed to appear as though they come from a trusted business colleague to request payment for a bogus transaction. In one such "whaling" case involving aircraft parts manufacturer FACC Operations GmbH, cyber criminals sent an email that appeared to come from the company CEO to its accounting department requesting the transfer of approximately $50 million for a fictional acquisition. Ultimately, the firm lost $40 million and both its CEO and CFO were fired.

Clearly, as cyberattacks continue to grow in volume and sophistication, companies need to look to new ways of containing them. The notion that cybersecurity is "IT's problem" ignores the reality that cybersecurity is more than just an information technology risk; it is a business risk with real implications for revenues, share price, and brand reputation. As such, executive management needs to take ownership of the cybersecurity risk management process across the company and its supply chain.

Develop a Cybersecurity Risk Management Plan

According to Gartner, by 2020 approximately 60% of digital businesses will suffer major service failures due to the inability of IT security teams to manage digital risk.[6] "Decision making, prioritization, budget allocation, measurement, reporting, transparency, and accountability are key attributes of a successful program that balances the need to protect with the need to run the business," the company notes in its 2016 report *Cybersecurity at the Speed of Digital Business*.

Effectively addressing cyber risk requires an organization-wide, cross-functional approach and the integration of cybersecurity and business strategy, says the World Economic Forum, which estimates cybercrime to be a $445 billion cost to the global economy.[7] Thus, while the IT department might understand system security, they are less likely to understand its implications for overall business risk. Finance, IT, and risk management staff need to be brought together to jointly develop a cyber risk management program.

Formulating such a plan requires first taking stock of what financial, customer, and employee data, intellectual property, and other digital assets a company holds, where they are stored, who has access to them—and, importantly, what the value of each is to the organization as well as to potential attackers. To help determine which of these assets are most valuable—and thus should receive the highest-priority protection—the National Institute of Standards and Technology advises asking the following questions:

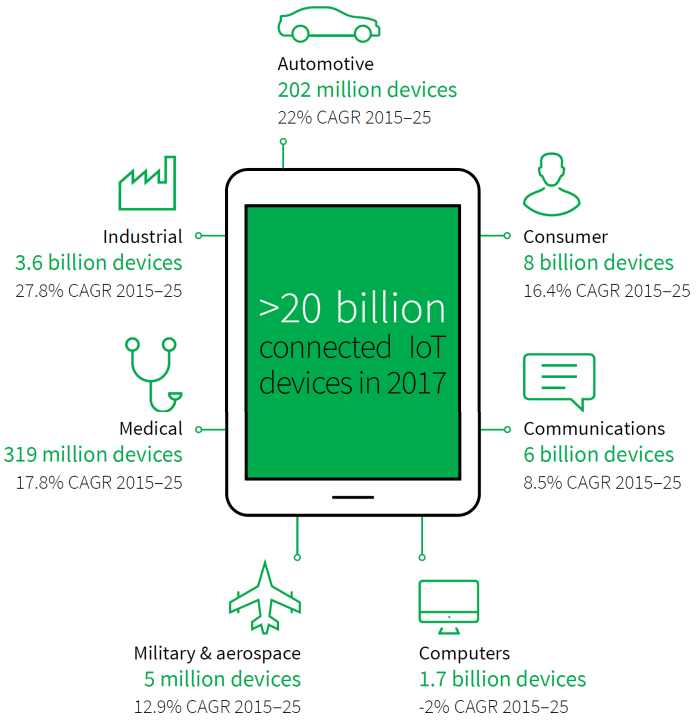
- What would happen if this information were made public?
- What would happen if this information were incorrect?
- What would happen if my company and/or customers couldn't access this information?[8]

Model the threat landscape and assess your company's vulnerabilities within it. While certain categories of risk are consistent across many businesses—software vulnerabilities, for example—others may be specific to an industry, location, or company. Estimate the likelihood that your company or organization will be affected by each identified threat or vulnerability to help determine specific strategies to protect against them—and regularly review and update the threat landscape model.

The predicted explosion in IoT applications across many industries and supply chains—IHS Markit forecasts an installed base of over 20 billion devices in 2017[9] and 30 billion devices by 2020[10]—brings with it a dramatic growth in the number of potential entry points that cybercriminals can exploit and thus requires special attention in any cyber risk management plan (see Figure 2). IoT devices, many designed with little in the way of security technology, expose companies to potential breaches that can result when an insecure device connects to their network. Firms need to audit and safeguard against the potential risks associated with the

deployment of IoT projects—a process that will necessarily involve input from product design, production, and supply chain teams.

