Keep Hires From Starting Fires

Executive Summary

John Adams said, "Facts are stubborn things." He was right.

The fact that trusted employees or contractors often create problems for the organizations they work for, is unfortunate, but remains a fact. But why?

Companies take steps to protect themselves against the risks that are inherent when bringing in new people. Interviews, background checks, reference checks, etc., are all designed to mitigate risk. Unfortunately, it's never enough.

This White Paper will present some common sense suggestions for improving the "beginning of the life cycle" risk mitigation process. In other words, ways to add a bit more intelligence beginning with the screening and hiring process. Then, we'll look at how to tie the efforts made at the beginning of the life cycle to the rest of the employee life cycle, using a combination of process and tools to significantly improve security, and reduce the chances of an insider incident.

Insider Risk Mitigation starts before a potential hire becomes an actual employee

All organizations engage in risk management when they screen potential new hires. Here's a look at a very common workflow for identifying and selecting a candidate for a given position

1. Job Requirements are drafted (or reused / updated in the case of a backfill)
2. HR is given a Job Description to use in recruiting
3. An existing team member or team members are designated to work with HR on filling the role
4. Applications are evaluated in light of the Job Requirements
5. A number of applicants are interviewed – likely starting with phone screens and then moving on to onsite interviews
6. A candidate is selected
7. An offer is made
8. A background screening process is completed
9. Should the offer be accepted and the background screen conclude satisfactorily, the candidate is hired

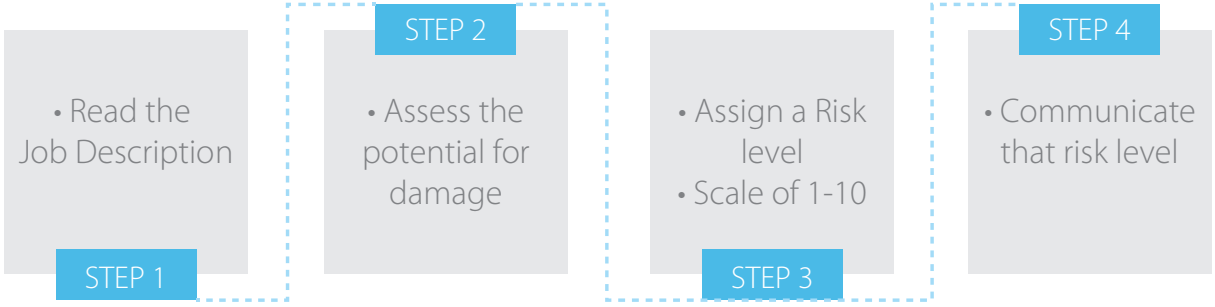
Looking a bit closer at this process, we can see steps being taken to insure the company is protected. The interviews and background screens are the first line in a company's defense against insider threat. In this process, the organization typically takes the risk associated with the hire into account. For example, the interview process and background screens for a potential Controller, CxO, or senior IT staff is (hopefully) more rigorous than that conducted for an entry level position in Sales or Marketing. This makes sense, because the risk associated with the position is higher in two ways.

First, the cost of getting the hire "wrong" – meaning a simple case of hiring someone that doesn't work out is greater given the nature of the position and the compensation associated with it.

Second, and of more interest to those of us focused on security, is the damage that can be done by a person in the position. Two words that should come to mind when looking at the Controller, CxO, or senior IT positions are "privilege" and "access." The positions require elevated privileges, and access to key systems and information. These job titles were selected because the fact that they will require privilege and access is clear. The greater the privileges and access, the greater the risk. (Highlight)

Key questions to answer in the pre-hire stage of the employee life cycle

Are the privileges and access required by every position you are hiring for clearly documented? Readily understood? Does everyone involved in the screening process understand the risk associated with the position you are hiring for? Can you answer the above questions in the affirmative, with a high degree of confidence?



Once you have your job requirements and job description drafted, step back and think about the positional risk. Document what level of privilege and access each position requires, and think about worst-case scenarios. What is the worst thing(s) someone in this could do in relation to company confidential information, key systems, finances, or reputation? Translate that information into a "positional risk score." A simple 1-10 scale can suffice. Then, make sure that information is shared out with HR, the department manager, Legal, and IT. Having a common designation for positional risk makes communication feasible in the later stages of the employee life cycle. This communication could be the difference between security and insider incident.

