IT and High Security Clearance Employees Termination

The security measures you would typically take with terminated employees to discourage malicious activity or retaliation are likely to be ineffective when terminating IT and high security clearance employees. There are several things to take into account when terminating an employee with access and control over information technology or other systems in your organization.

Challenges

One of the biggest challenges with these types of terminations is that IT or high security clearance employees often play a critical role in securing *other* employee terminations. They may lock down files, change passwords, delete accounts, and appropriately change email (for example, deleting an account, forwarding messages, and/or setting up an automatic e-mail response). They may also be responsible for the "provisioning" side of offboarding — collecting cell phones, laptops, tablets, etc. Accordingly, depending on the size and structure of your IT or security department, you may in fact be terminating someone who is generally integral to secure terminations.

On a related note, your IT or high security clearance employees are almost certainly in charge of critical passwords. There may be obvious ones, like the ones to administer your intranet, access to your company databases, and other security programs. But there may also be less obvious ones, such as the ones that would let them take control of your domain names and any social media presence you have established, such as company pages on Facebook and LinkedIn. Make sure to remember that there may not be anyone else in the company who could create a complete list of the passwords in your organization!

The most common technique in terminations is providing a terminated employee with a box for their belongings and then walking them to the door. As effective as this may be for most employees, it does not mitigate the risk when you are dealing with an information technology or high security clearance employee. After all, depending on their specific role, they may have multiple "backdoor" ways to access servers and systems either accessed remotely or at your facility. While many things are now stored in the cloud, most IT employees are expected to respond to issues during non-working hours and therefore will likely have access to close to everything they can access in the office from a remote location, regardless of storage location.

The Termination Process

Incorrectly terminating IT and high security clearance employees can have some serious repercussions. Here are two routes that will enable you to mitigate many of the risks.

The first route is what we'll call the "collaborative" path. This entails getting cooperation and buy-in from the employee you wish to terminate. There are several ways to help make this happen, depending on the specific circumstances:

- Offer severance and outplacement services. Supporting an employee while they look for their next job can make a big difference in how they respond to being let go.
- Create an offboarding plan. Consider involving the employee in training his or her replacement or having the employee create a document to transfer the knowledge about the current systems and processes, including all back door access points, passwords, and security codes.
- Offer incentives. For example, if immediate termination is called for, purchase a block of "consulting time" from the employee, to be used at your discretion. Also consider a deferred incentive — if six months passes, and the terminated employee has been supportive (i.e., not malicious or vindictive) they receive a lump sum. Either of these options should be in writing and reviewed by your legal counsel.
- Remind the employee how important a positive referral is to their future and how important it is to leave a positive impression with their co-workers and managers by handling the termination professionally. Also consider offering them the option of resignation so they do not have to explain an involuntary termination to future employers.

The second path may be necessary when cooperation is unlikely or undesirable. We'll call this the "adversarial" path. Depending on the size and structure of your current IT or high security staff, the adversarial path involves

rallying the troops and possibly bringing in external resources such as consultants or other security vendors. This team will need to prepare for the termination:

- Create a list of passwords, security codes, and back door access points the employee who will be terminated is likely to have access to. Create an action plan for changing or blocking all of them, with specific assignments with timeframes for the people on the team.
- If the employee being terminated is generally responsible for assisting with secure terminations, create a list of all the specific tasks for another employee to complete.
- Make a list of the hardware that must be retrieved from the employee: laptop, cell phone, tablets, etc.
- Most information technology and high security employees often have unlimited access to restricted areas in work facilities and may have keys to every lock on the premises. Create a plan to revoke keys or keycards or even rekey locks.
- If you have good reason to anticipate an overly aggressive response, consider talking to an attorney and/or local law enforcement in advance of the termination.
- Consider some of the incentives offered in the collaborative approach, such as providing outplacement and/or a lump sum deferred bonus if everything goes well after the termination.

As a last note, when terminating an IT or high security clearance employee, the matter of recruiting a replacement can also be difficult. Oftentimes, because of the circumstances, this is done on a “blind” or confidential basis. However, it can be difficult and sometimes impossible to successfully conduct a blind recruitment. If, as part of the job posting or screening process, you divulge the specific systems, programming language, hardware and software your company uses, chances are pretty good you will have inadvertently revealed your company’s identify. Many individuals working in the information technology and high security fields are well connected and talk freely. If your employee learns of his or her termination this way, it may create vindictive behavior, especially if they have an ax to grind.

The collaborative approach is the best route to go but if it becomes adversarial, you will be better prepared for how to address the issues when the termination is necessary.