Figure 2. Twenty billion IoT devices will be connected in 2017



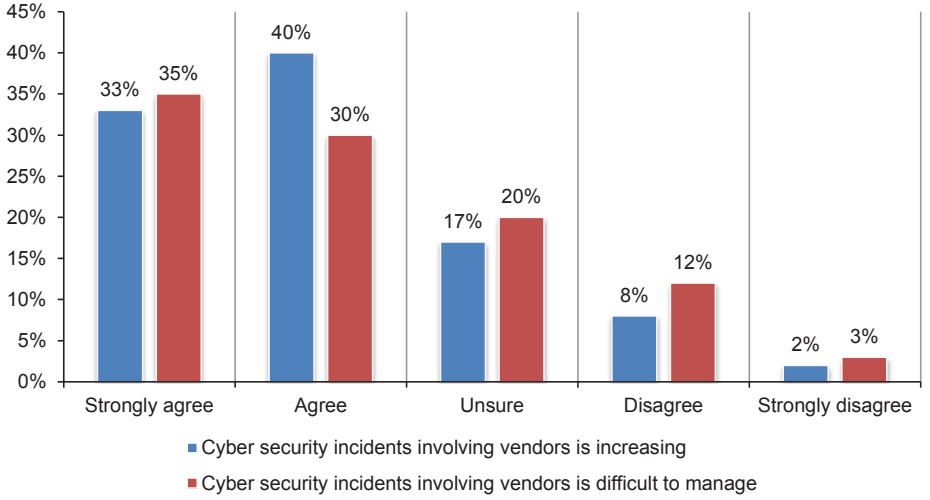
Source: IHS Markit

Penetration testing, in which a cyberattack is simulated against the company's network, is a useful method for gauging the effectiveness of an organization's digital security plan. Tests should include physical, social engineering, and cyber-based attacks, with the results used to inform changes to improve the company's security program. External cybersecurity firms can provide rigorous testing and assessment of system weaknesses.

Secure Your Supply Chain

According to a 2016 survey of 600 data risk managers across multiple industries carried out by the Ponemon Institute, 73% of respondents are seeing an increase in the number of cybersecurity incidents involving vendors (see Figure 3). Nonetheless, 60% of those surveyed say their companies do not monitor the security and privacy practices of vendors with whom they share sensitive or confidential information.[11]

Figure 3. Cybersecurity incidents are increasing and difficult to manage



Source: Ponemon Institute

Growth in the length, complexity, and connectedness of supply chains demands that companies boost their oversight of supply chain security practices. That means supply chain managers must work with their IT team, cybersecurity professionals, and supply chain partners to identify which of their third-party vendors are most vulnerable to cyberattack and data breaches.

For larger companies—which may have thousands of suppliers—eliminating supply chain risk altogether is likely infeasible. However, they can reduce their risk considerably by, first, identifying all vendors with

which they do business and, second, establishing which of those firms have the greatest access to the company's data and its network. A security breach at a vendor that is integrally involved in, say, product design might be considered a more significant risk than one with which the company contracts for occasional logistics support.

Vendors need to be scrutinized and evaluated as to the rigor with which they guard against cyberattacks and data breaches. How do they protect against malware, viruses, and intrusion? What, if any, encryption standards do they employ for data that is stored or in transit? Which employees will have access to company data? Has the firm ever suffered a data breach and, if so, how significant was it and what new controls were put in place to prevent future such incidents?

Contracts with suppliers should codify vendors' cybersecurity policies and procedures, including how company data should be handled and secured, and stipulate that third parties notify the company in the event of a breach of their data. Such contracts should spell out and allocate risk between both parties, including provisions that hold the third party financially responsible in instances where they are deemed to have failed to take sufficient action to prevent or mitigate a cyberattack. Legal documents should also stipulate restrictions on subcontracting to ensure transparency into the vendor's supply chain.

Vendor access to the company network should be restricted to the greatest extent possible, with the terms of such access specified in writing and subsequently monitored to ensure the frequency and type of access is compliant with the agreed-upon terms. Continuous-monitoring software can be an effective method for helping to verify that vendors are following through on their cybersecurity obligations.

Finally, a range of cyber liability insurance products are available to protect companies against supply chain risks. Although such coverage will not prevent against attack, it can help cover many of the costs associated with responding to a data breach, including expenses relating to damaged computer systems, investigation of the breach, and legal assistance.

By John Simpson

1."Seize the Digital Ecosystem Opportunity," Gartner Inc., 2017.
2."Data Age 2025: The Evolution of Data to Life-Critical," IDC, 2017.
3."State of the Endpoint Report: User-Centric Risk," Ponemon Institute, 2015.
4."The State of Cybersecurity and Digital Trust," Accenture and HfS Research, Ltd., 2016.
5."Everledger Secures the First Bottle of Wine on the Blockchain," Everledger, 2016.
6."Cybersecurity at the Speed of Digital Business," Gartner Inc., 2016.
7."The Global Risks Report, 11th Edition," World Economic Forum, 2016.
8."Small Business Information Security: The Fundamentals," National Institute of Standards and Technology, 2016.
9."IoT Trend Watch," IHS Markit, 2017.
10."IoT Platforms: Enabling the Internet of Things," IHS Markit, 2016.
11."Data Risk in the Third-Party Ecosystem," Ponemon Institute, 2016.