Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

The Greatest Cybersecurity Risk Comes From Within

Law360, New York (September 1, 2015, 10:50 AM ET) --

Ann M. Caresani

When businesses think of data security, they often think first and foremost of protecting the valuable, often intangible assets that make up the essence of the business from theft and release by malevolent outsiders. What typically does not come to mind first is protecting the enormous amounts of data that businesses collect on a regular basis about their employees. The employee data that businesses collect contains a wide array of sensitive and private information about what is arguably any business' most valuable asset: its people.

Yet, protecting employee data, and taking special measures to train employees to do so, is not always a part of the data security conversation. Recent events highlight that it is now time for businesses to institute appropriate measures to protect and secure their employee data and establish effective training programs to ensure those protections are not for naught.

Breaches of Employee Data Affect Millions

One only needs to turn on the news to see that the risk of data security breaches involving employee data are real and have the potential to affect millions. A recent, high-profile example of a serious employee data breach involved the U.S. Office of Personnel Management. In the spring of this year, the OPM identified two data security breaches. The first, in April 2015, involved the release of personnel data from 4.2 million current and former government employees, including their names, dates of birth, addresses and Social Security numbers. The second breach involved the compromise of background investigation records containing sensitive information, including Social Security numbers, for 21.5 million individuals (including co-habitants of persons applying for background investigations).

Not long before the OPM breach, Sony Pictures Entertainment Inc. suffered a massive data breach. While the headlines of the Sony breach tended to focus more on studio executives' impressions of Angelina Jolie and the withheld release of the studio's feature film *The Interview*, the breach also included the release of over 47,000 Social Security numbers, medical information and files on Sony employees. That breach prompted several class actions asserting claims against Sony for negligence, breach of contract and various data privacy laws. Both of these examples demonstrate how the threat to and vulnerability of employee data is real, and businesses need to take steps now to protect this data.

Sensitive Employee Data Is Everywhere — Find It

The first step in an effective plan to secure and protect employee data is to conduct an audit to determine where the organization is collecting and storing employee data. In most organizations, the human resources and payroll departments are the two prime locations for the collection and storage of such data. Employee files, leave requests, benefits documents, payroll tax forms, direct deposit records and other similar documents are often collected by these departments. Such documents carry with them real risk of legal liability for employers if the information contained within them were to be intentionally or negligently released.

For example, the Americans with Disabilities Act and Family and Medical Leave Act both contain provisions requiring employers to maintain the confidentiality of the information employees provide when making leave and accommodation requests, and employers can be found legally liable for the improper disclosure of the content of such documents.[1] Likewise, the Fair Credit Reporting Act contains provisions regulating the use and disposal of sensitive information gathered by employers during employee background and credit checks and provides for civil and criminal penalties for violators.[2] These are only a few examples of the network of laws that govern an employer's obligation to protect the privacy of its employees' sensitive data.

There may also be sensitive employee data hidden in places that a business may not necessary think to look. Such information is especially susceptible to unintended disclosure. For example, we have recently seen pension plan documents that list "grandfathered" benefits helpfully identifying the grandfathered participants by Social Security number. The plan administrator is required to distribute these documents to plan participants within 30 days of request. This example demonstrates that employers need to look around carefully and review their common practices from a data security perspective.

Recognizing that sensitive employee data is scattered throughout an organization, the first vital step of any effective data security plan focused on the protection of employee data should be to conduct a thorough audit to locate all of the sensitive employee data that needs protection. Not only should that audit examine what data an organization has and where that information is located, but also examine when and where the departments housing that data share such information with other internal departments or outside vendors, and, if so, what protections are in place to make sure security protections are maintained.

For example, the Health Insurance Portability and Accountability Act required covered entities, such as self-insured health care plans, to obtain "business associate agreements" from business associates, such as the third-party administrator of the plan. But when the Anthem Inc. data security breach occurred, employers sponsoring self-insured plans discovered that they not only had HIPAA issues, but also potentially had state law requirements to consider. Their business associate agreements, and actual experience with their third-party administrator, may or may not have been sufficient to satisfy any applicable state requirements.

Where Is the Real Risk of Employee Data Exposure?

There are essentially three categories of exposure risk for employee data. The headlines that grab and captivate the attention of the public tend to focus on the "malicious outsider," or hacker. These are individuals who set their sights on an organization and attack, stealing valuable information for nefarious purposes. The second category is the "malicious insider." These individuals are employees or former employees of an organization who wish to do the company harm and intentionally steal

information for their own personal gain or to do harm to the organization. It is against these two types of threats that many organizations already have measures in place to protect. Firewalls, encryption, passwords and other measures are all designed to protect against the malevolent threat.

