Veriato

5 Steps

to Quantifying Insider Risk

A practical guide to assessing, detecting and preventing insider threats

www.veriato.com

QUANTIFYING YOUR INSIDER RISK

Risk is one of those subjective concepts that usually fall into vague categories like "low" and "high" – which has very little meaning on its own, and only has value when you tie those categories to actions (which we will cover later in this guide). To properly quantify the insider risk within your organization, we want to initially walk you through how to begin thinking about insider risk, as it is more a fluid and shifting concept than, say, the static risk assessment associated with whether your systems and applications are completely up to date on their patches.

WHAT DOES IT MEAN TO "QUANTIFY YOUR INSIDER RISK"?

It goes beyond the simple establishing "are we at risk" (like assigning your company a DEFCON value), as that has no specific actionable outcome when it comes to individual employees. Quantifying your insider risk is about understanding the positional risk each role within the organization inherently has, based on criteria such as their access to data and systems, and then making that understanding actionable by putting controls in place to detect, and ultimately prevent, insider risk.

The quantifying of insider risk is also not a one-time exercise. It's actually about knowing on an on-going basis where your insider risk is before it impacts the organization.

Before you begin, it's critical to understand the four fundamental "laws" of the dynamic nature of insider risk.

INSIDER RISK LAW #1

Every position has an inherent risk level

Risk has a lot to do with the data a given position in the organization has access to. This makes employees like privileged IT an obvious candidate. While they, too, need to be monitored, everyday users – such as a sales person with access to customer records, or a scientist at a drug company developing a new drug – can also pose a threat to the organization.

INSIDER RISK LAW #2

Every employee represents a potential risk

If you take the position every employee & contractor carries some level of risk, regardless of how long they've worked at the organization, you set yourself up for success. New employees, who have therefore not yet built up any loyalty to the organization as a whole, are always a possible risk. Those that have had been employed for some period of time can become disgruntled due to changes in the organization that impact them personally. Tenured employees are also susceptible to thoughts of having put many years into the organization's success, generating a feeling of being entitled to more than just their current compensation. This does not mean you cannot or should not trust your people. It does mean that you should confirm your trust through verification.

INSIDER RISK LAW #3

Insider risk is constantly shifting

Unlike other forms of risk that are static and can simply be addressed and eliminated by making specific changes, insider risk uniquely poses itself as a shifting threat – where the risk can fluctuate, causing the organization's focus to move from one person of interest (POI) to another over time. Previously loyal employees and contractors can go through changes in their personal life (e.g. taking on additional debt, addictions, etc.), or changes in their career (e.g. being passed over for a promotion) that can shift their loyalties from the organization to themselves.

INSIDER RISK LAW #4

Insider threat actions are almost always Preceded by leading indicators

Insiders are people. So it should come as no surprise that threat actions don't occur in a vacuum, but nearly always follow other events or actions. In 92% of insider threat cases, the threat actions are preceded by a negative work event (such as being passed up for a promotion)[1]. These events leave digital exhaust that can be used to detect, but they also show up in ways that can simply be observed – if you are looking for them.

As you can see, insider risk begins the day a position is filled with, well, an insider. It continues to exist all the way through (and sometimes beyond) their last day of employment or engagement. This can make the task of effectively dealing with insider risk daunting. But if you invest some time in the groundwork of quantifying who poses a risk and to what degree, you focus efforts on those truly posing a active risk, and attain the goal of proactively identifying threat indicators or behavior – protecting both the organization and its employees.

[1] Deloitte, Insider threats: What every government agency should know and do (2016)

So, what steps do you need to take to quantify and address insider risk?

To quantify your insider risk, you need to address the following steps that will be covered throughout the remainder of this guide:

1) **Involve the right people within the organization** – How you define and address insider risk is something that will involve a number of positions within the organization.

2) **Adjust your Hiring Process to Address Insider Risk** – Preventing insider risk starts with specific actions taken on an employee's very first day.

3) **Define Risk Levels** – Defining the risk each position possesses will serve as the basis for establishing levels of controls necessary every day through the end of employment.

4) **Align Risk Levels with Everyday Controls** – Based on positional risk scores, you will determine which controls should be in place to detect and identify insider risk.

5) **Address Risk During your Termination Process** – Whether an employee is quitting or is being terminated, specific steps need to be taken to ensure no data is inappropriately taken.

step 1

Involve the Right People

Risk around company data normally falls to someone within IT, the security team, or to the CISO, as these individuals will play a crucial role in quantifying and addressing insider risk. But, to properly assess the state of insider risk, as well as ensure suitable controls are responsively in place, you will need the perspective and assistance of a number of positions within your organization.

