The Ultimate Guide to Building an Insider Threat Program

Shawn M. Thompson, Esq.
Mayank Choudhary

Shawn Thompson is the Founder and President of the Insider Threat Management Group, LLC, which provides strategic insider risk management advisory services to the private sector. He possesses over 20 years' experience investigating, prosecuting, and managing Insider Threats and is widely sought-after for his unique expertise. He is a former federal prosecutor and senior government official who held executive positions with several agencies including the FBI, DoD, and DNI. As a seasoned risk management professional, experienced prosecutor, credentialed special agent, and trained analyst, his cyber security acumen is second to none. He is a pioneer in the field of insider risk management, serving as a frequent guest speaker and thought leader on a variety of security topics. Shawn serves as a trusted advisor for the highest levels of government as well as private sector C-suite and Board of Directors alike. He is a member of the Maryland Bar.

Mayank Choudhary (MC), is a technology leader with more than 18 years of Cyber security and Content Management industry experience. MC is responsible for charting and executing the strategic course of ObserveIT's solutions. His prior experience includes serving as VP, Product Management at Intralinks where he built the enterprise business and managed the cloud platform, Director of Product Management, Identity Management & Governance, CloudMinder portfolio for CA Technologies and senior product management positions at Dell EMC. MC holds an M.B.A. from the University of Albany, a Masters in Computer Science from the University of Akron, a B.S. in Computer Science from Nagpur University and an Executive Education degree in Strategy & Innovation from MIT.

The Ultimate Guide to Building an Insider Threat Program

Shawn M. Thompson, Esq.
Mayank Choudhary

Contents

The Ultimate Guide to Building an Insider Threat Program

Preface

"Amateurs hack systems, professionals hack people."

Bruce Shneier

People are, unfortunately, the weak link in the cyber security chain, whether intentionally or unintentionally. It is these same people who have legitimate access to your facilities, systems, people, and data who pose the greatest threat. These are your "insiders." While the threat of insider-caused organizational harm is on the rise, most companies have not established a formal program to manage this risk. While there may be existing procedures in place to monitor corporate networks for intrusions and the collection of various logs for network analysis, there are likely few controls designed to monitor and respond effectively to insider *behavior*, especially unintentional threats. Moreover, few corporations have implemented holistic Insider Threat management programs.

Company insiders are responsible for 60–70% of security incidents.[1] Of these, roughly two-thirds are the result of negligence or other unintentional actions.[2] Unfortunately, today's piecemeal and ad hoc approach is simply not working. You need a holistic Insider Threat Management Program (ITMP) to effectively manage these threats and reduce the risk to your corporate assets.

An Insider Threat management program is often viewed as an expensive and resource intensive endeavor, as well as a privacy nightmare. While monitoring licenses, support and operation expenses, legal and consultant fees, can be expensive, costs can be reduced by utilizing existing capabilities and resources. Most companies will have existing departments that either share the objectives of a program or are currently responsible for performing some of the functions. The key is to leverage and use these existing resources and processes to meet the following objectives:

KNOW YOUR PEOPLE. Knowledge refers to the importance of developing a clear picture of the organization's insider population by ensuring a trusted workforce of employees, vendors, and partners; providing insiders with resources to properly protect assets; creating a culture of transparency and responsibility; and developing workflows that foster the identification and mitigation of behaviors that may adversely impact the organization.

UNDERSTAND INSIDERS' BEHAVIOR. Knowing how people interact with data, services and applications is crucial for evaluating the risk and likelihood of an Insider Threat. Monitoring user behavior will provide unequivocal proof during the investigation process and will significantly reduce the end-to-end investigation time.

MITIGATE RISKY BEHAVIORS. An important objective of any ITMP is to mitigate the risk of an Insider Threat, so a proactive approach is a key component. Clear security polices and the ability to deter as well as raise security awareness at the point of violation has been proven to be the most effective way to reduce insider risk.

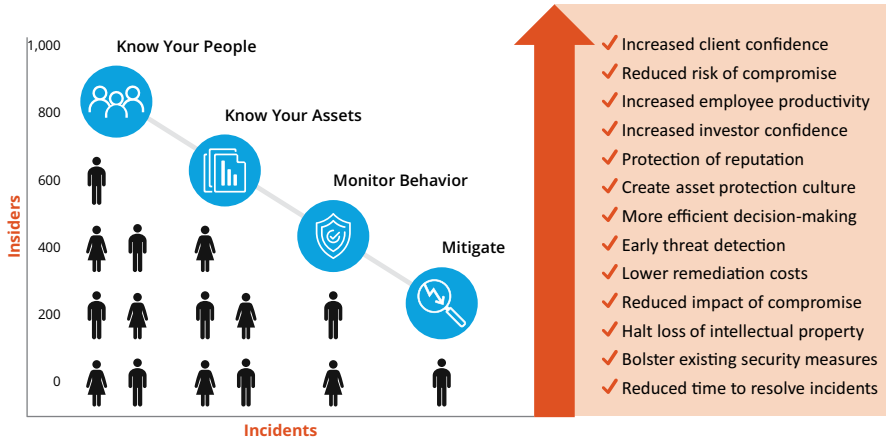
[1] Verizon DBIR 2019 (combining the categories of "privileged misuse," "miscellaneous errors," "physical theft," and "everything else" categories pertaining to insider involvement); IBM X-Force Threat Intelligence Index 2018

[2] IBM X-Force Threat Intelligence Index 2018, Ponemon 2018 Cost of Insider Threat Report

Return on Investment

A formally developed ITMP provides real and immediate ROI. Unlike traditional security models that focus on external threats and stove-piped processes, an ITMP will add immediate value by providing a framework and methodology to properly align resources with security objectives. The value proposition of a holistic ITMP is depicted in Figure 1.

Figure 1: Insider Threat Management Program — ROI



Introduction

The purpose of this guide is to provide a resource for initiating, developing, and implementing an Insider Threat management program (ITMP). This guide will assist you in effectively obtaining leadership support and assembling your team, developing a risk-based action plan, creating a policy and governance structure, implementing monitoring requirements, and building an oversight and compliance framework to ensure continued employee and leadership support.

Insider Threat management programs are quickly becoming standard practice throughout private and public industry. In today's data breach-ridden and high-velocity business environment, security practitioners must be able to understand and implement programs in the most efficient manner possible. This is significant, as this task also requires balancing the protection of corporate assets with the privacy of employees, which raises myriad legal considerations.

Developing an Insider Threat management program can be a difficult task even with a process or structure in place to follow and even more so without an established process. This critical action becomes even more challenging if the security professional has not had formal experience managing Insider Threats. Additionally, not knowing which questions to ask can not only lead to legal trouble, but also leaves your organization vulnerable to Insider Threats. This guide will prepare you for this challenge.

The guide covers the following Insider Threat topics:

- The Insider Threat problem
- The primary objectives of an ITMP
- The functional components of a holistic ITMP
- The fundamentals of Insider Threat management
- The importance of a security-aware corporate culture
- How to balance privacy and security
- Regulatory and legal requirements that incentivize creating an ITMP
- Insider Threat tools and solutions
- Sample charts and workflows

This guide was developed by a leading experts in the field of insider risk management. The authors utilized their experience and industry resources as well as input from practitioners who have demonstrated considerable skill in building and managing Insider Threat management programs.

The Insider Threat Problem

Without personal experience with Insider Threats, it's often difficult to understand the true scope of the problem. To that end, there are two primary sources that serve as proxies and can be used to approximate the size of the problem. The first are surveys, which are largely anecdotal responses to general questions pertaining to Insider Threat. Many Insider Threat tool providers regularly sponsor such surveys. The second primary source of information is from data on actual breaches and compromises of information. Companies such as Verizon and IBM conduct regular research in this area. Moreover, the Association of Certified Fraud Examiners issues an annual report on the extent of "occupational fraud," which is an excellent measure of insider fraud events. There are, however, numerous measurement problems that make it difficult to assess the true nature and size of the Insider Threat problem.

Lack of Definitions

There is a common misunderstanding of exactly what defines an Insider Threat. Most people narrowly define "Insider Threat" in the context of network activity. In other words, employee theft, fraud, sabotage, and physical violence are all left out of this definition. There is also a lack of consistent definitions between surveys and studies themselves, as each uses differing terminology related to Insider Threat *incidents, events,* and *breaches*. Verizon and IBM for example, focus on *breaches* and *attacks* and narrowly define these as confirmed disclosures of data to an unauthorized individual or identified IP address. For our purposes, an Insider Threat is *anyone—including employees, partners, and third-party contractors—who, with authorized access, intentionally or unintentionally compromises an organization's assets.*

Lack of Reporting Requirements

Lack of reporting requirements is another factor. Healthcare, GDPR, and other breach notification reporting requirements exist, but there are no requirements for specifically reporting Insider Threat events.

Underreporting

There is a consensus that most Insider Threat activities are largely underreported and often undetected, both inside an organization as well as to external sources. There is also a general consensus and many incentives to "keep quiet." Most companies do not disclose publicly or pursue criminal charges for this reason.

Limited to Network-centric Actions

Insider Threat also tends to be lumped in with studies examining computer intrusions. This leads to a network-focused context that ignores a sizable component and source of Insider Threat activity: in-network activity.

What Do Surveys Tell Us About Insider Threats?

A Large and Growing Problem

According to surveys,[3] Insider Threat is a growing problem. Most companies have experienced an increase in Insider Threat incidents, with most organizations experiencing more incidents within the last year.[4] Surveys also suggest organizations are not prepared to prevent, detect, or manage Insider Threats.[5] Organizations are increasingly implementing controls to monitor Insider Threats and user behavior.[6] Organizations also feel highly vulnerable to insider attacks. Surveys routinely highlight that greater than 90% of organizations feel vulnerable or highly vulnerable to insider attack.

Willingness to Engage in Threat Activities

Surveys also highlight the willingness of insiders to engage in threatening activity. According to a study by Osterman Research, 69% of employees retain confidential data (corporate strategy documents and IP are the most cited) upon leaving the organization, with other studies show over 85% engaging in this risky behavior (Deloitte 2016). This figure jumps to 90% when the employees are fired or involuntarily separated from the organization (Deloitte 2016). Moreover, nearly half of these individuals intend to use the data to advance their careers in their new jobs. Furthermore, 62% believe it is acceptable to transfer work documents to personal devices or online sharing applications, which further increases risk.

What does actual data tell us?

The terminology used by studies such as those conducted by Verizon[7] and IBM[8] sometimes make it difficult to understand the prevalence of Insider Threat events. For example, according to Verizon's study, only

[3] 2018 Insider Threat Report, Cybersecurity Insiders

[4] Kaspersky — The Human Threat in IT Security (2018); CISCO 2018 Annual Cyber Security Report; 2018 Insider Threat Report, Cybersecurity Insiders

[5] Netrwrix 2018 Cloud Security Report; 2018 Insider Threat Report, Cybersecurity Insiders

[6] 2018 Insider Threat Report, Cybersecurity Insiders

[7] Verizon DBIR (2019), Verizon Insider Threat Report (2019)

[8] IBM X-Force Threat Intelligence Index 2018

34% of "breaches" are carried out by insiders.[9] This is a bit misleading, however, as a breach is defined by Verizon as a "confirmed" disclosure of data to an unauthorized party. A breach is thus much more easily ascribed to an outsider since, by definition, they are an unauthorized individual. Whereas an insider, by definition, has some level of authorized access, which results in much more difficulty proving a breach, as so defined. When one looks at "security incidents" more broadly (including those resulting from negligence and misuse), the level of insider involvement rises to 73%, according to Verizon.[10] (An incident is defined by Verizon as a security event that compromises an information asset.) The incident metric appears more reliable in determining the true level of Insider Threat involvement in a broad sense. According to IBM, the percentage of "attacks" carried out by insiders is 60%.[11] This initially seems straightforward; however, IBM defines an "attack" as a "security event that has been identified by network tools as 'malicious' and sourced to an IP address." This definition ignores unintentional Insider Threat events, as well as any Insider Threat event that cannot be sourced to an IP address. Thus, the true number of Insider Threat events is likely much greater than 60%.

By comparison, the Association of Computer Fraud Examiners (ACFE) in their 2018 report collected and analyzed 2,690 actual cases of fraud, which they defined as: "Corruption, Asset Misappropriation, and Financial Statement Fraud." This figure is larger than the total number of "breaches" reviewed by Verizon and further supports the conclusions that 1) insider involvement should encompass more than just incidents tied to network activity and 2) insider incidents are likely much higher than the IBM figure of 60%, since they limited their definition to "network-based attacks" and the great majority of the ACFE cases fall outside of this scope. Lastly, according to most research[12], the majority of external attacks are facilitated by insiders (negligence — phishing victims, improper security settings, etc.), meaning even traditional "external" attacks often have a large insider component.

[9] Verizon DBIR (2019)

[10] Verizon DBIR (2019)

[11] IBM X-Force Threat Intelligence Index 2018

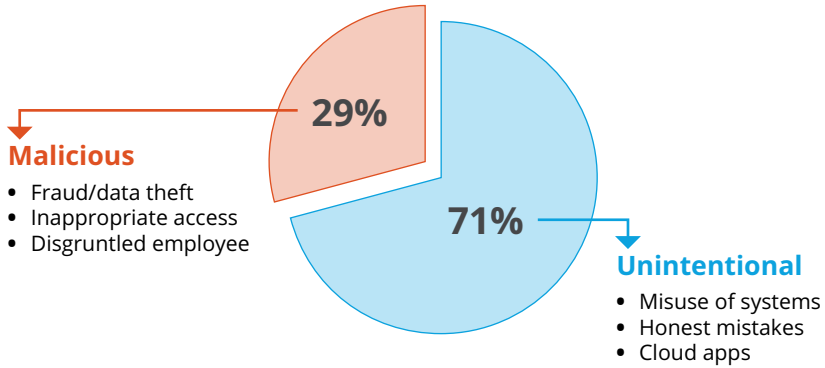
[12] Verizon DBIR (2019), IBM X-Force Threat Intelligence Index 2018

The Ultimate Guide to Building an Insider Threat Program

Insider Threats Are Real

Most experts agree that threats posed by insiders are a pervasive and growing problem. Employees continue to be the biggest threat to corporations[13] and cause twice as much damage as external threats.[14] In fact, roughly two-thirds of all security events are caused by insiders.[15] The great majority of these, however, are caused by unintentional Insider Threats.[16] Unintentional threats are, however, difficult to detect because traditional security devices and solutions are primarily designed for detecting malicious activities.

Figure 2: Insiders Are Responsible for 90% of Security Incidents



Sources: Verizon 2015 Data Breach Investigations Report
Kaspersky Lab 2016 Security Risks Special Report

[13] Kaspersky — The Human Threat in IT Security (2018); CISCO 2018 Annual Cyber Security Report; 2018 Insider Threat Report, Cybersecurity Insiders

[14] CERT Insider Threat Center

[15] Verizon DBIR 2019 (combining the categories of "privileged misuse," "miscellaneous errors," "physical theft," and "everything else" categories pertaining to insider involvement); IBM X-Force Threat Intelligence Index 2018

[16] More than 2/3 of all Insider Threats are unintentional. Ponemon 2018 Cost of Insider Threat Report; Verizon DBIR (2019)

Both surveys and actual data studies confirm the existence of a formidable and sizable Insider Threat problem, the exact scope and size of which is difficult to assess for the reasons outlined above. Educated assessments, however, strongly suggest that insiders are responsible for the majority of security events.

Key Takeaways: The Insider Threat Problem

- Insider Threat is a growing problem, and one that is still not fully understood.
- Both surveys and studies suggest an increase in Insider Threat events.
- Data strongly suggests insiders are responsible for the majority of security events.
- Organizations feel highly vulnerable to Insider Threats.
- Few organizations have the necessary Insider Threat controls in place.

What Are the Impacts of Insider Threats?

Impacts refer to adverse effects an organization experiences as a result of a security event. These impacts, or adverse effects, generally fall into five categories: value, operations, reputation, culture, and liability.

