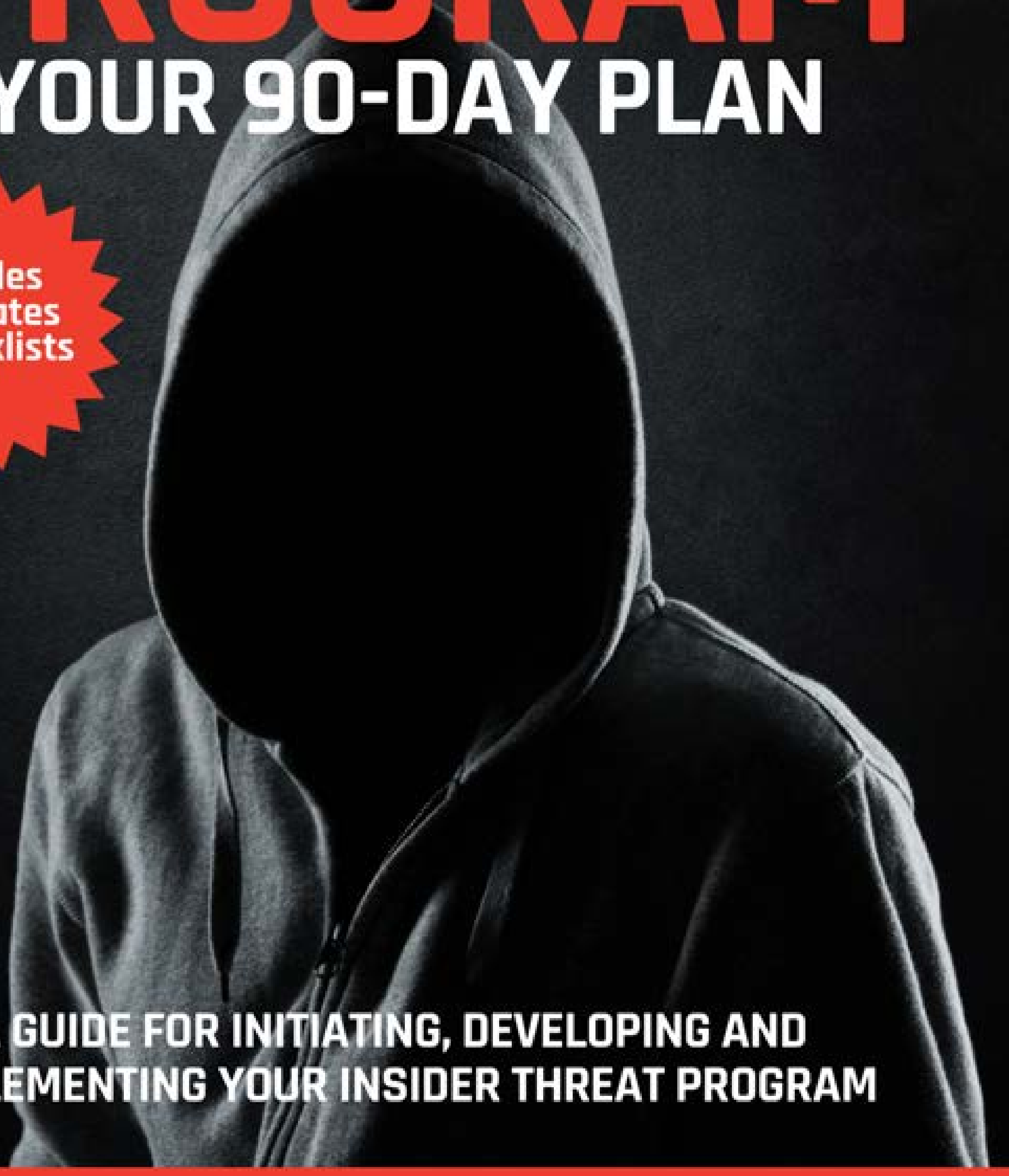
INSIDER THREAT PROGRAM

YOUR 90-DAY PLAN

Includes Templates & Checklists



A GUIDE FOR INITIATING, DEVELOPING AND IMPLEMENTING YOUR INSIDER THREAT PROGRAM

Shawn M. Thompson, Esq.

Gabriel Friedlander

Copyright © 2016 by ObserveIT
All rights reserved. This book or any portion thereof
may not be reproduced or used in any manner whatsoever
without the express written permission of the publisher
except for the use of brief quotations in a book review.
Printed in the United States of America
First Printing, 2016

ISBN-10:0-9978884-0-7
ISBN-13:978-0-9978884-0-9

INSIDER THREAT PROGRAM

YOUR 90-DAY PLAN

A GUIDE FOR INITIATING, DEVELOPING AND IMPLEMENTING YOUR INSIDER THREAT PROGRAM

Shawn M.Thompson, Esq.

Mr. 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 15 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. Mr. Thompson 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.

Gabriel Friedlander

Mr. Friedlander co-founded ObserveIT in 2006 with the singular goal of mitigating the growing risk of user-based threats for Security Officers, CIOs and IT managers. Since then, he has built ObserveIT into the leading Insider Threat Management Solution. He has expertise in IT security and databases.

Mr. Friedlander spends most of his days working with customers, helping them understand the growing risk of User-based Threats and how to mitigate them. When not working with customers, he is driving product direction and the future vision of the company. Mr. Friedlander is a frequent speaker on the topic of IT Security and Risk, and has presented throughout the world in more than 25 countries.

Copyright © 2016 by ObserveIT

ObserveIT disclaims liability for any personal injury, property or other damages of any nature whatsoever, whether special, indirect, consequential or compensatory, directly or indirectly resulting from the publication, use of, or reliance on this document. In issuing and making this document available, ObserveIT is not undertaking to render professional or other services for or on behalf of any person or entity. Nor is ObserveIT undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstance. All rights reserved. Permission is hereby granted to individual users to download this document for their own personal use, with acknowledgement of the authors and ObserveIT as the source. This document may not, however, be downloaded for further copying or reproduction nor may it be sold, offered for sale, or otherwise used commercially.

INSIDER THREAT PROGRAM GUIDE
YOUR 90-DAY PLAN

Table of Contents

PREFACE

“This Guide will make your job easier!”

After observing several instances of suspicious activity within his organization, CISO Rich Malewicz was faced with not one, but two daunting tasks: determining the cause of the activity, and developing a program to prevent it in the future. Rich quickly discovered that there is a dearth of documented, practical, and real-world advice from bona fide insider threat experts on how to build an Insider Threat Management Program. With no existing guide or playbook, Rich was fortunate to be able to rely on his past experience managing similar threats for the government, a luxury most CISO's do not possess. Malewicz says, "This Guide would have made my job much easier by allowing me to more efficiently create the governance, policies, and procedures to effectively manage future insider threats."

People are the weak link in the security chain. Unfortunately, it is these same people who have legitimate access to your facilities, systems, people, and data – your crown jewels. 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; specifically, unintentional threats. Moreover, there are few corporations that have implemented holistic Insider Threat Management Programs.

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, and legal and consulting 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 reduce cost and level of effort. This Guide will show you how.

