ISM Forward Scan
Insights for Today's Supply Leaders

Exclusively for Supply Leaders in the ISM Corporate Program Vol. 4:2 April 2014

Data Security and Privacy Under Compliance Spotlight

By Dr. Adriana Sanford

Multinationals and their supply chains are confronting a number of challenges as privacy concerns step into the compliance spotlight. Employers are being encouraged to appoint data protection officers to implement their global privacy programs, monitor compliance and raise awareness in connection with the cross-border data transfers that accompany international assignments, marketing strategies, internal investigations, legal actions and other business activities.

The complex frameworks of global legal requirements, (including more restrictive EU legislation with heftier penalties in the not so distant future) make it imperative that corporate legal departments and global supply chain leaders have a more sophisticated understanding of data information risk. Since the current economic downturn elevated the importance of supply chain collaboration, companies can no longer financially afford to track only their top 25 suppliers, as the legal expenses associated with a massive data breach can become insurmountable.

Companies working with significant web applications and highly connected supply chains must vigilantly manage every step of the information life cycle to ensure adequate protection along the supply chain and supporting systems. Managing supply chain interdependence includes implementing proper data security policies, procedures and protocols, as well as hardware and software systems.

Suppliers Can Be Your Weak Link

Many corporate cybersecurity attacks come through third parties, such as suppliers, that handle personal and confidential information, often stealing credentials from those

ISM®
institute for supply management

suppliers. Criminal hackers operate using anonymous networks, encrypted communications and virtual currencies in private forums referred to as "darknets." A comprehensive report by RAND Corp. and Juniper Networks Inc. shows that hackers from the U.S., Russia and Ukraine hawk computer exploits for as much as US$300,000 on an underground market fueled by digital currencies like Bitcoin[1].

The aftermath of these retail breaches leads to the absorption by banks of fraudulent charges made on the compromised payment cards, the cancellation and reissuance of compromised payment cards, lost profits and lost business opportunities. According to G. Robert Blakey, J.D., the foremost authority on the Racketeer Influenced and Corrupt Organization Act (RICO), a company that fails to promptly protect its customers' privacy inevitably bears responsibly for such losses from customers' banks, or alternatively, faces RICO class actions for treble damages.

According to Molly Snyder, a spokesperson for the nation's second largest general merchandise retailer, Target, cyber-intruders gained access to the company's system by using stolen credentials from a third-party vendor.[2] Hackers uploaded exfiltration malware to move the stolen credit card numbers to several staging points throughout the United States, making it difficult to track, before routing the information to computers in Russia. Target has recently made several changes to its technology and security roles, including revising its process for analyzing potential security leaks and separating the responsibility for assurance risk and compliance. Additionally, the company is accelerating its transition to chip-enabled cards or smart cards, which are more popular in Europe than the U.S.

Compliance With U.S., Foreign Laws and Regulations

The EU is on track to increase its privacy protections with an updated EU Data Protection Regulation, which, if approved by the European Council this summer, would become effective in 2016. In addition to the EU, a number of other countries have recently enacted privacy legislation.[3] More than 89 countries have laws and regulations protecting data privacy.[4]

Today, in-house counsel must be familiar with these initiatives for cross-border data transfers, as companies must not only comply with local laws, but also often with the privacy laws of the jurisdictions where the individuals identified in the data reside. If, for example, a U.K. subsidiary of a U.S. multinational plans to transfer data to its corporate headquarters in connection with an internal investigation, the U.K. subsidiary must first ensure local data protection authorities that adequate measures have been complied with.[5] Because U.K. laws have adopted a proceed-at-your-own-risk approach, the data exporter would not be required to obtain prior approval, but sanctions could be imposed if authorities later determined the exporter did not take appropriate steps to ensure adequate protection.[6]

Furthermore, according to Washington, D.C., attorney Bruce Zagaris,[7] U.S. multinationals should not only be careful to abide by the EU directive, but also by each of laws of the EU countries. Under the current EU system, each EU member has a data protection czar with responsibility for implementing the law. Also, there are civil and criminal penalties for violations. The U.K. Information Commissioner's Office, for example, has the authority to fine companies up to £500,000 for noncompliance with the U.K.'s Data Protection Act. In addition, the EU's initiatives to tighten cross-border data protection violations are in the wake of the Snowden disclosures of U.S. mass surveillance.

It is imperative that corporate officials identify any of their smaller or less significant suppliers that may have previously fallen off their radar, as they could become easy targets for cyberattacks, as well as any servers that may be owned by subcontractors in foreign countries. Companies

[1] The 83-page report comes amid warnings by U.S. government and industry officials that digital attacks are becoming more sophisticated and dangerous. Strohm, Chris, "Hackers Sell Exploits for Bitcoins in Underground Market," Businessweek, March 25, 2014. www.businessweek.com/news/2014-03-25/hackers-sell-exploits-for-bitcoins-in-underground-market

[2] Riley, Michael, Ben Elgin, Dune Lawrence, and Carol Matlack, "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," Businessweek, March 13, 2014. www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