Value

Value refers to the monetary qualities of the business. There are three categories of value: market value, intrinsic value, and revenue. Insider Threat events can have a direct impact on the market value of a business. For example, when the arrest of former Booz Allen contractor Harold T. Martin III was announced, Booz Allen's share price immediately fell by 5%.[17]

[17] "NSA leak: Booz Allen shares drop on arrest of contractor," https://money.cnn.com/2016/10/05/investing/nsa-leak-booz-allen-hamilton-stock/index.html

Another example involved an auditor for NCI Inc. who embezzled $18 million. Upon public disclosure of his arrest, the stock plunged 10%.[18]

Insider Threat events can also have a direct impact on the intrinsic value of a business, since intellectual property comprises 50% to 80% of the business's value.[19] Theft of new product designs and strategies, for example, can have catastrophic consequences for many types of businesses.

Insider events can also directly impact revenue. The intellectual property theft at American Superconductor immediately resulted in the loss of $800 million in revenue.[20] According to Cisco[21], nearly one-third of businesses that suffered a breach lost more than 20% of their revenue. That's real money!

Operations

Operations refers to the ability of a business to execute its mission. There are three general categories of operational impact: operational disruption, increased overhead, and remediation costs. Operational disruption is difficult to quantify but includes unplanned expenses, increased staffing, inability to deliver goods and services, and excessive or new R&D costs. A detailed study by Deloitte[22] estimated that for a large company that suffered intellectual property theft, the five-year operational disruption cost would be a whopping $1.2 billion! Increased overhead due to necessary cyber security improvements, staff retraining, etc. also impact business operations and can exceed $13 million for a large corporation.[23]

[18] "NCI controller accused of embezzling $18M over six years," https://washingtontechnology.com/articles/2017/01/23/nci-embezzlement.aspx

[19] The Commission on the Theft of American Intellectual Property (IP Commission, http://www.ipcommission.org/

[20] https://www.csoonline.com/article/3256305/sinovel-wind-group-found-guilty-of-ip-theft-valued-at-800-million.html

[21] Cisco 2018 Cost of Data Breach Study

[22] "Beneath the surface of a cyber attack," https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-beneath-the-surface-of-a-cyber-attack.pdf

[23] Id.

Introduction

Reputation

Reputation, although difficult to quantify, is often the second most affected aspect of the business following a compromise — second only to value. Reputation impact can be assessed by examining three areas: public relations expenditures, customer relationships, and the devaluation of trade names. According to Cisco, half of organizations that were breached expended significant resources to actively manage their reputation, and 42% of them lost nearly 20% of their existing customer base.[24] Moreover, a detailed study by Deloitte uncovered that new customer acquisition decreased by as much as 50%. The study also revealed that large companies spent an average of $1,000,000 during a 12-month period to restore their reputations.[25] The same study revealed a large company could experience an impact of $250 million over a five-year period due to the devaluation of its trade name alone.[26]

Culture

Culture is often ignored when Insider Threat incident impacts are discussed. However, culture is the lifeblood of any organization. Culture encompasses the shared values, norms, beliefs and assumptions that ultimately drive employees' actions. According to the Society for Human Resource Management, typical businesses experience 24% turnover each year and most employees only stay 4.5 years in a position.[27] Millennials have even shorter tenures, at two years on average. This results in financial and logistical problems, but also data protection problems. As previously stated, most employees intentionally take confidential data with them when they leave, and most will seek to use this to the detriment of the organization. Add a significant corporate event, such as a data breach, to this equation, and the impact on culture is dramatically magnified. This can result in additional turnover, increased distrust, and an erosion of morale, all of which can exacerbate the effects of a breach. In short, culture shapes everyday employee behavior, and a bad culture will lead to bad behavior.

[24] Cisco 2018 Cost of Data Breach Study, "Beneath the surface of a cyber attack," Deloitte (2018)

[25] "Beneath the surface of a cyber attack," Deloitte (2018)

[26] Id.

[27] Job Satisfaction and Engagement Study, https://www.shrm.org/ResourcesAndTools/business-solutions/Documents/2015-job-satisfaction-and-engagement-report.pdf

The Ultimate Guide to Building an Insider Threat Program

Key Takeaways: Impacts

- Insider Threats can have a profound impact on an organization.
- Beyond the lost value of affected assets, organizations can suffer immediate losses of intrinsic value or revenue.
- The ability to deliver goods and services may be adversely impacted.
- There may be significant damage to reputations — both corporate and individual.
- An insider event may adversely impact the culture of an organization.

Liability

Liability refers to the external costs that are levied on an organization. Liability costs include compliance fines, breach notification costs, increased insurance costs, and litigation costs including attorney fees. These costs can be large, ranging from $20 per record per customer breach, to $3 million in litigation costs, up to a 200% increase in insurance costs, and fines that can exceed $1 million and significantly more for violations of GDPR.[28] Moreover, litigation settlements can exceed tens of millions of dollars for large breaches.[29]

[28] Cisco 2018 Cost of Data Breach Study, "Beneath the surface of a cyber attack," Deloitte (2018)

[29] Id.

Introduction

GDPR

There are two tiers of administrative **fines** that can be levied as penalties for **GDPR** non-compliance

- Up to €10 million, or 2% annual global revenue — whichever is higher or
- Up to €20 million, or 4% annual global turnover — whichever is higher.

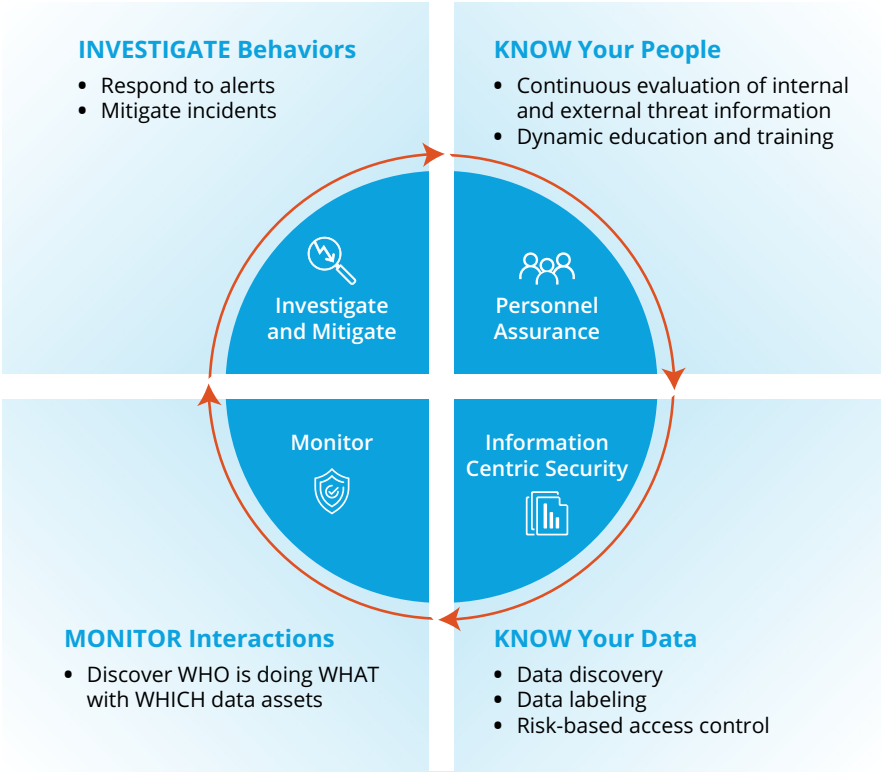
The GDPR imposes stiff fines on data controllers and processors for non-compliance. Fines are administered by individual member state supervisory authorities. The following 10 criteria are to be used to determine the amount of the fine on a non-compliant firm:

- **Nature of infringement:** number of people affected, damaged they suffered, duration of infringement, and purpose of processing
- **Intention:** whether the infringement is intentional or negligent
- **Mitigation:** actions taken to mitigate damage to data subjects
- **Preventative measures:** how much technical and organizational preparation the firm had previously implemented to prevent non-compliance
- **History:** past relevant infringements, which may be interpreted to include infringements under the Data Protection Directive and not just the GDPR, and past administrative corrective actions under the GDPR, from warnings to bans on processing and fines
- **Cooperation:** how cooperative the firm has been with the supervisory authority to remedy the infringement
- **Data type:** what types of data the infringement impacts
- **Notification:** whether the infringement was proactively reported to the supervisory authority by the firm itself or a third party
- **Certification:** whether the firm had qualified under approved certifications or adhered to approved codes of conduct
- **Other:** other aggravating or mitigating factors may include financial impact on the firm from the infringement

Insider Threat Management

Insider Threat Management[30] involves the *holistic* focus on managing risks that insiders pose to your corporate assets. This requires an ITMP that is free from the traditional walls between "security" (personnel-focused) and "InfoSec" (network-focused). It requires a unity of purpose, which is designed to objectively manage insider risk. The required *holistic synergy* is depicted in the following chart.

Figure 3: How to Effectively Manage Insider Threats



[30] The terms "Insider Threat management" and "insider risk management" are used interchangeably throughout the Guide. "Insider Threat management" is the colloquial term generally used to describe managing risks related to employees. Risks, however, include components of both threats and vulnerabilities of specific corporate assets. Thus, it is arguably more accurate to describe the managing of Insider Threats as "insider risk management," but for clarity purposes this Guide will use them interchangeably.

You must KNOW YOUR PEOPLE. What does it mean to "know your people?" In the context of insider risk management, it means having the knowledge necessary to make meaningful decisions about your employees. Too often, the sources of this knowledge are limited to pre-screening background checks and/or monitoring network behavior. The problem is that pre-screening background checks are often wholly inadequate, due to their limited scope. For example, many background providers simply check "national criminal databases" which are not regularly updated nor verified for accuracy. These "national" databases may be six months or more behind in reflecting a conviction.

Moreover, focusing only on network behavior ignores a large portion of an individual's work-life picture. Employees are much more than the sum of their network activity. As such, focusing solely on this activity misses a large portion of their otherwise relevant and valuable behaviors on other mediums. For example, off-network behavior (activity on endpoints or in-person interactions with co-workers, supervisors, and customers at work) as well as external behavior (publicly available information, e.g. social media, public records, etc.) is just as valuable, if not more so in certain cases.

There may be certain organizational sensitivities that preclude you from acquiring all of the information that pertains to your employees. This is understandable and requires a delicate balance between employees' expectations of "privacy" and productivity versus security. The important takeaway to consider and convey to senior leadership is, if you do not have full visibility into all areas of personnel assurance, you will either need to account for this gap through some other means or accept this risk and attempt to mitigate impacts if and when they arise.

You must UNDERSTAND INSIDERS' *BEHAVIOR*. Knowing how people behave when interacting with corporate data, services, and applications is crucial for evaluating the risk and likelihood of an Insider Threat. Establishing comprehensive visibility into user and data will provide unequivocal proof during the investigation process, as well as significantly reducing the end-to-end investigation time.

Monitoring is a key component, because comprehensive visibility into user and data activity is necessary to detect and prevent Insider Threats and to make risk-based decisions to mitigate those threats. Without comprehensive visibility, your organization is simply more vulnerable to Insider Threats, whether malicious or unintentional.

Monitoring includes "network monitoring," for example logs and related events via a Security Incident Event Management (SIEM) tool, but also includes monitoring user activity via a User Activity Monitoring (UAM) tool that captures all keystrokes and may include Data Loss Prevention (DLP) and other policy enforcement features. Monitoring also includes the ability to observe behavior indicative of Insider Threats via off-network behavior as well as via external information.

You must MITIGATE RISKY BEHAVIORS. As mentioned, an important objective of any ITMP is to mitigate the risk of an Insider Threat, so a proactive approach is a key component. Clear security polices and the ability to deter as well as raise security awareness at the point of violation has been proven to be the most effective way to reduce insider risk

You also need the ability to investigate incidents after they have taken place. Investigation must be integrated with all other objectives in a synergistic manner. Too often, investigation is bifurcated and viewed as a mutually exclusive component of a security or info-security program, which leads to silos and inefficiencies. To be effective, an investigation needs context. This can only be achieved through the proper alignment with all objectives within an overall ITMP strategy.

Quite simply, the investigative role should reside with the ITMP team, not within a separate CSO or CISO function. To be effective, an investigative team must possess cross-functional capabilities to 1) obtain necessary information 2) analyze cross-domain information and 3) leverage necessary resources to further the investigative effort.

Additionally, an important objective of any ITMP is to mitigate the risk of an Insider Threat, so a proactive approach is a key component. Clear security polices, regular policy training, and the ability to deter as well as raise security awareness *at the point of violation* has been proven to be the most effective way to reduce insider risk.

The Insider Threat Management Ecosystem

Accomplishing the stated objectives requires the alignment of various security functions and components into a unified ecosystem. A holistic ITMP will help foster this ecosystem and help your organization guard against Insider Threats. A formal program will assist with integrating traditional security and information security objectives and aligning those objectives with business priorities. A holistic ITMP includes ten primary components that range from background checks to user and data activity monitoring to incident investigation and response.

A holistic ITMP combines personnel assurance and information-centric security principles. The key objective is to monitor, audit, and understand the insider's interaction with systems and data. Different insiders will have access to different types of information, resulting in differing risk profiles. Thus, the focus, which will evolve over time, needs to be dynamic and attuned to how these different groups interact with (access, use, and store) the digital assets. Accomplishing this goal requires a paradigm shift and a new approach — The Insider Threat Management Ecosystem.

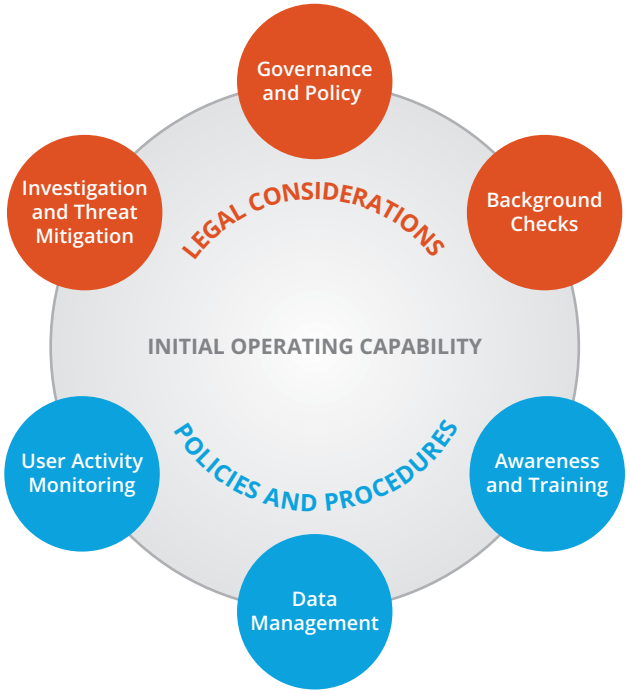
What constitutes an *Insider Threat Program*?

This answer is best understood in the context of an Initial Operating Capability (IOC) and Full Operating Capability (FOC). IOC is the minimum baseline and includes: Governance, Background Checks, Training, UAM, Data Management and Investigation. This should be easily obtainable by most organizations with a reasonable amount of resources. FOC will require a greater amount of resources to implement the remaining ecosystem components. Accordingly, organizations can achieve this end-state by systematically applying the methodologies described herein.

Initial Operating Capability

While a *full operating capability* may take years to develop, immediate value can be achieved by developing an *initial operating capability*, legally supported with documented policies and procedures, as described in Figure 4.

Figure 4: Insider Threat Management — Initial Operating Capability



User and Data Activity Monitoring

Even trustworthy employees need to be monitored to ensure they do not unintentionally engage in harmful conduct. As such, organizations need more than simply a tool to monitor "bad actors." They require a tool that compliments the other components of a program and serves as a force multiplier by 1) alerting employees of potentially harmful actions and policy violations 2) alerting about intentionally harmful actions 3) maintaining immutable logs and video recordings to support subsequent forensic investigations and prosecutions. A comprehensive Insider Threat management platform is also the only solution that provides you with the most important objective: comprehensive visibility regarding user and data activity.

