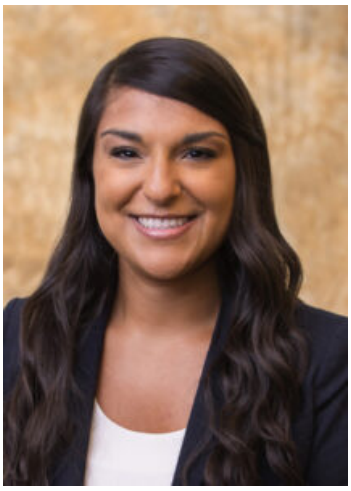
Guest Column: Keeping Adequate Distance Between Former Employees and Your Company's Data

By **Brooke Watson** - April 16, 2021



Brooke Watson

"Please stay 6 feet apart." Since last March, these signs have shown up everywhere to remind us to remain socially distant in order to slow the spread of COVID-19. However, the distance that must be maintained between a former employee and your business information is far greater than the minimum social distancing guidelines set forth by the Centers for Disease Control. In order to observe proper distancing between your company and an employee who is terminated or resigns, it is imperative to recognize the risks resulting from inadequate employee off-boarding and implement best practices to minimize such risks following the employee's resignation or termination.

The Risks

Throughout the course of employment, an employee learns information about your business operations, potential holes in your information technology systems, physical and electronic security measures, and your confidential information, among other things. This information gathered during employment creates significant risks when an employee leaves your company, whether through resignation or termination. The following are just some of the risks employers may face after an employee departs:

- Former employees may keep issued devices, including cell phones, computers and tablets. Such devices can allow access to on-site computers and other technology systems, giving past employees an opportunity to continue to monitor goings-on within your business.
- During the off-boarding process, former employees often fail to return all company property providing physical entry to the company's premises, including but not limited to keys, access cards, fobs, identification badges and passcodes.
- Human resources may fail to disable an employee's account, allowing the employee to retain access to the company's servers. Such access allows the opportunity for a prior employee to initiate a cyberattack and also, at the very least, permits continued access to the business's confidential and proprietary information.
- Particularly in the new "work-from-home" era, employees have increasingly used programs for remote access, including virtual workspaces and virtual private networks (VPNs). Without breaking the access point for former employees upon termination or resignation, these individuals have yet another means to access your network.
- Also, particularly relevant to the work-from-home environment, employers have granted employees access to third-party software, including video conferencing and teleconferencing systems. Without disabling such access, the former employee may be able to use previous access codes to continue to see and hear the company's information.
- Employers often fail to remind employees of previously signed confidentiality agreements and non-compete agreements when employment ends, which often leads to breaches of these covenants that can result in the divulgence of your company's valuable confidential and proprietary information.

Best Practices

It is important to note that the best way to ensure proper employee *off-boarding* is to ensure proper employee *on-boarding*. During on-boarding, you should track company property issued to the employee, including electronic devices, security cards and keys, and any other mechanism by which an employee may physically or remotely gain access to your premises or technology systems. On-boarding procedures should include confidentiality agreements and non-compete agreements for employees with access to confidential and proprietary information. After on-boarding, your company should continue to maintain complete records. During your company's off-boarding procedure, your company should:

- ***Always collect employer-issued devices.*** Such employer-issued devices may include cell phones, computers, tablets, and any other electronic devices that provide an access point to your company's systems. Your business should cross-reference the devices returned by the former employee with the list created during on-boarding and maintained throughout employment.
- ***Always require former employees to check-in keys, access cards, fobs, identification badges and passcodes.***Like employer-issued devices, it is imperative that such physical entry devices be checked against documentation created and updated by your company during the employee's employment.
- ***Always immediately disable the former employee's account on the server, including email accounts.***Passwords to the former employee's account should also be changed so that the former employee cannot gain unauthorized access to your network to allow the prior employee to remain privy to confidential information or facilitate a cyberattack. After a set period of time, the former employee's account should be deleted altogether.
- ***Always disable former employees' permission to use virtual workspaces and VPNs.*** Your business should maintain records of what employees have received virtual access to the network so they can be blocked when their employment terminates.
- ***Always disable the former employee's access to third-party programs through a corporate account.*** Such third-party programs may include video conferencing and teleconferencing platforms, as well as any other programming that allows external access to the company's communications. Access codes should be disabled. To ensure no external access by former employees on all third-party programs, employers should monitor the participants in meetings using these programs, as well as vary participant codes and passwords permitting users to sign into these meetings.
- ***Always conduct an exit interview.*** During the exit interview, remind the former employee of previously executed agreements requiring their cooperation and maintenance of confidential information, including confidentiality agreements and non-compete agreements, and provide the employee copies of these agreements. Pay attention to any red flags that might indicate a former employee is willing and/or capable of facilitating a cyberattack.

Unfortunately, there is no way to eliminate all threats to your company's cybersecurity. However, by engaging in an off-boarding process that eliminates a former employee's access to your physical location and information systems and requiring former employees to reaffirm covenants not to share information about your company (including data security processes), you can proactively limit unauthorized access that may compromise your company's system security and data privacy.

Brooke Watson is an associate in the Intellectual Property and Cybersecurity Group at Burr & Forman LLP in Birmingham, where she regularly assists clients with investigating and addressing data breaches and advises clients with regard to data privacy law compliance. The information contained in this article is only provided for informational purposes and should not be construed as legal advice.