[3] McConnel, Ryan,"EU Threatens to Upend Corporate Privacy Compliance," Corporate Counsel, April 3, 2014. www.corpcounsel.com/id=1202649405549/EU-Threatens-To-Upend-Corporate-Privacy-Compliance#ixzz2xrZp19ar

[4] Greenleaf, Graham, "Global Data Privacy Laws: 89 Countries, and Accelerating," Privacy Laws & Business International Reports, Issue 115 Special Supplement, February 2012. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000034

[5] The EU and U.S. Department of Commerce created a self-certification safe-harbor program that allows U.S. companies to certify their adherence to seven principles in order to become eligible to receive personal data from European Economic Area (EEA) nations. While the safe-harbor program was intended to cover all personal data, in practice, many U.S. companies have expressly limited their participation to certain types of data, such as human resources data. http://export.gov/safeharbor

[6] The number of security breaches affecting U.K. business continues to increase –93 percent of large organizations and 87 percent of small businesses experienced a security breach last year. 2013 Information Security Breaches Survey (Technical Report), UK Department for Business, Innovation and Skills. www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf

[7] Bruce Zagaris has served as a consultant to the United Nations and counsel for 14 governments on issues of international white-collar crime.

should check whether these businesses have a history of data security breaches (such information is available by consulting industry sources), as well as request recent third-party audit reports on their data security systems to ensure that appropriate safeguards are in place to protect personal information. The Privacy Rights Clearinghouse a nonprofit based in California that offers a chronology of data breaches, is an example of a privacy monitoring organization.

Consider an International HR Manager

For companies that outsource the functional side of their human resources department to foreign countries, or where EU employees are sent on foreign assignments to non-EU member countries, business and supply chain leaders should consider an international human resources management (IHRM) department, alongside the data protection officer. The IHRM department facilitates selecting, training and effectively managing these expatriate employees and their sensitive data. An IHRM function could prove to be vastly beneficial, especially when a company's employees are in countries where personal data information must be managed according to several data protection czars. Providing IHRM a seat at the management table would help businesses in handling other issues of strategic importance, as well, such as host government relations.

After all, a single point of failure in one application can potentially give corporate hackers access to sensitive data — and customer data could potentially be hosted on any of hundreds of servers owned by suppliers' subcontractors around the world.

Dr. Adriana Sanford recently was nominated by W.P. Carey School of Business as the Lincoln Professor of Global Business Ethics. She is a full-time professor of international management, ethical leadership and business law to more than 1,600 MBA and undergraduate students at W.P. Carey School of Business, Arizona State University (ASU), in Tempe, Arizona. She is also a broadcaster and weekly business ethics expert on "Money Radio," the longest-standing U.S. financial news-talk radio show. Dr, Sanford joined ASU after two decades of real-world experience serving as primary U.S. legal counsel and in-house counsel to U.S. and foreign companies and banks. She has six years of law school education, including a dual LL.M. from Georgetown University and a law degree from the University of Notre Dame. She is also fluent in French, Spanish and Portuguese.

Editorial Insights

In addition to maintaining legal compliance, ensuring the security of your supply chain is crucial to safeguarding your company's intellectual property, reputation and relationships with its customers and suppliers.

There are several recent examples of security breaches in the supply chain. In addition to the examples Dr. Sanford lists, in March 2014, a malicious app that steals users' passwords and credit card information was pre-installed on Android-based tablets and smartphones. The devices were produced by four different manufacturers and, while it's evident the breach occurred somewhere in the supply chain, investigators are still determining where and how the supply chain was compromised. Without a doubt, such breaches affect customers, company reputations, mobile device manufacturers and app developers — with both short- and long-term effects.

More and more, we're seeing cybersecurity breaches take place, and no industry is immune to these attacks. A recent article in *The Washington Post* states that cyberattacks are on the rise and healthcare data is the biggest target. It's important to remember that the responsibility of cybersecurity rests on the shoulders of many within an organization. It cannot be relegated to one department. IT, supply chain, finance and HR are all functions that must work together to combat this growing issue affecting business in such a paramount way.

While this may seem daunting when analyzing supply chains spanning multiple countries and suppliers, there are several sources to help you get started. The National Institute of Standards and Technology (NIST) at the U.S. Department of Commerce published the *National Supply Chain Risk Management Practices for Federal Information Systems*, outlining practices to help mitigate supply chain risk. While this report focuses on federal information systems, it offers solid advice for any company. This is your opportunity to take the lead by meeting with your business partners and asking questions to get the discussion started.

M.L. Peck is senior vice president at ISM.

ISM *Forward Scan* is an exclusive product for supply leaders in the ISM Corporate Program. This practical publication focuses on the profession's next imperatives affecting strategic supply management decisions today. The articles provide insights on emerging trends, technology, challenges and best practices in business. They give decision-makers both a macro and micro view of the supply horizon as a unique tool for supply leaders to impact their company's bottom line. Look for more ISM *Forward Scan* issues throughout the year as a benefit of being an ISM Corporate Program participant.

For additional information on the ISM Corporate Program, contact:

Candace Craig
Manager, Corporate Development
800/888-6276 or +1 480/752-6276,
extension 3089
ccraig@ism.ws

JC SC633 4/14