Legal Considerations

Some legal issues may arise when attempting to implement an Insider Threat management solution. This should not, however, deter you, as the benefits far outweigh the effort required to appease your lawyers. Some of the most prominent issues that you will encounter include:

- **Consent.** Do you have consent to monitor your employees? Do you need consent?
- **Scope.** Whom will you monitor? Everyone? Only a subset of employees?
- **Agreements.** Do you have the necessary employment agreements in place?
- **Policies.** Do you have documented support for the monitoring program?
- **Compliance.** Do you have a "watch the watchers" program in place?

INSIDER INSIGHTS: Where DLP and UAM Tools Fall Short

Most organizations lack real visibility into user actions because they fail to properly deploy and leverage UAM and DLP tools because they are difficult to set up and time-consuming to maintain. This creates a critical vulnerability and gravely impacts an organization's ability to detect, prevent, quickly respond to, and mitigate Insider Threats. Legal and privacy impediments are often cited as inhibiting factors for the greater use and leverage of monitoring technologies. There are, however, established best practices to effectively implement monitoring technologies while respecting legal and privacy requirements.

COMMON GAPS

- Monitoring policies and procedures are vague and unnecessarily restrictive.
- Removable media is not properly managed, monitored, or audited.
- UAM tools are not fully deployed and leveraged to detect Insider Threat activity.
- DLP tools are not fully deployed and leveraged to detect Insider Threat activity.
- Privileged users and those with access to critical assets are not subject to enhanced monitoring.
- Admin rights for all creates unnecessary vulnerabilities.
- Limited bring-your-own-device (BYOD) monitoring and remote worker policies.
- Tools are not properly tested and evaluated prior to deployment.
- CISO and CSO have failed to take proper ownership of monitoring.

The Ultimate Guide to Building an Insider Threat Program

Background Checks

Background checks represent the baseline personnel assurance component for an Initial Operating Capability (IOC). Whereas continuous evaluation should be the objective, and thus represents a Full Operating Capability (FOC) component, a background check has been the standard proactive solution for many years. A comprehensive check from a reputable provider can uncover indicators of potential workplace violence or indicators of Insider Threat precursors that will allow you to make more knowledgeable hiring decisions, in accordance with requisite legal authorities. That said, background checks are often limited in scope, and it should not be assumed that just because someone passed a background check they will never become an Insider Threat. Additionally, background checks are often seen as a one-and-done endeavor, when in reality periodic checks can lead to insights into shifts in employee behavior, financial distress, and other factors that could indicate an Insider Threat or a potential for one to develop.

Awareness and Training

Your people are the first line of defense against Insider Threats. While there will be basic security awareness and training information that is applicable to all insiders (employees, partners, and contractors), you should strive to tailor it to the tasks of their specific roles and accesses. The goal should be to take your users beyond mere awareness of security policies and issues, and truly educate them. They should be instructed in the why and how to assess the risk and security implications of various situations. You should verify that they know how to apply security best practices as they perform their job duties on a daily basis.

Training Resources

There are an increasing number of Insider Threat training instructors that can provide these services. The Insider Threat Training Academy (www.insiderthreattraining.com) has a wealth of educational material and training programs that can be utilized. The best training is always taught by true Insider Threat practitioners who have real-world expertise.

Introduction

An effective security training and awareness program will cover the following areas:

- Counterintelligence and security fundamentals
- Cybersecurity policy awareness and best practices
- Procedures for conducting Insider Threat response actions
- Applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information
- Applicable legal, civil liberties, and privacy policies
- The importance of reporting suspected risky activity to the Insider Threat team
- Methodologies of adversaries to recruit trusted insiders and collect sensitive information
- Indicators of Insider Threat behavior and procedures to report such behavior
- Regulatory and security reporting requirements

INSIDER INSIGHTS: Security Awareness Training

A majority of organizations lack formal training on workplace security policies, expectations, and parameters. Onboarding should include more substantive security topics and be delivered during orientation as well as ongoing updates / refreshes. While many organizations have training platforms, they often require the affirmative action of employees to find and review the material on their own time. This self-guided study requirement is ineffective, as it is only enforced by line-managers on an ad hoc basis.

COMMON GAPS

- Privileged users do not receive special training regarding roles and responsibilities.
- Lack of substantive training during onboarding and ongoing.
- Lack of formal training program for Insider Threat management personnel.
- Employees are not informed and trained on Insider Threat impacts, behaviors, and indicators.
- Training for contractors and partners with access to key data and systems is often minimal
- Lack of substantive annual training requirements.

The Ultimate Guide to Building an Insider Threat Program

Governance and Strategy

The purpose of the Insider Threat strategy is to combine the personnel assurance and information security disciplines into a unified and holistic information- and people-centric security framework. Unification will promote more robust tactics, techniques, and procedures to reduce the impact and consequences when a compromise occurs. It will also provide more granular optics into the risk posture of the organization. The policies and procedures are the official enterprise statements of authority and guidance and keep the enterprise in compliance with legal, privacy, and organizational objectives.

INSIDER INSIGHTS: Governance and Strategy

Most governance frameworks consist of separate and siloed functional components. Further, Insider Threat itself lacks definition of both scope and functionality, resulting in ambiguous roles and responsibilities. Current "Insider Threat management" processes and governance structures are largely defined within the context of investigative processes. This leads to a myopic and narrow strategy focused on responding to known threats and events, which is an overly reactive strategy.

COMMON GAPS

- Lack of Insider Threat Management framework.
- No formal Insider Threat management program governance structure.
- Insider Threat strategy is not well defined and communicated.
- Insider Threat management roles and responsibilities are not established, coordinated and aligned with governance structure.
- Legal and regulatory requirements regarding Insider Threat, including privacy and civil liberties obligations, are not fully understood and communicated.
- Governance and threat management processes do not adequately address Insider Threats.

Introduction

Investigation

Once a threat has been identified, it must be investigated and addressed. Mitigation can be as simple as the CISO, HR, and General Counsel interviewing an employee who has displayed suspicious behavior to determine if further action is required. It may also be as involved as an automated and integrated process for monitoring and alerting an analyst of suspicious behavior. A comprehensive Insider Threat management platform is particularly valuable for these types of investigations. In addition to alerting to suspicious behavior, an Insider Threat management platform provides detailed timeline-based logs or optional on-demand video-like playback of the user's session, which makes investigations easier and significantly more efficient.

INSIDER INSIGHTS: Investigation

Once a security alert is attached to an anonymized or named user, most organizations leverage existing resources to examine the user's actions and Insider Threat indicators to determine the level of threat. Identified threats are generally handled in accordance with established policies, existing business objectives, and legal parameters. The investigative capability is, however, limited by the level of authorized methods and tools. A more expansive toolset enables more effective investigations and supports a proactive strategy.

COMMON GAPS

- Lack of feedback loops and collaboration between Security Operations Center (SOC) analysts and investigators.
- Investigative strategies need to be more proactive; many are limited to DLP alerts or referrals.
- Collaboration with HR, legal and compliance is often ad hoc and informal.
- Lack of iterative learning model.

Full Operating Capability

FOC includes all of the IOC components and adds those related to: Personnel Assurance, Access Control, Analysis, Dynamic Risk Assessment, and Oversight. FOC components will require more time and resources to implement, but this guide will show you how to accomplish this in the most efficient manner possible. The hallmark of FOC is a more robust, information-centric and personnel assurance model that builds upon the

IOC components. Organizations may have some components in place and may choose to prioritize others under an IOC model. Regardless, the focus is on achieving the objective of robust insider risk management, not the dogmatic and ordered application of any particular component.

Figure 5: Insider Threat Management Ecosystem

*Of the ten components, those shaded in black represent an "initial operating capability" level for a holistic Insider Threat management program. The objectives (e.g. the ability and capability to **prevent, deter, detect**, and **mitigate**) are what is of importance, not dogmatic form and function.*

Personnel Assurance — Continuous Evaluation

Pre-employment screening and continuous evaluation are the foundations of the personnel assurance component of the Insider Threat ecosystem. A proper personnel assurance capability will not only alert to past relevant activity but should also provide information capable of informing organizations of potential future problems that may impact critical assets.

Current processes are snapshots and apply binary methodologies[31] to determine suitability. As a consequence, the ability to *continuously evaluate* employees is of greater importance. While the screening processes (background checks) are largely completed by third parties, the continuous evaluation portion can be implemented by the organization itself through a proper alignment and collaboration of internal entities. The focus must be on developing the ability to continuously evaluate both internal and external sources for possible threat and vulnerability information in a *risk-based manner*.[32]

Legal Considerations

The Fair Credit Reporting Act (FCRA) governs background investigations and prescribes rules for collection, use, and retention of personal information. Ensure that your provider is FCRA compliant and that you comport with its handling and use requirements.

INSIDER INSIGHTS: Personnel Assurance

Most organizations employ effective background investigation processes for full-time employees. Contract personnel and partners, however, do not receive the same level of vetting and, in most cases, are not vetted prior to being granted access. There is also a general lack of employee accountability that appears to be grounded in the lack of substantive onboard training. Lastly, visibility into employee behavior could be enhanced through more formal collaboration between HR and Security.

COMMON GAPS

- No or limited vetting of contractors and partners.
- Limited visibility into personnel behavior once onboard.
- Lack of employee accountability.
- Lack of effective messaging regarding threat.
- Termination procedures lack security effectiveness.
- Onboarding and offboarding procedures are too reliant on line-managers.
- Policy frameworks are fragmented and incomplete.

[31] Current processes and standards focus largely on what is easily measured and therefore more easily "evaluated" (e.g. criminal conviction, drug use, "yes/no").

[32] One of the major shortcomings of traditional personnel assurance models and programs is that they treat all employees as a single homogenous group. This is, of course, illogical and fails to, among other deficiencies, account for the differing accesses and capabilities of certain groups and individuals to inflict harm upon an organization.

The Ultimate Guide to Building an Insider Threat Program

Access Control

Insiders should have access to only those information assets for which they 1) have a need-to-know based on the role and duty and 2) that fall within the parameters of their risk profile. The integration of this analysis with data use provides real-time information for the Insider Threat management mission. Identity and Access Management (IAM) technology is the foundation of any strong access control and management strategy. The IAM industry is evolving into new products and services focused on monitoring and controlling access for "privileged users." The combination of user and role, identity, and data object-level access control provides granular control capability, thereby greatly reducing the potential impact of an insider data breach. The enterprise can achieve a higher trust level only when authenticated and authorized users are on the network and systems with logical access controls. This role-based access control (RBAC) approach can be considered for use as an enterprise solution for both on-premise system data or with a managed cloud-based service.

INSIDER INSIGHTS: Access Control

Access control processes and tools are generally effective, but implementation of some policies creates unnecessary vulnerabilities; foremost of which is granting all users local administrative rights, by default, on organization-issued computers. Access control implementation is, however, often too federated, with line managers solely responsible for a large portion of data group creation and access grants.

COMMON GAPS

- Too many users are granted administrative privileges and use is not fully understood.
- Access control is too federated.
- Accesses are not properly removed or disabled on a consistent basis.
- Role Based Access Control (RBAC) not widely used.
- Large number of Active Directory groups in some organizations nearly double the number of employees.
- Contractor accounts are less controlled and monitored than other accounts.
- The number of privileged users with super-user access is not fully understood.

Analysis

Traditional analytic methods fail to address the sheer volume of data generated by today's information systems. Deep and continuous user and data activity monitoring, enabling analysts to build context around events and incidents, should be employed to make sense of all available information on an insider's behavior.

INSIDER INSIGHTS: Analysis

Most large organizations deploy analytic resources to hunt for threats on the network and analyze log files with SIEM solutions. These efforts notwithstanding, most Insider Threat analytic efforts suffer from a lack of datasets to analyze. Fully deploying user and data activity monitoring will foster greater analytic maturity and promote a more proactive Insider Threat strategy.

GAPS

- Lack of analytic strategy.
- Lack of available data sets to analyze.
- Limited use of data analysis technology, organically within the DLP or UAM toolset or through the use of UEBA solutions.

Insider Risk Assessment

Insider risk assessment is a process that continuously and dynamically adjusts insider risk scores. An organization can achieve part of this objective through the implementation of an Insider Threat management platform that can assist analysts by triaging alerts based on general risk rankings. This can then be supplemented by regular insider risk assessments.

The objective is to obtain the most current and accurate risk information on your users. This will allow you to make more informed business decisions while also supporting a risk-based access control model. This moves the emphasis to proactive management solutions and away from simply responding to events and incidents as they arise.

INSIDER INSIGHTS: Risk Assessment

Most organizations' Insider Threat assessment capabilities are limited to specific and narrowly defined use cases and are best described as ad hoc and reactionary. A bona fide Insider Threat capability requires a thorough understanding of the organization's critical asset threat factors, the organization's insider population, and the existing vulnerabilities of certain types of data and systems. Once implemented, a mature Insider Threat assessment capability will enhance security awareness and support both reactive and proactive strategies, as well as foster greater enterprise threat management.

COMMON GAPS

- Crown jewels have not been identified.
- Lack of Insider Threat assessment strategy.
- Organization's Insider Threat tolerance has not been determined or clearly expressed.
- Organization does not adequately assess Insider Threat.

Oversight and Compliance

A fundamental tenet of the Insider Threat ecosystem model is to incorporate an iterative learning capability. This can only be accomplished through proper oversight and compliance that measures performance using appropriate metrics. This is more than simply conducting an impact analysis after a breach or related incident. The goal is to continuously learn from mistakes while striving to improve upon the successes of the program. Constant evaluation is key to "staying on course" and will provide continued legitimacy and efficiency to the program.

Legal Considerations

Greater access to sensitive information requires more safeguards and procedures for protecting this information. Failure to properly protect this information can expose your organization to liability. Implement best practices to ensure information is collected, stored, and used properly.

A key aspect of an Insider Threat management oversight component is the "watch the watchers" program. The ITMP will collect, retain, and use extremely sensitive employee information. Despite the ability to anonymize this data, policies and procedures must be documented and implemented to ensure information is properly safeguarded. Nothing will impact the continued viability and resources of your program more than abuses of this power and authority — intentional or unintentional.

INSIDER INSIGHTS: Oversight and Compliance

Oversight of Insider Threat management functions and activities are generally shared between the CSO, CISO, CPO, and legal. A lack of a defined ITMP creates an activity- or issue-centric oversight model that creates inefficiencies and lack of operational enablement. A clearly defined ITMP with established roles and responsibilities will foster operational enablement, as well as create a more effective oversight and compliance framework.

COMMON GAPS

- Lack of formal oversight and compliance processes and procedures.
- Personnel are not assigned to oversight and compliance roles and responsibilities.
- Insider Threat analysts and investigators are not formally monitored ("Watch the Watchers").
- Insider Threat requirements, laws, and regulations are not fully understood and communicated.
- Lack of procedures for non-compliance.
- Insider Threat stakeholders are not trained on requirements and standards.

Key Considerations

Cybersecurity Culture

What is the security culture of your organization? This is an important threshold question to ask, because the answer will inform your overall Insider Threat management strategy going forward. Some questions will help frame this answer.

- What are the current security expectations of your workforce?
  - > Do you have a robust security awareness program?
  - > Do you have security policies in place?
  - > Do your employees understand the importance of security to the organization?
- How would an Insider Threat management program be viewed by your employees?
  - > Part of their job?
  - > An "invasion of privacy"?
  - > A necessary means to protect the company?
- Have you recently experienced a data breach or other type of security incident?
  - > What was the effect on employee morale?
  - > Can this be a catalyst to support the program?

