7 Steps to Building an Insider Threat Program

Veriato
www.veriato.com

Introduction

Since you're reading this guide, it's likely you recognize the threat insiders pose to an organization and the need to proactively build a plan to monitor, detect, and respond to potential and active threats. Insiders pose a real threat – 28% of data breaches are perpetrated by insiders[1], and institutional fraud is almost always an insider[2]. With 53% of organizations experiencing at least one insider attack within the last 12 months[3], it's appropriate for organizations to begin down the path you've chosen and build out an Insider Threat Program.

This kind of program requires shifts in corporate culture, corporate communications, hiring and firing processes, and a daily concern that any employee – even those you believe are trustworthy – can, at any moment, become a threat.

This Getting Started brief provides some high-level guidance around the steps necessary to implement an Insider Threat Program (ITP) to proactively identify potential and active threats, as well as to appropriately respond should a threat arise.

[1] *Verizon, Data Breach Investigations Report (2018)*
[2] *ACFE, Report to the Nations (2018*
[3] *Cybersecurity Insiders, Insider Threat Report (2018)*

STEP 1

Understand the Obstacles to Building an ITP

Any new program designed to be implemented organization-wide will face obstacles. So, before you even begin to build an insider threat program, it's important to understand exactly what you're up against – in the interest of being able to overcome each obstacle.

1. **Funding** – This is the most common obstacle to any new program. You should work to get general approval for some amount of funding, but table the specific funding needs until after you've established the goals of the program, outlined what activity needs to be monitored, and what technology will be used.

2. **Privacy** – Questions around whether employee privacy is being maintained will be raised. The means by which you monitor insider actions, to whom that information is made available to, and how that information is reviewed and secured will help overcome this obstacle.

3. **Culture** – Putting an ITP in place changes the culture of an organization. Will you be using a "See something, say something" policy around the office? As you can see, even something as simple as that policy changes how employees perceive the company. It's important to review how a program like this could impact the culture.

4. **HR** – This department has their pulse on the organization. They may see an Insider Threat program as something negative. You may need to meet with HR to talk about how an ITP can augment the desire for HR to maintain a productive and secure workplace.

5. **Legal** – your legal counsel may be worried about the organization being sued for invasion of privacy, etc. Double-checking local, regional, and national laws concerning the monitoring of employee activity may be necessary before moving ahead.

6 **Stakeholders** – This includes the C-Suite, department heads, and even line of business owners that may be concerned that the monitoring of employee activity may impact their part of the business.

7 **Employees** – While the organization has a duty to protect itself, it should be noted that even employees may take issue; no organization wants key employees to leave because an ITP was implemented. Discuss this with HR and stakeholders.

STEP 2

Build the Insider Threat Program Team

Because defining, monitoring, alerting, and responding to insider threats isn't going to just be the responsibility of IT, it's imperative for the success of the program that a team of individuals representing several parts of the organization be created. These individuals will help to ensure the decisions made around the who, what, and how of this program will be implemented are in the best interest of the organization.

Your ITP Team should consist of one or more of the following parts of your business:

1. **Senior Management** – someone from the executive team should participate to help make final decisions, as the remaining players all have equal representation in the discussion.

2. **Human Resources** – HR will play a role throughout the implementation and execution of this program. Acting as the representative of the employee, HR can provide guidance around how the program may impact productivity, morale, etc. HR will also act as a source of vital information for the program, providing guidance around which employees represent a risk to the organization.

3. **Legal** – Monitoring is done because of risk. Legal participates to ensure the means by which the monitoring is performed will keep the organization in the best possible legal stance.

4. **IT** – Without considering the specifics of what's technically possible and how a solution is implemented, etc., the UABM plan is theoretical exercise. IT participates to ensure the desires of the team can be executed.

5 **Security** – Understanding where your organization's critical, sensitive, protected, and valuable data is, as well as who has access to it, is the job of the Security Team. They participate to ensure accurate monitoring of users with access to the organization's most valuable asset – its' data.

