3 Steps to Protect Your Data During The High Risk Exit Period

Veriato

www.veriato.com

Someday, sometime, an employee with access to sensitive data, intellectual property, or trade secrets is going to leave your company, which makes their departure risky to the organization. Sure, you've "trusted" them as part of their employment, but when the time comes to change jobs, you can't always be certain about the motive for the move. The assumption should always be they're leaving to go to a competitor; while you normally hope for the best, you should expect and plan for the worst.

Recently, companies like Lyft, Seagate, and Jawbone have sued, or are in the process of publically suing competitors over the theft of intellectual property or trade secrets by former employees. These cases bring to light the abundance of sensitive data that can be of use to a competitor, as well as the ease of ability in the actual data theft itself.

BUT, JUST BECAUSE IT'S IN THE NEWS, SHOULD YOU BE WORRIED?

Those are pretty big companies listed, and most of you aren't in such large, well-known enterprises. So does your organization need to be concerned when employees leave? In a word, yes. Remember, those companies are in the news because they are name brands; far less interest would be found in an article about how the local mom and pop operation next door experienced theft from a former employee – but it happens just the same.

In fact, it's not just one or two employees you need to be concerned about; multiple studies within the past few years have shown approximately half of employees, when leaving an organization voluntarily or involuntarily, say they take sensitive data with them[1],[2] . This number has risen more recently in 2016 to 59%[3] . And when it's IT employees being forced out, that number jumps to 90%[2].

59%
SENSITIVE DATA TAKEN BY EMPLOYEES IN 2016

It's important to note that those stats don't point to employees being willing to take sensitive data, but the actual taking of data. The reality is, it's already happening… more often and by more employees than you think.

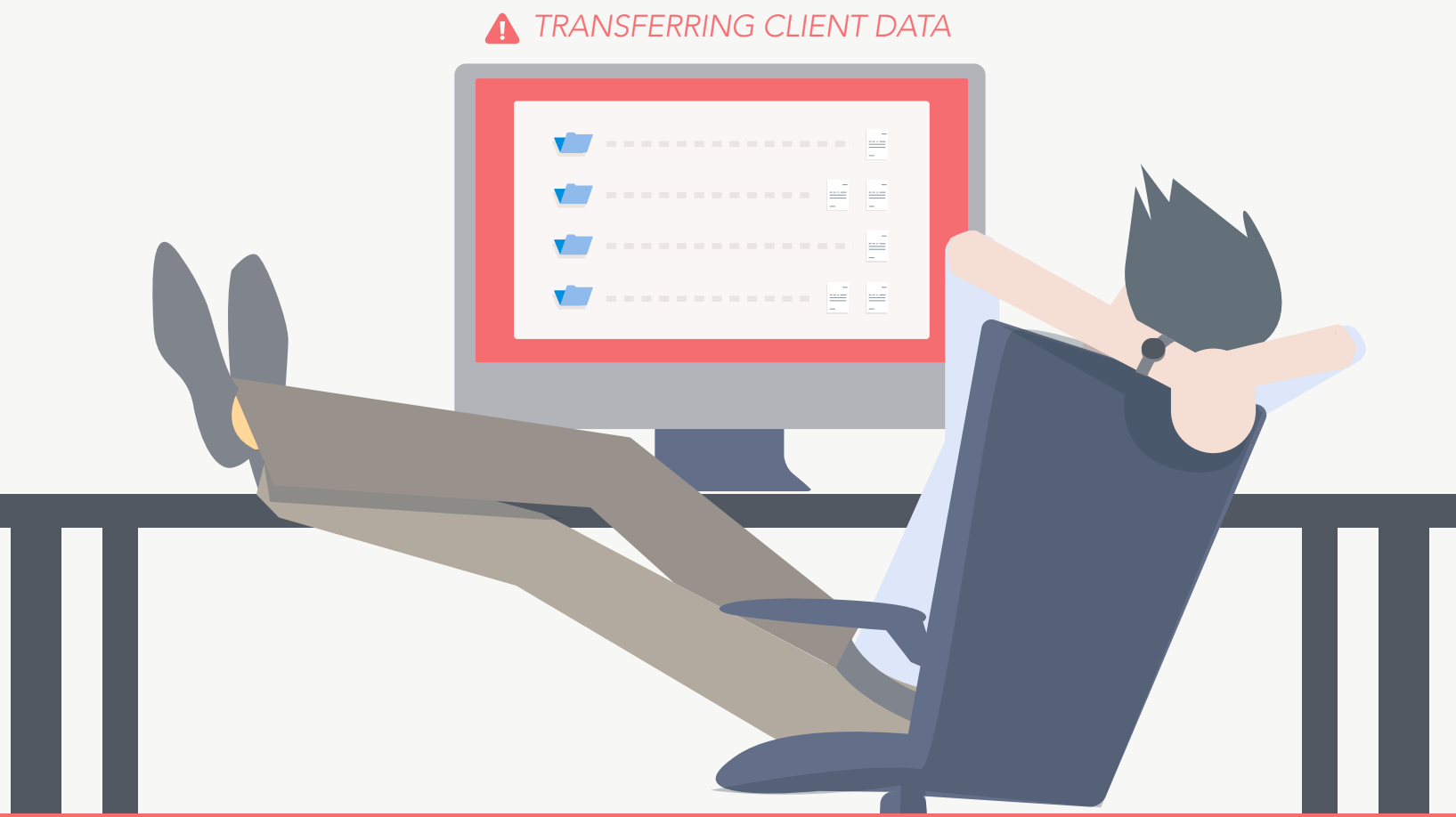
So, what should you be doing to avoid these high-risk exits?