EXECUTIVE LEADERSHIP

This should include the CEO or equivalent, who needs to understand both the risk that exists, as well as the specific actions that will be taken as a result of that risk. This is becoming a board level issue at many organizations – that's how seriously cyber-security in general and the threat posed by insiders specifically should be taken. If your senior management is not engaging on this subject, view it as an opportunity for you to demonstrate real leadership within the organization. It will increase your value to the company while you deliver on the promise of greater security.

HUMAN RESOURCES

Someone at the head of your HR efforts will help balance the needs of the company to protect its' assets and the concerns of the individual employee as controls are put in place. Additionally, involving HR unlocks a source of intel about your employees that you already have but aren't using to identify risk. HR knows about changes in employee productivity, personal issues, etc. – all that can provide context around where your focus should be. There are ways to do this without compromising employee privacy.

LEGAL

Your general counsel, or external legal resource will be utilized to draw up specific documents as part of this process, helping to ensure the company takes the necessary compliance steps as controls are put in place, and taking point in presenting evidence should legal action need to be taken.

There are obviously more roles within the organization that will become involved should you elect to implement technological solutions designed to help detect, and reduce the resources needed to investigate, insider threats. These resources will depend on your organizational structure, and may report up to the CISO in an enterprise, or be part of IT in smaller and mid-sized organizations.

Once you've identified those individuals that need to be involved, the first step is to put some level of insider control in place on an employee's first day of employment.

step 2

Adjust your Hiring Process to Address Insider Risk

Insider risk begins the moment you grant access.

What's required on an employee's first day is to present them with a Confidentiality & intellectual Property Agreement (CIPA). This agreement is designed to put a number of insider risk controls in place:

1) **Define Confidential Information** – The new employee should understand what categories of information constitute confidential data and the organization's intellectual property. By communicating what the organization considers confidential information, the new employee begins their employment aware of the organization's desire to protect its' confidential information. This should be very specific, relying on IT and Security staff to define what kinds of information are of a sensitive nature.

2) **Convey Confidentiality Requirements** – An awareness of what actions are and are not appropriate when it comes to the handling of confidential information needs to be detailed. By describing how the organization wants an employee to conduct themselves when working with and when coming in contact with confidential information further conveys the organization's strong stance on protecting its' confidential information. Legal and Security staff can provide guidance on what kinds of actions are inappropriate to ensure employees understand their usage limitations.

3) **Communicate Expected Behavior** – An emphasis on how the employee should err on the side of confidentiality should be communicated. By establishing expected behavior, the organization makes absolutely certain the employee has a clear picture of the organization's assumptions around how the employee is to treat any confidential data.

4) **Inform of Need to Return or Destroy** – The employee should have an understanding that any and all data that falls subject to the CIPA or is owned by the organization is expected to be returned or destroyed upon termination of their employment.

This CIPA should be presented to every employee regardless of the employee's position, title, level of perceived access to sensitive information, etc. The goal of the CIPA is to level-set every employee about how the organization seeks to safeguard their confidential information and the employee's role in helping maintain that protection. This is something that is commonly, but not universally done. If you were asked to sign one when you started, you can feel good that your organization has addressed one of the most basic building blocks of an effective insider threat program.

Making the CIPA Understandable

Because the CIPA is a legally-binding document being given to people normally having little more experience with contracts than perhaps their mortgage, tenant, or car lease agreement, it is important to have the CIPA written using as close to "plain English" as possible. Using clear everyday language helps establish the effectiveness of the document as a deterrent, spelling out exactly what the organization defines as confidential and what it expects of an employee.

It's equally important to spell out those expectations and not have brevity be the default. For example, if the CIPA states that "all company data and assets must be returned", does that mean an employee simply needs to forward a copy of an email they have, but can keep the original? Of course not. So the CIPA, in this instance, would need to use language like "return and destroy" spelling out that an employee (or contractor) is to have no physical or digital copies of any company data, emails, information, etc.

step 3

Define Risk Levels

In order to establish controls that allow the organization to properly detect insider risk, you must first know where you should be looking. Each position within your company has a relative level of risk associated with it. For example, a position that has access to and works directly with intellectual property puts the organization at a much higher level of risk than someone who has limited access to customer contact data. A measured response is needed for each position, relative to its level of risk. Put not enough emphasis on monitoring risky users and you will find your organization a victim of an insider attack. Put too much emphasis on 'eyes on glass" monitoring of users that pose no real risk to the organization, and you will have wasted time, budget, and energy.

How Should You Assign Risk?

