CONSTITUTION
RISK MANAGEMENT

Keeping Data Safe From Departing Employees

As you have likely heard, cyber-attacks and “hacking” are becoming an ever-increasing part of our world. If you are like many business owners, you have probably started to worry that an external hacker might target your business and your business’s data. But what most owners don’t realize is that their biggest threat may actually be much closer to home: their own former employees.

Unfortunately, employee turnover is a fact of life: the typical organization in the United States, for example, can expect that 22 percent of its employees will separate each year, although some companies experience much higher turnover. According to Osterman Research, one in five employees uploads sensitive and confidential data to an outside cloud, specifically for the purpose of sharing it with others. Further, of those departing employees, a survey by Biscom found that 87 percent of employees who leave a job take with them the data they created at that job, and 28 percent take data others created. Among those departing employee that took data with them, 88 percent of respondents took company strategy documents and/or presentations, 31 percent took customer contact lists, and 25 percent took intellectual property (“IP”).

SAFETY STARTS WITH PREPARATION

So, what can you do to ensure your data is safe after employees leave? First, you, like all business owners, must understand what is being protected before protecting it. As such, you must determine exactly what data you have and where it is stored. One way to do this is by creating a data map. To do so, in as much detail as possible, map out where your organization’s data is located, who has access to specific files, when each file was created and/or modified, and where each file is stored. Once you understand where your data is, and who has access to it, then, you can begin to proactively secure it by:

- Developing a comprehensive privacy and security policy.
- Distributing the policy to all of your employees and requiring each employee to sign a document stating that they have read and agree to the policy.
- Establishing employee access levels to sensitive and confidential data based on role, function, need to know, etc.
- Review your employment agreements (if any) for provisions about ownership of sensitive, confidential and trade-secret data or create policies and practices around employee’s use of and access to confidential data.

- Encrypting sensitive and confidential data in transit, at rest, and in use—regardless of its location—through an encryption platform that’s integrated with your existing systems and workflows.
- Require two-factor authentication for all employees who access sensitive data.
- Properly managing mobile devices and laptops, allowing yourself the ability to remotely wipe every mobile device that may contain company data
- Frequently reminding and training employees on data policies and procedures to reinforce that the data belongs to the company and of management’s intent and right to monitor employee activities.
- Regularly audit employees using any resource with access to corporate data.
- Updating and training managers and members of company leadership frequently so they are aware of the various data risks involved when employees leave.

These steps, if followed, can help to significantly mitigate the risk of employee data theft and misuse; however, you can’t prevent it altogether. So, you must take extra precautions once an employee is let go or gives his/her notice of resignation or retirement.

BEFORE THEY LEAVE

- On an employee’s last day, physically obtain custody of their company-supplied computer(s) and mobile device(s), as well as external hard drive(s), thumb drive(s) and backup disc(s). If the employee had access to company systems and networks (e.g., e-mail, project management, etc.), phone systems, or cloud based software, make sure to change their passwords and have the employee’s access and privileges removed. Also, collect company credit card(s), security access card(s), key(s) to the building, and parking tag(s) or decal(s).
- During the exit interview, ask the employee questions about their future plans for employment to help determine the potential risk of intellectual property (“IP”) theft. Remind the employee of the confidentiality agreement he/she signed upon being hired, give them a copy of the confidentiality agreement, and have him/her sign a document stating that he/she has returned all company data and have not retained a copy of anything.
- Before issuing the departed employee’s computer, tablet and/or phone to another employee, you can consider making a forensic copy of any of their devices. While this step may be expensive, it may become important later on if you discover (or fear) that the departed employee might have misappropriated your data. Companies that fail to

complete this step significantly hinder their ability to prosecute IP theft. Be sure to have licensed or certified personnel or vendors handle the process, called "imaging," which

goes beyond what an IT backup can do. It not only copies active files, but also deleted files and fragmented files, and it preserves unallocated space on the drive

- Once you have a forensic image of a device (if you choose to have one made), and if you suspect a departed employee stole company data, your team can use the forensic copy to look for unusual activity, such as:
  - File transfers involving a high volume of copied files or specific, confidential files moved to another device or cloud account
  - Proprietary files residing locally (like a downloaded customer list)
  - CAD files on a computer that doesn't have the CAD program
  - Unusual after-hours, weekend or holiday activity
  - Significant increase in outbound emails
  - Recently added or deleted software, such as a disk-wiping tool
  - Recently upgraded or downgraded software and/or applications

IN THE EVENT OF SUSPICION

If needed, a forensic team may be able to recover deleted files, expose hidden files and even recover temporary files, such as data that was copied to another storage device. Depending on your company's setup, it may also be smart to check the server backup tapes and remove them from rotation so they are not overwritten.

If an investigation shows suspicious activity, these actions will provide the information you need to decide how to proceed: be it either by confronting the former employee or escalating the matter with the use of attorneys, demand letters, and/or potentially litigation. In any case, when dealing with electronic data, time is of the essence.

When dealing with valuable, sensitive company data, it's important to be as comprehensive as possible, and to remember that not all threats are external. Your employees know where you store your files, what information is important, and they have the knowhow and ability to access them. While you don't want to ostracize employees, its always best to think ahead and try to avoid any potential troubles later on.