Balancing Privacy and Security: Legal Considerations

A foundational theme that permeates this entire strategy is the balancing of privacy and security. The former includes ensuring users are not subjected to invasive intrusions that breach their reasonable expectations of privacy. The latter involves protecting organizational assets — including people, information, facilities, intellectual property, and brand reputation. Each must be viewed symbiotically, as both are essential components of an effective ITMP. Privacy policies must not be overly restrictive, but rather must strike the proper balance between protecting employees without unnecessarily restricting legitimate and tailored security efforts. Similarly, security must be tailored and should pursue a "least restrictive means" methodology to strike the proper balance between protecting the organization's assets without unnecessarily impacting legitimate privacy interests of employees. These should be viewed as complimentary, not competing, interests. Let's explore each in detail.

Privacy

The primary data privacy regulations impacting businesses are The General Data Protection Regulation (GDPR)[33] and the California Consumer Privacy Act (CCPA)[34]. Each regulation has far reaching impacts around the world as companies either have customers in the EU and California or are based there or both. Generally, compliance with each of these privacy standards requires thinking through the following concepts:

- Data collection
- Data retention
- Data movement
- "Right to Forget"

[33] The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy for all individuals citizens of the European Union and the European Economic Area. It also addresses the export of personal data outside the EU and EEA areas

[34] The California Consumer Privacy Act (CCPA) is a bill that enhances privacy rights and consumer protection for residents of California, United States. The bill was passed by the California State Legislature and signed into law by Jerry Brown, Governor of California, on June 28, 2018, to amend Part 4 of Division 3 of the California Civil Code. Amendments to the CCPA, in the form of Senate Bill 1121, were passed on September 23, 2018.The CCPA becomes effective on January 1, 2020.

- Audit/Watchdog mechanisms
- Protection mechanisms to maintain confidentiality
- Obtaining user consent

What exactly is "privacy"? At its core, privacy is the right to be left alone. In the United States, it is understood that residents are to be free to conduct our lives without fear of intrusion into our personal affairs. This includes our homes, our communications, and our personal information. There are limits, of course. Knowingly exposing information or actions to the public would not support a claim of privacy. Thus, in our private capacities, we generally have the right to keep people out of our homes and free from observing our personal communications. In the employment context, however, the paradigm is different. In this context, businesses have legitimate needs to protect their people, information, and facilities. In the U.S., employers generally possess a legal right to collect personal or private information if it is stored or transmitted over employer networks or devices and in support of a legitimate business interest.[35] Consequently, in the employment context, its most often the "use" of collected information that potentially implicates privacy concerns.

The two general common law privacy rights are "intrusion upon seclusion" and defamation or "false light." The former protects employees from intrusions by employers upon areas where the employee has a "reasonable expectation of privacy." As discussed, a proper consent banner and user agreement will generally make the employee's use of corporate devices and networks open to monitoring by the organization. The latter (defamation or false light) protects an employee from unsubstantiated accusations that impugn the character and integrity of the employee. Consequently, the employer's use of collected information must be closely guarded to ensure proper treatment and handling by the Insider Threat team. For example, disclosing investigation details or results of computer monitoring beyond the Insider Threat team will risk creating liability for the company if negative information is disseminated beyond those who need to know.

[35] GDPR requires a legitimate business reason to collect user information stored or transmitted over employer networks and devices. While the U.S. doesn't have a similar federal regulation, CCPA coming into effect in 2020 will have similar intent to GDPR. Cybersecurity and protecting other users' data from compromise is a recognized legitimate business interest. (See Electronic Communication Privacy Act of 1986).

Security

Security interests of employers are well-established. Employers have the right to protect people, property, information, and facilities in manners that support a **"legitimate business interest"**. They have rights, but also obligations and duties of care. It's undisputed that an employer has the right to protect its property, but employers also have the duty to protect their employees from harm, and failure to do so can result in liabilities. Similarly, failing to protect certain "property," especially customer data (PII, PHI, etc.) can also result in liability to the employer. So, there is a strong interest that courts and the government have recognized in employers protecting their business interests. These interests are, however, not without limits. Viewing legal considerations in the context of the primary Insider Threat objectives provides a useful construct to understanding the legal equities that apply to all Insider Threat programs.

The Overlap of Privacy and Security

To put a finer point on the matter, online privacy is the idea that users should have the freedom to avoid unauthorized intrusion into personal data online; the ability to protect sensitive, personally identifiable information from being collected, stored, or misused without consent.

Cybersecurity is about maintaining the confidentiality, integrity and availability of organizational assets and customer data — including people, information, facilities, intellectual property, and brand reputation.

The need to protect online privacy involves using cybersecurity processes and tools, while many regulations in the U.S. and in Europe now require protecting customer and user data as part of cybersecurity compliance.

Thus, online privacy and cybersecurity are very intertwined.

Know Your People

Knowing your people is often about "preventing" harmful actions from occurring or implementing prophylactic measures to detect potentially harmful activities. So how much are employers legally allowed to "know their people"?

Background Investigations

Employers have the right to hire trustworthy employees and, in certain cases, duties to conduct investigations (such as in industries like finance, healthcare, childcare, trucking, etc.). Investigations may be quite broad and involve interviews with former employers and references. However, most are typically limited to the last seven to 10 years due to restrictions on obtaining and using criminal conviction information. Employees also have rights, however, which are governed by the Fair Credit Reporting Act (FCRA) that requires employers to 1) give employees notice 2) obtain consent 3) allow them to correct inaccurate information and 4) provide notice if information used from a FCRA check will be used against them.

Agreements

Most states abide by "at-will" employment laws, which afford employers the ability to make user activity monitoring, among other types of monitoring, a condition of employment. Most states do not require employers to obtain employee "consent to monitor," although it is a best practice to do so.

Policies and Training

It is increasingly important to have clear security policies and training programs. These set the tone of the company culture and create transparency while promoting understanding of boundaries. Documentation of policies can be used as evidence to show knowledge and training in support of discrimination and unlawful termination lawsuits. Additionally, policies are important for setting standards and objectives for the monitoring program.

Obtain Visibility: How?

Employers may lawfully use video or CCTV to monitor employees, contractors, and partners in common workspaces from which they have a lawful vantage point, meaning they are not allowed to videotape intimate areas such as: locker rooms, bathrooms, and changing areas. Employers may also record audio of employees under certain circumstances, although there are many more restrictions than for video monitoring. For example, some states require two persons to consent to monitor a conversation, which would prevent most monitoring without the explicit

consent of the other party. Those employers who monitor phone calls and other employee actions must do so with explicit consent.

Employers may also monitor external publicly available data sources, such as criminal databases, social media, court filings, and other electronic information. Furthermore, employers may monitor their networks and devices for **"legitimate business interest"** that include the protection of people, property, information, and facilities. Such monitoring generally involves obtaining the consent of employees in the form of a computer banner at login or a specific computer use agreement. Such consent gives employers wide latitude in collecting information traversing corporate-owned networks and devices.

When it comes to the "how," the following channels must be monitored:

- Desktop applications (e.g., Microsoft apps, downloaded apps & custom software)
- User actions (e.g., copy, cut, paste, mouse clicks, keystrokes)
- Web applications (e.g., CRM, finance, source control, corporate portals, databases, ERP, design tools, chat tools, cloud storage & collaborative platforms)
- Files & text (e.g., rename, download, upload, save, attach, move, delete)
- Exfiltration media (e.g., personal email, web apps, chat apps, social media, removable media & printers)

These channels should be monitored irrespective of whether the user is on the corporate network, guest Wi-Fi or working remotely.

Obtain Visibility: Who?

As discussed, employers are granted wide latitude to monitor corporate-owned networks and devices. Questions arise regarding *who* may be subject to such monitoring. For example, does everyone in the organization need to be monitored? Can subgroups within the organization be subject to greater monitoring? Can you monitor third parties who are not part of the organization but have access to key data and systems and are engaging in conversations with organization employees? The simple answer is that any information traversing corporate-owned devices or networks is subject to monitoring. As a result, third parties and other non-employees may be subject to this collection. This is where the difference between collection and use is of paramount importance. For example, although an employer may lawfully collect information on third parties, they would not be allowed to use such information to the party's detriment. Similar issues arise regarding the tailored monitoring of subgroups within an organization, such as only monitoring privileged users. Singling out groups in an organization is lawful if properly supported by business objectives. In this case, since privileged users have the greatest amount of access and the ability to cause harm, an organization would be justified in monitoring only this group. However, the organization would not be justified in monitoring a subset of employees based on protected characteristics such as gender, race, or religion.

Obtain Visibility: What?

As discussed, communications on corporate-owned devices and networks may be lawfully monitored. This is, however, not without restriction. For example, courts have placed restrictions on monitoring doctor-patient privilege and attorney-client privilege communications. Still other courts place restrictions on monitoring permissible "personal communications" of employees, such as those that occur during employees' lunch breaks and the use of web application email systems (like a personal Gmail account).

Obtain Visibility: When & Where?

Courts have also placed restrictions on monitoring the movement of employees. For example, while employers may properly place GPS monitoring devices on corporate-owned vehicles or other electronic devices, monitoring of movements is limited to during work hours. Monitoring movement during non-working hours is not lawful in the U.S.

As mentioned, courts make a distinction between employees on-duty and off-duty. Courts respect the personal time of employees and expect employers to do the same. This line blurs, however, with the increase of telework or work from home policies. For example, an employer who seeks to monitor the employee's activity while on duty yet at home must

specifically tailor monitoring policies to ensure that only on-duty activities are monitored.

Respond to Actions

Organizations Must Ensure Discoverability — This requires proper collection and storage of information. As discussed, "collection" poses fewer legal challenges, while "storing" that information raises more issues. For example, organizations need to properly store personally identifiable information (PII), personal health information (PHI), or payment card information (PCI) that they collect according to relevant compliance mandates. So, they will need proper tools, policies, and procedures.

Organizations Must Also Ensure Enforceability — Ensure that policies, procedures, and agreements are legally enforceable.

Lastly, Organizations Must Ensure Usability — Ensure "evidence" is collected and investigations are conducted in a legally sufficient manner.

Key Takeaways: Balancing Privacy and Security

- Each organization must first identify the legal and regulatory requirements that affect the implementation of its ITMP.
- These will vary depending on jurisdiction, any regulated industry requirements, and corporate culture.
- Culture is of particular importance and may impact your choice of Insider Threat tools and solutions.

The Ultimate Guide to Building an Insider Threat Program

Regulatory Compliance

Compliance refers to the imposed rules and regulations on certain industries and sectors. There are five general categories of government regulations that impose affirmative obligations to monitor employee behaviors and thus impact Insider Threat programs.

Financial

The Gramm-Leach-Bliley Act is a federal law enacted to control the ways that financial institutions deal with the private information of individuals. This act is best known for deregulating the financial sector and creating companies that were "too big to fail," which is widely blamed for causing the 2007 subprime mortgage crisis. This act imposes two Insider Threat requirements: identify and assess risks to determine mitigating actions and monitor user behavior to ensure proper access and use of customer records.

The Bank Secrecy Act (BSA) requires financial institutions to prevent money-laundering by monitoring their network activity. While the BSA itself does not specifically require employee monitoring, all transaction accounts, including those of employees, must be monitored for unusual activity. Logically, employee monitoring can be useful in detecting and preventing Insider Threats and should be part of a financial institution's fraud prevention toolkit, which can also be a useful regulatory shield.

Healthcare

The Health Insurance Portability and Accountability Act (HIPAA) provides data privacy and security provisions for safeguarding medical information. This act imposes four security requirements:

- monitor access rights to files containing PHI information
- detect behavior deviations and identify possible security violations
- monitor electronic and physical accesses
- monitor file attributes for access and changes

Public Companies

The Sarbanes-Oxley Act is designed to protect investors from the possibility of fraudulent accounting activities by corporations (think Enron and WorldCom) and mandates strict reforms to improve financial disclosures of corporations to prevent accounting fraud. This act also imposes the following Insider Threat requirements:

- monitor to ensure access is limited to authorized users
- perform risk assessments
- monitor for unauthorized access to corporate confidential financial information

Retail

The Payment Card Industry Data Security Standard (PCI-DSS) is a set of security standards designed to ensure that all companies that accept, process, and transmit credit card information maintain a secure environment. PCI imposes three monitoring requirements:

- monitor access of cardholder data to uncover unusual trends
- monitor and uncover the sharing of credentials
- baseline user behavior and monitor for deviations

National Security

The National Industrial Security Program Operating Manual, or NISPOM, establishes the standard procedures and requirements for all government contractors regarding the access, processing, and storage of classified information. The NISPOM requires covered entities to establish a formal Insider Threat program, a key component of which is to implement user activity monitoring to detect Insider Threat activity.

The Ultimate Guide to Building an Insider Threat Program

Legal Entanglements All Organizations Must Consider

If you're not a regulated entity, you might be thinking you are off the hook. Not so fast! Beyond regulatory incentives to monitor employees, there are several legal entanglements or risks that can often be mitigated through proper employee monitoring.

Duty of Care

A duty of care is a legal obligation imposed on individuals under tort law when performing acts that could foreseeably harm others. Courts have created a liability regime where monitoring employee behavior has become a matter of corporate self-interest. Employers now possess "affirmative obligations" to prevent and eliminate harassment in the workplace, prevent retaliation, prevent workplace violence, and prevent the disclosure of protected information (i.e. manage Insider Threats). In fact, the United States Supreme Court has made it clear that employers may be vicariously liable for the actions of their employees. One mitigation defense that courts apply is to explore the extent to which the employer attempted to "prevent and correct" the behavior that led to the incident. Since knowledge of employees' behavior is required to meet this standard and potentially avoid liability, the only logical result is for businesses to invoke employee monitoring solutions to meet these burdens of proof.

Negligent Hiring and Retention

These claims generally arise in the context of a workplace violence incident when facts exist that show the employee perpetrator had a violent history and that the employer could have reasonably learned of this behavior. Similarly, if an employer is aware or could have become aware of an employee's violent propensities, liability could attach. While the standards for determining liability in this area vary somewhat from one jurisdiction to the next, most jurisdictions examine whether an employer knew, or *should have known*, of an employee's unfitness for a position or dangerous propensities. Here, monitoring could help the

employer prevent, detect, and mitigate such behaviors and provide adequate proof to meet legal obligations and limit liability, as described above.

Retaliation

Retaliation claims arise when an employee alleges that they have participated in a "protected activity" and, as a result, were subsequently subject to an "adverse employment decision." Defending such claims can be difficult for employers, since courts have created a framework that tends to require an omniscient employer who possesses knowledge of all activities and relationships within their organization. Thus, employee monitoring represents the only logical approach to attempt to meet this standard and to properly defend against a claim of retaliation.

Disclosure of Sensitive Information

The need to protect their own sensitive information notwithstanding, businesses may be liable for the unauthorized disclosure of sensitive personal information of their employees and customers, as well as the sensitive business information of their partners. As discussed, employers may be vicariously liable for the actions of their employees, so monitoring employee behavior may be the only way to adequately prevent, detect, and mitigate this behavior.

Hostile Work Environment

These claims arise when an employee alleges that an employer has created a workplace that a "reasonable person would consider intimidating, hostile, or abusive." Claims of sexual harassment fall under this category. For example, employers may subject themselves to liability if they freely allow the sending of sexually explicit or harassing emails. Logically, monitoring employee communications may be the only way to detect and mitigate such actions.

The Ultimate Guide to Building an Insider Threat Program

Key Takeaways: Compliance and Legal Entanglements

- The decision to monitor employees must be made within the context of current regulatory and legal frameworks
- These often incentivize "keeping a close watch" on employees.
- Insider Threat-related compliance regulations are becoming increasingly important and more frequently enforced.
- In many cases, monitoring employee behavior might be the only regulatory shield or legal defense available to an organization.

Key Considerations

Insider Threat Management — Solutions

Technical: Legacy Approaches

Insider Threat technical solutions come in many varieties. Some are network security tools rebranded as "Insider Threat tools" and others are simply aggregators of network log data. Let's examine.

