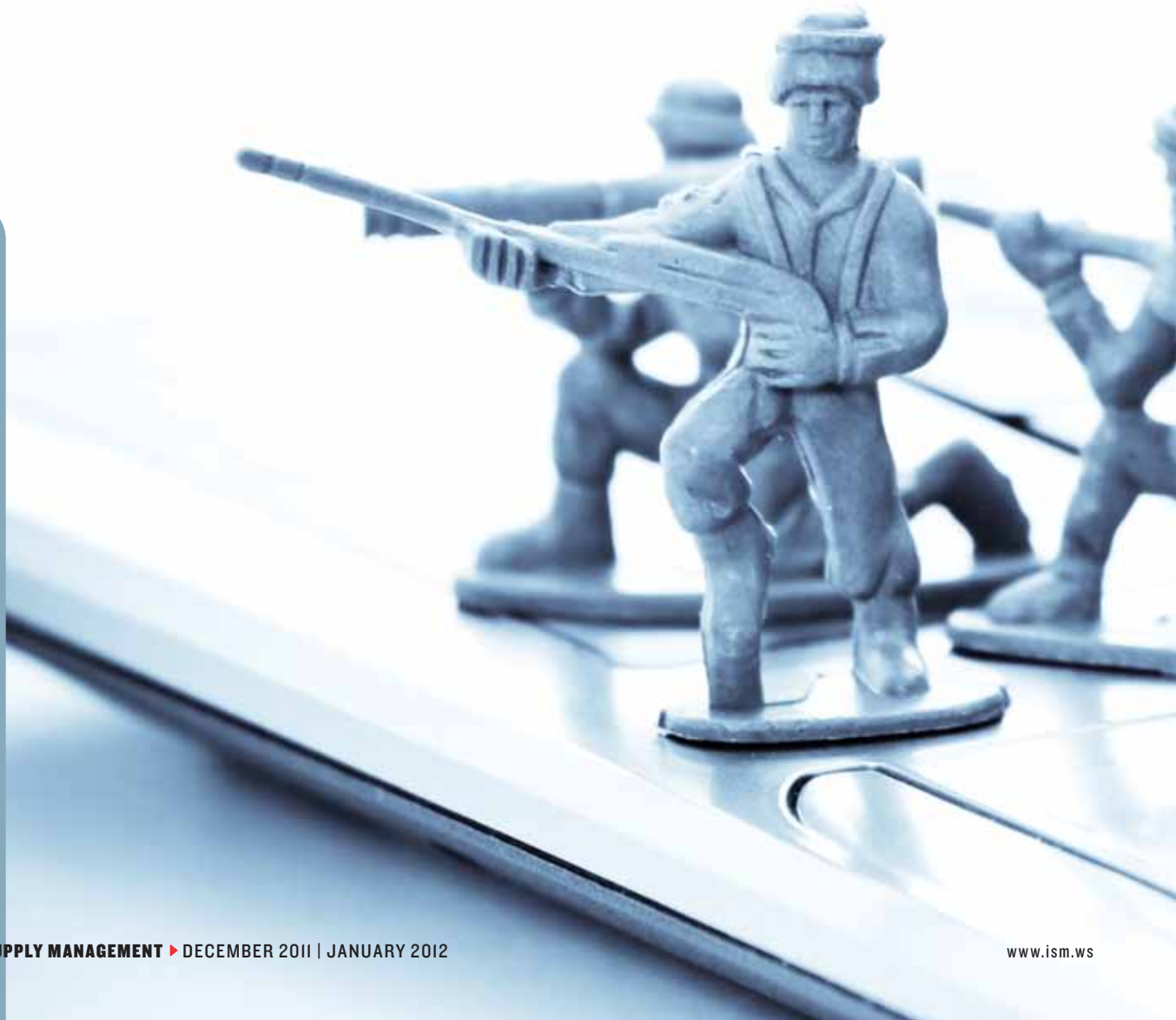
DEFENDING Cyberspace

Businesses search for ways to protect their computer networks and supply chains against relentless attacks by cybercriminals.



cover story

By Mary Siegfried

With the click of a mouse, an employee can unknowingly open the door to a company's computer network, leaving the system vulnerable to cyberattacks that have become more sophisticated, more targeted and more sinister over the past several years. Securing the wealth of information tucked inside a company's technology system and its ever-growing supply chain is one of the greatest challenges facing businesses today.

News stories detailing bold cyberattacks on businesses and governments are capturing the attention of organizations worldwide as they search for solutions to a threat they know will not go away, or even dissipate, in the near future. Cybersecurity experts readily admit there is no easy answer — no silver bullet — because the "bad guys" are always one step ahead of the newest solution. They also agree that businesses need to be more proactive in developing technology, education programs and supply management practices to defend against attacks.

