EMPLOYMENT LAW COMMENTARY

Volume 26, Issue 7
July 2014

San Francisco
Lloyd W. Aubry, Jr., Editor
Karen J. Kubin
Linda E. Shostak
Eric A. Tate

Palo Alto
Christine E. Lyon
Raymond L. Wheeler
Tom E. Wilson

Los Angeles
Timothy F. Ryan
Janie F. Schulman

New York
Miriam H. Wugmeister

Washington, D.C./Northern Virginia
Daniel P. Westman

London
Ann Bevitt

Berlin
Hanno Timner

Beijing
Paul D. McKenzie

Hong Kong
Stephen Birkett

Tokyo
Toshihiro So

Check out our newest international resource "A Guide to Hiring and Firing in Europe"

BUILDING A WORKFORCE CULTURE OF DATA SECURITY IN THE POST-SNOWDEN ERA

By Daniel Westman

Last month's *Employment Law Commentary* discussed the high level of international attention now being paid to protecting trade secrets from misappropriation, with recommendations for practical steps that companies may take to prevent misappropriation. This month's issue follows on with a discussion about how to build a workforce culture of data security protecting not only trade secrets, but also personal information and third-party confidential information in the possession of most businesses. As illustrated by Edward Snowden's activities, no organization is immune from the insider threat posed by a determined individual. Even well-intentioned employees pose an inside risk when they fall victim to sophisticated "spear-phishing" attacks. The perennial risk from insiders,

MORRISON FOERSTER

continued on page 2

currently put in the spotlight by Snowden and spear-phishing, allows businesses to educate employees about prevention of data breaches while appealing to both employees' personal interest in their privacy, as well as the corporate interest in confidentiality.

An Overview of Snowden's Activities

Whatever one's belief may be about where Snowden belongs on the traitor/hero spectrum, his activities highlight the risk posed by an insider with privileged access normally given to IT professionals. Snowden's revelations have raised citizens' concerns about the privacy of their personal data, corporate concerns about deterring similar breaches of confidentiality in the future, and similar concerns on the part of the U.S. and foreign governments. In 2014, businesses now have an opportunity to educate their employees about data security in a manner that appeals to both their personal interest in privacy of personal information, in addition to their duties to protect corporate confidentiality.

The precise facts about what Snowden did—beyond gaining access to large volumes of NSA information within a short period of time—are hard to pin down. Snowden is under federal indictment and seeking asylum in Russia. To protect their litigation positions, both Snowden and the U.S. government appear to be avoiding public admissions about how Snowden went about obtaining the NSA's confidential information without the NSA's permission. Nevertheless, some "facts" that are highly likely to have occurred can be gleaned from news accounts attributing statements to Snowden and the criminal complaint filed against him.

One article suggests that in March 2013 Snowden took a position with a government contractor to the NSA for the purpose of obtaining access to the NSA's confidential information.[1] The criminal complaint filed against Snowden implicitly alleges, by accusing him of theft of government property and related offenses, that Snowden acquired the NSA's information by obtaining unauthorized access to such information.[2] Snowden appears to have accomplished his acquisition of the information he later disclosed within approximately 45 days, using a widely used "web crawler" tool.[3] The "web crawler" activity may not have been identified by the NSA as improper because Snowden worked in a remote Hawaii office of the NSA, where the NSA's latest intrusion-detection technology may not have been deployed.[4]

At least three instances of "social engineering"[5] likely were at play in the Snowden situation. First, it is highly likely that Snowden did not disclose to his co-workers his intent to misappropriate the NSA's confidential information, or his reasons for doing so. Rather, it is likely that Snowden portrayed himself to co-workers as a rule-following IT professional. Second, given the massive amount of information obtained by Snowden within a relatively short period of time, it is likely that he induced co-workers to share passwords or otherwise provide access to information that Snowden himself was not authorized to have. Third, after obtaining the information he wanted, in early May 2013, Snowden informed his employer that he was ill and needed to take time off.[6] Then he disappeared. His employment was terminated on June 10, 2014. This last instance of social engineering appears to have been intended to allow Snowden to travel to what he considered to be a safe location.

Snowden's activities have caused (i) citizens around the world to be concerned about government surveillance of their personal information, including metadata about their private communications, and (ii) businesses and government agencies to be concerned about social engineering by insiders, and how it can be prevented, detected, and mitigated. In this climate of concern about data security, companies now can provide valuable education to their employees about not falling victim to social engineering in their personal lives, as well as during their work.

Sophisticated "Spear-Phishing" Attacks

Snowden is a classic example of the internal threat posed by determined insiders who conceal their agendas. However, another internal threat is posed by well-meaning employees who may fall victim to a common modern hacking technique to gain access to confidential information called "spear-phishing." Spear-phishing is on the rise across the globe.[7]

While emails from supposed "Nigerian princes" still find their way into our email inboxes, such crude "phishing" activities are relatively easy to spot. However, many of today's cyber-attacks are nuanced, highly tailored, and show signs of accelerating in frequency.[8] Known as spear-phishing, these attacks use publicly available information about the recipients to tailor them to a recipient's particular background or preferences to craft more convincing pretexts than traditional phishing. The pretexts are designed to remove "as many suspicions, inhibitors, and natural reluctances as possible on the part of the victim while simultaneously providing motivation to take an action."[9] While computer users in 2014 may scoff at an email purporting to be from a Nigerian prince that blatantly solicits the recipient to wire the sender money, these same recipients may be lulled into clicking on malicious links when pretexts are tailored to them personally.

continued on page 3

Imagine that you have posted on your Facebook profile (or LinkedIn, or others) seemingly harmless information under "Interests." You may, for example, be an avid volunteer for the local animal shelter. If an attacker knows your affiliation with that animal shelter, then they might send you—at your corporate or personal email account—a malicious link to a fake celebratory video about the success of recent fundraising efforts. You click the video link. By clicking the link, the attacker might now be able to exploit a bug in your browser or in Java, running code on your computer that could compromise the entire operating system. The compromised computer may contain work documents—or may even *be* your work computer. Even worse, if you have used your personally owned device for work under a "Bring Your Own Device" to work policy, you may have compromised your personal information as well as your employer's data. You are now a victim of spear-phishing.