User and Entity Behavior Analytics (UEBA)

User and Entity Behavior Analytics solutions offer profiling and anomaly detection. Detection is based on a range of analytics and approaches, usually using a combination of basic analytics methods (e.g. rules that leverage signatures, pattern matching, and simple statistics) and advanced analytics (e.g. supervised and unsupervised machine learning). Vendors use packaged analytics to evaluate the activity of users and other entities (hosts, applications, network traffic, and data repositories) to discover potential incidents commonly presented as activity that is anomalous to the standard profiles and behaviors of users and entities.

Insider Threat GAPS: UEBA is primarily focused on identifying and detecting intentional insider events through baselining and detecting "anomalous" and "threat" activity. As such, UEBA lacks some of the productivity and compliance functionalities of EM and still fails to complete the full Insider Threat picture. It also depends heavily on the quality of the data fed into it, and does not have comprehensive capabilities. The machine learning-based alerts are difficult to configure, and baselining can be difficult if not impossible given the complexity of the modern work environment and various roles.

Employee Monitoring (EM)

The employee monitoring market consists of technologies that collect data about the location, movement, communications, and actions of employees. Because of their narrow focus, these tools are often integrated with other tools within the tech stack to support broader purposes. The most prevalent use cases for EM products are:

- Optimizing employee, team, and process productivity and efficiency by tracking physical and electronic activities.
- Reducing bandwidth costs emanating from inappropriate use of devices and networks.
- Ensuring employees comply with corporate policies and applicable laws and regulations.

Insider Threat GAPS: EM tools are primarily focused on supporting a client's understanding of employee productivity and compliance practices. EM tools are not specifically threat-focused and thus lack comprehensive Insider Threat management functionalities.

Data Loss Prevention (DLP)

Gartner defines the DLP market as those technologies that, as a core function, provide remediation for data loss based on both classification of data at rest and content inspection on data in transit. DLPs require setting up policies and rules, which can be arduous to get started with and to continually fine-tune. DLP products can execute responses — ranging from simple notification to active blocking — based on policies and rules defined to address the threat of inadvertent or accidental leaks,

or exposure of sensitive data outside authorized channels. In theory, DLP products incorporate detection techniques to help organizations address their most critical data protection requirements.

Insider Threat GAPS: By definition, DLP is asset-centric and thus fails to capture the broader user-behavior context necessary to fully understand the "interaction" between people and data that is integral to an effective Insider Threat management strategy. DLPs are difficult to implement and too static to effectively monitor the rapid pace of modern data. Moreover, they cannot provide context around user and data activity. They are also trivial for users to bypass. For these reasons, DLPs have major gaps.

Security Information and Event Management (SIEM)

Security information and event management refers to technology that supports threat detection and security incident response through the real-time collection and historical analysis of events from a wide variety of event and contextual data sources. SIEM technology aggregates event data produced by security devices, network infrastructure, systems, and applications. The primary data source is network log data.

Insider Threat GAPS: Since SIEMs are primarily focused on collecting and analyzing network log data, they lack the user behavior focus required to properly manage Insider Threat.

Key Takeaways: Insider Threat Tools

Aligning the legacy solutions to the four primary objectives, we see that no one technical solution meets all objectives. This leaves gaps that must be filled by other solutions or simply go unmitigated, which will result in increased threats to the organization.

Technical: Modern Approaches

Insider Threat Management

One of the best options to address Insider Threats is a purpose-built Insider Threat management platform. These tools are intentionally designed to look "inward" as opposed to the outward-facing posture of many security tools on the market today. Insider Threat management tools may be used to complement one of the legacy tools described above, or, in some cases, can provide a standalone approach to detecting and mitigating Insider Threats. One popular tool on the market is ObserveIT, the sponsor of this book.

How ObserveIT Aligns to the Four Objectives

ObserveIT's Insider Threat management platform aligns with all four objectives through its comprehensive user and data visibility, rich analytics, proactive detection, and rapid response capabilities. Let's take a look at these features and how they apply to Insider Threat management in more detail.

Gain Visibility into User and Data Activity

ObserveIT empowers Insider Threat management teams to "know their people" by creating a baseline of user interaction with various systems and tools. Teams can leverage the platform's robust Insider Threat Library, which consists of 350+ indicators of Insider Threat. These indicators can be tuned to alert security teams when users are engaging in potential Insider Threat activity. Additionally, the platform continuously collects detailed records regarding internet and application usage, which provides a comprehensive view of how a user is interacting with corporate data and systems.

ObserveIT allows the client to gain comprehensive visibility — and, therefore, context — by monitoring the actions and behaviors of users. Monitoring includes keyword usage, files accessed, and actions taken that indicate a behavioral or workflow issue. For example, these could include using another employee's login credentials or visiting suspicious websites.

Detect Risky User and Data Activity

ObserveIT also tracks the movement of data. The platform monitors data "in motion," such as when files are moved to cloud storage solutions such as Dropbox, transferred to a USB (and flags when the USB is approved or not), attached to an email, or moved to insecure directories. It also tracks copy/paste and file renaming. This info can also be used to support the actions of other security tools as well.

Streamline Investigations

These out-of-policy actions trigger an alert; when the alert is triggered, analysts have the ability to search through the timeline-based metadata related to that alert to quickly produce all of the relevant context around an incident. If the organization is using optional activity recording or Activity Replay capabilities, they are able to gain immediate visibility into the whole story — who, did what, when, and which assets, systems or data were impacted. This illuminates behaviors exhibited by a user that could indicate either a personal or an organizational threat. For example, this would include the use or viewing of inappropriate or violent keywords, use of unapproved login credentials, or moving or accessing sensitive data in an inappropriate manner.

Respond and Protect Against Insider Threats in Real Time

ObserveIT allows organizations to effectively and efficiently respond to suspicious user actions by incorporating alerting and investigative tools that provide additional correlation and tracking of events across all categories of data. This includes events currently taking place, current and historical trends, and event correlation between multiple users or departments. ObserveIT further supports investigation by displaying all events taking place in the system in chronological order in an easy-to-read format. In addition, a variety of filters can be applied to gather specific groups of events that may pertain to a potential incident or investigation.

ObserveIT also supports this objective by providing tailored oversight and compliance functionality and can provide tailored monitoring of those individuals responsible for managing Insider Threat programs ("Watch the Watchers"). The alerts and events can be sent to specific individuals responsible for oversight. Data can also be anonymized to maintain privacy. ObserveIT also provides strategic advising to clients to assist with the development of compliance policies and procedures that can be integrated with the technical solution.

Key Takeaways: Value Proposition

ObserveIT's Insider Threat Management platform delivers comprehensive visibility into user and data activity providing security organizations with a powerful tool for protecting valuable assets and users while saving time and resources. With more than 1,900 global customers across all major verticals, ObserveIT empowers security teams to proactively detect Insider Threats and data exfiltration, speed up the investigation process and enable rapid response.

Key Takeaways: Insider Threat Services

Most organizations lack internal Insider Threat expertise and can benefit from employing objective third-party Insider Threat management professional services.

These services can provide the visibility and justification needed to develop, implement, and sustain a strategic Insider Threat program.

Insider Threat Services

The Insider Threat risk by definition involves people with some level of access. Employees, contractors and third-party vendors have far greater access and internal know-how to cause harm than does an external threat. Most cybersecurity teams are not prepared with people, process nor technology to deal with these threats proactively. This is where expertise and services to provide the necessary insight and understanding on applying these controls, both technical and non-technical, in your organization helps programs get results faster. Let's review some types of Insider Threat management services.

Assessments

Baseline Review Assessment

A thorough assessment requires a full spectrum review of current programmatic operating capabilities and threats posed by insiders to your critical assets. The baseline review provides an objective and holistic assessment of an organization's current Insider Threat operating capability. This capability is measured against objective Insider Threat capability criteria. Baseline reviews require discovering and baselining your organization, business environment and security program. Based on that, would be a report with recommendations and achieving strong returns on investment focused on augmenting your existing operating capabilities across the security program and the rest of the organization.

Insider Risk Assessments

Understanding your risk posture is an essential step in developing an Insider Threat program strategy. Assessments should explore the entire organization, including assets, business environment, threats, vulnerabilities, security governance, and legal issues. Assessments should strive to answer the following questions:

- What is my organization's current Insider Threat management capability?
- Which components do I need to develop?
- What is the maturity level of each?
- What is the level of effort required to achieve an Initial Operating Capability (IOC)?
- What is the level of effort required to achieve a Full Operating Capability (FOC)?
- What are the resource requirements to achieve IOC/FOC?
- Which components should I create first to maximize effectiveness and utilize resources most efficiently?

The Role of Consulting in Building an Insider Threat Program

Program Development

An Insider Threat program consists of and requires synergy between an ecosystem of ten interrelated functional components, as discussed above. Third parties can provide the objective insight needed to build component frameworks and necessary bridges between stakeholders.

Technical Consulting

Effective Insider Threat management requires obtaining the necessary visibility into assets, user behaviors, and, most importantly, user interactions with assets. Insider risk management service providers can assist with tool selection, implementation, integration, and policy tuning and development.

Strategic Advising

As discussed, the standard cybersecurity model and ad hoc approach to Insider Threats is simply not working. You need a holistic Insider Threat Management Program (ITMP) to effectively manage these threats and reduce the risk to corporate assets. To that end, service providers and partners can help accomplish the three primary objectives:

- Know Your People
- Understand Insiders' Behavior
- Mitigate Risky Behaviors

Legal and Privacy Consulting

Implementing an ITMP raises myriad privacy, regulatory compliance, operational liability, criminal and civil enforcement, and employment considerations. Service providers can advise your Insider Threat stakeholders on the parameters and best practices of implementing an Insider Threat program.

Training

Awareness Training

Awareness programs should be specifically designed to provide your users with a comprehensive understanding of the organization's policies in place to mitigate Insider Threat risk as well as threats posed by insiders. This should include discussions of the common tactics, techniques, and methods used to compromise corporate assets and should cover the following topics:

- **Policies.** Understand specifics of the cybersecurity policies and why they have been implemented
- **Definition.** Learn the components and parameters of "Insider Threat."
- **Impact.** Learn the level of impact Insider Threat activities can have on mission and business operations and value, and why they need to be formally managed.
- **Scope.** Learn how Insider Threats compare to external threats and the differences in the degrees of harm caused.
- **Types.** Explore the different types of Insider Threat personas and how they can be used to better understand mission and business aim.
- **Research.** Review current statistics and research pertaining to Insider Threats to understand the prevalence and impacts of such threats.
- **Case Studies.** Examine recent Insider Threat cases to fully highlight the scope, type, and prevalence of Insider Threats.

Program Development and Operational Training

Program development courses should cover the fully panoply of insider risk domains, including program strategy, development, and implementation. In addition, legal and regulatory parameters should be fully explored and delivered by a licensed attorney and experienced insider risk practitioner. Operations training programs should provide your insider risk management personnel with the knowledge and skills necessary to function in analytic or investigative roles. Program topics should include tactical areas like behavioral indicators, Insider Threat tools, data sources, interviewing, Insider Threat law, and more. They should also cover the following strategic topics:

- **Threat.** Define and understand the concept of threat, how it applies to insiders, and how it can be measured to foster business and mission objectives.
- **Ecosystem.** Explore insider management functions and work roles — skillsets, job functions, and personnel.
- **Management Framework.** Explore the organization's Insider Threat management framework — challenges, requirements, equities, and foundations for managing Insider Threats.
- **Principles.** Discuss the principles of Insider Threat management and what it means to manage Insider Threats — responsible officials, work roles, development and implementation processes.
- **Objectives.** Fully analyze and explore the four Insider Threat management objectives and how they form the foundation of an effective program. Identify the goals of Insider Threat management and how they align with general mission and business objectives.

Key Takeaways: Insider Threat Services

- Most organizations lack internal Insider Threat expertise and can benefit from employing objective third-party Insider Threat management professional services.
- These services can provide the visibility and justification needed to develop, implement, and sustain a strategic Insider Threat program.

Developing an Insider Threat Strategy

Organizations face a changing risk environment with increasing numbers of remote workers and contractors, new competitive challenges, increasing privacy regulations, and the constant need to better protect their most valuable assets. Most organizations also have insider risk management capabilities that are best described as "nascent," resulting in a high risk of compromise to the organization's assets. Most have numerous insider risk management capability deficiencies, including the lack of a formal Insider Threat management strategy. This strategy is, however, the bedrock of an organization's Insider Threat Management Program (ITMP).

The Insider Threat strategy should: (1) Focus on insider risk management and incorporate this strategy into the organization's broader corporate risk management framework. In other words, create and maintain insider risk management leadership and capabilities across the enterprise and align it with business objectives. (2) Build greater connectivity among stakeholder components, including business units, by developing new integrations, boundary-crossing structures, and productive synergies. Greater connectivity will foster collaboration between stakeholders and make boundaries as permeable and seamless as possible.

How an Insider Risk Strategy Supports Mission

An insider risk strategy is more than managing and mitigating harm to an organization; it's about business enablement. To be effective, an insider risk management strategy must be aligned with business objectives. As a business enabler, an insider risk strategy promotes and enables:

- Employee security and privacy
- Protection of corporate data and assets
- Workforce productivity
- Compliance with rules, both external and internal

By fostering these business-enabling objectives, an insider risk strategy supports an organization's mission by providing a safe and secure workplace for employees to be ***inspired*** and protects corporate data and assets that are the foundation of ***innovation***.

Building a Program

If you are like many security leaders, you have a small team of IT security professionals and a group of IT infrastructure administrators of varying roles and functions. You may have an in-house legal adviser and likely an overtaxed HR department. Your company just experienced an Insider Threat incident, and you're now tasked with making sure this doesn't happen again . . . Where do you start?

This portion of the guide focuses on providing pragmatic information and systematic processes to assist you in your efforts. Creating a program does not have to be resource-intensive nor difficult. What follows is practical, real-world advice from noted and experienced insider risk management experts, using sample checklists, flowcharts, and worksheets as a means to providing a complete, granular, and purpose-driven approach.

Preliminary Considerations

An effective Insider Threat program requires clear goals and objectives that serve as guideposts to ensure the most efficient use of both capital and human resources. To that end, it's important to clearly articulate the *reasons* for implementing an Insider Threat management program. Are you simply trying to fulfill a compliance or legal requirement? Or are you responding to an Insider Threat incident? Are you trying to be proactive or simply in a position to efficiently react? Are you focused solely on security? Or productivity as well? Some initial and useful considerations to frame your strategy and to determine your level of effort include:

Current Security Program

This will be explored in more detail during the *Methodology* discussion, but it's an important step here to help you understand and set realistic goals and appropriately manage expectations.

- What are your current security practices?
- Do you conduct background investigations or currently monitor network activity?
- How are these viewed by your workforce?
- Are there existing components upon which you can build an Insider Threat management program?

Senior Leadership Support

Senior leadership support is essential to the success of any security program. Establishing the level of effort needed to obtain their "buy-in" will inform your overall objectives.

- How is information security viewed by senior executives?
  - > Necessary evil?
  - > Value add?
- What are the funding plans for the information security and security programs for the next fiscal year?