6 **Key Employees** – Department heads and line-of-business owners should also be considered. They can provide vital feedback around adoption, employee-program friction, and an employee-centric view from someone with the organization's best interest in mind.

Designating an ITP Senior Official

The program needs an owner. This individual should play a key role in the organization, will be responsible to oversee the development of the written insider threat program plans. So, as the team is brought together, someone needs to be appointed the ITPSO.

STEP 3

Start with Some Program Definitions

As you begin your journey down the path of building an ITP, it's important that the team first establish some key definitions that will impact exactly how this program will operate on a daily basis. We've outlined them below as questions that need to be answered.

What do you consider an Insider Threat?

To many organizations, it may be the malicious insider – someone that is intent on stealing data or committing fraud – that is the focus. But there are other insider threats to consider. The unwitting insider may become the pawn in an external attack simply because they weren't being security-conscious when clicking on email attachments. And there's the negligent insider who makes data available on the Internet, causing a data breach. By deciding on one or more of these insider threat types, you provide context for the remainder of the program's definition.

What assets are of value?

This may appear easy at first – you simply point at the organization's most precious data sets. Customer data, credit card information, personally identifiable information, intellectual property, and more all come to mind. But it's important to also "think like an insider" – how can they leverage data that sits outside the list of "usual suspects". For example, the use of a vendor list by someone in Accounts Payable could be used to help launch a competing business. Measure the value of the data to the risk it presents to the business should it fall into the wrong hands.

What are the goals of the Insider Threat Program (ITP)?

As you consider the answers to the previous two questions, you can see how those answers begin to provide context to answer the question of the program's goals. If the team only considers the negligent insider a threat, it's going to change the asset focus, as well as what activity you need to be looking out for. So, it's important to establish the program's overarching goals. There are 5 common goals of any ITP:

- **Identify Potential Threats** Insiders almost always display leading indicators through shifts in communication and behaviors. Some programs seek to spot these shifts and attempt to stop threats from ever coming to fruition.
- **Detect Insider Threats** – Specific activities can be established as threats (such as copying of files, printing data, etc.) and program initiatives can focus on these specific actions.
- **Discover Inadvertent Breaches** – Again, by defining the types of actions that inadvertently make data "breachable", programs can be tailored to spot this kind of activity.
- **Enhance Investigative Abilities** – Once a threat action occurs, organizations need to understand the scope of the threat in order to remediate it. Some programs seek to make investigating insider threat activity easier by collecting more activity data to augment their ability to investigate the threat action.

STEP 4

Understand the Foundational Elements for an ITP

Before the ITP team dives into developing the inner workings of your program execution, it's important to understand three guidelines you must meet in order to successfully establish the program.

1. **You Need Executive Buy-In & Support** – We've already outlined how you need to have executive representation on the ITP Team, but this program "sinks or swims" based on whether you have buy-in that insiders are a threat to the organization, it's operational ability, its revenue, and its' very survival.

2. **Communications Between Departments is Crucial** – This is the very basis for a framework that addresses Insider Threat behavior and the organization's response. As you build out response plans, you will see how many departments need to work in concert to address potential or active threats in a timely manner.

3. **Visibility into Employee Behavior is a Necessity** – The success of the program hinges on the organization's ability to be aware of and understand each employee's actions, and the any context surrounding those actions. Without visibility into the intelligence sources listed in the next section, it will be impossible for the organization to know when insider activity that threatens the business either occurs or may occur.

With these three foundational elements in mind, the ITP needs to next determine what sources of insider activity will be used as part of the program.

STEP 5

Select Intelligence Sources

To achieve the visibility required to have insight into the motives and actions of insiders, the organization will need to solicit detail from a number of sources. Each of the sources below provide context around a different aspect of an employee. The goal is to have all of the following sources in play within your program.

