PUBLICATION

Disgruntled Employees and Other Internal Threats to Your Cybersecurity

Authors: Samuel Lanier Felker
June 27, 2017

Baker Donelson's Data Protection, Privacy and Cybersecurity attorneys are pleased to continue a series of client alerts that address significant cyber-threats to your business and discuss ways you can protect your business with thoughtful and timely planning before an emergency arises. Proper planning includes recognition of the threats, assessment of the risk and then examination of the facts and tools at your disposal to mitigate the risks. The series will address your options, from adopting appropriate IT policies and procedures to acquiring contractual indemnity and insurance for specific loss risks. When there is a recommended technical solution available, we will consult with leading expert vendors and provide their input. We often hear that in today's tech environment, it's not a matter of whether you will be hacked or attacked, but when; therefore, we want to help you be well prepared for future challenges.

Our series will help you get ahead of the game. We offer guidance on shopping for cybersecurity insurance; protecting your business from DDoS attacks and ransomware; establishing a smart data management plan; and evaluating vendor relationships.

Disgruntled Employees and Other Internal Threats to Your Cyber Security

With the media focus on external attacks such as malicious email attachments and ransomware, internal threats remain one of the most common cybersecurity issues facing any organization. The impact of data breaches involving employees can be significant because disgruntled, internal bad actors many times have administrative privileges to systems and data that others cannot access.

According to a 2017 Verizon report, 25 percent of data breaches last year were carried out by insiders. *See* Verizon 2017 Data Breach Investigations Report, 10th Edition. Unfortunately, companies spend significantly more time and resources working to prevent external threats while ignoring the potential damage from insiders. Because internal threats can be difficult to detect, they can cause more lasting and significant harm.

Motivation for Attacks

One of the most common motivations for internal data breaches is simple – greed. In some cases, an employee wants to gain a competitive advantage for a competing business or new employer. In other cases, an employee gathers information to assist with other financial crimes such as identity theft or tax return fraud. Regardless of the reason, a disgruntled or financially motivated employee, especially one with information technology experience and access to sensitive company materials can cause significant disruption and damage.

In many cases, internal breaches often coincide with employees leaving the company. They use their remaining access to steal data, delete data, steal software and/or steal business intellectual property that they could use at their next job or to assist with other financial crimes. The malicious insider is the most difficult to catch because they know their way around the network and typically they attempt to hide their tracks.

Although malicious insiders are a significant threat, do not ignore the potential for a careless employee to accidently delete or modify critical information or unwittingly share sensitive information by not following established company protocols.

Best Practices for Detection and Prevention

Let's start at the beginning. To set a tone of compliance, require new employees to sign non-disclosure agreements preventing them from taking any intellectual property, employee or customer data when the employees leave the company. It is also important to remind them about their responsibility to keep the company data confidential.

Next, the company must be diligent in creating safeguards and training for its employees to prevent unintended disclosure of confidential information. Employee carelessness can be limited through appropriate training in the handling of material and the use of monitoring tools. Moreover, the severity of this type of data breach can be lessened if your company devices are properly encrypted.

A monitoring system is key to ensure compliance and to manage employee accounts that have access to sensitive data. An effective monitoring system will allow you to track, log and record account activity and create alerts to allow for a quick response when suspicious activity is detected. For example, multiple failed access attempts or bulk file copying may signal that a disgruntled or greedy employee is attempting to access the network in a malicious manner.

One of the most effective ways to safeguard your company's sensitive data is to limit each employee's access to only the information that they need to perform their job. The more unnecessary access available in your company's system, the more opportunity there is for security breaches. Always make sure that you limit administrative access to only employees that absolutely require it.

As discussed above, breaches often occur around the time that an employee leaves the company or immediately thereafter. Recognizing this trend, you should establish a system for terminating an employee's credentials immediately upon the employee's departure to prevent unauthorized access. This includes changing all of the associated passwords that the former employee used to access the system.

It is also a good practice to regularly review your employees' access rights and terminate any credentials and accounts that are no longer in use. Although many employees complain about the practice, requiring employees to change their passwords frequently can decrease the risk that fellow employees will be able to gain unauthorized access to data or information. This is true while that employee is still employed and especially true when that employee leaves because he or she may be able to guess a generic password that one their co-workers often uses. In addition, you should analyze and monitor the data that your employee was able to access at the time of their departure.

Key Takeaways:

- Require non-disclosure agreements;
- Train your employees;
- Protect devices and encrypt those that store your company's most sensitive data;
- Monitor user behavior and identify any unusual patterns;
- Manage access by regularly checking that user permissions are granted only for needed job responsibilities; and
- Disable unnecessary accounts promptly.

If you have any questions regarding this alert, please contact any member of the Firm's Data Protection, Privacy and Cybersecurity Group.