Onboarding: The next phase in containing insider risk

Now that we have our new hire coming onboard, and we've taken the simple steps necessary to quantify the positional risk associated with the role, how do we translate this knowledge into action that helps protect the company?

Remember, we are talking about positional risk. We know that different positions have varying levels of inherent risk. We also know that elevated privileges and accesses present challenges to security. The person in the position is inside the perimeter defense. They have been given keys to some (and sometimes all) of your critical data and systems. We can't lock them out and expect them to do their jobs.

Key Questions to answer in the onboarding stage of the employee life cycle

How does your organization insure that access is being used properly? Does your organization use a probationary period with new hires (typically 90 days)? How does your organization assess the new hire at the end of the probationary period?

Recommendation #2

Translate the assigned risk levels into appropriate levels of scrutiny.

There's an old management adage that says "you get what you inspect, not what you expect." The positional risk inherent in some positions in your organization (those with higher assigned risk levels) means that inadvertent or malicious actions taken by the person in that position expose you to significant potential problems, you must make sure that the access you are granting is being used appropriately.

> "While this paper is focused on insider risk and threat, and steps you can take to mitigate them, there are numerous other benefits to monitoring user activity and behavior. One of these benefits occurs during employee onboarding. Collecting data on the activity of new employees provides managers and HR with an invaluable resource for evaluating the employee during the initial probationary period. Hiring mistakes happen; catching them early and rectifying them promptly reduces the costs, and the pain, associated with a wrong fit.

To do so, you need a method for monitoring user activities and behaviors. High-risk level positions should be actively monitored. This means collecting and retaining data on user activities and behaviors, receiving and reviewing reports that summarize that data, and, in the case of the highest risk positions (highly privileged users) spot-checking their activity from time to time.

Lower risk positions are not without risk. They may be without known risk. Did you know that 77% of employee fraud occurs in one of the following 6 departments: Accounting, Operations, Sales, Senior Management, Customer Service, and Purchasing. Not many companies assign high-risk ratings to Customer Service. But there is still risk.

These lower risk positions should be passively monitored. This means collecting data on user activities and behaviors, scanning it for signs of insider risk / threat, and alerting when those signs are detected.

Assessing positional risk, assigning risk levels, and aligning appropriate levels of scrutiny are 3 keys steps to improving security against insider threat that should be taken at the beginning of the employee life cycle.

We've talked about the beginning of the employee life cycle. For simplicity, we break the life cycle into 3 main parts – beginning, middle, and end. Now let's look at what is typically the longest portion of the life cycle – the middle.

Continuous Risk Requires Continuous Mitigation

To this point, we have been focused on positional risk. Because people occupy positions, we need to look at "people risk" and how that has the potential to alter your risk levels.

Facts are still stubborn things. And the fact is, Insider Risk does turn into Insider Threat. Not always and not everywhere, but enough that steps have to be taken to protect your organization. "They didn't get through the perimeter" is no consolation when an organization suffers financial or reputational losses stemming from an insider driven incident.

One of the leading causes of Insider Threat is the disgruntled employee. Employees become disgruntled for many reasons. This can range from a perception that they are being treated unfairly by their boss, through poor annual reviews, smaller than expected pay increases, failure to secure a promotion, and being put on a performance plan. A co-worker being let go, or rumors circulating about potential staffing changes, are also known triggers of employee disillusionment.

Key Questions to answer about your insider risk level

Do you alter your internal security during periods of elevated risk? Are you aware of all of the factors that may contribute to elevated risk?

While surveys have shown that as many as 50% of organizations are taking steps to increase internal security at times, that leaves fully ½ of organizations without a plan or process to effectively deal with elevated insider risk. And very few organizations have the information sharing in place to insure that the people directly charged with keeping the organization secure have the knowledge they need to do their jobs.

Recommendation #3

Enhance monitoring of employees when they are involved in personnel issues, during times of corporate uncertainty, and when "outside factors" exist that are known to drive insider threat behaviors. Put your risk level rating system to work.