There's an opportunity during this "high-risk exit period" to improve your organization's security. It's been demonstrated, by both statistically relevant data and real-world examples,

[1] Ponemon, What's Yours Is Mine: How Employees are Putting Your Intellectual Property at Risk (2013)

[2] Veriato, Insider Threat: Alive and Thriving (2013)

[3] Deloitte, Insider threats: What Every Government Agency Should Know and Do. (2016)



Who is a High-Risk Employee?

High-Risk Exits aren't limited to a particular type or level of employee. You probably think of the insider as someone lower in the organization. But it can be anyone from the lowest positions with access to confidential data, all the way to the top – as in the case of Lyft, where the COO's actions were in question. There are some specific areas within the organization where high-risk exits appear to be common. Members of the Sales and Product teams tend to be higher risk. The reason? They have a sense of ownership around the IP and data they've created. - they believe it's theirs too. So, they aren't necessarily out to get you; they just believe it equally belongs to them.

Organizations can improve their security stance during this period by taking a few steps that work to both protect against and prevent risky exit behavior.

step 1

Have a Signed CIPA in Place

The first step in protecting against data theft is to establish that it's unacceptable in the first place. As part of your organization's hiring process, a Confidentiality & intellectual Property Agreement (CIPA) should be provided to the candidate, with a requirement that it be signed prior to beginning their employment.

The CIPA should outline what categories of information constitute confidential data and intellectual property of the organization, describe the company's confidentiality requirements, and emphasize that the employee should err on the side of confidentiality when in doubt.

Because we're talking about a legally binding document here, the verbiage used can tend to be misunderstood by employees, who often have little experience with legal agreements. So, it's important to push for the CIPA to contain plain language, understood by the average employee. Should your legal team side with using more traditional legal language, ask for the CIPA to be presented in that format and then again in plain English, in order to avoid any doubt.

Remember, the purpose of your agreement is more just that of a signed legal document that affords you legal remedy if breached; you're putting a CIPA in front of a new employee in order to communicate to them what is and isn't confidential, and what is and isn't acceptable to do with it.

So, be certain to spell it out for them to give employees a better idea of how the organization see's the data the employee interacts with daily, rather than leaving it up to the employee to determine what does and doesn't belong to the organization. Take the following statement around trade secrets as example:

Trade secret information may include source code, CAD designs, research and development tests, business plans, customer, vendor, and supplier information, and other commercially sensitive information which gives the business a competitive advantage.

Being this specific in your CIPA will put the employee in the proper "confidential" mind frame, work to deter them from casually taking these kinds of documents, and arm the organization with a stronger legal stance should post-employment litigation become necessary.

This first step is a proactive measure. But, much of your risk occurs in the timeframe around the actual exit, making the remainder of the steps more protective in nature, in response to the specific exit scenario.

step 2

Build a Risk-Lowering Termination Procedure

Your HR department already has some formal or informal procedure in place for employees that provide notice, those that simply quit, and those that are being terminated. But, it's far more likely that process is built purely to satisfy HR requirements. Organizations need a termination procedure that reduces the risk of damage from departing employees.

Carnegie Mellon University's Software Engineering Institute (SEI), which includes their world-renown CERT division, released a Common Sense Guide to Mitigating Insider Threats.
It contains 19 practices to protect your organization from insider threats. What is interesting is practice #14: within a guide devoted to mitigating insider threats, you find a practice entitled Develop a Comprehensive Employee Termination Procedure.

One normally doesn't think of a departing employee as an insider threat. In reality, because their loyalties are shifting from the organization to themselves during the exit period, the employee is a greater risk to the organization – and should be treated as a potential insider threat. And the related practice found in the SEI guide underpins this belief.

Create the necessary processes and procedures that outline each aspect of the termination process. At a minimum, create a task checklist that outlines each termination task, who it is assigned to, who will verify the task was completed, and signoff on each task.