Human Resources

HR is a fantastic source of intel on where risk lies within the organization. They know who didn't get a raise, who was passed up on a promotion, who is having health issues, hears the gossip about who is having financial issues, who is quitting, who is being fired, and more. These human factors need to be a part of the insider threat equation – they provide the Team with clear indicators of potential risk. Take the example of someone thinking of quitting. The manager catches wind of the possibility and talks to HR about proactively looking for a replacement. HR can then inform the members of the ITP Team responsible for monitoring activity, looking for possible inappropriate actions, such as the stealing of data, etc.

Physical Security

The activity detail found in access card systems, phone records, video, etc. can all provide valuable context and corroborating evidence that a user is up to no good. For example, if a user logs into the network at 3pm on a Sunday (a day they never come in on) and you have the badge scans showing they physically entered the building, should there be an issue, you can confirm it was actually the employee who owns the user account.

User Behavior Analytics (UBA)

UBA monitors for shifts in behavior and communications by insiders to proactively identify indicators of a potential threat. Using analytics, employee activity is compared to a baseline of activity to determine if a shift has occurred. Psycholinguistic indicators are used when analyzing communications, looking for changes in tone (e.g. from generally positive to generally negative) and in the use of specific focus words (e.g. when the employee shifts from using "we" and "us" to primarily using "I" and "me", there could be a problem).

User Activity Monitoring (UAM)

UAM monitors all user activity, providing the ITP Team with granular detail about a user's actions. Activity data is collected and normalized, allowing it to be used for alerts, reporting, searches, and investigations. In many cases, the user's screen is recorded, allowing video playback of their activity.

IT and Security team members will need to coordinate the implementation, monitoring, collection, alerting, and reporting for each of the sources above used in your program. As you implement each, it may be necessary to review the types and depth of data collected with the remainder of the ITP team to ensure there are no raised concerns.

STEP 6

Critical Documentation & Notices

As you consider the answers to the previous two questions, you can see how those answers begin to provide context to answer the question of the program's goals. If the team only considers the negligent insider a threat, it's going to change the asset focus, as well as what activity you need to be looking out for. So, it's important to establish the program's overarching goals. There are 5 common goals of any ITP:

- **Confidentiality and Intellectual Property Agreement (CIPA)** – This document should be used on an employee's first day of employment. It should communicate what kinds of data the organization deems "confidential" and establishes the expectation of the employee that confidentiality will be upheld throughout and even after employment.

- **Acceptable Use Policy** (AUP) – This document should outline the kinds of computer-related behavior the organization condones. Topics like personal privacy, use of company resources for personal use, etc. should all be covered in this document. Like the CIPA, this document should be used on the first day of employment.

- **Security Acknowledgement Agreement** – This document serves as the security-side of the AUP. In it, the organization stipulates that the employee agrees to protect the technology assets of the organization, abide by stated security policies, report violations, and more.

- **Logon Banners** – Prior to logon to the network, security banners should be presented reminding users of the need to maintain security, ensure proper use, and uphold confidentiality when using the organization's network.

Seek legal counsel regarding the need for all documents and notices agreeing on terms and the contents necessary.

User Behavior Analytics (UBA)

UBA monitors for shifts in behavior and communications by insiders to proactively identify indicators of a potential threat. Using analytics, employee activity is compared to a baseline of activity to determine if a shift has occurred. Psycholinguistic indicators are used when analyzing communications, looking for changes in tone (e.g. from generally positive to generally negative) and in the use of specific focus words (e.g. when the employee shifts from using "we" and "us" to primarily using "I" and "me", there could be a problem).

User Activity Monitoring (UAM)

UAM monitors all user activity, providing the ITP Team with granular detail about a user's actions. Activity data is collected and normalized, allowing it to be used for alerts, reporting, searches, and investigations. In many cases, the user's screen is recorded, allowing video playback of their activity.

IT and Security team members will need to coordinate the implementation, monitoring, collection, alerting, and reporting for each of the sources above used in your program. As you implement each, it may be necessary to review the types and depth of data collected with the remainder of the ITP team to ensure there are no raised concerns.