Earlier in the paper we discussed how taking the time to install a risk level rating system would pay dividends down the road. This is one of those times. Human Resources, or business line managers, are privy to information that Information Security folks do not have access to. For example, when 1 employee is promoted, how many people know who else from within the company applied for the promotion and are now potentially disgruntled because they did not get it? How does Information Security know that a sales rep is on performance plan? They don't, and shouldn't know. They should, however, know that there is elevated risk associated with the person in a position. This information is easily transmitted from HR or the business manager to Information Security by using the risk level system.

"Please elevate the risk level associated with "Joe" from "4" to "8."

Because Information Security knows that they monitor risk level "8" differently, and likely more actively, than risk level "4," they know exactly what to do. After a period, when it's clear that elevated risk is not translating into threat, a simple "revert to '4'" is all that's needed.

This system allows for Human Resources to elevate the risk level when outside factors exist as well. It's been proven that personal financial difficulties are a precursor to employee fraud and theft. HR sees things like hardship 401k withdrawals, mandatory payroll deductions caused by unpaid debts, etc. Giving HR a way to communicate elevated risk, without breaching employee privacy, is a powerful tool in improving security against insider threats.

There are certainly factors beyond employee disgruntlement that contribute to insider threat behaviors. By employing a risk rating, and aligning monitoring strategies to that risk rating, you are putting in place a combination of tools and process that improve the ability to deal with both positional risk and people risk.

While the middle segment of the employee life cycle is typically the longest, it is not the highest risk.

The High Risk Exit Period

When an insider decides to leave an organization, or believes that they are going to be made to leave the organization – that's when risk is the highest.

[1]1 out of 2 employees surveyed stated they think it is OK to take corporate data with them when they leave. [2] 18% of employees admitted to stealing corporate intelligence. If 18% admit it …

IT sabotage by outgoing administrators is a recurring theme in the news.

Bad things happen when people leave. Especially if they are being forced out, or suspect they may be forced out. Here again, the risk level system and aligned monitoring strategy pay dividends.

Key Questions to answer during the High Risk Exit Period

Are you reviewing the activities of existing employees for IP Theft or other insider threats? Is your Information Security team in the loop about impending departures early enough?

If your answer to either of these questions is "No" or "I don't know," you may have a problem. IP Theft is one of the most damaging. Most costly forms of Insider Threat, and it occurs most frequently during the high risk exit period.

Recommendation #4

Review the online and communications activity and behaviors of all departing employees for the 30-day period leading up to their notice of resignation, or their date of termination.

There is simply too much at stake not to take this simple step. While the effort may be daunting if you have not prepared for it, organizations that employ tools that collect user activity and behavior data are well positioned to handle this critical security task. Whether the employee was being actively monitored or passively monitored, a record of all of their activity exists for quick review.

[1] What's Yours Is Mine: How Employees are Putting Your Intellectual Property at Risk
[2] http://www.lawfirmnewswire.com/2013/04/employee-theft-no-longer-an-if-now-it-is-how-much/

Recommendation #5

Inform Information Security as soon as you become aware of a resignation, or prior to a termination decision being acted on.

Tools and processes are maximally effective when the experts who use them have adequate time to react. Often, Information Security is told an employee is leaving on, or close to, the date of departure. By the time they are able to complete their security review, the insider may be gone and the damage may be done. Here again, the risk rating system comes in to play. We've used a simple 1-10 scale to represent a risk rating system in this paper, with 10 being the highest risk designation. When a departure is known or suspected, HR or the business manager should immediately communicate to Information Security that the risk level is "10" for that employee. That should trigger an immediate review of the past 30-days of activity. While this is occurring, HR can review confidentiality agreements and IP agreements with the departing employee, reminding them of their obligations and asking them to confirm that they have destroyed any corporate data they may have taken off the network. This discussion can have a powerful deterrent effect, and when conducted in conjunction with a review of departing user activity, goes along way towards mitigating a serious insider threat.

Watch the
"Mitigating Employee Risk"
Webinar

VIEW NOW

Go to www.veriato.com for a Free Trial or email us at: sales@veriato.com

Corporate Offices

Veriato, Inc.
4440 PGA Boulevard, Suite 500,
Palm Beach Gardens, FL 33410
1.888.598.2788
1.772.770.5670

International

United Kingdom
C2, Dukes Street
Woking
Surrey, GU21 5BH
+44 1483 397744