So, you can see that it is important to first assign risk levels and then, based on the risk assessment, make decisions on the controls that should be in place. There are a few levels at which you can assess and assign risk:

1) **Based on Position** – Risk can most easily and accurately be assigned by looking at a given role or position within the organization. While the person occupying a position may change over time, the position itself will have similar access, working locations, employee autonomy, etc.

2) **Based on Department** – In some cases, an entire department – regardless of specific role – presents a similar risk to the organization based on their access to confidential information, an ability to transmit/export data, etc. A good example is the Sales department.

3) **Based on an Individual** – In extremes cases, an individual may have extenuating access to company data regardless of title, position, or functional role, such as the founder of a company.

The goal is to quantify a degree of risk using some method of scoring (can be 1-10, grading A-F, even by asking Y/N questions and adding up all the Y answers). The calculation method isn't as important as is working through the assigning risk process and doing it consistently. The scores should be determined using a number of both objective and subjective criteria (to properly inject the organization's view on the risk a position, department, or individual poses), such as:

- Access to confidential information
- Ability to export data
- Ability to freely transmit data over unsecured channels
- Amount of supervision
- Whether they work locally or remotely
- How much damage would a given employee (based on department, position, or themselves) do if they decided to steal information

The list above is by no means comprehensive, but does provide direction around the types of criteria you should use to start developing a scoring system. The focus should be on the ways any employee can pose a risk to your organization, and how detrimental the repercussions of malicious actions would be if they were to be taken by a given employee.

Once you have decided upon and finalized the questions used on your risk scoring worksheet, along with the associated scoring method, you will work through each of the positions, departments, and individuals, and have a number of scores.

See Guide Essentials: **Quantifying Positional Risk Worksheet** – use this worksheet to see examples of how you might assign risk scores.

It's important that the criteria used be consistently across every single position, department, and individual. Why? Because when you run your very first assessment of risk and, based on your model, come up with a risk score of, say, 7 – what does that even mean? Right. Initially, nothing.

It's not until you look at various positions, individuals, and departments and begin to see the similarities and differences in how you scored each, and use those comparisons to group risk scores into simpler levels – such as Low, Medium, and High (shown below) – that will correspond to everyday controls you will implement to detect and prevent risk (detailed in the next section).

Figure 1: Simplify risk scores into risk levels

Lastly, because risk will shift over time as new technologies, security policies, and IT processes are put in place, it's important to perform a periodic review process to ensure the correct risk levels are assigned (and, therefore, risk controls are in place). This can be quarterly, semi-annually, or annually. You'll need to decide how often to review both the questions and scoring system used.

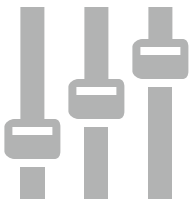
Once a given risk score has been defined for a given position, department, or individual, the score should be communicated - to HR to empower them as a source of intel around personal and personnel issues that may signify a need for elevated scrutiny by your security team, and to your security team itself so they can align proactive measures to risk.

step 4

Align Risk Levels to Everyday Controls

At a very high level, the risk scores equate to how much the organization sees the position, department, or individual in terms of potential exposure. Because a successful insider attack will result in harm to the organization, the appropriate response is to watch for signs or elevating insider risk (metastasizing into threat), using an appropriate level of scrutiny aligned to their risk level. In general, those with a lower level of risk only need to be monitored with a level of scrutiny that looks for leading indicators of elevating risk. Those posing a higher level of risk need to be monitored far more carefully –with an ability to rapidly review their actions in detail if necessary.

You should group your assigned risk scores into two or more categories that correspond to implementations of the following technical controls (more detail on how to best take advantage of each of the technologies below is provided in the Guide's Epilogue):



Lower-Risk Everyday Control – User Behavior Analytics

While those determined to pose a lower level of risk (as determined by the outcome of your Assigning Risk process) appear to be of no significant threat to the organization, it is critical to remember that risk can shift without warning, making it necessary to – at a minimum – analyze their behavior to proactively detect if the low-risk individual one day poses a higher risk based on leading threat indicators.

User Behavior Analytics (UBA) watches both an individual's interaction with company resources and their communications, baselining what is considered "normal" in order to detect anomalies that suggest an insider threat. Using a combination of machine learning algorithms, data science, and analytics, UBA can quickly identify when an employee is demonstrating behaviors synonymous with malicious insiders – or if an external actor intent on harming the organization has compromised the credentials of the employee.