Building a Workforce Culture of Data Security

How confident are you that all of your employees fully appreciate the threats posed by social engineering as illustrated by Snowden and spear-phishing? Less than 100% awareness within any workforce creates vulnerability that needs to be addressed.

The following practical steps should be considered to weave safe data security practices into the fabric of corporate culture. While there is no guarantee that future Snowdens and spear-phishing attacks can always be prevented, these steps may help reduce their frequency.

- **Talk about data security:** Regular employee training should include data security with respect to trade secrets, personal information, and third-party information, as well as specific discussion of social engineering and risks of social media use;[10]
- **Write about data security**: Revise corporate policies and procedures, as well as confidentiality agreements with employees, consultants, and third parties entrusted with confidential information, with a focus on data security;[11]
- **Show commitment from the top:** Whenever your executives speak or write to employees, include discussion of data security;
- **Train managers:** Managers must lead by example with respect to data security if they wish employees to believe it is important to the company;
- **Focus on high-risk functions:** Consider implementing strict controls on computer users with privileged access (e.g., two-person permission for access to highly sensitive information);[12]
- **Condition computer usage on strong passwords:** Require frequent changing of passwords, and require use of strong passwords to log on;[13]
- **Condition participation in Bring Your Own Device programs on compliance with security measures:** Organizations must recognize that their networks may include personally owned devices, and should require implementation of appropriate security measures on such devices;[14]
- **Measure employee compliance:** Include data security as an element of performance evaluations, and eligibility for bonuses, sales commissions, and stock option grants;
- **Empower workers to report lax data security:** Train employees to use confidential hotlines to report questionable data security behavior;[15]
- **Monitor anomalous computer usage:** With many employees working remotely, managers may need to review logs regarding activity on the network;[16]
- **Focus on international travel:** Train employees about particular data security requirements (e.g., compartmentalizing sensitive data, taking only "clean" devices) when traveling to countries known for piracy of intellectual property;
- **Clean entry/clean exit:** Conduct entrance interviews to emphasize data security, including not bringing confidential information from competitors, and exit interviews to ensure return of confidential information whether stored on employee-owned devices or in storage in the cloud.[17]

Conclusion

While technology continues to change rapidly, what may never change is human susceptibility to social engineering. Listen to what reformed hacker Kevin Mitnick, who once was on the FBI's "Most Wanted" list and spent time in federal prison, has to say: "In this age of firewalls, Intrusion Detection Systems (IDS), anti-virus, and <insert security technology here>, the shortest path into a network is through the weakness embodied in human behavior."[18] Businesses should capitalize on the current climate of concern about data security to inform their workforces about practices that will help them to avoid data breaches, both as employees and private citizens.

Daniel Westman is a partner in our Washington, D.C. and Northern Virginia offices, and can be reached at (703) 760-7795 or dwestman@mofo.com.

To view prior issues of the ELC, click here.

continued on page 4

1 *South China Morning Post*, June 24, 2013, available at http://www.scmp.com/news/hong-kong/article/1268209/snowden-sought-booz-allen-job-gather-evidence-nsa-surveillance?page=all.

2 U.S. v. Edward Snowden, Case No. 1:13-CR-265 (CMH) (June 14, 2013 E.D.Va.). The affidavit supporting the complaint has been filed under seal so only conclusory allegations are contained in the complaint available to the public.

3 *New York Times*, Feb. 8, 2014, available at http://www.nytimes.com/2014/02/09/us/snowden-used-low-cost-tool-to-best-nsa.html?_r=0.

4 Id.

5 "Social engineering" is the term information security specialists use to describe the practice of manipulating individuals into performing specific actions or divulging confidential information. *See generally* http://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering.

6 *The Guardian*, Jan. 31, 2014, available at http://www.theguardian.com/world/2014/feb/01/edward-snowden-intelligence-leak-nsa-contractor-extract.

7 The Consumer Reports National Research Center estimates that in 2013, 11.3 million people fell victim to targeted spear-phishing scams, with the number of victims up 22% from 2012. http://www.consumerreports.org/cro/magazine/2014/07/your-secrets-aren-t-safe/index.htm?EXTKEY=AFOXDIG01.

8 http://www.consumerreports.org/cro/magazine/2014/07/your-secrets-aren-t-safe/index.htm?EXTKEY=AFOXDIG01.

9 http://www.forbes.com/sites/ericbasu/2013/10/07/spear-phishing-101-who-is-sending-you-those-scam-emails-and-why/.

10 "Common Sense Guide to Mitigating Insider Threats, 4 Edition," pp. 17-22, Carnegie Mellon Software Engineering Institute, Dec. 2012.

11 Id., pp. 13-16.

12 Id., pp. 48-51.

13 Id., pp. 35-38.

14 Id., pp. 60-64.

15 Id., p. 19.

16 Id., pp. 56-59.

17 Id., pp. 65-68.

18 http://www.forbes.com/sites/ericbasu/2013/10/07/spear-phishing-101-who-is-sending-you-those-scam-emails-and-why/.

Wende Arrollado | Morrison & Foerster LLP
12531 High Bluff Drive, Suite 100 | San Diego, California 92130
warrollado@mofo.com