PUBLICATION

Cybersecurity in the Workplace: Obama's Proposals and More

Authors: Zachary B. Busey
January 20, 2015

In the past five years, employers both big and small have become accustomed to social media and increased technology in the workplace. Everyone and their parents are on Facebook, and one cannot go anywhere without being asked to "follow" something or someone on Twitter. Employers routinely deal with social media as part of the recruiting and hiring process as well as when it comes to disciplining and terminating employees. Employers have also adapted to increased technology in the workplace, such as smartphones, tablets and an array of other internet-connect devices. Cloud computing (computer systems that electronically store data and files on a centralized computer accessible by many devices) has become mainstream, and the "go paperless" chant is repeated often in workplaces of all sizes.

This technology boom in the workplace has had a number of consequences. Most notably, business and employers now store (and routinely analyze and rely on) large amounts of electronic data. This data can be anything from private e-mails and sales numbers to employee files and patient health records. The one common theme among all of this electronic data: it contains confidential and private information; whether it is about the company, its businesses or its employees, every company wants to keep its electronic data protected and secured.

Protecting electronic data can be a time consuming and expensive task, and depending on the nature of the data and the company, it can be very, very difficult. In 2014, data protection and cybersecurity dominated news headlines. eBay was hacked and the latest estimates show that 145 million users were affected. JPMorgan Chase sustained a cyberattack that reports claim accessed data related to 76 million households and seven million small businesses. Home Depot suffered a data breach that put a to-be-identified number of customers' credit card numbers at risk. Earlier this month, the federal government mandated a "social media password and account audit" after Twitter accounts for the Pentagon and CENTCOM were taken over by individuals sympathizing with terrorist groups in the Middle East. And, of course, Sony was hacked because of the release of the movie "The Interview." The Sony breach involved a large amount of data related to current and former employees, such as e-mails and personal information (dates of birth, addresses, etc.). The breach has already spawned a number of lawsuits, including a class action brought by current and former employees. Our firm recently published an update on that litigation, which can be found by clicking here.

Whether out of necessity or opportunity, President Obama has just recently announced a cybersecurity proposal. The purpose of the proposal is to enable "cybersecurity information sharing between private and government entities, as well as among private entities, to better protect information systems and more effectively respond to cybersecurity incidents." At the heart of the proposal is civil and criminal immunity for companies that make public (or share with the government) information about the attempt or existence of a data breach or attack. Among other things, the immunity encourages companies to make data breaches public so that potential victims, such as customers or current and former employees, can take appropriate steps to guard against the after-effects of a data breach, which most often include identity theft. Opponents of the proposal note that it does not do enough to encourage or require companies and employers to protect their electronically stored data and information.

Politics and viewpoints aside, there currently is not a uniform or required approach for protecting electronically stored data. But companies and employers of any nature or size can implement some best practices:

- **Control data access points.** Employers need to monitor what devices can access its electronic data. For example, if smart phones and devices are allowed to access company e-mail or data, the company needs to know what the device is and who owns it. This can be as simple as a form that an employee completes at the start of his or her employment.
- **Treat data access points like physical access points.** Employers have policies about who can access security doors and entrances to a building, as well as to specific areas of a building. Employers need to treat computer terminals, smart devices and computer systems the same way. There should be policies identifying who can have access to what systems and when they must be locked. For example, employers should require employees to lock their computers and smart devices at all times when not in use, even if that is only for a matter of minutes (like running to the restroom or answering the front door while at home).
- **Require *real* passwords.** "Password123" is not an appropriate password. Employers need to require that computers and smart devices have *real* passwords. For example, passwords must contain at least one number, one letter and one symbol. (While "Password123abc!" is better, it is still not recommended.) Employers need to require that passwords are changed routinely and not stored or written in places accessible to others. Employers also need to require that passwords are not shared with others inside or outside of the workplace, except for when required to address company-specific issues.
- **Don't go phishing & be mindful of attachments.** Employers need to put policies in place and educate their workforce on how to handle e-mail and telephone scams. They also need to be clear that attachments should not be opened if the sender of the attachment is not immediately recognizable and the attachment is expected. E-mail addresses can be copied (or spoofed). So simply recognizing the e-mail address is not always enough.
- **Involve persons with knowledge.** Whether it is an IT professional or partnering with an established company like Amazon, Google or Cisco (all of which offer cloud-based and data solutions), be sure to partner with an individual or an entity that knows this area well and has the ability to keep that knowledge current.

The steps needed to secure the modern electronic workplace will of course vary by employer and workforce. Employers, however, need to be proactive. The amount of technology in the workplace will only increase, as will the amount of data and information stored electronically. The best way to tackle new obstacles in the workplace is with appropriate written policies and effective training.