Risk Appetite

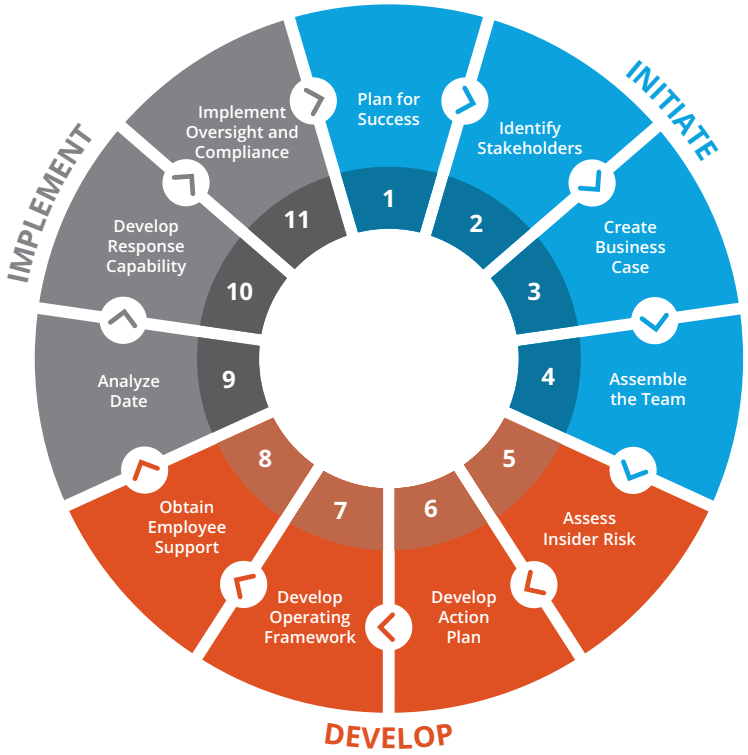
Determining your organization's overall risk appetite or risk tolerance is essential. The corporate view of risk will dictate the parameters of your Insider Threat management program. This will require a closer examination and a risk assessment (See Step 5), but at the outset it's important to understand how risk aligns with your overall strategy by keeping the following questions in mind:

- Will the risk be *shared* with a service provider or through the purchase of insurance?
- Will the risk be *avoided* by altering operations or access?
- Will the risk be *accepted* and treated as a cost of doing business?
- Will the risk be *reduced* by employing risk management practices?

The Process

Initially, all steps will should be completed regardless of which ecosystem components you are developing. Subsequent iterations, however, will only require you to complete steps 5–7 of the *Development Phase*. This will create efficiency and ease of application as you build out your holistic program. For example, if you decide to focus on developing an IOC, you will apply steps 1–11. Then, for each subsequent component or groups of components, you will only need to work through steps 5–7, since the groundwork has been created and the development of the particular component is all that is required.

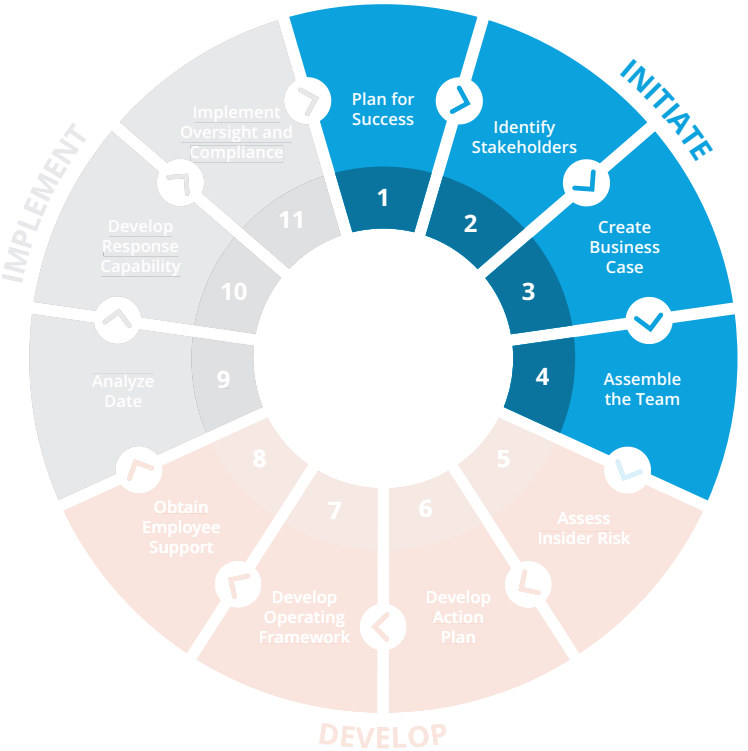
Figure 6: Insider Threat Management Program Methodology



Initiation Phase

A strong program foundation is necessary for the continued viability of any Insider Threat management program. This phase will guide you through obtaining senior leadership support, resource authorization, and the authority to hire the necessary personnel. Advocacy and collaboration are essential and will require synergy between senior security managers and the C-suite. Steps 1 through 4 will help you establish those communication channels and prepare for success. A note: this process should include HR, legal and privacy stakeholders from the very beginning in steps 1–4, whether you are a large enterprise or mid-market business. In mid-market, these steps would be done in a more abbreviated fashion, and there would likely be no official team. Teams often put together a working group to do this part-time. In this case, step 4 would be a point to consider who will help you part-time. In comparison, for an enterprise, you would likely create a separate cross-functional team that sits within the SOC.

Figure 7: Initiation Phase



Building a Program

STEP 1: PLAN FOR SUCCESS

This is more than simply baselining your existing capabilities. This is your chance to lay the groundwork for the Program itself. Your primary role is to convince decision makers that the Program will have value. Through your interactions with key leaders, you will gain insights into the gaps, needs, and opinions of the overall security of the organization.

Practice tip: *Interviews are the preferred method to ensure responsiveness and completeness. Surveys will likely be ignored and completed haphazardly.*

You should have a clear understanding of how your current capabilities compare to the best practices based on the ten program components. This in invaluable information to use in your discussions with stakeholders and formulating your business case.

GOAL
Create a baseline of your current security program.

PARTICIPANTS
CISO, CSO, senior security managers, and, possibly, outside consultants.

OUTPUT
A gap assessment and strategic roadmap of supporting recommendations.

JUSTIFICATION
This step is necessary because integrating and building upon existing resources saves time and minimizes costs.

HOW
To complete this step, you must determine which Insider Threat ecosystem components are already in place, as well as their maturity level. A review of current resources allocated is also necessary to obtain a complete baseline. This is not a risk assessment, but an initial review of existing capabilities and resources in order to baseline the current program. ***See* Baselining Template — Resources Section, page 91.**

The Ultimate Guide to Building an Insider Threat Program

Figure 8: Insider Threat Management Ecosystem

Building a Program

STEP 2: IDENTIFY STAKEHOLDERS

This is another important opportunity to lay the groundwork for the program. Arrange personal meetings via phone calls or emails to seek initial input and thoughts regarding the program. Stakeholders will be able to assist with identifying potential hurdles and objectives as well as the main "pain points" that you will need to address in your business case.

Practice tip: *While the majority of the key stakeholders will be corporate executives, pay close attention and seek out the informal leaders as well. These non-executive decision-makers are often the lifeblood of the company and their support will be essential. You should have a clear understanding of who will have the most impact on your program. This will help you foster the necessary relationships across your organization.*

GOAL

The goal of this step is to build the corporate team responsible for overall business strategy and operations.

PARTICIPANTS

CISO, CSO, and Insider Threat Program Manager (ITPM). CHRO or Head of HR should participate too.

OUTPUT

Clearly defined and identified governance framework.

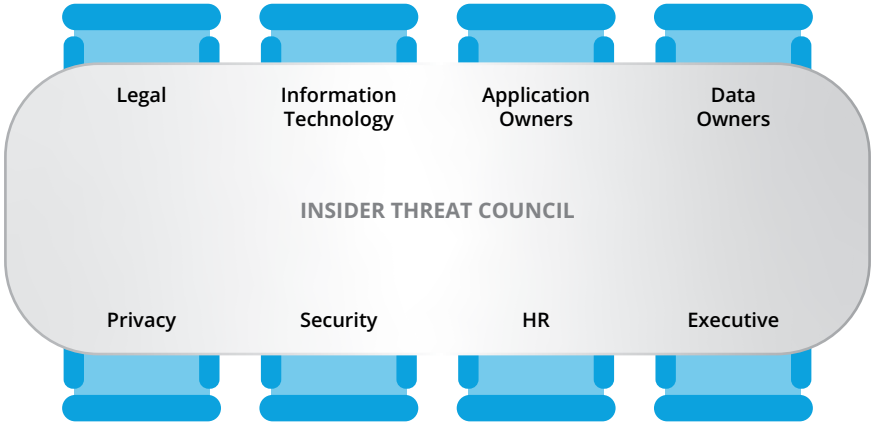
JUSTIFICATION

This step is necessary because the stakeholders have the necessary business responsibilities that you will need to leverage in order to advance your program objectives. Stakeholders are the lifeblood, and their involvement is essential to the creation of a successful program

HOW

To complete this step, you must identify the key personnel from key business groups, to include, but not limited to: legal, HR, IT, communications, security, and operational business components. You may find creating a committee or council of key personnel is most effective as depicted below in a notional example.

Figure 9: Insider Threat Council



STEP 3: CREATE THE BUSINESS CASE

The business case provides the justification for a project. Resource requests must be in support of a well-defined need and must capture the quantitative and qualitative value prospects.

The objectives are 1) capture knowledge about how the business will benefit from the project 2) verify that the project meets the needs of the business 3) provide a consistent message.

Preliminary Questions:

- Why is the project needed?
- How will it address the needs?
- How does it align with corporate mission?
- Outcome of inaction?
- Recommended solution?
- Resources required?

Practice tip: *Initially focus on mitigating "unintentional" Insider Threats. They represent the greatest risk and one that is more easily understood by executives. An educated employee is a safer employee. This will reduce costs by decreasing security events, thereby promoting efficient threat detection.*

GOAL

The goal of this step is to justify the expenditure of resources.

PARTICIPANTS

The participants in this step include the CISO/CSO, ITPM and senior security managers.

OUTPUT

Clearly defined business case to support resource requests and allocations.

JUSTIFICATION

This step is necessary because, as a traditional "cost center," any security program will need both initial and continued operating resources. A thorough business case will also assist with developing the ROI metrics and continued justification for future resources.

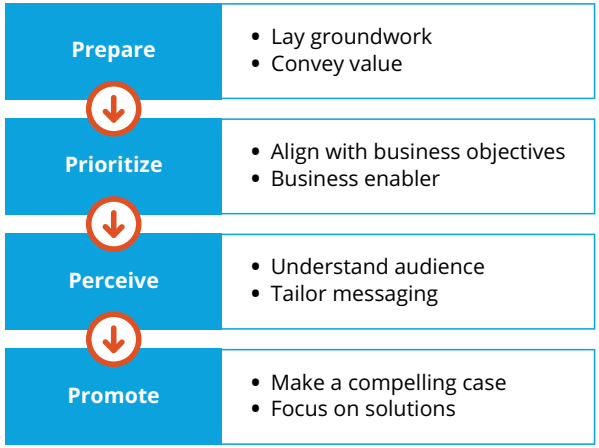
HOW

***See* Business Case Template — Resources Section, page 94.**

PREPARATION is key. You must convey value to stakeholders. Your job is to manage and develop positive perceptions of the program. You must reach out across business units and show them how you will support their mission. **PRIORITIZATION** is accomplished by aligning your goals with business objectives. Keep the focus on value to the business. Security must be viewed as an enabler, not a gatekeeper. **PERCEPTION** is crucial and the ability to understand and tailor the messaging cannot be overstated. Business managers will be more interested in how you will support their mission. Business executives are more interested in external effects to the bottom-line.

PROMOTION requires you to become a "security evangelist." Explain how security is relevant to their jobs. You must be seen as an effective communicator who understands how to collaborate. The case must also be compelling. Focus on a value-added end-state.

Figure 10: Business Case



STEP 4: ASSEMBLE THE TEAM

"Crawl, Walk, Run"

Start with what you have available. Build upon Step 1. Utilize the personnel and departments that have been involved with some of the functions (e.g. security, information security, HR).

For example, if you already have a fully functioning SOC, leverage those analysts to begin your employee monitoring program.

Practice tip: *The team might be a "committee" of existing personnel to start, but that's OK. The long-term goal should be, however, to develop a wholly independent Insider Threat team in the future to ensure proper separation of duties and objectivity. You should have all necessary work roles assigned or have engaged HR to fill the necessary positions.*

GOAL

The goal of this step is to create the work roles and identify the personnel needed to implement the program.

PARTICIPANTS

The participants in this step include CISO, CSO, ITPM, and senior security managers.

OUTPUT

Clearly identified and defined Insider Threat team personnel and stakeholders.

JUSTIFICATION

This step is necessary because clarity of roles and functions creates ownership of responsibilities that lead to a more efficient program.

HOW

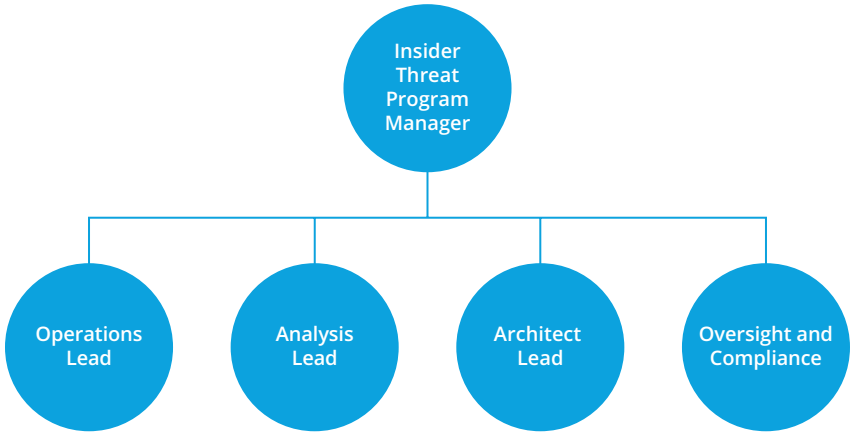
To complete this step you must do the following:

1) *Determine work roles* — Figure 9 represents a notional Insider Threat management team. The composition and requirements will vary for each organization. However, the roles themselves are agnostic and represent best practices. The Operations Lead is responsible for investigations and incident response. The Analysis Lead is responsible for monitoring alerts, drafting reports, and generating leads. The Architect Lead is responsible for tool operations, optimization, and data ingest. The Oversight and Compliance Lead is responsible for measuring performance and ensuring Insider Threat policies and procedures are followed.

2) *Align current human capital with roles* — Review current personnel capabilities and determine which roles are already met. Some organizations might simply appoint one person to function across all roles to start or split duties among several individuals. The focus should be on the roles and objectives of each role versus requiring a full-time employee for each. This will reduce initial operating costs and start-up requirements.

3) *Seek to hire for remaining vacant roles* — Address human capital shortfalls by seeking to hire appropriate personnel.

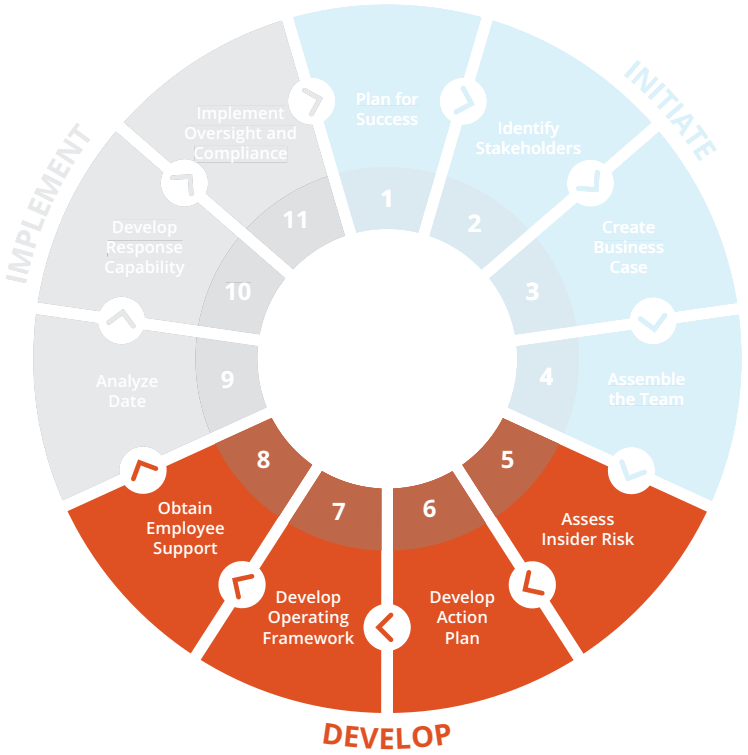
Figure 11: Insider Threat Management Program Team



Development Phase

A robust Insider Threat management program requires an understanding of the true risk posture of the organization. This phase will guide you through conducting an insider risk assessment, developing action plans and governance, and creating supporting policies and procedures. Steps 5 through 8 will help you obtain a holistic understanding of risk necessary to tailor a program for your organization.