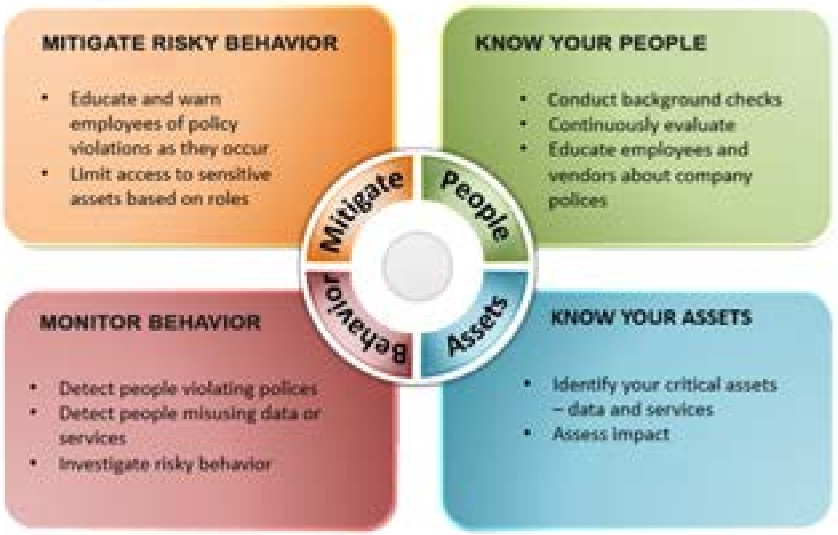
Using our three-phased approach and step-by-step process, you can create an effective and best-in-class Insider Threat Management Program for your organization.

Let’s get started!

EXECUTIVE SUMMARY

Company insiders are responsible for 90% of security incidents. Of these, 29% are due to deliberate and malicious actions, and 71% result from unintentional actions. 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. To that end, you must do four things well to accomplish this objective, as shown in Figure 1.

How to Effectively Manage Insider Threats



MITIGATE RISKY BEHAVIOR

- Educate and warn employees of policy violations as they occur
- Limit access to sensitive assets based on roles

KNOW YOUR PEOPLE

- Conduct background checks
- Continuously evaluate
- Educate employees and vendors about company polices

MONITOR BEHAVIOR

- Detect people violating polices
- Detect people misusing data or services
- Investigate risky behavior

KNOW YOUR ASSETS

- Identify your critical assets – data and services
- Assess Impact

Figure 1

You Must Know Your People. This is the foundation of any solid security program. You must aim to achieve an acceptable level of personnel assurance. This includes incorporating continuous evaluation processes as a supplement to a robust pre-employment background check. Continued personnel education and training is of particular importance, since the vast majority of insider threats are unintentional (social engineering victims, out-of-policy behaviors, and other negligent activities).

You Must Know Your Assets. What are your critical assets? Where are they located? Who has access? How can they be accessed? If you have trouble answering these questions, you're not alone. A good data governance and inventory strategy is essential for an effective ITMP. Full knowledge of your assets will allow you to properly align and manage the risk to those assets. A solid strategy begins with discovering where your assets reside and employing data asset tracking processes. This will allow you to properly label and classify your data and limit access in a risk-based manner.

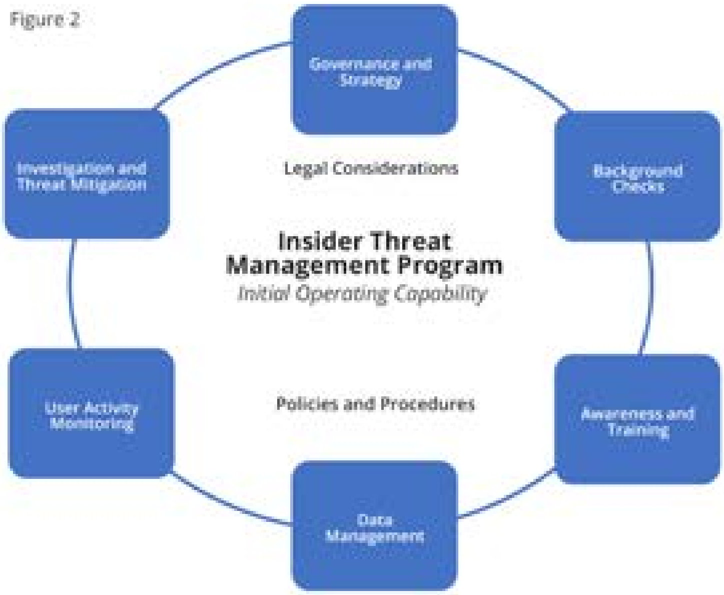
You Must Monitor Insiders' Behavior. Knowing how people behave within data, services, and applications is crucial in order to evaluate the risk and likelihood of an insider threat. Monitoring user behavior, coupled with full video captures of risky behavior, will provide unequivocal proof during the investigation process. It will also significantly reduce end-to-end investigation time.

You Must 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 policies, the ability to deter threats, and the ability to raise security awareness at the point of violation have been proven to effectively reduce insider risk.

QUICK WINS

The next-generation ITMP consists of ten complementary components, ranging from personnel screening and evaluation to monitoring and investigation. While a *full operating capability*[1] 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 2.

Figure 2



Governance and Strategy. A clear strategy outlining goals and objectives is a necessary guidepost. Clarity of roles and responsibilities is also essential to ensure efficient use of resources.

Background Checks. Background checks represent the baseline personnel assurance component for Initial Operating Capability (IOC). Whereas continuous evaluation should be the objective, and thus represent 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 insider threat precursors that will allow you to make more knowledgeable hiring decisions in accordance with the requisite legal authorities.

Awareness and Training. Training is a critical, yet often underutilized component. Since most insiders do not intend to harm your company, training helps them stay within the bounds of acceptable security conscious best practices.

Data Management. A foundational requirement of the information-centric security component is to know what data you have, where it lives, who uses it, and its sensitivity level. Data discovery is fostered through the application of the risk assessment model.

User Activity Monitoring. Even trustworthy employees need to be monitored to ensure they do not unintentionally engage in harmful conduct. As such, User Activity Monitoring (UAM) is more than simply a tool to monitor "bad actors"—it is a necessary tool that complements 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 you to intentionally harmful actions 3) maintaining immutable logs and video recordings to support subsequent forensic investigations and prosecutions.

Investigation and Threat Mitigation. Once threatening behavior is detected (whether intentional or not) it must be properly addressed.

[1] See Full Operating Capability discussion, page 19.

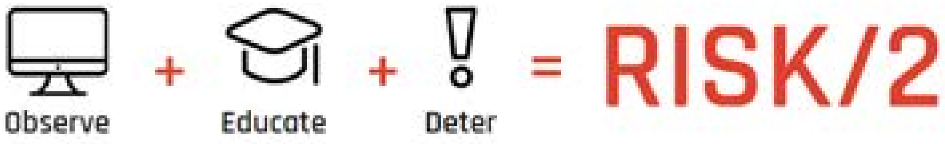
RETURN ON INVESTMENT

A next-generation ITMP provides real and immediate ROI. Unlike traditional security models that focus on external threats and stove-piped processes, this program will add value by providing you a framework and methodology to properly align resources with security objectives. The value proposition of a holistic ITMP is depicted in Figure 3.

- ✓ Increased client confidence
- ✓ Reduced risk of compromise
- ✓ Increased employee productivity
- ✓ Increased Investor confidence
- ✓ Protection of reputation
- ✓ Create asset protection culture
- ✓ More efficient decision-making
- ✓ Early threat detection
- ✓ Lower remediation costs
- ✓ Reduced impact of compromise
- ✓ Halt loss of intellectual property
- ✓ Bolster existing security measures
- ✓ Reduced time to resolve incidents

Figure 3

Insider Threat Management Program - ROI



Fewer Security and Compliance Incidents

Security training, real-time security awareness, and deterrence at the time of violation significantly reduces the number of security incidents resulting from unintentional or malicious behavior by more than 50%. Fewer security incidents streamlines incident and response, which results in less time chasing false alarms, and more time focusing on real threats.

Faster Forensics and Troubleshooting

A key component of an Insider Threat Management Program is a UAM solution that provides full visibility and video playback of actual screenshots showing user activity. This results in faster forensic investigations and reduces end-to-end investigation time from hours to minutes. No sifting through logs. No combing through data.

INTRODUCTION

The purpose of this Guide is to provide a resource for initiating, developing, and implementing an Insider Threat Management Program. This guide will help you effectively obtain leadership support and assemble your team, develop a risk-based action plan, create a policy and governance structure, implement monitoring requirements, and build 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 industries. In today's data breach and high-impact 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 when having 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 having the knowledge to know which questions to ask can not only lead to legal trouble, but can leave your organization vulnerable to insider threats. This Guide will prepare you for this challenge.