STEP 7

Build Incident Response Plans

The program is as much about how the organization responds to a potential or existing threat as it is about detecting threats in the first place. So, it's important to build response plans to at least some high-level scenarios. We've outlined four scenarios below to act as starting points for your response plans. Keep in mind, your organization may have other specific requirements needed in your plans.

Leading Indicators Identified

Organizations should be monitoring for activity or signs that indicate the employee may be a potential risk. For example, HR may hear that an employee is having financial difficulty. Your UBA solution can determine an employee has become negative toward the organization. Badge scans show an employee abnormally coming in on weekends. Or even your UAM solution can identify when an employee is visiting websites looking for a new position.

Your response plan can include anything from HR calling a meeting with the employee, to requiring regular reviews of employee activity.

Active Indicators Identified

Monitoring of activity should include looking for actions the organization deems threatening. For example, the copying of specific data, excessive printing, multiple simultaneous logons from different regions of the world, etc.

In these cases, the response actions should be swift and decisive, and include an immediate review of employee activity, along with the ability to immediately revoke their access to the network, should it be necessary.

Employee Giving Notice

An employee notifying you of their intent to leave the organization is a leading indicator of a potential threat. Employees leaving the organization have the opportunity during their notice period to access, review, copy, or print sensitive company data. It's also possible they may have already done so prior to them providing notice.

So, responses should include a review of their activity a specified number of days prior to the date of notice, a review by HR of the CIPA with the employee, a continual review of activity during their notice period, and terminal activities such as terminating access, returning company property, and signing a Certification of Return and Destruction (a document that legally certifies the employee has not taken, nor has in their possession, any company data or property.

Employee Being Terminated

This is similar to the Employee giving notice, but with the activity sped up to reflect the organization's desire to end employment immediately and have the employee removed from the premises. The reasons why the employee is being terminated impacts the response timeframe – which can be anywhere from immediately to a few days of time in which the ITP team can perform response actions.

Each of your response plans should outline specific ITP team actions, who is responsible, if any other team members are to be notified, and what the timeframe for the response activity should be. Take the example abbreviated response plan below for an employee being terminated – it demonstrates each of the actions that need to take place, who should perform them, when they are to be performed and who should be notified of the findings.

Task	Responsible Role	Notified Role	SLA
Prior to Involuntary Termination (if possible. If not Day of Involuntary Termination)			
Notificaiton of desire terminate	Manager	HR	
Notify IT of termination and employee last day	HR	IT	Immediately
Conduct +/- 30-day Activity Review	Security		Same Day
Notification of any inappropriate activity found	Security	HR, Legal	Immediately
Badge Scans			
Day of Involuntary Termination			
Employee notification of termination	HR, Manager		
Review of Signed CIPA with employee	HR		Same Day
Terminate Access	IT	HR	Same Day
Return of Company property	HR		Same Day
Obtain signed Certificate of Return and Destruction	HR	Legal	Same Day

Getting your Insider Threat Program Started

The steps outlined in this guide provide quite a bit of high-level direction and detail. Begin by at least building the ITP team and getting executive buy-in. Once you're over that hurdle, the remainder of the work can grow gradually. Do keep in mind that the longer you wait to fully implement the ITP, the more at risk the organization is.

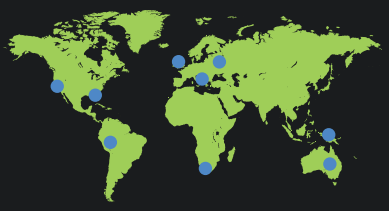
You should expect your initial definitions, processes, etc. will be somewhat rudimentary. Over time, your planning, processes, procedures, and methods will mature as you expand the program.

Veriato Resources

Veriato 360 Information – Veriato.com/360
Veriato Recon Information – Veriato.com/Recon

To learn more about how Veriato can help you with employee investigation, contact a Veriato representative today.

Over 3,000 enterprises, & thousands of SMBs have placed their trust in our solutions



Our solutions are deployed in **110+ countries**

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/