CORPORATE COUNSEL
An ALM Website
corpcounsel.com | February 21, 2018

Protecting Company Information From Disloyal Employees

Rasha Gerges Shields

In the era of telecommuting and daily cyberbreaches, companies face an ever-increasing challenge protecting their data from improper disclosures. Although many companies have invested in technology that protects them (to a certain extent) from outside intruders, these technological advancements do very little to stop the insider threat—disloyal and disgruntled employees.

Disloyal employees often have free reign over company servers, and they can cause just as much harm—if not more—than the average hacker. In recent years, more and more companies have turned to the criminal justice system for recourse against these disloyal employees.

Many lessons can be learned from these criminal prosecutions, both in terms of understanding how disloyal employees have gained unlawful access to company information, and what companies can do to prevent them from doing so in the future.

Keep Network Credentials Secure & Constantly Changing

One recent case has highlighted the need to ensure that employees are keeping their network credentials secure from prying eyes, and that they change their credentials frequently—particularly after the departure of a potentially problematic employee.

In mid-2017, a Tennessee man was sentenced to 18 months in prison for unlawfully accessing the computer networks of his former employer—for almost two years! On hundreds of occasions, the former employee accessed the email account of a former colleague, which gave him access to the engineering company's marketing plans, project proposals, company fee structures and the rotating account credentials for the company's internal document-sharing system. It is unclear how the former employee initially obtained the credentials of his former colleague—the former colleague could have shared them at some point, left them in plain sight, or the credentials could have been simple enough to guess (i.e., the most common password is "123456"). In any event, it is particularly troubling that the former employee was able to use this method of entry for nearly two years, before he was detected by the engineering firm. Even though the firm had instituted a mechanism to protect its sensitive documents—rotating account credentials for its internal document-sharing system—the former employee was able to bypass it completely by using his colleague's credentials.

Similarly, in *United States v. Nosal*, 844 F.3d 1024 (9th Cir. 2016), a former employee was able to access his former company's database using the

computer access credentials of his former executive assistant, who was still employed by the company. Even though the company had promptly revoked the credentials of the former employee and his accomplices upon their departure from the company, they "nonetheless accessed trade secrets in a proprietary database through the back door when the front door had been firmly closed."

Employees should be cautioned against sharing their credentials with anyone inside or outside the company. Understanding that we do not live in a perfect world though, companies should take additional precautions when employees are terminated to ensure that their colleagues change their network passwords immediately, and then periodically thereafter. And to prevent current employees from voluntarily providing their passwords to their former colleagues, they should be trained that such conduct is tantamount to aiding and abetting criminal conduct.

Emphasize the Importance of Unique Passwords and Strongly Consider Requiring Two-Factor Authentication

As with the examples discussed above, former employees may be able to gain access to company networks by using their colleagues' passwords—wittingly or unwittingly. To avoid being an unwitting entry point for disgruntled employees, current employees should be reminded to develop unique passwords that cannot be easily guessed by others that know them well.

This is particularly important advice for new employees coming from competitor firms. The much-publicized prosecution of the former director of baseball development for the St. Louis Cardinals illustrates this point. In that case, the former St. Louis Cardinals official was prosecuted because he unlawfully accessed the Houston Astros' confidential data, including scouting reports, statistics and contact information, and emails. How he gained access to this information is very interesting. In one instance, he obtained an Astros employee's password because that employee was previously employed by the Cardinals, and was required to turn over his Cardinals-owned laptop and password to the former Cardinals official. The former Cardinals official was able to access the now-Astros' employees email accounts and Astros' proprietary data by using a variation of the password the employee used with the Cardinals. Thus, companies should make sure that their new employees develop unique passwords that are not variations of any of the passwords they used at their former jobs.

Unfortunately, many employees may default to simplistic passwords or leave their complex passwords on post-it notes near their computers, despite watching hours of security training to the contrary. And, as the saying goes, you are only as strong as your weakest link. To add an additional layer of protection, companies should seriously consider requiring two-factor authentication. Two-factor authentication requires an employee to provide a secondary form of identification—such as a temporary password token or an identification badge chip—in addition to a password, to gain access to the company's networks. Requiring two-factor authentication would have likely thwarted the intrusions discussed above.

Immediately Disable Remote Access Capabilities

In addition to disabling network access for terminated employees, companies should also ensure that terminated employees can no longer remotely access the company's network.

Several prosecutions of former information technology professionals demonstrate the importance of promptly disabling remote access. In one case, an IT specialist and systems administrator of a large paper manufacturing company, who had been terminated and escorted from the paper mill, was able to remotely access the paper plant's computer system shortly after his termination. Once he accessed the company's computer system, he intentionally transmitted code and commands that resulted in over $1 million in damage to the company's networks and operations.

In another case, the former IT director for a nonprofit organ and donation center was terminated from employment, and all of her previous administrative rights and access to the company's computer network were revoked. Yet, on the day she was terminated and the next day, she was able to repeatedly access the company's computer network via a remote connection from her home, and she then intentionally deleted organ donation database records and other important files, including their backup files.

Similarly, over two months after a senior database administrator at an energy company was terminated, the employee was able to use his home computer to connect to his former

company's computer network and a database that contained information on approximately 150,000 energy customers. Once he gained access to this information, he caused damage to the company's computer network and the customer database, and he copied and saved to his home computer a database file containing personal information on the energy customers, including names, billing addresses, social security numbers, dates of birth and driver's license numbers.

Companies can limit their exposure to these destructive actions by former employees (and the corresponding civil liability) by immediately disabling all remote access capabilities and collecting all two-factor authentication cards/tokens once an employee is terminated. While the public records do not reveal exactly how these employees were able to remotely access their former companies' networks when their administrative rights had been revoked, it is possible that these employees had access to multiple credentials because of their positions within their IT departments. When information technology employees are terminated, special measures should be taken—such as consulting with outside professionals—because these employees pose additional threats to companies given their specialized knowledge and ability to exploit network vulnerabilities. At a minimum, companies should immediately change all passwords that were known to the terminated IT employee, such as administrative or group accounts.