This Guide contains the following key components:

- The context for, and definition of, an Insider Threat Management Program
- The primary objectives of an ITMP
- The functional IOC and FOC components of a holistic ITMP
- The fundamentals of an Insider Threat Management Program
- The basics of developing a program utilizing risk-based methodologies
- Sample charts and workflows

This Guide was developed by leading experts in the field of Insider Threat and 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.

SCOPE

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[2], and cause twice as much damage as external threats.[3] In fact, ninety-percent of all security events are caused by insiders.[4] The great majority of these, however, are caused by unintentional insider threats.[5] Unintentional threats are difficult to detect because traditional security devices and solutions are primarily designed for detecting malicious activities.

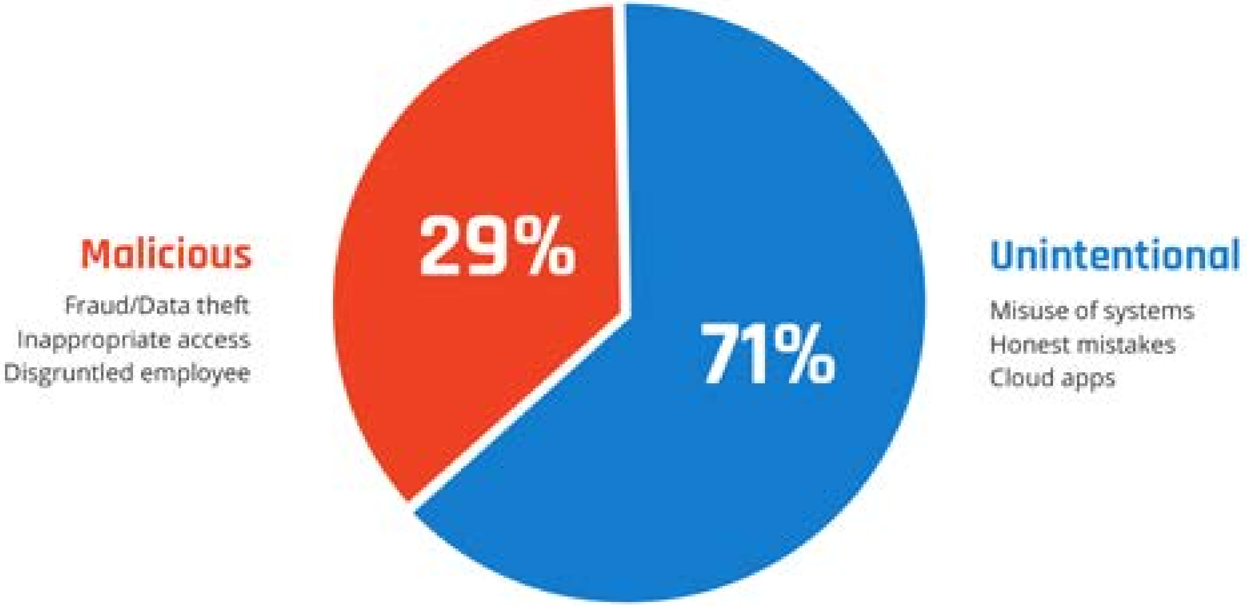
The Unintentional Insider Threat

- Improper use of systems
- Policy violations
- Social engineering victims
- Negligent use of email and web browsing

[2] Experion 2016 Data Breach Industry Forecast
[3] CERT Insider Threat Center
[4] Verizon DBIR (2015)
[5] More than 2/3 of all insider threats are unintentional. Verizon DBIR (2015)

Insiders Are Responsible for 90% of Security Incidents *

Figure 4

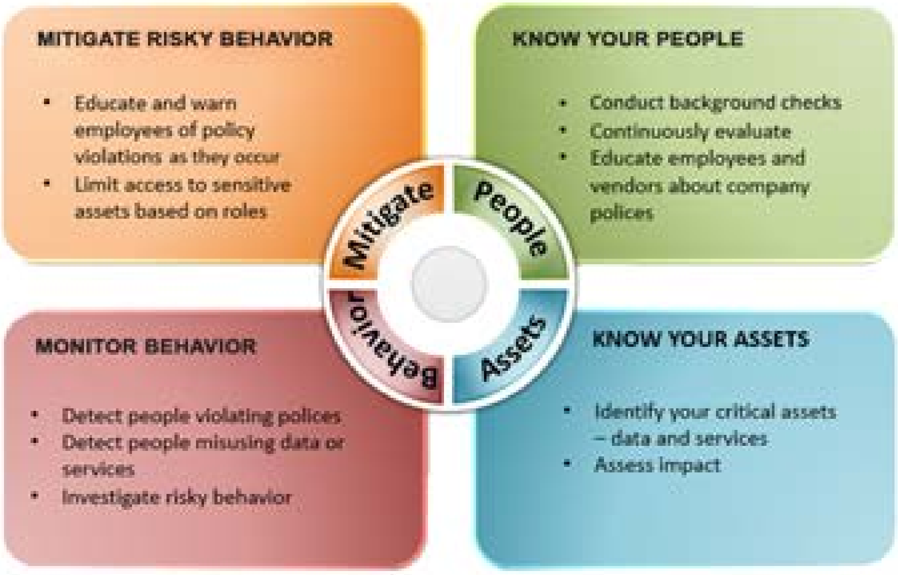


* Verizon 2015 Data Breach Investigations Report
* Kaspersky Lab 2016 Security Risks Special Report

INSIDER THREAT MANAGEMENT

Insider Threat Management[6] involves the holistic focus on managing risks that insiders pose to your corporate assets in a synergistic manner. 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.

How to Effectively Manage Insider Threats



MITIGATE RISKY BEHAVIOR

- Educate and warn employees of policy violations as they occur
- Limit access to sensitive assets based on roles

KNOW YOUR PEOPLE

- Conduct background checks
- Continuously evaluate
- Educate employees and vendors about company polices

MONITOR BEHAVIOR

- Detect people violating polices
- Detect people misusing data or services
- Investigate risky behavior

KNOW YOUR ASSETS

- Identify your critical assets – data and services
- Assess impact

Figure 5

You Must Know Your People. This is the foundation of any solid security program. You must aim to achieve an acceptable level of personnel assurance. This includes incorporating continuous evaluation processes as a supplement to a robust pre-employment background check. Continued personnel education and training is of particular importance since the vast majority of insider threats are unintentional (social engineering victim, negligence, carelessness, etc.). So what does it mean to "know your people?" In the context of insider risk management, it means having the knowledge necessary to make meaningful risk management decisions about your employees. Too often, these sources are limited to either pre-screening background checks or network behavior, or both. The problem is that pre-screening background checks are often wholly inadequate due to the scope of coverage - or more specifically - the lack of coverage. 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.

[6] 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.

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 aspect misses a large portion of their otherwise relevant and valuable behaviors on other mediums. For example, off-network behavior (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 that if you do not have full visibility into all areas of personnel assurance, then you will either need to account for this gap through some other means, or accept this risk and attempt to mitigate as it arises.

You Must Know Your Assets. What are your critical assets? Where are they located? Who has access? How can they be accessed? If you have trouble answering these questions, you're not alone. A good data governance and inventory strategy is, however, essential for an effective Insider Threat Management Program. Full knowledge of your assets will allow you to properly align and manage the risk to those assets. A solid strategy begins with discovering where your assets reside and employing data asset tracking procedures. This will allow you to properly label and classify your data and limit access in a risk-based manner.