Figure 12: Development Phase



STEP 5: ASSESS INSIDER RISK

Risk management is the process of selecting and implementing countermeasures to achieve an acceptable level of risk at an acceptable cost.

Risk: The likelihood that a threat will compromise an asset. The level of risk is a combination of 1) the impact a compromise would have on an asset and 2) the likelihood that a specific vulnerability will be exploited by a particular threat.

Vulnerability: Any weakness that can be exploited by an adversary to compromise an asset.

Threat: Any motive, opportunity or circumstance that has the potential to lead to the compromise of an asset.

Practice tip: *In conducting insider risk assessments, the effective application of this process requires the skills, knowledge, and experience of a variety of personnel, including stakeholders and subject-matter experts. This team approach ensures the recommendations are credible and based on objectively collected data.*

GOAL

The goal of this step is to discover the overall insider risk posture of your organization.

PARTICIPANTS

The participants in this step include the internal Insider Threat team but may also include outside consultants who can provide both tailored expertise and objectivity.

OUTPUT

Risk registry capturing the impacts, threats, and vulnerability to critical assets.

JUSTIFICATION

This step is necessary because efficient resource allocation requires an understanding of the current organizational risk posture.

HOW

To complete this step, you must do the following: 1) identify and prioritize critical assets 2) identify and prioritize threats 3) identify and prioritize vulnerabilities and 4) assess risk utilizing a *repeatable methodology*. ***See* Resources Section, page 96.**

The purpose of this process is to provide a systematic approach to acquiring and analyzing insider risk information for the purposes of making informed resource allocation decisions. Resources will always be limited, and prioritizing security requirements allows you to apply them to the most critical assets. With this methodology, the goal of security planning shifts from achieving maximum security to achieving maximum effectiveness in the allocation of limited resources (i.e. reducing the greatest amount of risk at an acceptable cost).

Figure 13: Assessing Insider Threat Risk

STEP 6: DEVELOP ACTION PLAN

An action plan is your roadmap for implementing controls, solutions, and countermeasures.

An effective action plan should have one or more of the following components:

- **Clear risk statement (what are you protecting)**
- **Mitigation requirements (how will you manage this risk)**
- **Implementation requirements (what resources are needed)**
- **Solutions or tools (that will meet these requirements)**
- **Timeframe (to implementation)**

Practice tip: *When evaluating solutions, it is important to ask the following questions and to explore vendor capabilities in these areas:*

- Cost
- Effectiveness
- Collection scope
- Analysis capability
- Triage function
- Low noise
- Scalability
- Performance impact
- Interoperability

GOAL

The goal of this step is to develop an implementation roadmap utilizing the results of *Step 5*.

PARTICIPANTS

The participants in this step include the Insider Threat team, vendors, and consultants.

OUTPUT

Report capturing objectives gaps, requirements, tasks, and level of effort.

JUSTIFICATION

This step is necessary because a prioritized plan ensures the greatest amount of risk will be managed at the lowest possible cost.

HOW

To complete this step, you must do the following:

1) *Have a clear understanding of the risks identified in Step 5* — The risk assessment will provide you with a granular and rank ordered understanding of which corporate assets are at greatest risk. Be sure to determine the root cause of each. Is it a lack of monitoring or auditing? Is it a lack of governance or oversight? Is it a weakness in personnel processing? Once the cause is clear, proper controls can be developed and implemented.

2) *Develop requirements* — A helpful framework for developing requirements is to utilize the People, Process, and Technology model. Ask yourself: Are the risks identified in Step 5 best addressed by adding or training people, improving or developing processes, or applying technical solutions? People may be the most cost-effective approach and should be your first option, especially if training existing personnel is involved. Processes are also a very cost-effective approach and can often yield positive results by simply organizing and creating more efficient decision-making. Technology will likely always be costlier but may be the only option depending on the particular operational requirements. This is also an appropriate moment to consider your privacy requirements and how you must go about addressing them.

3) *Identify solutions to support each requirement* — This may involve hiring or assigning existing personnel to fill needed roles; creating new processes or procedures; or implementing new technical solutions.

STEP 7: DEVELOP OPERATING FRAMEWORK AND POLICY

Strong governance and policy frameworks are the glue that holds the program together. Weak frameworks lead to ineffective and failed programs.

Governance requires top-level awareness, understanding, authorization, and, most importantly, positive action. Senior leaders must take an active role in the development and implementation of the program.

Similarly, strong policies will ensure parameters are followed and alignment of security and corporate objectives. The baseline results from Step 1 should provide you with an understanding of your policy gaps.

Practice tip: *An Insider Threat program is strongest when it is integrated with both the security and information security divisions. The ITPM should bridge any gaps between the CISO and CSO, creating a unified mission focused on managing Insider Threats.*

GOAL

The goal of this step is to develop the operating framework to support the Action Plan through documented policies and procedures.

PARTICIPANTS

The participants in this step include the Insider Threat team and leadership.

OUTPUT

Clearly defined governance framework and operating structure.

JUSTIFICATION

This step is necessary because clarity of roles and responsibilities will enhance long term program viability.

HOW

To complete this step, you must do the following:

1) *Create a corporate leadership engagement mechanism (e.g. annual or quarterly briefing for the board of directors)* — This can be a slide deck or similar presentation that covers successes measured against Key Performance Indicator metrics (e.g. incidents managed, decrease in alerts, fewer unauthorized logins or accesses, etc.). The objective is to gain a regular audience with your leadership and advise them of your Team's progress.

2) *Develop strategy documents that support the Action Plan and governance structure* — Documentation is key to a successful program since it serves to capture and memorialize the organizations support and dedication to securing the enterprise.

3) *Develop policies that support the Action Plan* — Each component must be supported by a corresponding policy and procedures statement. This is not to suggest that each component requires its own dedicated policy or procedure. What is required, however, is to ensure that the processes, roles, and objectives of each is captured and documented. This may take the form of a single ITMP policy or be broken into individual documents. The focus is on substance not the form in which it is captured and delivered. Remember also that having a clear and actionable privacy plan will be part of obtaining employee support.

STEP 8: OBTAIN EMPLOYEE SUPPORT

Employee support is a crucial part of any insider risk management program for myriad reasons. Most importantly, without it, employees may leave the company for another place where they feel more comfortable. Employee turnover inhibits confidence and undermines morale. Their support is also necessary because many Insider Threats are discovered through the observations of managers and coworkers. Effective employee support encompasses three pillars: 1) They understand the importance of security 2) They agree to operate within the confines of security 3) They want to be an active participant in the security process.

Practice tip: *Messaging that focuses on how security can enhance an employee's work life is far more effective than focusing simply on the ramifications of wrongdoing. To that end, focus on personnel assurance (preventing workplace violence and harassment) and business viability (preventing theft of IP and sensitive information) themes in your messaging.*

GOAL

The goal of this step is to establish employees, partners and contractors as partners in the operation of the program.

PARTICIPANTS

The participants in this step include HR and senior leaders.

OUTPUT

Engagement plan to communicate ITMP equities to the workforce.

JUSTIFICATION

This step is necessary because employees are the first line of defense and are the greatest asset to the program itself. Moreover, without employee support, the program will lose credibility and legitimacy that could result in unintended consequences (e.g., turnover and disgruntlement).

HOW

To complete this step you must do the following:

1) *Develop the messaging plan* — This will depend on your corporate culture and whether you have recently experienced an incident or have a history of security incidents and compromises. If you are starting at ground zero, then you will need to put time and energy into formulating a more holistic message. This will require coordination with your HR, legal, and senior managers.

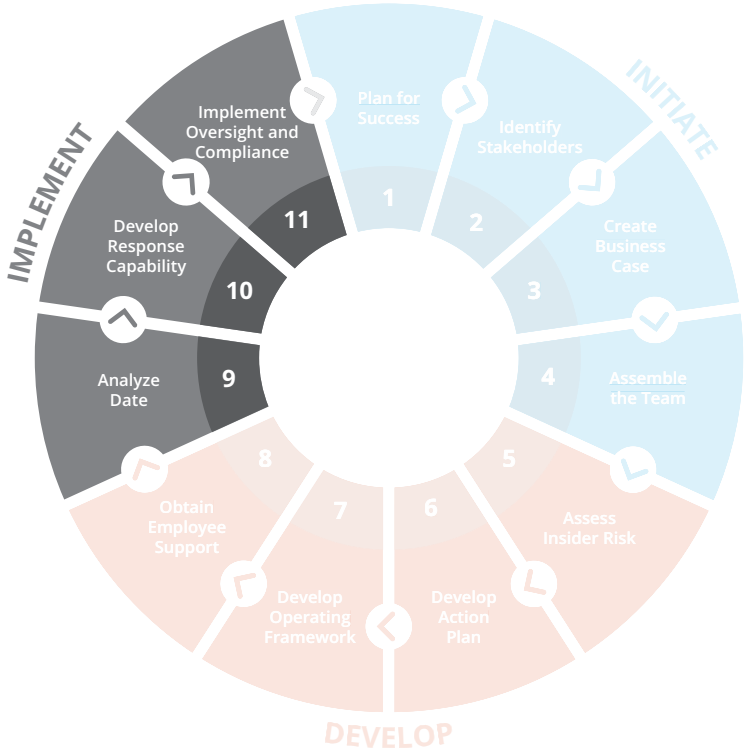
2) *Craft communications (email, posters, etc.)* — Communications should be simple and provide clarity about the reason for the new changes to security protocols or why new solutions or tools are now being utilized. (Note: this is not to suggest that sources and methods should be disclosed; to the contrary. What should be disclosed, however, are the programmatic changes and the value to the corporation and employees themselves.)

3) *Deliver message* — The message should preferably come from senior leadership, not from the program managers themselves. A message delivered by senior executives will carry with it a tone of legitimacy and credibility that only they can provide. This will also demonstrate to the workforce that they themselves (senior managers) have "bought in" to the program and value its contributions.

Implementation Phase

The goal of this phase is to *operationalize* the program. The participants in this step include the entire Insider Threat team. This phase is necessary because only an operationalized program will yield results. To complete this phase, you must do the following: develop an analytic capability, develop an ability to respond to an event, and create an oversight and compliance program.

Figure 14: Implementation Phase



STEP 9: ANALYZE DATA

Identifying available data sources is a critical first step in developing an effective analytical capability.

The parameters of your sources will be dictated by the scope of the program that you are authorized to create and the legal parameters of each.

Corporate culture is important here as well. You may now be authorized to collect, for example, UAM information, but you must also be prepared to align that with the culture and expectations of your employees.

Practice tip: *A robust tool like ObserveIT provides immediate ROI and a shortened time to value by collecting and aggregating relevant data sources into one tool.*

GOAL

The goal of this step is to ensure that you have the ability to analyze collected data.

PARTICIPANTS

The participants in this step include the Insider Threat team

OUTPUT

Defined processes for reviewing and aggregating available threat sources.

JUSTIFICATION

This step is necessary because data must be analyzed to be useful.

HOW

To complete this step you must do the following:

1) *Identify your existing and available data feeds. These may include:*

Internal Sources		External Sources
Endpoints	HR	Criminal
Networks	Cloud storage	Public information
Applications	Web activity	Social media

2) *Develop necessary data sharing agreements* — The data owners will likely be in different divisions of your organization. Ensuring that you have mapped out the necessary sharing protocols is essential.

3) *Understand the form and shape of the data* — Data may be structured or unstructured. It may be stored in a spreadsheet or capable of being sent to your team in "real-time." Understanding this will allow you to more efficiently create your analytic methodologies.

4) *Identify analytic solutions* — The more robust your data set, the likelier it is that you will need an automated solution. Seek solutions that map well to your data sets.

5) *Properly staff with intelligence analysts* — Map existing resources to analytic needs. Do you have the expertise to properly analyze this data?

STEP 10: DEVELOP RESPONSE CAPABILITY

Developing a response capability is much broader than simply creating an incident response plan. It requires identifying and understanding your entire response framework — data sources, alerts and events, types of incidents, and partner network.

Alerts and events or "tips" will generally come from five categories of sources: HR, reporting (managers or coworkers), InfoSec, or outside sources (e.g. law enforcement or regulatory agencies). Do you have clear processes and procedures to obtain this information in a timely manner?

Tips can generally be grouped into five categories: misconduct, policy violations, fraud, sabotage, and theft of IP or trade secrets. Do you understand the proper procedures for handling each type?

Practice tip: *Collection of information to support a criminal case requires specific knowledge, skills, and abilities to ensure that it is legally admissible and useable by law enforcement. Seek help from outside experts early in the process if there is evidence of criminal activity.*

GOAL

The goal of this step is to develop an efficient process for investigating and responding to threats.

PARTICIPANTS

The participants in this step include the Insider Threat team.

OUTPUT

Defined workflows and procedures for mitigating threats.

JUSTIFICATION

This step is necessary because time is of the essence after a security event or incident, and a clear plan will facilitate efficient response and remediation.

HOW

To complete this step you must do the following:

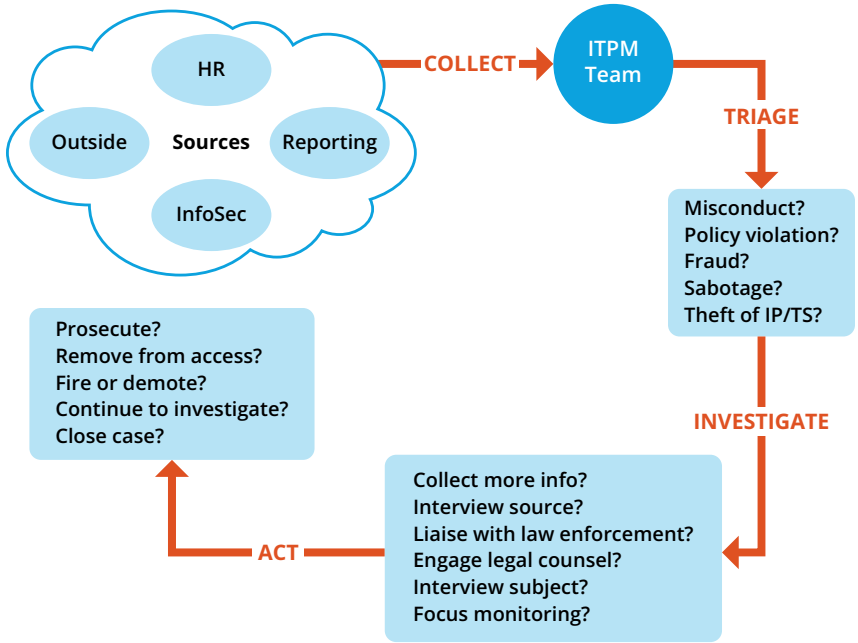
1) *Identify potential investigative and response needs* — The size of your organization will largely dictate your needs. Other factors include: recent history of incidents, implementing new monitoring solutions, physical locations, new acquisitions, etc.

2) *Identify in-house personnel, hire, or outsource* — Do you have the personnel to follow-up with interviews and logical investigations? Do you have in-house forensic capabilities? Once you understand your response needs, assign roles to current personnel or hire accordingly.

3) *Develop a liaison network of providers and law enforcement* — Identify outside consultants, forensic experts, and local law enforcement and prosecutorial officials.

4) *Draft investigative workflows* — Map how responses will be handled and processed, including roles and responsible officials.

Figure 15: Response Flow



STEP 11: IMPLEMENT OVERSIGHT AND COMPLIANCE

Oversight and compliance (O&C) is an essential, yet often overlooked, component of an effective ITMP.

In this context, O&C refers to the operational oversight of Insider Threat team members. In colloquial terms, this is a "watch the watchers" program.

Unlike traditional security programs that may collect general data about an employee, an ITMP will collect vast amounts of highly sensitive and personal information. Safeguarding and properly using this information is of utmost importance.