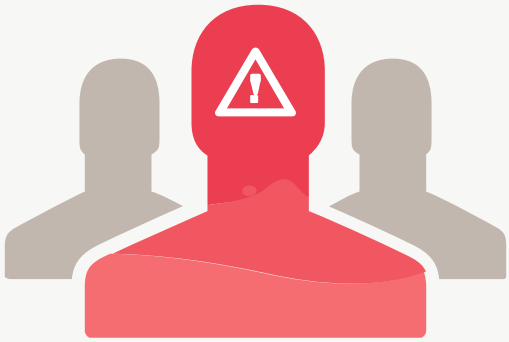
Tasks should include:

1) **Review CIPA** – As soon as notice is given or a termination decision is made, HR should sit with employee and review the employee's signed CIPA. The restrictions in the CIPA that still apply after employment should be pointed out, the employee should be reminded that all confidential data will need to be returned or destroyed, and the employee should be asked to be mindful of (as they complete their last days of employment) what information fits the description of confidential data.

2) **Notify IT** – HR must communicate to IT that an employee will be leaving as soon as a resignation is received or suspected, or as soon as a termination decision is made.

3) **Terminate Access** – When appropriate, IT should remove access to all data, applications, systems, and networks. This should include login credentials, cloud services, and VPN access. For privileged users, passwords for shared or service accounts should be changed.

4) **Obtain Signatures** – HR should require the departing employee to sign a Certificate of Return and Destruction. This should optimally be included in the original CIPA so the employee knows it's coming. At a minimum, it should be covered when reviewing the CIPA. In cases of termination, consider linking the signing of this document to providing severance.



Termination is a Team Effort

When dealing with any kind of insider threat, there is an extended team – beyond that of just IT – that is involved. HR, Legal, and management all become necessary parts of a threat investigation and response. The same stands true during the exit period.

Legal's role started well before the exit with the crafting of the CIPA. HR provides context around the departing employee – whether they are leaving on good terms or are mad at the company. Business line managers provide context around the work the employee was doing and what kinds of confidential data they may have worked with. And IT will ensure all access has been removed, and that no confidential data has been taken.

Proactively building the team and tying them to the termination tasks will lower exit risk and increase security against insider threats overall.

By implementing these tasks and involving the extended team, your termination period becomes a controlled effort of setting confidentiality expectations, securing resources, and lowering the risk of theft during this time.

Even with a solid termination process, you still aren't aware of whether data has or hasn't been taken, requiring an additional step.

step 3

Conduct an Activity Review

Given that such a material portion of employees admit to taking confidential data when leaving (and, more so, when terminated) – regardless of whether an employee is simply putting in their notice, or are being terminated for cause – it's critical that the organization have context around the actions of the employee. So, as part of the termination process, once IT has been notified of a departing employee, IT needs to review the activity of the employee in question, looking for insider-related actions.

By having this information, organizations can be aware if confidential data has been taken and, if so, eliminate further risk by immediately terminating the employee and their access. The SEI's Common Sense Guide puts an emphasis on this as part of the separation process:

> *Finally, organizations should conduct a review of the departing employee's online actions during the 30 days prior to termination, and the 30 days before and after the date of a notice of resignation, if that date is different from the termination date.*

In addition to SEI's guidelines, activity reviews should be encouraged in instances where an employee is believed to be leaving, as well as when insider behavior is suspected.

Specifically, actions involving any means by which to copy, move, or transfer company data (which includes the use of cloud-based storage, USB drives, internal and web-based email, and file transfer applications), as well as all methods of communication (including email, chat, instant message, and even social media) should be reviewed. Additionally, don't discount low-tech methods as well – screenshots and printing, while inefficient, are still effective ways to steal information. In each case, IT should begin with the activity type in question, and then begin to look for data types specified by line of business managers.

The most effective and efficient way to accomplish this is by utilizing an Employee Monitoring solution. These solutions record all user activity, alerting HR or IT to specific actions, where activity can be reviewed and even replayed back. These solutions spare IT the need to create a picture of the departing employee's activity by cobbling together pieces of a puzzle from numerous disparate sources of information.

Creating a Low-Risk Exit

No employee is a permanent fixture, and many have access to data that shouldn't otherwise be found outside the confines of the organization. Given the reality of employee views on taking data with them when leaving, it is evident organizations need to treat the high risk exit period as an insider threat.

The tasks performed during the exit period need to shift from just addressing the necessary HR paperwork, to ensuring the security of your organization's most valued asset – it's confidential data and intellectual property. By putting in place a CIPA, a security-focused termination process, and a review of employee activity, organizations can lower the risk of data leaving the organization – even in the event of an employee exit.

ABOUT THE AUTHOR

David Green is Chief Security Officer for Veriato.

He is responsible for digital security and physical security, data loss prevention, and incident response as well as business continuity planning.

Prior to joining Veriato, he served as CIO for XL Vision. Prior adventures include aircraft design and prototype development, and marine electrical equipment manufacture for ships and submarines.

Veriato
www.veriato.com

Veriato USA
4440 PGA Boulevard , Suite 500
Palm Beach Gardens, FL 33410

Veriato EMEA
3rd Floor, Crossweys House
28-30 High Street
Guildford, Surrey
GU1 3EL United Kingdom

https://plus.google.com/+Spectorsoft
https://www.linkedin.com/company/veriato
https://twitter.com/veriato
https://www.youtube.com/SpectorSoft
https://www.facebook.com/VeriatoInc/