Attempting to protect organizational data without knowing the answers to the questions above is analogous to being asked to bake a cake without a recipe. You might have all the ingredients but you have no idea about how much of each to add or for how long to bake it. Similarly, you may know generally what data is valuable and what you need to protect, but without full knowledge, you will have no idea how to effectively apply controls and countermeasures in an efficient and cost-effective manner.

Knowing your data requires a proper risk assessment. There is simply no other way to obtain this information. It will require you to roll up your sleeves and ask specific questions of data owners to obtain the answers necessary to understand the complete picture. Once completed, it will be worth the effort as you will now be operating from a position of knowledge.

You Must Monitor Insiders' Behavior. Monitoring your entire network and SIEM is good, but it's not enough. User Activity Monitoring (UAM) that captures all key strokes and includes DLP and other policy enforcement features is crucial to get full visibility into the Insider Threat. Monitoring user behavior, coupled with full video captures of risky behavior, with a solution such as ObserveIT, will provide unequivocal proof during the investigation process as well as significantly reduce end-to-end investigation time.

Monitoring is a key component because visibility is necessary to prevent and detect insider threats and to make risk-based decisions to mitigate those threats. Without a robust monitoring capability, you have no visibility. Without visibility, your organization is simply more vulnerable to insider threats, whether malicious or unintentional.

Monitoring includes your entire network—for example, logs and related events via a SIEM—but also includes monitoring user activity via a UAM solution that captures all key strokes and may include 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. 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, and this can only be achieved through the proper alignment with all objectives within an overall ITMP strategy.

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.

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.

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 and continuous evaluation techniques and workplace behavior policies, to network auditing, user behavior monitoring, and 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 the 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) digital assets. Accomplishing this goal requires a paradigm shift and a new approach – The Insider Threat Management Ecosystem.

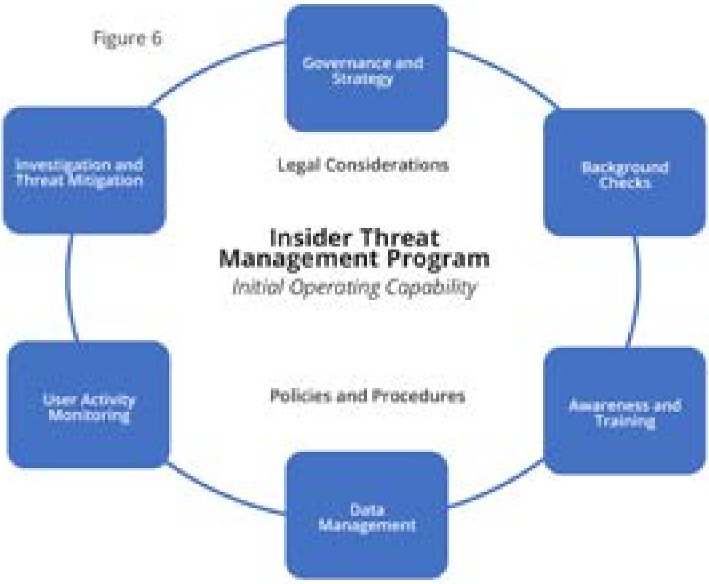
So what constitutes an Insider Threat Program?

This answer is best understood in the context of Initial Operating Capability (IOC) and Full Operating Capability (FOC). IOC is the minimum baseline and includes: Governance, Background Checks, Training, User Activity Monitoring (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

The next-generation ITMP consists of ten complementary components, ranging from personnel screening and evaluation to monitoring and investigation. 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 6.

Figure 6



User Activity Monitoring

Even trustworthy employees need to be monitored to ensure they do not unintentionally engage in harmful conduct. As such, UAM tools like ObserveIT are more than simply tools to monitor "bad actors"—they are necessary tools that complement the other components of a program and serve as a force multiplier by 1) alerting employees of potentially harmful actions and policy violations 2) alerting you to intentionally harmful actions 3) maintaining immutable logs and video recordings to support subsequent forensic investigations and prosecutions. UAM is also the only solution that provides you with the most important objective — visibility regarding employee network actions and how they interact with your data.

Legal Considerations

Creating and implementing an Insider Threat Program raises legal points that will also need to be considered. While the full scope of those issues is outside of the purview of this book, implementing a UAM solution, for example, raises particularly delicate issues. The most prominent of those 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?
- This reinforces the need to incorporate other organizational leaders (legal counsel, compliance, etc.) as you develop and launch your ITM

Background Checks

Background checks represent the baseline personnel assurance component for IOC. Whereas continuous evaluation should be the objective, and thus represents an 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 the requisite legal authorities.

Unfortunately, pre-screening background checks are often wholly inadequate due to the scope of coverage or, more specifically, the lack of coverage. 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.

In searching for a background check provider, be sure to obtain a list of their sources of information: specifically, the source of the "criminal" information. As stated, many will simply search national databases which is often outdated or inaccurate. Seek providers who search criminal data at the source, e.g. at the local county criminal courts or federal trial courts. Obtaining this level of detail requires more effort on the part of the provider and can thus be more expensive, but this effort is required by the Fair Credit Reporting Act for all background check providers.

Data Management - Discovery and Classification

A foundational requirement of the information-centric security component is to know what data you have, where it lives, who uses it, and its sensitivity level. Data discovery is fostered through the application of the risk assessment model, as discussed in Step 5.

The data discovery and classification process should be concurrent with the enterprise info-centric risk planning. Tools available today can crawl throughout an enterprise and identify all data, both structured and unstructured, and assist with organizing it into a comprehensive data asset management system.

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, you should strive to tailor it to the tasks of their specific roles and accesses. The goal should be to take your employees beyond mere awareness of security issues and actually educate them. They should be instructed in the "why and how" of assessing the risk and security implications of various situations 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. Carnegie Mellon also has a wealth of educational material and training programs that can be utilized. The best training is, however, taught by true insider threat practitioners who have real-world expertise.

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

- Counterintelligence and security fundamentals
- 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 activity to the insider threat team
- Methodologies of adversaries for recruiting trusted insiders and collecting sensitive information
- Indicators of insider threat behavior and procedures to report such behavior
- Regulatory and security reporting requirements
- Indicators of insider threat behavior and procedures to report such behavior
- Regulatory and security reporting requirements

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 which is always evolving, updating, tested, and improving or evergreen. 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 policy and procedures are the official enterprise statements of authority and guidance and to keep the enterprise in compliance with legal, privacy, and organizational objectives.

