The CYBERSECURITY LAW REPORT

Schulte Roth&Zabel
New York | Washington DC | London | www.srz.com

www.cslawreport.com Volume 1, Number 1 April 8, 2015

THREAT SOURCES

Strategies for Preventing and Handling Cybersecurity Threats from Employees

By Amy Terry Sheehan

Not all data breaches stem from trained cybercriminals – in fact, many cybersecurity incidents come from the inside. They are initiated by an employee's inadvertent mistake or intentional act. In this interview with The Cybersecurity Law Report, Holly Weiss, a partner in the Employment & Employee Benefits Group, and Robert Kiesel, a partner and chair of the Intellectual Property, Sourcing & Technology Group, at Schulte Roth & Zabel LLC discuss: the two categories of internal cybersecurity threats (inadvertent and intentional); specific ways to protect against those threats, including effective training methods and "bring your own device" policies; and the effect of relevant regulations.

Two Categories of Threats

CSLR: What are the most important internal cybersecurity risks?

Weiss: The risks fall into two categories. First, there is a disgruntled or disloyal employee who is out to do harm to the company. That person might steal the company's information by downloading it or take trade secrets on the way out the door.

Second are the innocent, loyal employees who aren't out to hurt the firm, but who make mistakes: losing smart phones or having them stolen; accessing firm information on an unsecure wireless network like at an airport; responding to a phishing attack; downloading malware; or not being careful with the information that they have on their phones by using bad passwords or leaving their devices out. Employers need to prepare for both types of risks.

CSLR: Between those two groups, inadvertent and purposeful, is there a way to quantitatively say which is causing more cybersecurity and data privacy issues for firms?

Weiss: Not with any kind of precision.

Kiesel: People are inadvertently foolish more frequently than they are maliciously bad actors. So the prevalence is toward the inadvertent, but the severity of breach skews the other way. If someone is malicious, then they are definitely targeting information that is sensitive and important like customer lists, proprietary software or trading algorithms.

Categorizing Information and Limiting Access

CSLR: For each of these two groups, what should firms do to prevent internal and external incidents?

Weiss: With a disgruntled employee or former employee, employers often have a pretty good idea when somebody poses a risk. The first thing to do is cut off access as soon as possible. Second, make it difficult to download information by, for example, disabling employees' ability to put flash drives into their computers.

Kiesel: With respect to the intentional thief, just about any significantly bad data release involves a large data download. A company's monitoring systems at the C-level, the Chief Information Security Officer level, need to determine if large downloads are being made and have a response. Companies should restrict access to flash drive downloads. Also, they should limit the ability people have to send large data chunks through email, or at least be notified of that and have the ability to respond to that quickly.

Other than that, a company can limit its password and authentication access levels to employees who need to know sensitive information. For example, if a company has proprietary software inside the organization that needs to be maintained by IT professionals, salespeople

don't need access to it. Similarly, salespeople may need access to the customer list, but the IT professionals don't need that. A company should come up with a way to categorize access to sensitive information based on who really needs that information.

Categorizing sensitive information is a defense against both internal and external threats. When dealing with an intentional thief, internally, if someone doesn't have access to information, he is not going to steal it when he walks out the door. And if his individual workstation password has been given to somebody outside the firm, that person can only access the information that the employee has the rights to. For the unintentional threat, it's all about training people to not respond to the Nigerian Prince (and more targeted) emails.

Precise Policies and Training

Weiss: It's important for employers to have policies and procedures and make sure that the employees within their firm know about them, understand them and are trained. As an example, it is important to train employees how to recognize a phishing email and how to interact with one when received. It's important to tell people what they can do and what they can't do or shouldn't do. That's where policies, procedures and training come into play.

There are also the technical measures, like the ones we just talked about, basically keeping people away from information—compartmentalizing information—so that if their computer is hacked and entered, the hacker cannot go get more information. For things like lost and stolen devices, some employers will impose a penalty if a device provided by the firm is lost.

Kiesel: For lost or stolen equipment, a company must be able to wipe company data from the equipment immediately. But, the employees need to report losses promptly.

Weiss: Right. There needs to be a corporate policy – if an employee loses a device or has a device stolen, then the employee has to report it immediately so that it can be wiped of the company's information. The same thing happens when employees leave – the company's information should be wiped from all devices.

Private Devices and Company Secrets

CSLR: How has the prevalence of people bringing their own devices (BYOD) as opposed to firm-issued equipment required firms to put new procedures in place?

Weiss: People bringing their own device that has company information on it is a different situation than when people are only using their company-owned devices for work. It raises questions about record keeping and privacy issues on both ends. As far as cybersecurity goes, the only real difference is that more often people are carrying these devices around in their pockets and are more likely to lose them or have them stolen than a laptop or a computer in their home.

Kiesel: What you have technologically is a schizophrenic device that has different personalities. It has a work personality and a home personality. When the employee leaves or employment is terminated, the company can't wipe the whole thing because it doesn't really have the right to unless the employee consented to having the whole thing wiped if they lost the device or employment was terminated. The company needs to have the technological ability to wipe just the corporate "sandbox" from the device.

Weiss: I think that the other issue that comes up more often with BYOD is people accessing corporate information on unsecure wireless networks. I think a lot of employers are looking to instruct their employees not to do that.

Kiesel: There are so many people who are traveling on the road, working at coffee shops, airports or hotels all the time.

Weiss: It's a challenge. There is a risk there that employers should be thinking of – airports, airplanes, trains, etc.

CSLR: What do you advise clients about best practices for archiving data?