Higher-Risk Everyday Control – User Behavior Analytics + User Activity Monitoring

For those demonstrating higher levels of risk, the organization needs to collect and maintain a system of record of their activity, while mining that activity for signs of insider threat. Employing UBA with a tighter sensitivity around anomalies makes sense here, as does a more layered, defense in depth approach that includes User Activity Monitoring (UAM).

UAM provides the organization with ability to record, alert on, and review insider activity. To demonstrate how UAM provides value, let's re-use example of the Accounts Payable person in a construction company pulling a list of customers. With UAM, someone in IT or Security could be notified when an Export of details is run within the AP application. A review could then be performed by playing back the activity in detail before, during and after the export to see why the insider (now a POI) pulled the list of contractors and what they did with it.

It's this context that allows organizations to understand the intent of the employee. If it was found that the AP employee copied the exported data to a USB drive with no evidence of any request for it on the part of any superior in the company, you know you have an insider threat action. But if an email was received prior to the export from the CFO wanting to run an analysis on the data, and the export itself was printed out, it becomes clear it was an action take as part of doing their job.

Aligning Controls to Risk Levels

We've provided just two types of controls. But, based on organizational need and the chosen solution(s), you may desire to take your assigned risk scores and group them into more than just two control levels. It's important to consider the capabilities of your chosen UBA and UAM solution(s), with an eye towards making sure they deliver the ability to

1) **Analyze** – the activity and behaviors in your organization,
2) **Detect** – meaningful events or shifts that suggest imminent risk,
3) **Prioritize** – where your focus should be by presenting only meaningful information without contributing to 'over-alert syndrome', and
4) **Respond** – effectively and efficiently, without significant strain on the organizations people and resources.

For example, you may have three control levels, representing those the organization deems are a low threat, those of medium risk that have access to some valuable – but not critical – data, and those of high risk with access to sensitive, confidential data.

There will need to be some work done to align the specific features of UAM and UBA solutions back to the risk-mitigating intent of each of the risk levels. It's this alignment that will help both choose the correct solution(s), while also establishing the right number of control levels.

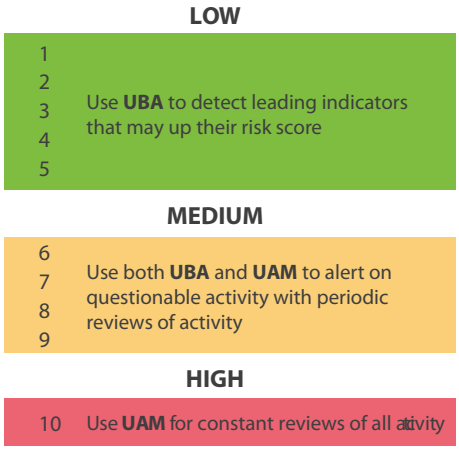


Figure 2: Designating controls to risk levels

step 5

Address Risk During your Termination Process

One of the best practices found in the Common Sense Guide to Mitigating Insider Threats – a document written well ahead of its time by the world-renown CERT division of Carnegie Mellon University's Software Engineering Institute (SEI) – is the need to develop an employee termination process that takes into account the threat a departing employee can pose.

Whether being terminated or leaving on their own accord, the exit period poses one of the highest risk timeframes to an organization. Loyalties quickly shift from the organization to the individual, and thoughts move from responsibilities to their soon-to-be "former" employer to a focus on the next job and its' requirements.

To mitigate insider risk during this high-risk exit period, two processes must be put in place – one to address an employee that is being involuntarily terminated, and another to address a voluntary termination (resignation) involving a notice period. It should be noted that this guide touches on steps normally taken by HR. However, this guide is strictly focusing on those steps that help to mitigate insider risk and, therefore, should not be misconstrued as presenting a comprehensive termination process.

While having very similar steps, they should be considered separate processes to ensure service levels are properly defined and met when put into action.

Involuntary Termination

This involves a situation where an employee is being laid off or discharged. Since in most cases this is not a pleasant separation, the assumption is that the employee's loyalties will quickly diminish to zero, putting the responsibility of ensuring confidentiality and the security of organizational data and resources firmly on members of the Security team. The process should begin the moment the decision is made to terminate employment, and will include one or more of the following tasks (depending on your organization):