Practice tip: *Ideally the O&C lead should be someone from outside of the ITMP daily operations. This will mitigate any potential conflicts of interest as well as provide a true objective perspective to the ITMP itself.*

GOAL

The goal of this step is to ensure the ITMP is implemented in accordance with acceptable business practices and complies with existing legal and privacy requirements.

PARTICIPANTS

The participants in this step include the Insider Threat management team.

OUTPUT

Clearly defined oversight governance and framework.

JUSTIFICATION

This step is necessary, because it will create legitimacy, protect against unlawful disclosure, and clarify handling rules and procedures.

HOW

To complete this step, you must do the following:

1) *Identify an Operations and Compliance lead* — A full-time employee is not required, but you must identify a responsible person to take ownership of the function.

2) *Identify requirements* — The objective is to ensure members of the Team adhere to proper collection, use, and dissemination of sensitive information and conduct themselves accordingly.

3) *Draft compliance policy and procedures* — Clear policies will drive an effective Program while also instilling organizational support.

4) *Create reporting metrics and mechanisms* — Create a mechanism to capture: lessons learned, mistakes, successes, etc.

5) *Create feedback loops* — Create a process to review and analyze program effectiveness. Create a process to incorporate changes to the program based on lessons learned and feedback.

The Ultimate Guide to Building an Insider Threat Program

Building a Program

Takeaways

Insider Threat is a growing problem. Both surveys and studies suggest an increase in Insider Threat events. The data also strongly suggests that insiders are responsible for the majority of security events causing organizations to feel highly vulnerable to Insider Threats. This is both a result of the foregoing data points but also the fact that few organizations have the Insider Threat controls in place to obtain the visibility necessary to detect, prevent, and stop these threats.

Insider Threats can have a profound impact on an organization. Beyond the lost value of any assets that are removed, disclosed, or destroyed, organizations can suffer immediate losses of intrinsic value as well as lost revenue. The ability to deliver goods and services may also be adversely impacted, and there may be damage to reputations – both corporate and individual. Lastly, an insider event may impact the culture of an organization, which can lead to increased turnover and distrust, further exacerbating the effects of the breach and increasing security vulnerabilities.

Each organization must first identify the legal and regulatory requirements that affect the implementation of its ITMP. These will vary depending on the state or jurisdiction where you seek to implement ITMP components, any regulated industry requirements, and corporate culture. As discussed, culture is of particular importance and may impact your choice of Insider Threat processes, tools and solutions.

While no company wants to be viewed as Big Brother, the decision to monitor employees must be made within the context of current regulatory and legal frameworks that often incentivize user and data activity monitoring. Current "Insider Threat" compliance regulations are becoming increasingly important and more frequently enforced. In many cases, monitoring employee behavior might be the only regulatory shield or legal defense available to an organization.

Aligning the legacy solutions to the four primary objectives, we see that no one technical solution meets all objectives. This leaves gaps that must be filled by other solutions or simply to go unmitigated which will result in increased threats to the organization. Many organizations lack organic Insider Threat expertise and can benefit from employing objective third-party Insider Threat management professional services. These services can provide the visibility and justification needed to develop, implement, and sustain a strategic Insider Threat program.

Building an Insider Threat Management Program is an iterative process. It requires persistent attention, evaluation, and top-to-bottom support. New solutions, laws, and best practices will continually be developed that will impact your program. You must be vigilant and become an active participant and member of the insider risk management community.

When building your program, it is important to be systematic and objective. Focusing on the four primary objectives will help you stay on track — *Know Your People, Know Your Data, Monitor Interactions*, and *Investigate*. Objectivity will allow you to freely establish relationships across your organization regardless of pre-defined barriers or "traditional" security stovepipes. Remember, this is a team effort that requires the support and involvement of everyone in your organization.

It is the hope of the authors that this guide has added to your understanding of how to develop an Insider Threat Management Program. Our goal was to provide a practical guide backed by the experience of true Insider Threat practitioners. We encourage you to reach out to the authors and provide us with your feedback on how we can improve upon this guide for future releases.

Authors

Shawn M. Thompson, Esq.
Founder and CEO, Insider Threat Management Group
shawn@itmg.co
www.itmg.co

About ITMG

ITMG is the leading provider of tailored insider risk management advisory services to Fortune 500 companies. ITMG is focused solely on helping organizations ensure a trusted workforce by providing a range of insider risk management services including — strategic advising, insider risk assessments, program development, training, and staffing. ITMG's Insider Threat experts comprise the largest network of insider risk management practitioners in the world and include dozens of former Intelligence Community senior cyber security and insider risk management professionals. Our experts are pioneers in insider risk management and have served with numerous agencies including the FBI, DoD, DNI as well as several large corporations. Our network includes experts in all Insider Threat disciplines including program development, governance, data management, user monitoring, data governance, identity and access management, training, investigation, privacy, incident response, compliance, behavioral psychology, and privacy.

Mayank Choudhary
SVP Strategy and Products, ObserveIT
mayankc@observeit.com
www.observeit.com

About ObserveIT

ObserveIT, the Insider Threat Management company, proactively addresses the constant threat of accidental and malicious data theft from within organizations. More than 1,900 global customers across all major verticals depend on ObserveIT to detect risk, speed up critical investigations and enable rapid response.

Resources

Baseline Survey Worksheet

Use the chart below to capture your baseline results and the questions that follow to measure maturity levels. The questions are suggested inquiries for you to benchmark your program and are not concrete component requirements. The focus is on assessing the maturity level of each ecosystem component against the components objective. Thus, the assessor should have the flexibility to assign a maturity level based on their knowledge gained and understanding of objectives of each component.

Maturity Level = 0 to 5 ("0" = no progress and "5" = fully developed)

Insider Threat Management Ecosystem

	POC	Contact info	Comments	Maturity level	Resources allocated
Governance and Strategy					
Personnel Assurance					
Awareness and Training					
Data Management					
Access Control					
UAM					
Data Analysis					
Investigation					
Insider Risk Assessment					
Oversight and Compliance					

Governance and Strategy

- Formal Insider Threat strategy?
- Formal governance structure?
- Formal Insider Threat management policy?

Personnel Assurance

- Background check policies and procedures?
- Continuous evaluation program?
- Criminal record checks only?
- Fully incorporated into HR processes.

Awareness and Training

- Security training program in place for all users including partners and contractors?
- Train on acceptable use of network?
- Trained on social engineering techniques?
- Trained on ability to identify behaviors indicative of Insider Threat?

Data Management

- Have you identified critical assets?
- Do you know where they are located?
- Do you know who has access to them?
- Do you know how they can be accessed?
- Have assets been classified?
- Are insiders' interaction with data and systems logged and audited?

Risk-Based Access Control

- Access control policies and procedures in place?
- Access based on least privileged concept?
- Access adjusted based on role and individual risk level?

User Activity Monitoring

- Do you monitor user activity on network and endpoints?
- Do you have user monitoring policies and procedures in place?
- Do you have specific policies and procedures governing the collection, use, and dissemination of monitoring data?

Data Analysis

- Do you have the ability to analyze insiders' interaction with systems and data?
- Do you have analytic tools in place?
- Do you integrate multiple data sources to include both internal and external, network and off-network?

Investigation and Threat Mitigation

- Do you have a current investigative capability?
- Do you have a current forensic capability?
- Do you have a formal incident response plan?
- Do you have legally sufficient NDAs, covenants, and IP documentation?

Insider Risk Assessment

- Do your currently conduct insider risk assessments using a repeatable methodology?
- Do you conduct assessments on a regular basis?
- Do you assess assets, threats, and vulnerabilities?

Oversight and Compliance

- Do you currently have an oversight and compliance program in place?
- Do you possess the ability to measure program effectiveness?
- Do you have a value-added feedback mechanism?
- Do you have a "watch-the-watchers" capability?

Insider Threat Management Program Business Case Template

Figure 16

I. Executive Summary

- No longer than a paragraph, five to six sentences
- Summarize the main points, tell the story
- Pull value points from the body of the document
- Highlight benefits and how the project aligns with business objectives
- Draft with the executive audience in mind; write for the CEO, CFO, and Board

II. Project Value Proposition

- Describe the project; introduce details to help define the rest of the discussion
- Include goals, objectives, performance criteria, assumptions, constraints, and milestones
- Include clear statements of the problem and solutions
- Focus on two main points
  - > Value — What will the project offer the company?
  - > Importance — Why should this project be funded instead of other projects?

The Ultimate Guide to Building an Insider Threat Program

III. Impact and Resource Requirements

- For each solution define costs
  - > Human capital
  - > Licenses
  - > Operations & Management
  - > Equipment
  - > Space

IV. Cost-Benefit Analysis and Alternatives

- Why should your project be funded?
- Focus on value verses costs per se (need to guard against the bias that any security expenditure is simple a cost with little or no ROI)
- Cover both financial and non-financial (“intangible) benefits
  - > Increased client confidence
  - > Reduced risk of compromise
  - > Increased employee productivity
  - > Increased investor confidence
  - > Protection of reputation
  - > Creation of asset protection culture
  - > More efficient decision-making
  - > Early threat detection
  - > Faster investigations with irrefutable evidence
  - > Reduced impact of compromise
  - > Halt loss of intellectual property
  - > Bolster existing security measures
  - > Reduced time to resolve incidents

V. Recommendation

- Bring it all together
- Use a phased approach to discussing alternatives and impacts of each
  - > Do nothing
  - > Good
  - > Better
  - > Best
- Support each with evidence from prior sections and relate directly to business impacts and value proposition

Resources

Insider Risk Assessment Outline

These activities should be conducted on a continuing basis, because risk management is a dynamic process requiring monitoring of changes to asset value, threat, and vulnerability. Where significant risks have been accepted, it is important to include contingency planning as part of the risk management process.

This methodology uses a systematic approach. Each step outlined below is further broken down into sub-steps. Risk management includes cost as a major variable in the decision-making process. Resources will always be limited, and prioritizing security requirements allows the client to apply them to the most critical assets. With this methodology, the goal of security planning shifts from achieving maximum security to achieving maximum effectiveness in the allocation of limited resources.

Figure 17: Risk Assessment

This five-step process is iterative versus sequential, i.e., each step may yield further information and provide context that affects previously developed information. In this regard, each step requires clear documentation that can be further analyzed as needed.

The process begins with an assessment of the value (qualitative or quantitative) of assets, the degree of a specific threat, and the extent of the vulnerabilities. These three factors determine risk. A decision is then made as to what level of risk can be accepted and which countermeasures should be applied. Such a decision involves a cost-benefit analysis, giving decision-makers the ability to weigh varying security risk levels against the cost of specific countermeasures.

Step 1. Identify assets and loss impacts

- 1.1 Determine critical assets requiring protection
- 1.2 Identify undesirable events and expected impacts
- 1.3 Value and prioritize assets based on consequence of loss

Step 2. Identify and characterize the threat

- 2.1 Identify threat categories
- 2.2 Assess knowledge and motivation of the threat
- 2.3 Assess capability of the threat
- 2.4 Determine frequency of threat related incidents based on historical data
- 2.5 Estimate degree of threat relative to each critical asset and undesirable event

Step 3. Identify and analyze vulnerabilities

- 3.1 Identify potential vulnerabilities related to specific assets and undesirable events
- 3.2 Identify existing countermeasures and their level of effectiveness in reducing vulnerabilities
- 3.3 Estimate degree of vulnerability relative to each asset and threat

Step 4. Assess risk and determine priorities for asset protection

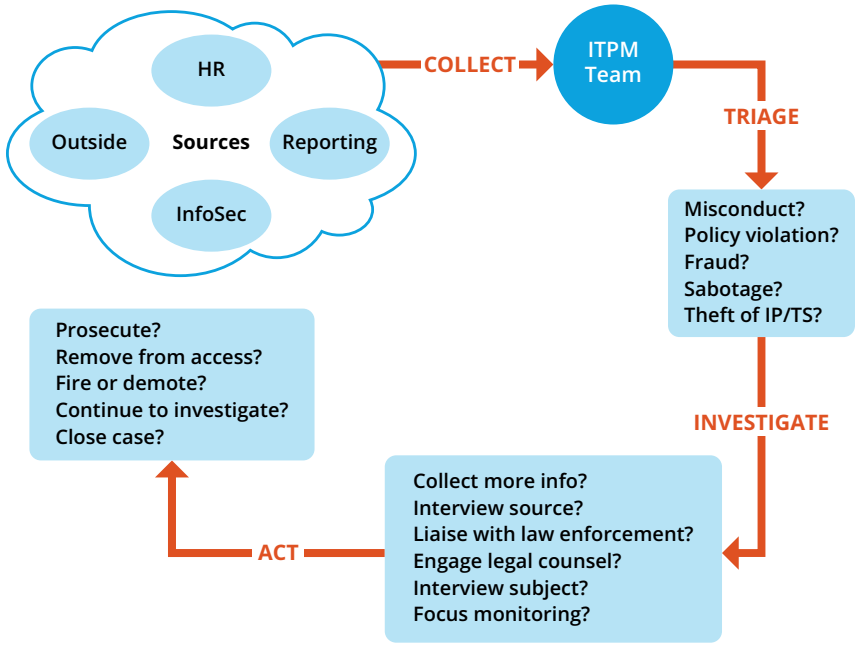
- 4.1 Estimate degree of impact relative to each critical asset
- 4.2 Estimate likelihood of attack by a potential threat
- 4.3 Estimate likelihood that a specific vulnerability will be exploited
- 4.4 Determine relative degree of risk [R=I(T*V)]
- 4.5 Identify unacceptable risks and determine risk mitigation priorities

Step 5. Identify countermeasures, costs, and tradeoffs

- 5.1 Identify potential countermeasures to reduce vulnerabilities
- 5.2 Identify countermeasure capability and effectiveness (i.e. risk reduction)
- 5.3 Determine degree of risk reduction (the benefit) provided by the countermeasure
- 5.4 Identify countermeasure cost
- 5.5 Conduct countermeasure cost-benefit and tradeoff analysis
- 5.6 Prioritize options and prepare recommendations for decision-maker

Response Workflow

Figure 18: Response Workflow



InfoSec Reporting Example Scenario

Collection: Infosec reports to the Insider Threat Team about a potential data leak event triggered by the existing Insider Threat management solution.

Triage: Insider Threat Team obtains additional information from InfoSec, HR and management on whether the DL event is within:

- The scope of what the employee is allowed to do
- Within his job role
- Was actually performed by the employee or by an impersonator
- Was it malicious, negligence or within company policy

Investigate: The Insider Threat team reports the DL event to HR and requests employment status such as whether the employee is under a performance review. The Insider Threat Team also consults with the employee manager about whether the employee actions were legitimate and within the normal business policy. The Team then conducts logical follow-on investigation to determine all facts and root cause of the event.

Action: If the employee's activity was within the acceptable business policy, the incident will be closed, and the Insider Threat Team will report back to InfoSec with suggestions to properly configure the DL in order to exclude these types of alerts again. The incident will be documented, and policies may need to be revised.

If the employee's activity was not within the acceptable business policy, the Team will initiate deeper user activity monitoring including screen recording. The Insider Threat Team will request that the InfoSec Forensic Team review all logs for that employee for any additional risk indicators.

Based on the forensic investigation result the Insider Threat Team will either close the case or consult with the legal department on necessary follow-up actions.

The Ultimate Guide to Building an Insider Threat Program

Insider Threat management programs are quickly becoming standard practice throughout private and public industry. In today's data breach-ridden and high-velocity business environment, security practitioners must be able to understand and implement programs in the most efficient and effective manner possible. This is significant, as this task requires balancing the protection of corporate assets with the privacy of employees, which can raise a myriad of legal considerations.

Developing an Insider Threat management program can be a difficult task even with a process in place — it is even more so without an established process. This critical action becomes more daunting if the security professional has not had formal experience managing Insider Threats. Not knowing which questions to ask can not only lead to legal trouble, but also leaves your organization vulnerable to Insider Threats. The Ultimate Guide to Building an Insider Threat Program provides you with the knowledge and tools to ensure you and your teams are prepared to meet the challenge head on.