Insights, News & Events

6 PROACTIVE TIPS TO ADDRESS EMPLOYEE DEFECTION CONCERNS BEFORE A CRISIS UNFOLDS

Insights
Jan 19, 2023

It is often said that the best defense is a good offense. That is certainly true if you are an employer conducting a risk assessment of potential employee defections that could expose your company to losses of valuable intellectual property, trade secrets, and goodwill. The happy news is that you can conduct a meaningful risk assessment and take steps to minimize the exposure and potential losses. Indeed, a robust risk assessment is key to addressing serious flight risks. This Insight offers six simple steps you should consider to protect your company's most valuable non-human assets.

1. Figure Out What Matters Most

The first step is ascertaining what your company values the most. What would hurt the most if it was stolen? Is it intellectual property such as patents and trademarks? Is it your key customer information, such as customer lists, important contacts, business volume, pricing information, and potential expansion of existing customer business? Is it your business processes? Is it your research and development? Is it your future business plans?

2. Deploy Basic Protections

Once you have identified the company's valuables, it is important to know where they are housed, how they are protected, and who has access. That will help you build the necessary protections. Questions you should ask to help construct proper proactive defenses include:

Related People

Barbara Jean D'Aquila
Partner
612.216.2743

Service Focus

AI, Data, and Analytics

Employee Defection and Trade Secrets

Resource Hubs

AI Governance Hub

- Do you have strong security and safety procedures? Traditional security tools are inadequate as they are typically not best designed for compliance.
- Do you require multiple layers of security clearance before someone can access sensitive information? Do you employ levels of security access keeping your extremely key information (*g.*, patents) accessible to only a trusted few employees?
- Have you internally classified what information you believe is a trade secret or highly sensitive information? Remember: If all your information is "highly sensitive" or "confidential," then none of it really is.
- Do your handbook and other written policies clearly identify what is proprietary and the employee's obligations?
- Do you use measures with your employees to protect your data, including warnings and certifications whereby the employees verify understanding confidentiality obligations and certify compliance when they sign on to your system?
- To the extent legal in your applicable jurisdiction, do you use legally enforceable confidentiality, non-disclosure, non-competition, and non-solicitation provisions with important key employees? Do you store these restrictive covenants in a safe place?
- Do your hiring agreements require the employee, when they depart your employment, to provide all personal devices on which company information was accessed or stored so that they can be examined upon departure? Do the agreements allow you to permanently delete company information before returning the personal devices?
- Do you have more sophisticated protections including restricted access available only from a secure computer? Do you employ anti-download protections, meaning certain information is only available on a secure computer and may not be copied, printed, or downloaded? Do you have pre-set flags that warn IT if excessive information is being downloaded? Does your IT group have the capability to block the use of external storage devices on your company laptops? And can IT block the use of applications like Dropbox in concerning circumstances?

3. Ascertain Where Your Biggest Exposure Exists

Not every potentially departing employee is of concern. Figuring out who poses the most significant risk is critical. Take the time to consider who has access to the keys of the kingdom and could do real damage if they so choose.

When trying to answer that question, a good place to start is examining the level of the employee, the type of work performed, and the access they have to sensitive and confidential information.

Interestingly, most companies worry about people like the IT administrators because of their broad access to information, but they are not known to be big risks. On the other hand, executives, top business managers, key salespeople, technical staff (like the IP specialists), engineers, and programmers often pose the bigger risks. With these employees, take the extra effort to watch for the warning signs listed below.

4. Recognize Factors that Increase the Ability to Steal Your Valuables

Some circumstances increase the risk of theft. Remote work has led many employees to remain off premises full time or led them to only return a few days a week. As a result, we have the growth of Shadow IT — the use of company hardware or software by an employee (or entire department) with the full knowledge of your IT department or security group. This new paradigm has resulted in the loss of an important ability to control your company's valuables.

Additionally, in this age of electronics, both remote and non-remote employees use non-company devices to do work. This includes personal computers, cell phones, printers, scanners, and cameras. Tracking someone's access to your valuable information is complicated when it is obtained from your system and downloaded to email, a flash drive, or some other storage device outside of your control.

5. Look for Suspicious Departure Signs

Often, when you look back after an employee has left and taken your company's valuables, you realize there were warning signs that should have alerted you to the risk. So, recognizing the signs before they result in theft becomes paramount. Typical signs include:

- **Disgruntled employees:** Are there signs of unhappiness? Has the employee expressed job dissatisfaction with pay, duties, workload, etc.? Have they been silent in or absent from key meetings without explanation? Are you hearing rumblings on social media?
- **Odd behavior:** Is there odd, unexplained behavior (*g.*, secret meetings among certain employees, strange requests for information being given to assistants, excessive use of the printer, unwarranted after-hours work, etc.)?
- **Past activities:** Did the employee try to bring their prior employer's information to your company? If done once, it can happen again.
- **Changed performance:** Has the employee's performance inexplicably declined? Do they seem less engaged? Are they hoarding information?
- **Unauthorized access or abuse of privileges:** Is the employee trying to access information when they are not authorized to do so? Even if authorized, are they abusing access privileges, accessing at odd times, or otherwise engaging in similar concerning behavior?
- **Significant absences, unusual vacations, numerous trips:** Has the employee been gone from work during long periods of time without an apparent reason? Are they suddenly using all remaining PTO, especially where your company has a use-it-or-lose-it policy? Have they taken a number of business trips to visit customers, especially in an out-of-the-ordinary sequence? Are they engaging in other unusual activities to shore up customer relations?
- **Lack of access to calendar or blocked personal appointments:** Has the employee curtailed access to their calendar, so that others who typically could know their schedule are not able to view it? Do they have a large number of blocked personal appointments? Does their calendar seem unusually busy or unusually open, especially without any apparent business reason for the change?
- **Lack of sharing:** Has the employee stopped sharing ideas or business plans? Are they being super secretive? This phenomenon has become such a problem that it actually has its own name — "knowledge hoarding."