Kiesel: In a perfect world, companies would delete data as quickly as possible to limit the information that can be stolen or released. But the practice, in at least the financial services area, which is now becoming a regulatory expectation, is that firms are keeping emails indefinitely.

Looking at the Sony breach, the news stories weren't about trade secret information, they were about embarrassing emails. When companies keep emails forever, it greatly expands the likelihood of disclosure of embarrassing emails. In the data archiving sense, a company can't limit its exposure to credit card data breaches or an Anthem or Target type of breach, but could limit its exposure to embarrassment.

Training Methods

CSLR: What are some of the ways you have seen firms successfully getting people engaged and effectively trained?

Weiss: They're doing the same sort of thing that happened many years ago with sexual harassment policies. They have had to change over to BYOD and had to reevaluate their policies and figure out how to layer that in a way that makes sense and that coordinates with other policies. As a part of that roll-out, some firms are doing live training, meaning bringing groups of people into a room and talking to them about the kinds of risks that are out there and what the rules are and answering questions.

For example, showing a hypothetical or an actual phishing email or spear phishing email and saying "these are the kind of things to look for" is an effective way of teaching, rather than sending emails around that people may never read. The live in-person training is something that is starting to happen more and more.

Kiesel: There are two specific kinds of spear-phishing threats that specific education and specific departments should address. For example, the accounts payable (or other department that controls wire and check payments out of the company) department of any business should be aware that it may get emails from people purporting to be C-level executives in the firm telling them to wire money to some vendor. "We've got to pay this guy this week – getting on a plane, see you next week." That sort of thing may be a fraudulent but convincing email. People need to be educated about that.

The other things that are kind of crafty that are happening recently are fake purchase orders under an existing vendor's account. For example, if a bank has an account with CEW where they routinely order servers, someone may obtain the bank's account information from CEW and order a bunch of equipment on the bank's CEW account, and the bill gets sent to the firm. Then the goods get shipped to who knows where and the bill goes to the purchasing department or procurement department of the bank. The bank's procurement department and accounts payable departments need to know serial-number-by-serial-number whether it actually ordered the particular devices that it is being billed for so that it can confirm that it actually got the goods and that it actually placed the order.

CSLR: That kind of examination of bills is a time and resource issue, correct?

Kiesel: That's exactly right. The second specific kind of threat would involve training a certain amount of people rather than the whole firm. The whole firm doesn't need to know what the procurement and accounts payable departments know about those particular threats.

CSLR: How do you train somebody to identify when something is a spear phishing email?

Kiesel: In the case of the one that purports to come from the boss to wire money to a vendor, a company has to have a policy in place saying that a single person is not the one that approves a payment, even if the CEO or CFO seems to be forwarding the payment. There have to be more steps in the process.

CSLR: Could phishing be addressed through required confirmations? What other requirements should be in place?

Kiesel: Yes, a confirmation and more steps. Having an informal process where the CEO can send an email to somebody in accounts payable and suddenly a check goes out ten minutes later – that's not the kind of sophisticated process that you have in a large organization, for that reason. Treasury frauds have gone on for a long time so companies have internal controls. A company needs sign-offs usually from three or four different people before a check is written to a vendor.

With that kind of policy, a spear phisher won't be able to comply with all of the signatures that are necessary to write a check. And in the case of the fake invoice issue, employees just need to be on the lookout to verify invoices. The thing about that type of attack is that the attacker's communications don't even go to the company, they go to the vendor. The company just gets the fake invoices but doesn't get the goods.

Weiss: For general training, the idea is to change the mindset of employees from every email being a legitimate email to recognizing the kinds of things that are happening out in the world. Employees should be taught that when they are in doubt, they should not click on a link, and if they think they have received something that might be an illegitimate email or it might be a phishing attack or have malware, they should send it to the [Chief Information Officer] to get it checked out. It's a question of changing the mindset from every email is legitimate to not every email is legitimate. Employees have to be aware that there are people out there doing social engineering electronically. It's not just a question of trying to get money from one place to another, it may also be trying to get information from employees about what their employer is doing.

Regulation and Enforcement

CSLR: What cybersecurity regulations come into play when protecting against insider cyber breaches?

Kiesel: Financial institutions, such as registered investor advisors or broker dealers, and SEC-regulated institutions have Regulation S-P; and other types of businesses, such as banks, insurance companies and retailers that take credit cards, each has a similar set of rules laid down by their federal functional regulators. Additionally, there are state personal data protection laws. All these rules boil down to having data security that is reasonably calculated to protect the sensitive data.

That's all that the rules will tell a company to do. Regulators cannot regulate with any specificity because it takes a long time to regulate and they don't want to say something technologically specific that becomes stale before the ink has dried on the regulations or do anything that hurts commerce. But the general rules have been there for a long time and they're not particularly helpful. They just say companies have to be reasonable.

The one exception is that the State of Massachusetts has said that personally identifiable non-public data regarding human beings has to be encrypted when it's in transit.

CSLR: Have you seen a change in the enforcement of those rules?

Kiesel: What we have seen is the federal regulators caring a lot more than they used to about cybersecurity. The SEC has been sending out requests to banks and financial institutions to respond to directed and specific questions about their data security.

Financial firms want to participate and be helpful in the process of informing the government about current data security practices. The firms are working together and coordinating with representatives from various industries to make sure that they are coordinated. The general mood of the industry seems to be that data security is not an area where individual companies seek to go it alone to obtain a competitive advantage, rather that companies should cooperate to develop fair standards that apply to all companies.