Supply management plays a pivotal cybersecurity role because supply chains are complex, highly integrated and increasingly dependent on information technology. Supply management professionals manage numerous suppliers, handle outsourcing contracts around the globe and often purchase technology components for the company, all of which have the potential to weaken a company's cybernetwork.

The complexity of supply chains is one of the major security challenges for supply management organizations, says Edward G. Amoroso, Ph.D., chief security officer at AT&T, headquartered in Dallas. Noting that there is no "quick fix," he adds that professionals "must adopt a

defense-in-depth strategy of continuously deploying additional layers of security behind the network perimeter defenses." A defense-in-depth strategy is a layered defense strategy that includes technical, organizational and operational controls to achieve information assurance in today's highly networked environment. In the supply chain, defensive strategies include stronger supplier relationships, employee education and technology solutions (see the sidebar below).

Changing Landscape

Cybersecurity involves the technology, processes and practices used to protect computer systems, networks and data from unauthorized access or attack. In examining the cybersecurity landscape over the past two to three years, it is evident that significant trends are taking shape — ranging from the motivations to the methods — that make defending a business's cyberspace a constant battle.

Motivations. Attacks on government and business networks are proof that the adversarial side of computer hacking is shifting, says M. Eric Johnson, director of the Glassmeyer/McNamee Center for Digital Strategies at Tuck School of Business at Dartmouth College in Hanover, New Hampshire. "If you go back 10 years, it was all about pranksters who found it fun to hack into a network," he says. "The motivations today have become far more economically driven, and there is a wide range of organized cybercriminals out there."

In the last year, Johnson says "cyberactivists" have been added to the mix. He describes these attackers as "looking for widespread media coverage around an issue they care about." He notes that groups such as WikiLeaks have created a "megaphone" for these activists, and that most of the information they gain through the attack is used to embarrass a country or company. Johnson emphasizes, however, that business and supply management professionals are most concerned about cyberattacks that target an organization's intellectual property or financial information. "The other attacks are embarrassing and painful, but what supply professionals really worry about is the loss of a trading algorithm or the detailed plans of the next product release," he says.

Methods. With an estimated US$10 trillion in international electronic transactions crisscrossing cyberspace each day, organizations have to be constantly strengthening and protecting their networks. Unfortunately, experts agree that most security efforts are merely "reacting" to the sophisticated work of active adversaries. Amoroso notes that hackers, organized crime groups, terrorists and even foreign governments use a "broad array of tools and techniques such as spamming, phishing, malware, denial of service attacks, viruses and botnets to infect computers and applications, mine for sensitive information or disrupt service."

Spear phishing is a method being used by cybercriminals that is especially disconcerting to business professionals. It is a rising cyberthreat that targets employees who

DEFENSIVE STRATEGIES

Securing and protecting an organization's cybernetwork involves a variety of strategies. Following are some steps supply management professionals can take to tackle cybersecurity challenges.

Supplier relationships. Strong relationships with suppliers are important to maintaining a secure supply chain. James A. Lewis, senior fellow and director of the Technology and Public Policy Program at the Center for Strategic and International Studies in Washington, D.C., believes supply managers must focus on suppliers' trustworthiness, their downstream suppliers and their ability to track and trace throughout the supply chain. "It's not just how secure you are, but how secure the people you connect with are, as well," he says.

Education. Experts and government agencies are emphasizing education as a tool to reinforce the importance of cybersecurity. They say businesses must encourage employees to "pay attention" to security issues. The U.S. Department of Homeland Security (www.dhs.gov) offers a variety of cybersecurity resources, including "Protect Your Workplace" posters to educate workers about cybersecurity.

Technology. There are numerous technology tools available that can be the first line of defense. They include firewalls, user authenticity, intrusion detection systems, software tools that identify vulnerabilities and unauthorized configuration changes, and newer, developing encryption technologies. However, to ensure that an organization chooses the right technology, the National Security Agency (www.nsa.gov) recommends establishing policies and processes for technology acquisition that include a security policy, system-level information assurance architectures and standards, and acquisition of products that have been validated by a third party. (See the article *Software Sourcing Complexities, Inside Supply Management®*, June/July 2011.)

Assess supplier risk. Supply management professionals should be actively assessing suppliers' processes, performing network and system audits, and examining what data suppliers are sharing with downstream suppliers as well as the degree of risk if those data are exposed.