- **Excessive downloading:** Does the employee seem to be downloading more information than usual? Are they keeping hard copies of important materials that would ordinarily be accessed online?
- **Mirror IT:** Does the employee have mirror IT (personal and professional accounts on the same platforms) that would enable them to move information from the professional account and store it on the personal account?
- **Potential of Infiltration Risks:** How your vulnerable is your system? Could a departing employee harm your information in any way (*g.*, wiping out key data)?

6. Consider Meaningful Options to Bolster Your Defenses

Best practices include tools, processes, and procedures that you can access and employ to help identify risks and protect against employee theft. But before using any of these options, make sure they are legal in your applicable jurisdiction.

- **Prevent downloading:** Set company devices and information to a read-only function. Do not enable an employee to download highly sensitive information by putting it on a USB-drive, dragging and storing it to the cloud, or printing it. Allow downloads only to company-encrypted devices and only in specific IT-authorized circumstances, and keep track of the company-encrypted devices.
- **Offer employee education and training:** Train your supervisors to understand what is valuable to the company and to be your eyes and ears in the workplace to unearth potential risks. Train all of your employees to understand what your company values, what you expect from them, and how you will engage if they fail to follow company protocol (*g.*, discipline, termination, lawsuits).
- **"If you see something, say something":** Teach people to speak up and tell you what they are seeing. This is particularly important for administrative employees, as they may be more reticent to identify issues. The administrative assistant who gets asked to download and print a large volume of information for their boss should speak up if the request is unusual.

- **Deploy forensic searches:** As soon as someone you have identified as a potential flight risk indicates a plan to leave or leaves, immediately deploy a forensic search of databases, emails, and other electronics to search for items that have been downloaded to various platforms. This includes USB drives or items forwarded to personal email accounts.

- **Consider User and Entity Behavior Analytics (UEBA):** UEBA is a solutions-based analytical software that uses machine learning and algorithms to detect and identify behavioral anomalies of not just users in a corporate network but also the machines in that network (*g.*, servers, routers, information endpoints). The technology works to uncover behavior that is not typical, unearthing irregularities in ordinary usage. IT can then analyze the abnormalities to determine if the behavior is suspicious, concerning, or explainable. Certain analytics software can also be set to employ automatic protections, like shutting down a user's access to the IT system or denying service to a particular machine or system.

- **Use other artificial intelligence (AI) tools:** Other AI can help alert your company to fraud, theft, and other suspicious behavior. Your company may develop its own AI designed to ferret out these employee risks. Indeed, many sophisticated companies have their own AI designed to work on their platforms and to uncover worrisome conduct, with their IT personnel addressing respective alerts.

- **Look into predictive analytics (PA):** PA can also be beneficial, as they help spot potential problems before they happen. Historical data is used to predict what may happen in the future. The analytical information may help you to identify flight risks, employee dissatisfaction, causes of employee turnover, and other important HR information. It may enable your company to strengthen its employee retention, thereby keeping the valuable employee in your workforce and preventing a departure to a competitor.

Note: Make sure any UEBA, AI, or PA you use does not violate applicable laws in your jurisdiction. Talk to your legal counsel to assess and help you establish best practices.

- **Conduct exit interviews:** When an employee leaves for any reason, you should always conduct an exit interview.

Use a standard checklist, so you don't miss anything and add additional items as appropriate for the situation. This is the perfect time to inquire about the reason for the departure and listen carefully to see if they respond or engage in behaviors that heighten your concerns. It is also the time to remind them about obligations to the company both under any legally enforceable agreement and under the law in general.

- **Recover what's yours:** Upon a departure, you not only want to recover your company equipment, but also, you want to recover company information from the departing employee wherever it exists. This includes hard copies of information and electronically stored information on their own equipment. Require the departing employee to sign a termination certificate of compliance, whereby they swear under oath that they have fully complied with your requirements and do not possess any company valuables, including confidential information.

- **Use warning letters:** A letter that warns a departing employee to cease and desist from unlawful conduct can be very powerful. You can even include a draft complaint and information describing any wrongful conduct of which you are aware. You can demand immediate compliance including return of the wrongfully taken proprietary information. The cease-and-desist letter can also be good evidence in a suit to stop the unlawful competition. The employee's failure to comply with the letter's requirements may be circumstantial evidence of intentional unlawful conduct. Additionally, a letter to a prospective or future employer warning of the departing employee's obligations to your company can enlist the help of this third party to ensure your confidential information is not used in the new employment. But assume anything you put in writing to a departing employee will be seen by a jury. Make sure you are assertive but do not come across unreasonably or like a bully.

Conclusion

The procedures you put in place today can help you prevent catastrophic employee defections tomorrow. Don't be caught off-guard. Act now. If you have questions or want to establish a proactive system to prevent problems, please contact the author of this Insight, your Fisher Phillips attorney, or any attorney in our Employee Defection and Trade Secrets Practice Group.

We will continue to monitor the latest developments related to trade secrets and confidential business information, so you should ensure you are subscribed to Fisher Phillips' Insight system to gather the most up-to-date information.