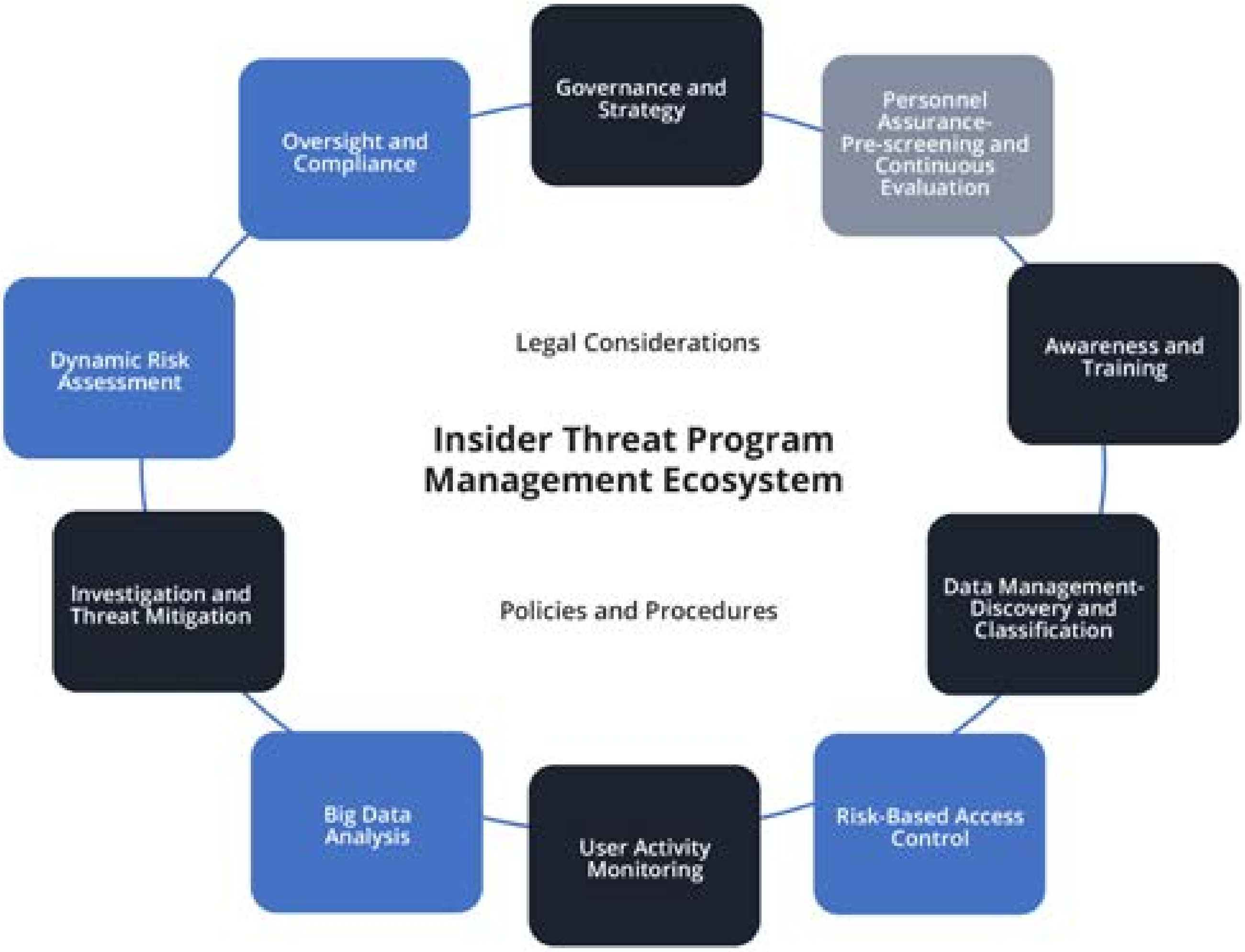
Investigation and Threat Mitigation

Once a threat has been identified, it must be investigated and mitigated. Mitigation can be as simple as the CISO, HR, and GC interviewing an employee who has displayed suspicious behavior to determine if further action is required. It may also be as complex as an automated and integrated process for monitoring and alerting an analyst of suspicious behavior. UAM tools are particularly valuable as an investigative tool. In addition to alerting to suspicious behavior, they can provide on-demand playback of the user's session, which makes investigations easier and more efficient.

FULL OPERATING CAPABILITY

FOC[7] includes all of the IOC components and adds those related to: Personnel Assurance, Access Control, Big Data 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. Some organizations may have some components in place and may choose to prioritize under an IOC model. Regardless, the focus is on obtaining the objective of robust insider risk management, not the dogmatic and ordered application of any particular component.

Figure 7


Governance and Strategy
Personnel Assurance-Pre-screening and Continuous Evaluation
Oversight and Compliance
Awareness and Training
Dynamic Risk Assessment
Legal Considerations
Insider Threat Program Management Ecosystem
Policies and Procedures
Investigation and Threat Mitigation
Data Management-Discovery and Classification
Big Data Analysis
User Activity Monitoring
Risk-Based Access Control

[7] 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 foundation 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 largely snapshots and apply binary methodologies[8] 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*.[9]

Legal Considerations

The Fair Credit Reporting Act 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.

Risk-Based Access Control

Insiders should have access to only those information assets that 1) have a need-to-know based on the role and duty and 2) fall within the parameters of their risk profile. This process will enable the innovation for the future fusion of role and duty monitoring of people in virtual and physical environments by integrating this analysis with data use into real time for the insider threat mission.

Identity and Access Management (IAM) technology is the foundation of any enterprise security solution. The IAM industry is evolving into new products and services focused on monitoring and controlling the access for the "privileged users." The combination of user and role, identity, data object level-based access control provides a previously unequaled granular access control capability and greatly reduces the potential impact of an insider data breach. The enterprise can achieve a higher trust level when only 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 with data stored in the cloud.

Big Data Analysis

Traditional analytic methods fail to address the sheet volume of data generated by today's information systems. Even though 80% of the threat can be mitigated by creating simple rules and monitoring, 20% of the insider threat requires big data analytics. Big data analytics lead to more insights and better understanding of insider behavior by revealing previously unknown patterns and insights about their behavior. In basic terms, big data analytics produces insights from data. Big data analytics are characterized by their ability to scale beyond traditional analytic constraints and to make sense of disparate data sources – structured and unstructured.

Techniques used primarily in the commercial world are beginning to be applied to security. For example, the use of MapReduce and Hadoop are equally applicable in determining the anomalous behavior of an Amazon customer or an insider threat. One approach employed by big data analytics is to determine a baseline of user activity and behavior. This baseline is then used to determine deviations from normal activity, resulting in alerts and investigative events. Big data analytics should be employed to make sense of all available information on an insider.

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

[9] 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 scope and type of acceptable data sources will largely depend on your organization's culture, risk tolerance, and resources, but it should include both internal and external data sources.

There are a growing number of vendors who provide threat intelligence, analysis, correlation and detection as a service from the cloud or as an on premise solution with SME staffing. Regardless of which solution you choose, good analysis requires trained experts that are schooled in advanced analytic techniques.

Dynamic Insider Risk Assessment

A Dynamic Insider Risk Assessment is a process or procedure that continuously and dynamically adjusts insider risk scores. While risk registry solutions have been prevalent for many years, a dynamic insider risk registry is a new and revolutionary concept. Currently, an organization can achieve part of this objective through the implementation of a UAM solution 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 insiders. This will allow you to make more informed business decisions, while also supporting a risk-based access control model. This moves the emphasis on proactive management solutions instead of simply responding to events and incidents as they arise.

Oversight and Compliance

A fundamental concept 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 not only from mistakes, but to also improve upon the successes of the program itself. 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. Policies and procedures must be documented and implemented to ensure that information is properly safeguarded. Nothing will impact the continued viability and resources of your program more than abuse of this power and authority – intentional or unintentional.

LET'S GET TO WORK!

This Guide is modeled for the mid-size business, but remains agile and adaptable for companies of any size and maturity level. If you are like most security managers, you have a small team of IT Security professionals and a group of IT infrastructure administrators in varying roles and functions. You may have an in-house legal adviser and a likely 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? What is an Insider Threat Program? What are the legal and policy parameters? What are the security requirements? How do you create it? Where can you find these answers?

This 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 and granular purpose-driven approach. Let this Guide. . . be your guide.

Goals and Objectives

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:

Culture

What is the culture of your organization? The relevant focus here is specifically on the security culture. 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?

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 added?
- 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 METHODOLOGY

This methodology is divided into three phases – Initiation, Development, and Implementation. Each phase is agnostic and designed to be applied to the creation of any of the ecosystem components – individually or collectively. Each step is organized around five key concepts:

Goal: The desired objective of the step.

Participants: Who should be responsible for completing the objective?

