# **4 Steps** to Reduce the Risk of Malicious Insider Activity

Veriato

www.veriato.com

The risk of malicious activity has never been more of a reality for organizations. End users today access, process, and manage privileged data more than ever as part of their job. This need for employees to use privileged data puts the organization at risk of malicious actions that include data theft, destruction, manipulation, and ransom. And it's not just theory, a full one-third of reported insider incidents in 2015 involved end users who access sensitive data as a requirement to do their jobs[1].

This raises the question of why a seemingly loyal employee would turn and even contemplate stealing data, let alone take action. Approximately half of insider incidents have a financial motive[1]. There are plenty of buyers of credit card data, social security numbers, and healthcare data – all with per-record market rates ranging from one cent to well over $1,000. Additionally, organizations with intellectual property and trade secrets are also at risk of insider espionage, which has increased as the primary motive from less than 5% of attacks in 2009 to 25% in 2015[1].

## CAN'T YOU JUST SPOT MALICIOUS INSIDER ACTIVITY?

The challenge in detecting malicious actions exists because, in most cases, employees are simply taking advantage of the access to data, applications, and systems that your organization has authorized as part of their job. It's usually a simple case of privilege misuse, which was the top threat action, occurring in 53% of insider incidents[1]. For example, a user who normally accesses documents containing intellectual property can simply exfiltrate those documents as attachments via any web-based email platform.

[1] Verizon, Data Breach Investigations Report (2016)

## SO, HOW DO YOU TELL IN WHOSE INTERESTS THEY ARE WORKING - THE ORGANIZATION'S OR THEIR OWN?

70%

OF INSIDER INCIDENTS TAKE EITHER MONTHS OR YEARS TO BE DETECTED

It's so utterly difficult to spot the difference that 70% of insider incidents take either months or years to be detected[1]. To help address the growing problem, Carnegie Mellon University's Software Engineering Institute (SEI), which includes their world-renown CERT division, released a Common Sense Guide to Mitigating Insider Threats. The guide contains 19 practices to protect your organization from insider threats. One of the key ways to reduce the risk of insider threats this paper will focus on is found in Practice #4, entitled

**Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.**

The only real way to tell the difference between an employee doing their job and an insider is right there in the middle of Practice #4 - monitor their behavior. Now, we're not talking about "Big Brother" here – in fact, quite the opposite. What's needed is risk-based monitoring of specific user activity to reduce the likelihood of insider threats.

[1] Verizon, Data Breach Investigations Report (2016)

## SO, THEN WHAT, WHEN, AND WHO SHOULD YOU MONITOR? AND WHAT EXACTLY ARE YOU LOOKING FOR?

It's not that simple. To properly implement a risk-based moni-toring program, you'll need to follow four key steps, which culminate with an ability to appropriately monitor user activity at various levels, ensuring security and privacy is maintained.

step 1
BUILD

step 2
ASSIGN

step 3
IDENTIFY

step 4
ESTABLISH

step 1

## Build the Insider Risk Team

While the idea of monitoring user activity likely stems from the security folks in IT who both understand the security risks and what's possible with technology today, IT can't implement a program like this on their own. There are a number of hurdles within the organization that need to be addressed, which requires that your organization first build a project team that oversees the what, when, and who of monitoring user activity.

The team should include members of your:

1) **Executive Team** – You'll need buy-in from the C-suite to ensure the other departments represented on this team have the authority to establish a risk-based monitoring program.

2) **Legal Counsel** – Legal will want to ensure all monitoring activities are within the bounds of local law. They will also help define what is permissible to monitor (e.g.: recording an employee logging into their banking website could put the company at legal risk should something happen to the employee's bank account). Additionally, because the potential exists for those watching in IT to not be authorized to review activity of higher-level employees, legal will work with Security teams to determine exactly which roles in the organization can review which sets of activity.

3) **Human Resources** – HR will help create the processes necessary to ensure any need for monitoring employee activity is warranted and documented. They also will help to address any "big brother" perception and employee morale issues.

4) **IT / Security** – IT will provide the other non-technical team members with context around which users have access to what sensitive data, as well as what's possible when it comes to monitoring activity – all of which will be invaluable when putting the planning and preparation output of this team into practice.

**The goal of the team is to come to an agreement of why monitoring is necessary within your organization, and begin to define the processes and procedures necessary to be used when monitoring is actually performed. This will be critical to ensure uniform monitoring occurs, in accordance with written policies.**

step 2

## Assign Risk Levels

The term risk-based monitoring itself implies that the organization first needs to define when there is risk. So, before any monitoring of activity can begin, you first need to assign risk levels to employees within the organization. The risk levels assigned should be aligned with a specific level of monitoring and will help to establish both who should be monitored and how to properly monitor them.