Disable Access to Cloud-Based Accounts

Companies are increasingly relying on cloud-based applications to conduct their business. Employees routinely use Google Drive, Dropbox, Box and other similar accounts to easily share information with each other and third-party providers. Companies should vigilantly track the accounts that are being used by their employees so that they can quickly ensure that terminated employees can no longer access these accounts.

The importance of disabling access to cloud-based accounts was highlighted in a recent civil case that accused a former employee of unlawfully accessing a company's Google Drive account one year after he was terminated from his employment, as in *Estes Forwarding Worldwide v. Cuellar*, 16-CV-853-HEH (E.D. Va. Oct. 21, 2016). According to the complaint, the former employer (while working for a competitor) accessed the company's Google Drive account, created an archive of the account, downloaded trade secret information from the archive and deleted the entire company account. The parties eventually reached a settlement after the court rejected the former employee's argument that his conduct was not "unauthorized" because he helped create the account with Google, and Google granted him authorization to access the account.

The plaintiff in this case could have avoided theft of its trade secrets and the costs of initiating a federal lawsuit if it had quickly (or at least within one year) revoked the terminated employee's access to the company's Google Drive. Also, to easily defeat similar claims by former employees that their conduct was not "unauthorized," companies should include in their employment contracts and termination documents a restriction against accessing any company-related electronically stored information upon separation from employment.

Track and Immediately Collect all Digital Storage and Network-Related Devices

When an employee is terminated, companies should immediately collect all digital storage devices (such as laptops, external hard drives, thumb drives, DVDs, etc.), as well as all devices used to access the company networks, such as two-factor authentication tokens or cards. Companies will only be in a position to do this properly and promptly if they maintain accurate records of all such devices issued to employees.

Limit Employee Access to Sensitive Information

While it might not be possible to safeguard against all intrusions by disgruntled employees, one way to minimize improper disclosures is to limit employee access to proprietary company information as much as possible. Not all employees need access to all of the company's crown jewels. By providing access to the company's sensitive information on a need-to-know basis, companies can compartmentalize information and reduce the risk that one disloyal employee can access and disclose the bulk of its propriety information.

Monitor Network Access

In some of the examples discussed above, former employees had unlawful access to their former employer's networks for a significant period of time after their termination—not simply a matter of days after termination, but years. Companies should use available technologies to log, monitor, and

audit employee actions. While it is important to routinely monitor the company's network to identify suspicious and unusual activity, such monitoring is imperative when a problematic employee has been terminated—particularly if that terminated employee was a member of the company's IT group. Many of the former employees discussed above would not have been able to perpetuate their crimes (or continue to perpetuate their crimes for months or years) if their former employers had actively monitored their systems to detect these types of intrusions. Indeed, in a recent study of serious data and security breaches, approximately 70 percent of informational technology and security professionals at over 1,000 companies around the world reported that they believed their breach could have been prevented (or, at the very least, the loss could have been materially mitigated) if their companies had a more rigorous network monitoring policy or used a monitoring data loss prevention technology, which focuses on data flowing out of the system.

Train Employees About the Consequences of Unlawful Access

Employee training can play a crucial role in preventing employers from becoming disloyal in the first place. Like juvenile hackers who hack into systems for no other reason than to see if they can, disloyal employees often initiate their unlawful conduct out of mere curiosity. "I wonder if I can still get into the system … I wonder if my login credentials still work … I wonder if my boss changed his password …" And once they discover that they *can* access the company's network, they access it without ever asking themselves if they *should* access it.

As discussed above, companies can take many steps to ensure that former employees *cannot* access their systems. However, companies can also explain to employees why they *should not* even try to do so. One way companies can do this is by educating their employees about the consequences of non-compliance. Put bluntly, companies can put the fear of God—or at least the federal government—in their employees. The criminal penalties for unlawfully accessing a former employer's confidential information are serious, and have resulted in lengthy prison sentences. For example:

- Former employee sentenced to 18 months in prison for unlawfully accessing his former colleague's email account for nearly a two-year period;
- Former employee sentenced to 34 months in prison for remotely accessing his former company's computer network and transmitting malicious code that damaged the company's network and operations;
- Former employee sentenced to 24 months in prison for unlawfully accessing her former employer's computer network via a remote connection from her home and intentionally causing damage by deleting numerous database files and software applications, as well as their backups;
- Former employee sentenced to 12 months in prison for remotely accessing his former employer's computer network, damaging information on the network, and retaining personal information about the company's customers;
- Former employee sentenced to one year and one day in prison for unlawfully accessing his former company's proprietary database using the computer access credentials of his former executive assistant; and
- Former employee sentenced to 30 months in prison for sending malicious computer code to his former employer's computer servers and deleting intellectual property.

It is probably safe to say that none of these individuals ever imagined that what they were doing would cause them to become convicted felons and spend more than one year in prison. Yet, one of the primary purposes of sentencing is general deterrence. These lengthy sentences cannot act as a deterrent, if would-be disloyal employees are not made aware of them. Companies should work with their legal counsel to incorporate this important and powerful information into their employee trainings and departure procedures.

Rasha Gerges Shields *is a partner in Jones Day's Los Angeles office, where she focuses on white collar defense, corporate investigations, and complex civil litigation. Prior to joining Jones Day, Shields was a federal criminal prosecutor for over seven years, serving also as the deputy chief of the Organized Crime Drug Enforcement Task Force in the criminal division of the U.S. Attorney's Office for the Central District of California.*