The third category of risk, however, is frequently an afterthought for many businesses, which is particularly troublesome in light of the fact that it is this third category that creates the greatest risk to the security of employee data. This category involves the "negligent insider." This is a current employee with no ill will toward an organization who, through carelessness, negligence and/or lack of proper training, unintentionally exposes sensitive data to the outside. Several studies over the last 10 years have consistently found that an organization's employees — and not hackers — are the most likely threat to information security.[3]

In a recent study, employers reported that the most common root cause for data security breaches, accounting for 35 percent of total breaches, was an employee's loss of a laptop or mobile device.[4] Only 22 percent were reported as resulting from a malicious insider, and only 8 percent of breaches were reported as resulting from an outside hack.[5]

Thus, whether it is losing a laptop or mobile device, emailing sensitive information to personal email accounts, failing to create secure passwords or posting confidential information online, it is an organization's employees — its most valuable assets — that also pose the biggest risk.

Training Is Everything

One of the best ways to protect against breaches of employee data resulting from carelessness or negligence on the part of employees is to properly train employees to recognize what information is sensitive, to know the proper procedures to protect that information and to avoid common mistakes that can result in a breach. Despite the fact that an organization's employees pose the largest risk to the security of sensitive data, 56 percent of employees report that they have received *no* data security training whatsoever.[6]

But, just as important as deciding to train employees on effective ways to secure and protect employee data is deciding how to train employees on this important topic. It is entirely possible that some of the 56 percent of employees who reported no data security training at all actually did have some training that they subsequently forgot. It is essential that employees are not only instructed on how to ensure the security of all sensitive data, but that it is done so in a way that will keep them focused and engaged. It is also important that organizations develop a culture of training that reinforces that learning and allows employees to fully internalize the message the organization wants them to receive and retain it. Here is how:

Training Sessions Should Be Short

Once an organization identifies the policies, procedures and practices it wants to communicate to its employees as part of a data security training (which will be different for each organization and highly dependent on the organization's operations), those topics should be presented to employees is short, manageable sessions. A once-a-year marathon, which is information-dense will merely leave employees overwhelmed and likely to forget most of what they have heard.

Training Sessions Should Be Focused

Similar to the need to keep sessions short, training sessions should focus on one or two topics at the most. Shorter sessions that present slices of information in a thorough, thoughtful way will be more likely to "stick" and more likely to actually be applied when needed.

Training Sessions and Opportunities Should Be Frequent

So many employers believe that having a data security training session once per year should be enough to ensure that all of its employees will know what to do when any situation arises, but employees need to be frequently reminded to be thinking of data security risks and the ways they can prevent a breach. Otherwise, it is very easy for employees to allow the training they have received to slip to the back of their minds as the other, more pressing issues of their day-to-day jobs demand their attention. In addition, the risks to data security are constantly evolving. Having regular opportunities to not only refresh employees' minds on their obligations to protect employee data and advise them of new threats can only improve outcomes.

Training Should Be Engaging

While data security is not the most thrilling of topics, it is important to find ways to keep employees engaged in their ongoing obligation to watch for data security risks and avoid them. Make training sessions interactive, and follow through in the days and weeks that follow a training session. Develop a culture of training. Some employers have used periodic games and quizzes and offered incentives or prizes for employees who properly identify risks or the proper course of action in response to hypothetical scenarios. Catchy flyers, posters and email "tips" that serve as constant reminders of what employees learned during their training sessions can keep the topic at the front of their minds.

It Is Time to Get Serious

The risks to employee data are real, and as much as hackers draw the big headlines, the biggest risks to most organizations' sensitive employee data are also receiving paychecks. Now is the time to minimize that risk. Now is the time to identify what information needs protected and where that information is located within the organization. It is also the time to start implementing effective training programs to educate employees on their vital role in protecting employee data and preventing breaches. It's time to get serious before the danger within strikes.

—By Ann M. Caresani and Christine M. Snyder, Tucker Ellis LLP

Ann Caresani is counsel and Christine Snyder is an associate in Tucker Ellis' Cleveland office.

[1] 42 U.S.C. §12112(d); 29 U.S.C. §2601 et. seq.; *Doe v. U.S. Postal Serv*., 317 F.3d 339, 344-45 (D.C.Cir.2003).

[2] 15 U.S.C. §1681 et. seq.; 16 C.F.R. §682.

[3] *The Human Factor in Data Protection* (2012) Ponemon Institute LLC. Available at:http://www.ponemon.org/local/upload/file/The_Human_Factor_in_data_Protection_WP_FINAL.pdf;

Cisco Systems Inc. (2008) *Data Leakage Worldwide: Common Risks and Mistakes Employees Make* (white paper). Available at: http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.pdf; *U.S. Survey: Confidential Data Risk* (2006) Ponemon Institute LLC. Available at: http://online.wsj.com/public/resources/documents/report20060815.pdf;

[4] *The Human Factor in Data Protection* (2012) Ponemon Institute LLC. Available at:http://www.ponemon.org/local/upload/file/The_Human_Factor_in_data_Protection_WP_FINAL.pdf

[5] *Id*.

[6] David Monahan (2014) *Security Awareness Training: It's Not Just for Compliance*. Enterprise Management Associates, Inc. Available at:http://info.wombatsecurity.com/hs-fs/hub/372792/file-1842832356-pdf/EMA_Wombat-SecurityAwarenessTraining_2014-RR_SUMMARY.pdf

---