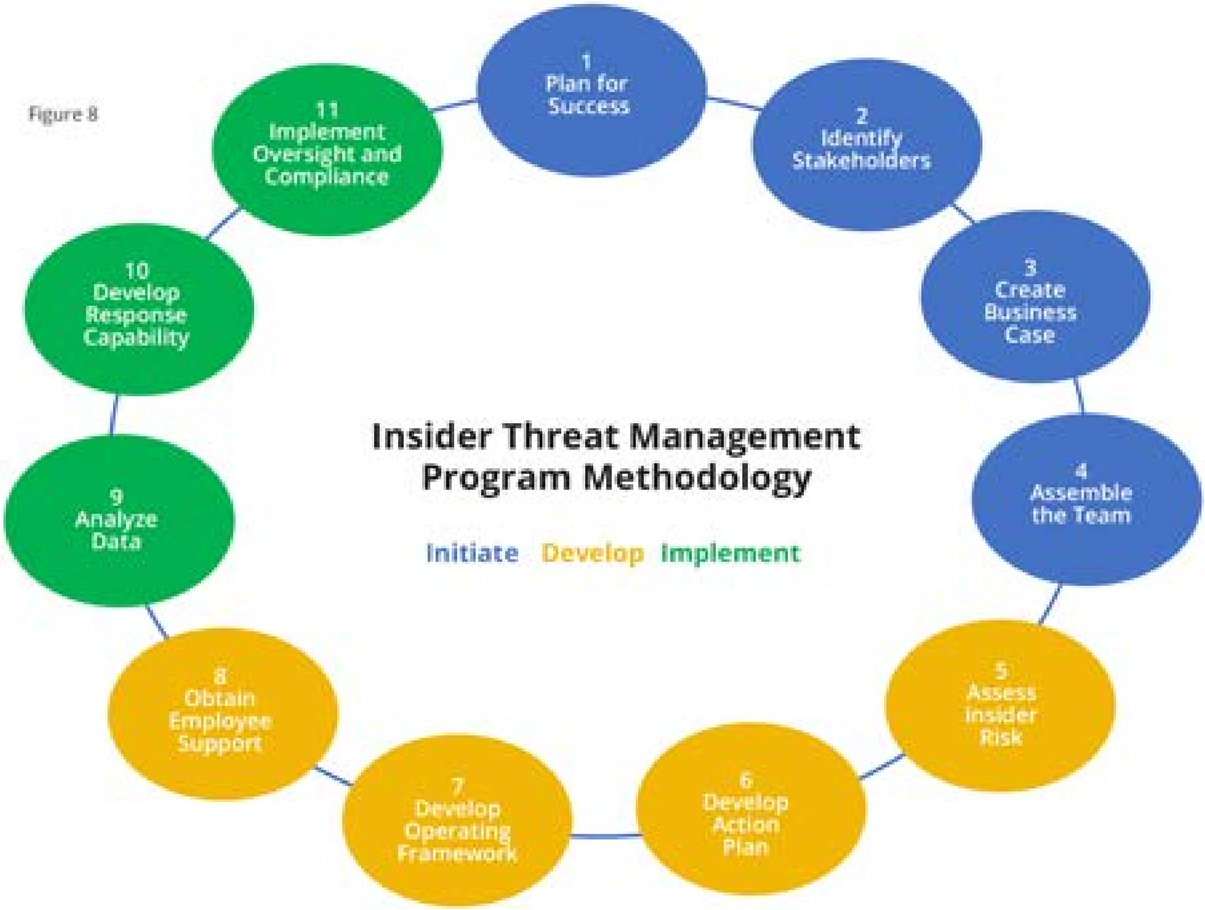
Timeframe: The time that should be allotted for the step.

Justification: Explains why the step is necessary.

How to accomplish: Describes the essential actions to complete the step.

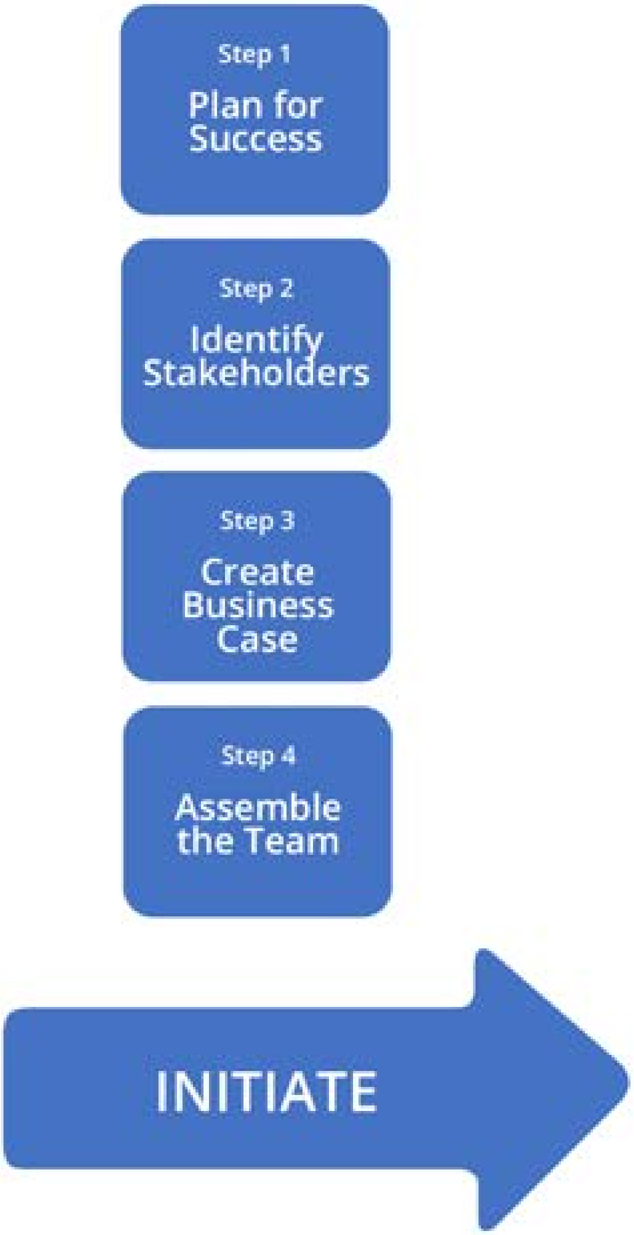
Initially, all steps will need to be completed regardless of which ecosystem components you are developing. Subsequent iterations, however, will only require you to complete steps 5-7 of the Development Phase. This will create efficiency and ease of application as you build out your holistic program. 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 8


1 Plan for Success
2 Identify Stakeholders
3 Create Business Case
4 Assemble the Team
5 Assess Insider Risk
6 Develop Action Plan
7 Develop Operating Framework
8 Obtain Employee Support
9 Analyze Data
10 Develop Response Capability
11 Implement Oversight and Compliance
Insider Threat Management Program Methodology
Initiate
Develop
Implement

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 to prepare for success. This phase should take approximately 4 weeks to complete.



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: *Outside consultants can provide valuable subject matter expertise that is necessary to conduct a more advanced baseline review and assessment of your program, which is especially useful for establishing your subsequent business case. 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 is invaluable information to use in your discussions with stakeholders and formulating your business case.

Goal: Create a baseline of your current security program.