- **Notification of desire to terminate** – This is the first step in the process where internal management notifies HR (or equivalent) of the need to terminate an employee. This needs to be done as soon as the decision is made.
- **Notify IT of termination and employee last day** – IT needs to be informed that an employee's access will need to be revoked, and when to revoke it. This also should initiate an audit around any organizational assets currently possessed by the employee.
- **Conduct a 30-day Activity Review** – A review of the last 30 days of the employee's online and communications activity must be conducted. In many cases, involuntary termination isn't a surprise to the employee and loyalties may have shifted weeks prior, giving the employee ample time to exfiltrate data, etc. This 30-day period has been shown to be the time when a great deal of IP and other confidential information are taken. Completing a comprehensive review without the type of detailed information that UAM can provide in a single pane of glass can be difficult, but if you cannot convince your organization to provide you with purpose built tools, make best efforts using what you have – but be sure to let management know you are giving them a report based on what you had available to you.
- **Notification of any inappropriate activity found** – Should any questionable, or unquestionably inappropriate actions be found during the activity review, HR and Legal should be notified. The actions found may have consequences on how the termination itself will proceed.
- **Employee notification of termination** – This begins the actual process of terminating employment.

- **Review of Signed CIPA with employee** – One of the first steps in every termination, the CIPA should not just be presented to the employee, but reviewed, explaining the obligations this document lays out – that the employee has previously agreed to. At this point, it is also prudent to mention that the employee will be asked to sign a Certificate of Return and Destruction from the employee prior to leaving.
- **Terminate Access** – While notifying the employee and reviewing the CIPA, access to all data, systems, applications, and resources should be terminated by IT.
- **Return or destruction of company property** – All company property should be returned and all company data (in all possible forms – printed, in email, stored in files on a USB drive or cloud storage, etc.) should either be returned or destroyed.
- **Obtain signed Certificate of Return and Destruction** – The employee is asked to sign the legally binding document, indicating they are taking, nor have access to, any company data – whether confidential or not – with them once they leave the organization.

Each task should have a responsible role or individual and a service level timeframe assigned. This way expectations are communicated to each person involved regarding expected response times. The timeframes will vary, based on risk scores and perceived immediacy, noting that exceptions to these will occur. Some tasks require another role or individual to be notified; this should also be documented with a given task, when appropriate.

Voluntary Termination

When an employee leaves of their own volition, this process begins the moment notice is given (one of the differences between this and the involuntary termination process). Voluntary termination can also be initiated by an employee no longer showing up for work a designated number of days without providing any notice, in which case, the process begins based on HR's definition of Job Abandonment.

The process for a voluntary termination is very much like that of the Involuntary Termination, with a few task exceptions:

- **Employee provides notice** – There is an assumption (putting job abandonment aside) that the employee will provide notice, kicking off the termination process.
- **Notice period determination** – The organization needs to decide whether they wish to accept the notice period, or modify it.
- **Conduct a +/- 30-day Activity Review** – Should an employee's notice period be accepted, their activity from the date of notice to the date of employment termination should be reviewed in addition to the 30 days prior to the date of given notice.

Another difference will be the timeframes for each task. For example, the review of the CIPA should happen on the day of notice given, rather than the day of termination – as in the case of the involuntary termination. Lastly, service levels may also differ – such as notification of termination to IT. In the voluntary termination scenario, IT should be notified the same day notice is given, but immediately during an involuntary termination.

See Guide Essentials: **Risk-Lowering Termination Process** – Use this document as the basis for defining termination process roles, actions to be performed, assignments of actions, and service levels to be met.

Quantifying Risk: Where to Start?

While the entire process has been simplified down to just 5 steps, determining where to begin can be pretty daunting. Do you need to start scoring every position within the organization? You already have a job to do, so it's unlikely you could even if you needed to.

In reality, the most important part of where to start is simply starting. Begin with any open positions that are being filled by HR – these will be filled by people you know the least. Score those positions, along with a few positions you know should be of higher risk as a point of reference. Once you have those completed, you can begin to profile positions you know represent an insider risk (just not how much) – those that daily interact with confidential data, intellectual property, customer data, and the like - and begin to build out a comprehensive set of positional risk documents.

Even if you don't have a UAM or UBA solution ready to implement, quantifying insider risk at least gives you some perspective on how big the problem is within your organization – which may help speed up the selection and purchase of a solution to help monitor user behavior and activity.

Conclusion

Insider threats represent one of the greatest challenges of organizations today. Not only are they capable of involving your organization's most confidential and valuable data, but they are also the most difficult to identify. Insider risk begins the moment the employee steps foot in the door, and ends the moment the door permanently closes behind them. So, it's important to follow this guide from beginning to end, to properly implement controls that protect the organization from insider risk at all stages of an employee's tenure within the organization.

By taking the steps outlined in this guide, you will have a better understanding of just how much insider risk exists, and – more importantly – where it exists. The guide also provided enough direction to put preventative steps in place to be able to thwart, detect, and – if needed – document insider threat activity.

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/