The first place to start is to look at a given employee's role. If their role has them accessing sensitive information, intellectual property, trade secrets, customer lists, etc., their risk level should be higher than someone who has no access to any of that information. Use a simple scale of 1-10, with 10 being the highest risk. Or, if it better suits your organization's needs, go with Low, Medium, and High. Keep in mind, there is no specific right or wrong risk model; the important thing is to establish levels of risk for every employee based on their current role, levels of privilege, and required access. The higher the risk in a worst-case scenario, the more need for monitoring of activity.

As you assign levels of risk, it's critical to be aware that risk shifts throughout an organization. Take an individual that has no access to sensitive data today, but gets a promotion tomorrow that requires interacting with financial systems. That person's risk level has increased. Additionally, changes in their personal life and financial situation (increased debt or expensive purchases) can also elevate their level of risk. The same is true for changes that reduce an individual's level of risk. In either case, there should be a process in place to communicate to HR that a risk level has changed.

You'll note that the Common Sense practice mentioned above states "Beginning with the hiring process..." Mitigating risk should also start before an employee is hired. Placing a risk on a role pre-hire empowers your monitoring program to place an unbiased level of scrutiny on the employee once hired.

step 3

## Identify Inappropriate Behavior

Just because a particular employee's role brings risk to the organization, it doesn't necessarily mean that they are doing anything malicious. And because insider actions often can be mistaken for normal job-related duties, organizations should also rely on inappropriate behavior as a leading indicator of a change in risk level. Unlike the change in role previously mentioned (which clearly indicates the need for an elevation in risk level), think of inappropriate behavior as a "less-obvious" indicator – but an important and, often, more reliable real-time indicator of risk.

It's important to have methods of identifying inappropriate behavior – as a leading indicator of elevated risk – that are both technical and non-technical in nature in place.

## Technical Methods of Detecting Inappropriate Behavior

User Behavior Analytics (UBA) solutions focus on baselining an individual's behavior, looks for anomalies when compared to the baseline, and alerts the appropriate staff within your organization of the anomaly for further review. UBA solutions are typically looking for:

1) **Shifts in Communication** – An employee whose sentiment about the company changing from largely positive to largely negative can indicate elevated risk. As can changes in words used, such as lots of use of the terms "us" and "we" changing to more use of "I" and "me." A UBA solution watches both sentiment and words used to intelligently determine if leading indicators of risk exist.

2) **Shifts in Behavior** – Watching behavior that may indicate elevated risk, UBA solutions watch the resources accessed, data consumed, and where/how often data is moved by a given employee. An employee just doing their job provides a UBA solution with what "normal" looks like for that user. Any deviation outside the norm, may indicate an insider threat.

## Non-Technical Methods of Detecting Inappropriate Behavior

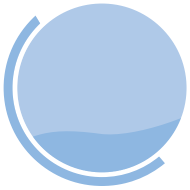
Organizations should have policies and procedures in place, instructing employees how to report concerning or disruptive behavior by co-workers. This could include boasting (e.g. someone stating they could easily hack the network), and malicious threats focused on an employee or the organization.

Utilizing both methods is important, as insiders who have become a risk may indicate themselves in both the activities they perform on their computer, as well as how they act around their co-workers.

step 4

## Establish Insider Monitoring

In step 2, you assigned risk levels to roles and individuals in the organization. When thinking about the practical application of the monitoring of those individuals, your project team needs to establish what kind of monitoring goes with which risk level. In general, you can break down risk levels into two basic groups: Low, Medium, and High. Each will require a different type of activity monitoring based on the risk they present to the organization.



**Low Risk** users pose little threat, and likely have no access to any kind of sensitive data. These users may simply be subject to the non-technical monitoring and detection methods previously described.

**Medium Risk** users have access to sensitive data, but don't appear to be a risk. They should have the addition of being monitored by a UBA solution. This will allow the orga-nization to quickly detect if there is a shift in behavior and, therefore, risk.

**High Risk** users are those with the greatest levels of access, and/or pose the greatest risk to the organization (for example, the CFO who has access to all bank accounts). They are also those medium risk users with whom inappropriate behavior has been detected. These users will have their activity actively monitored and reviewed.

Remember, monitoring insider activity is an on-going process – from hire to fire – where risk levels have the potential of constantly changing. Having uniform monitoring steps taken for each of these levels in reaction to concerning or disruptive behaviors, according to written policies, will eliminate biased monitoring and produce a more effective monitoring program.

## Reducing the Risk through Risk-Based Monitoring

The potential for malicious insider activity exists in every organization. It merely is a question of which employees present the greatest risk. Without putting a risk-based program in place, you end up with one of two situations. Either you're left with everyone being over-monitored (which only results in lowered morale and productivity) or the under-monitoring of those creating risk.

But, by putting a risk-based monitoring program in place, you correctly equate an appropriate level of monitoring based on an individual's risk level. That means you're always in the right place at the right time with the right level of monitoring, elevating the organization's ability to detect and respond to risky behavior.

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/