PUBLICATION

You Asked: Can My Employees Hack My Company?

Authors: Zachary B. Busey
January 18, 2017

Yes! Employees and other insiders – think Edward Snowden – can, and in fact, do play a role in most data breaches or cyber-security incidents. Companies must ensure their data protection policies include not only training but consequences for policy violations. And like with all workplace policies, data protection policies must be routinely and uniformly enforced.

Data breaches and other cyber-security incidents have dominated the headlines. Attention usually focuses on what was taken, and rightly so. Important for companies, however, is also who and how they did it. Whether through intentional or unintentional acts, employees are often involved. The Democratic National Committee hack, for example, started with a phishing email scam. DNC employees were sent a fraudulent email advising them to change their email passwords. Clicking the link within the email led the employees to a fabricated website monitored by the hackers. The fabricated website promoted the employees to enter their passwords, thereby revealing them. In similar fashion, every tax season we see stories of companies responding to fraudulent emails with tax and other payroll information. Phone scams prompt employees to provide electronic access by claiming to be "IT" or support from Apple or Microsoft. Downloads infect computers and devices with malware. Employees leave electronic access points unsecured, or they use easy-to-guess passwords. Even worse, employees simply download information onto a flash drive and walk out the front door.

What Can Companies Do?

Any employee-focused approach must start with written policies and training. Written policies, for example, should focus on Internet usage as well as Internet-connected devices. Such devices – like cell phones, tablets or other smart devices – can easily be used as a back door into a company's private network. For this reason, written policies should make clear that only approved Internet-connected devices can be used in the workplace, and even then, personal devices should not connect (wirelessly or otherwise) to the company's private network. A separate, secured network should be used. By doing so, the Internet-connected devices can access the Internet, but they cannot access shared drives, computers or printers on a company's private network. This same logic applies to the Internet-connected refrigerator in the break room, the smart TV in the waiting area or the wirelessly connected thermostats throughout the building. None of these devices should be connected (wirelessly or otherwise) to the company's private network. All devices should be on a separate, secured network.

As for devices connected to the private network, companies need to proceed with caution. Convenience should not trump security. Internet-connected printers, shared drives, displays and videoconferencing equipment provide tremendous convenience, but they also create yet another access point that must be secured. Think about a brick-and-mortar building: a brick-and-mortar building with five doors is easier to secure than a brick-and-mortar building with 15 doors. A private network is no different: fewer access points makes it easier to secure.

As for training, it should focus on educating employees. Training should teach employees how electronic information should be secured and accessed. The guiding approach is to treat access to electronic information like access to physical information. Access should be regulated, monitored and capable of being re-traced. Companies don't give employees blanket access to the vault or a file room containing sensitive documents.

Likewise, employees should not be given blanket access to electronically stored information of similar importance. Additionally, training should educate employees on how to identify – and avoid – email and Internet scams. Examples should be provided and employees should be required to report such scams. This allows a company to notify other employees when appropriate. All companies have workplace reporting requirements for harassment and discrimination. Employers should likewise require reporting of electronic scams or instances of improper access of electronic information.

Do Companies Have Legal Recourse Against Employees?

Likely yes, but a number of considerations go into whether a company should pursue legal action against a current or former employee. Nonetheless, a company has several legal options. The most powerful option is Section 1030 of the Computer Fraud and Abuse Act (CFAA), the federal anti-hacking statute. CFAA provides both criminal and civil liability for anyone who intentionally accesses a computer network or system without authorization. In the employment context, "authorization" is typically set by the company's written policies. Should an employee violate a written policy or go beyond his or her access, Section 1030 may apply. Civil actions under CFAA are limited to economic damages (i.e., actual, tangible damages tied directly to the unauthorized access). Examples of CFAA economic damages may include costs of conducting a damage assessment or repairing a damaged system or network.

Traditional common law causes of action may also be available, for example, trespass, conversion (i.e., damaging systems such that they can no longer be used) and interference with business relationships (i.e., taking a website offline so customers can't access it). To the extent an employee assists but does not directly execute a hack, the employee could also be held criminally responsible as an accomplice or liable in court as part of a civil conspiracy. The options for taking legal action against a current or former employee will vary, but the sooner we get involved, the more likely we can hold responsible those who harm your company.

If you have any questions or need any additional information about this topic, please contact Zachary B. Busey or your regular Baker Donelson attorney.