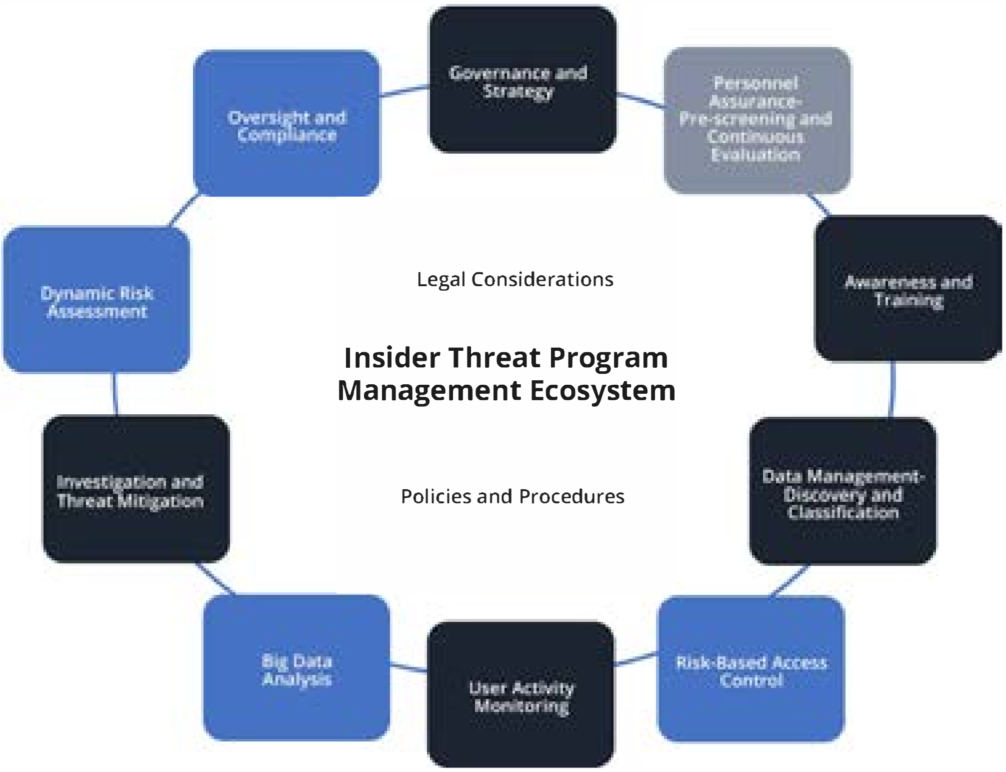
Participants: CIO, CISO, and security managers.

Timeframe: This step should take approximately one week to complete.

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 – Appendix A

Figure 9


Governance and Strategy
Personnel Assurance- Pre-screening and Continuous Evaluation
Awareness and Training
Data Management- Discovery and Classification
Risk-Based Access Control
User Activity Monitoring
Big Data Analysis
Investigation and Threat Mitigation
Dynamic Risk Assessment
Oversight and Compliance
Legal Considerations
Insider Threat Program Management Ecosystem
Policies and Procedures

STEP 2: IDENTIFY STAKEHOLDERS

This is another important opportunity to lay the groundwork for the Program. Arrange personal meetings instead of 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.

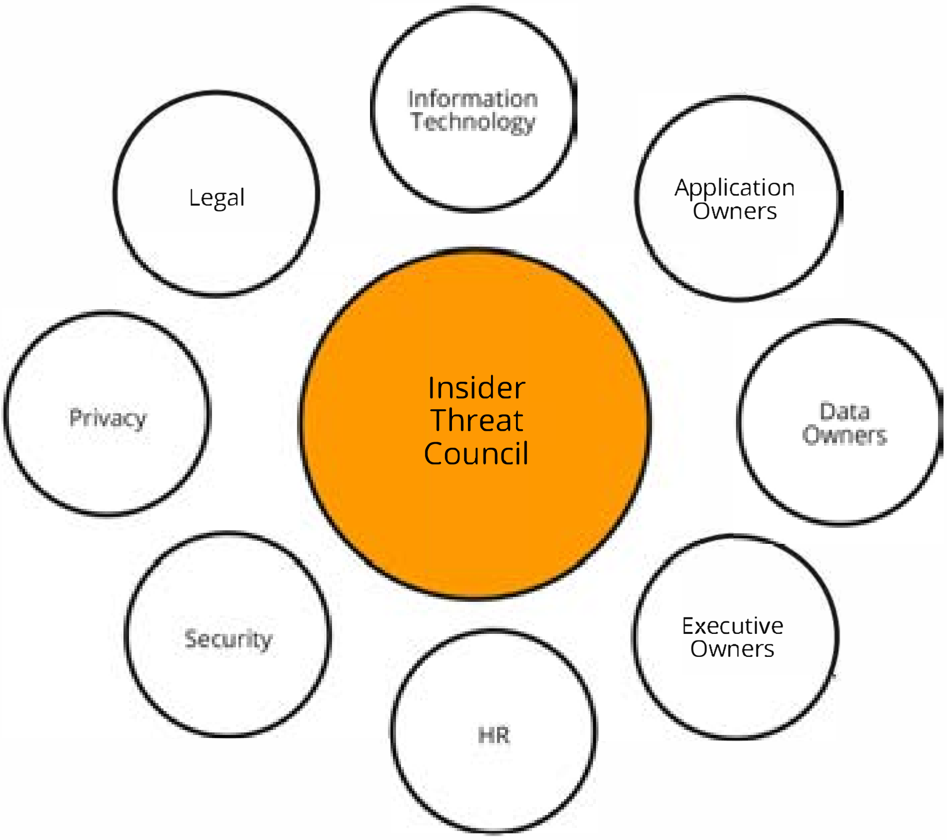
Participants: CISO and CIO.

Timeframe: This step should take approximately 1 week to complete.

Justification: This step is necessary because the stakeholders have the requisite 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

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 10



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.*

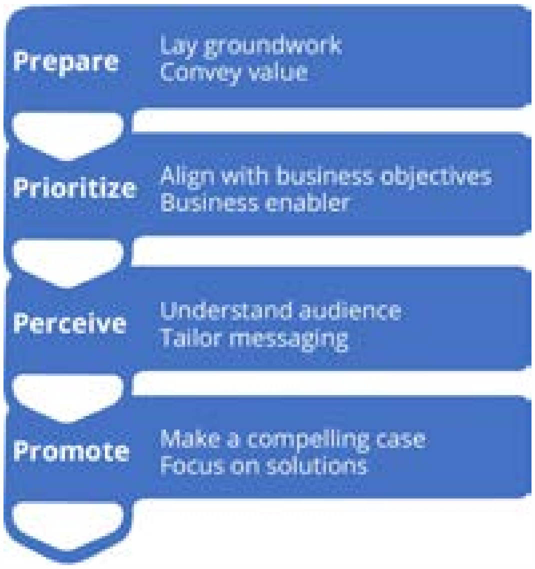
Goal: The goal of this step is to justify the expenditure of resources.

Participants: The participants in this step include the CISO and senior security managers.

Timeframe: This step should take approximately 1 week to complete.

Justification: This step is necessary because as a traditional "cost center" the 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 – Appendix B.



PREPARATION is key. You must convey value to stakeholders. Your job is to manage and develop positive perceptions of the Program itself. 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. Must be viewed as an enabler, not a gate-keeper.

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.

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 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 and senior security managers.

Timeframe: This step should take approximately 1 week to complete.

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

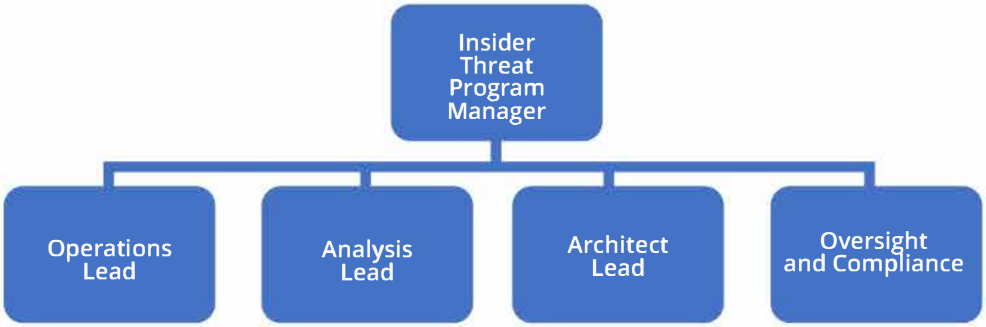
How: To complete this step you must do the following:

1) Determine work roles – Figure 11 represents a notional insider threat management team. The composition and requirements will vary for each organization, however, the roles themselves are agnostic and represent a best practice. The Operations Lead is responsible for investigations and incident response. The Analysis Lead is responsible for monitoring alerts, drafting reports, and lead generation. 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 instead of requiring a full-time employee for each. This will reduce initial operating costs and start-up requirements.