Senior-level support. Cybersecurity must become part of an organization's DNA and that's only possible with support at the senior level. Edward Amoroso, Ph.D., chief security officer at AT&T, says the best way to accomplish that is "to make security a marketing differentiator for the company because this quickly establishes security as a priority, especially in supply management." This concept is similar to organizations that have adopted socially responsible practices and found a competitive advantage as a result.

can unwittingly compromise a company's network. Johnson says it is a "very focused deception" that is hard to protect against.

While most tech-savvy employees know about the fake spam email from the Nigerian banker, spear phishing emails are addressed directly to an employee by name, contain personal details and look like they come directly from a supplier or someone the employee does business with on a regular basis. The email always contains a link. By opening the link, malware can be loaded into a company's network, "opening many back doors and creating major problems," Johnson explains.

Human Challenge

At first glance, cybersecurity appears to be a technology issue, but there is a human aspect to it, as well. In fact, experts agree that businesses need to focus more of their defensive strategies to target the human side of the cybersecurity equation. Johnson says information leaks and security breaches often are related to human behavior issues. Reports about a company's computer network being compromised lead people to believe it is always the work of "very technical hacks," Johnson says. "But, often it is an inadvertent human mistake that leaves doors wide open for people [cyberattackers] to walk through," he says.

Karl Frederick Rauscher, chief technology officer at the EastWest Institute (EWI) in New York, says it is critical to understand the human element in cybersecurity. "Humans have the potential to be fatigued, deceived and have divided loyalties," he says. "Businesses need to be absolutely aware of the vulnerabilities humans bring to this issue." The human aspect can include the employee who falls victim to spear phishing, an insider who steals information for financial or retaliatory reasons, or an executive who misplaces a company laptop or smartphone.

In fact, if you add the expanding use of mobile technology into the cybersecurity equation, the threat becomes even greater. AT&T's Amoroso says the rapid adoption of mobile technology in the business world will "soon make security concerns in the wireless environment at least equal to those in the wired world." He says a cultural shift is needed to view smartphones as dynamic entry points to the enterprise network. The number and types of threats are multiplying because of the increase in available applications and the diverse functionality available once those apps are downloaded to a user's phone, Amoroso cautions.

Supply Chain Cybersecurity

Cybersecurity is essential in supply management because organizations are increasingly and vitally dependent on information technology to keep the supply chain functioning. Rauscher, a Bell Labs fellow, says supply managers need to realize that the essential ingredients needed for cyberspace to exist and function, such as software, hardware, power, networks and so forth, all have intrinsic vulnerabilities. He adds that businesses certainly have taken advantage of the efficiency and speed that technology provides, but have not fully planned for failures that can occur. "We have flung ourselves fully into a reliance upon this (technology), but too often do not have a 'plan B'," he says.

The complexity, criticality and connectivity in a supply chain's technology network demands that supply management organizations do more than simply react to the current challenge. "Ten years ago, if there was an access or integrity issue in a supply organization's computer network, the impact would be limited," Rauscher says. "But the criticality and connectivity in today's supply chains are absolutely staggering."

Supply chain security has grabbed the attention of businesses because of government pressure and self-interest, explains James A. Lewis, senior fellow and director of Technology and Public Policy Program at the Center for Strategic and International Studies in Washington, D.C. Governments are demanding that suppliers, especially those that provide products for critical infrastructure or national defense, have the ability to ensure a secure supply chain, he says. "Also, companies are realizing that cyberattacks can damage brand reputation and the customer base, so it is in their self-interest to have a trustworthy supply chain," he adds.

Threats and attacks on computer networks will continue, and most likely even increase. "It's a sad truth that is part of the modern age we live in," Johnson says. "We have been arguing for a long time that there is a tremendous benefit to supply chain integration, which there is," he adds. "The downside is that the potential and impact of a supply chain disruption becomes greater." ISM

WHAT WORRIES SECURITY OFFICERS?

The threat of a business disruption or breach of security through a cyberattack is uppermost on the minds of many information technology officers at U.S. companies, according to a survey conducted by Dartmouth University's Tuck School of Business. The school surveyed about 25 chief information security officers from Fortune 1,000 companies earlier this year:

- More than 90 percent of those surveyed believe the risk to their information networks had either "significantly" or "moderately" increased in the last 12 months.
- More than 70 percent say it is "somewhat" or "very likely" that their company would experience a significant disruption or breach within the next 12 months.
- More than 80 percent report that the human aspect was more troublesome than the technical.
- More than 70 percent say their department had been allocated more resources over the past 12 months to fight cyberattacks.

Mary Siegfried is a senior writer for *Inside Supply Management®*. For more information, send an email to **author@ism.ws.**