When Employees Leave With Your Secrets

January 28, 2017 by James Pooley

Recently I shared the podium with an FBI agent who was asked what frustrated him the most when trying to help businesses with trade secret theft. His answer was a surprise: they fire the guy too fast! He explained that when you discover someone might be mishandling information, your most important objective is to know what's going on, and you could learn a lot more by keeping them around and watching what they do.

That observation stayed with me as I pondered what many have accepted as standard operating procedure: when you are told that someone is leaving for the competition, walk him (or her) out the door immediately. The idea is to avoid having a provocateur in your midst, someone whose lost loyalty might rub off on others. But while that's understandable, it may not always be smart, especially in the age of electronic communications.

I have seen too many cases where the company has reflexively marched the employee out, only to learn later that they spent their time that day at home, wiping data off their laptop. Whether they think they're doing you a favor or covering their tracks is not the point; you may have lost the best proof of what they've been doing that puts your confidential information at risk.

When you first learn of a departure, you are engaged in triage with two parallel priorities: find out what's going on, and lock down the evidence. In most circumstances that may give you time for an initial meeting to get some details and perhaps try to turn the situation around. But you also have to be ready immediately to take actions that guarantee you get control over your data.

The initial investigation is low key, brief and uses internal resources. Talk to the supervisor, find out what the departing employee knows and the apparent level of risk presented by the departure. Identify relevant contracts, especially noncompete, nonsolicitation and invention assignments. Get a quick read on any unusual recent behavior, including

attempts to access information outside normal areas of responsibility, emailing documents to a personal website or uploading to a cloud storage site.

At this point you may be ready for an initial meeting to confront the employee with any disturbing facts or inferences and make a further assessment of the risk. Where are they planning to go and what will be their responsibilities? How long have they been looking at this? What are the attractions of this new opportunity, and what are the negatives with their current position? If you don't want to lose them, ask about their willingness to change their mind and stay. If not, make sure that no one else is involved in the move, and assess whether there is any project that would be seriously hurt if they left immediately. (If so, then you might want to arrange a carefully controlled and swift transition process.)

Now you need to find out where all of your data are located. Where are the company laptop and other mobile devices, including USB drives and security keys? Is anything on a home computer system, in personal email accounts or stored in a cloud account such as Dropbox? All of these assets, as well as physical files, need to be located and secure in company premises. Be sure to emphasize clearly – and confirm this in writing – that nothing is to be deleted, even personal files, until the exit interview that will be scheduled to debrief and to separate personal from company data.

If the employee has given notice of willingness to stay on for a period of time, you can take them up on that without necessarily having them be present in the facilities. Beyond tasking them with gathering and producing all company devices and data, and remaining available to answer questions, you may want to just send them home. Preserve evidence by duplicating (preferably through a forensic service) all of the drives and accounts to which the employee had access. And avoid any new damage by terminating the employee's access to electronic systems.

The initial phase is often completed in the same day that notice is received, and in the process you will have made a basic assessment of the significance of the departure and the level of risk it poses. If that assessment is moderate to serious, then the next step will often involve bringing in outside counsel to perform a deeper investigation. This carries several advantages. First, the entire process will be protected against disclosure by attorney communication and work product

privileges. Second, you will have the benefit of specialists who know what questions to ask and how far they can properly and usefully dig for the story. Third, you will get sober, independent advice that is not affected by the emotional reaction of some managers when troublesome departures happen on their watch.

Outside counsel can assist with tying down the forensic record and reviewing it for evidence of improper behavior. They will help you prepare for the exit interview, and in some circumstances they may participate in that process. More typically you will conduct the exit interview internally, with two primary goals: first, learn as much as you can about where the person is going and what they are going to do; and second, deliver a clear and firm message about the importance of respecting their legal obligations, and the consequences if they don't.

Here is a common exit interview checklist:

- Confirm that all company property and information has been returned.
- Ask about why they are leaving and how it might have been prevented. This might provide information about others who are at risk.
- Identify who they have talked to about their leaving; if the person is a manger, remind them of their duties relating to solicitation.
- Find out about how they got the new job and precisely what they will be doing.
- Ask them how they intend to ensure that they can perform their new functions while scrupulously protecting your confidential information.
- Provide copies of their relevant agreements and point out their continuing restrictions and responsibilities; ask if they have questions, and emphasize that these promises are extremely important and serious and that the company will enforce them if it believes there is a breach.
- Ask them to sign a "termination statement," for example:I certify that I do not have in my possession, nor have I failed to return, any files, data, notebooks, drawings, notes, reports, proposals, or other

documents or materials (or copies or extracts thereof) or devices, equipment, or other property belonging to XYZ Corporation.

I also certify that I have complied with and will continue to comply with all of the provisions of the Proprietary Information and Employee Inventions Agreement which I have previously signed, including my obligation to preserve as confidential all secret technical and business information pertaining to XYZ Corporation.

Following the exit interview, review the results with counsel and formulate a strategy. In most cases, the only followup will be a "warning letter" addressed either to the employee alone or also to the new employer, noting the company's concerns, citing any relevant restrictive agreements, and offering the assumption that everyone will comply with their obligations. A variation on this approach might include a request for a meeting to discuss assurances required to provide comfort that the employee will not be placed in a position that will imperil the integrity of your data.

Of course if you believe that there's evidence not just of risk but of actual misappropriation of your trade secrets, you need to take prompt action. You should have outside counsel involved immediately, to help you balance the need for a basic understanding of the facts with the imperative of prompt legal action. But where you can afford the time to prepare before you act, your decisions will be better informed and less likely to cause collateral damage.