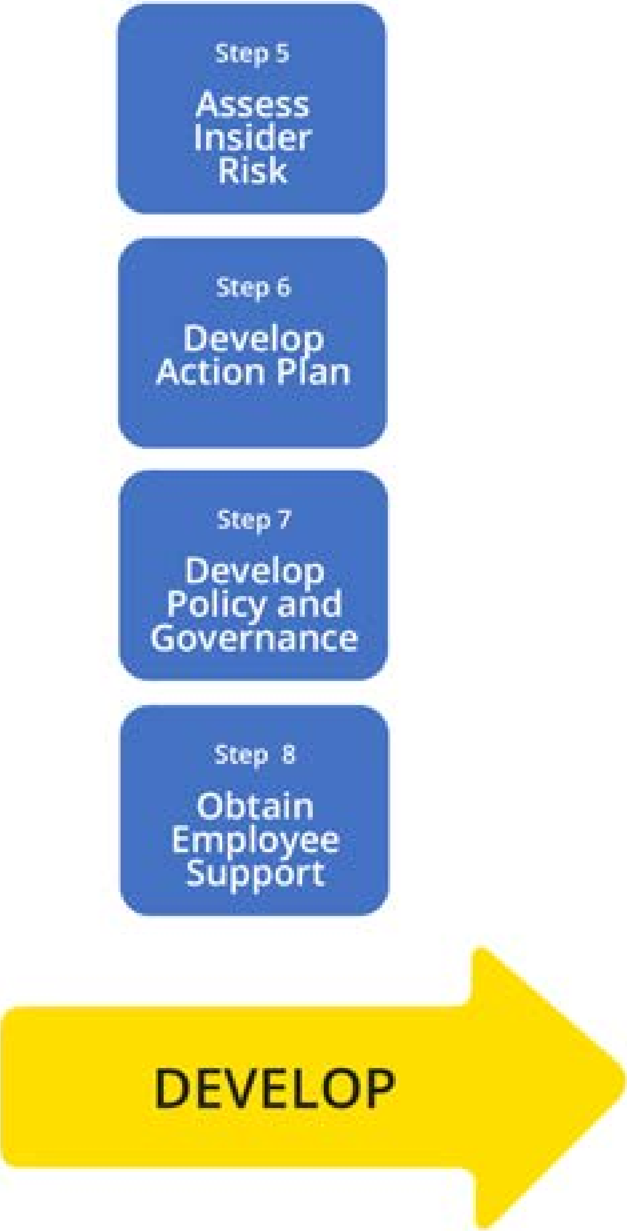
3) Seek to hire for remaining vacant roles – Address human capital shortfalls by seeking to hire appropriate personnel.

Figure 11



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 the risk necessary to tailor a program for your organization. This phase should take approximately 8 weeks to complete.



Step 5

Assess Insider Risk

Step 6

Develop Action Plan

Step 7

Develop Policy and Governance

Step 8

Obtain Employee Support

DEVELOP

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 develop an implementation roadmap utilizing the results of Step 5.

Participants: The participants in this step include the Team, Vendors, and Consultants.

Timeframe: This step should take approximately 2 weeks to complete.

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) identify and prioritize critical assets 2) identify and prioritize threats 3) identify and prioritize vulnerabilities and 4) assess risk utilizing a repeatable methodology. See Appendix C.

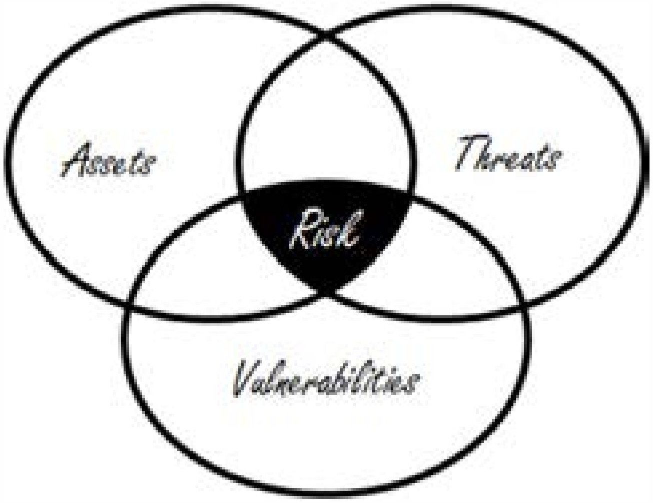


Figure 12

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*

The purpose of this process is to provide a systematic approach to acquiring and analyzing insider risk information for 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).

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 Team, vendors, and consultants.

Timeframe: This step should take approximately 2 weeks to complete.

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.

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 Team and leadership.

Timeframe: This step should take approximately 1 ½ weeks to complete.

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 PowerPoint slide 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.

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 research and anecdotal evidence supports the finding that the majority of insider threats are discovered through the observations of managers and co-workers, not technological solutions. 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 as partners in the operation of the Program.

Participants: The participants in this step include HR and senior leaders.

Timeframe: This step should take approximately 1 week to complete

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:

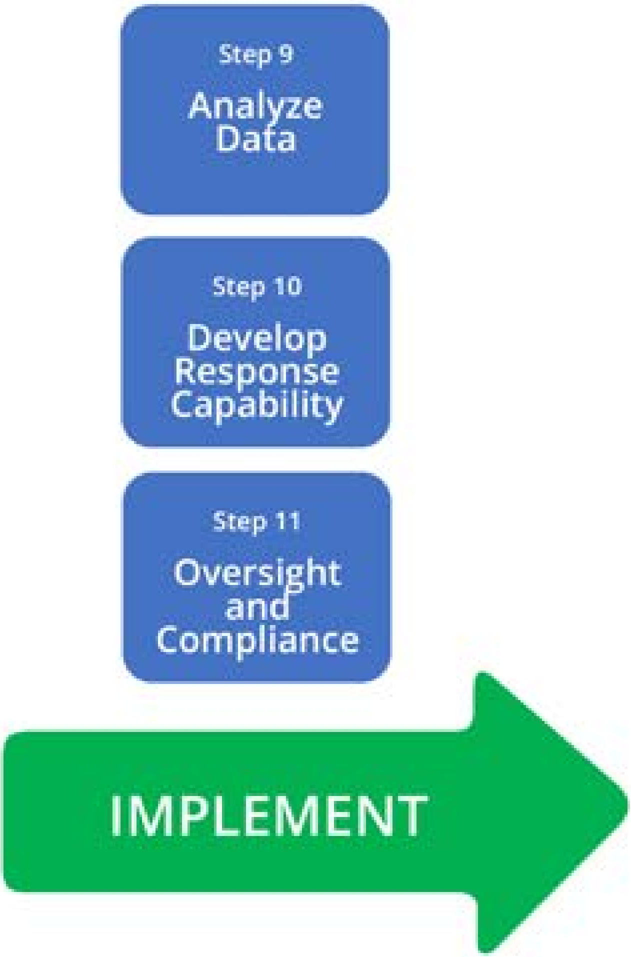
1) Develop the messaging plan – This will depend on your corporate culture and whether you have recently experienced an incident or have a history of security incidents and compromises. If you are starting at ground zero, then you will need to put forth more time and energy into formulating a more holistic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

2) Craft communications (email, flyers, 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 Team. This step should take approximately 4 weeks to complete. 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.



Step 9

Analyze Data

Step 10

Develop Response Capability

Step 11

Oversight and Compliance

IMPLEMENT

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: *You should strive to be as transparent as possible with your employees. Their involvement and support is critical to the continued viability of your Program.*

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 Team.

Timeframe: This step should take approximately 2 weeks to complete.

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
Network	Criminal
Off-network	PAI
HR	SM
Reporting	
Badge	

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

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 Team.

Timeframe: This step should take approximately 1 week to complete.

Justification: This step is necessary because time is of the essence after a security event or incident. 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, as well as local law enforcement and prosecutorial officials.

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

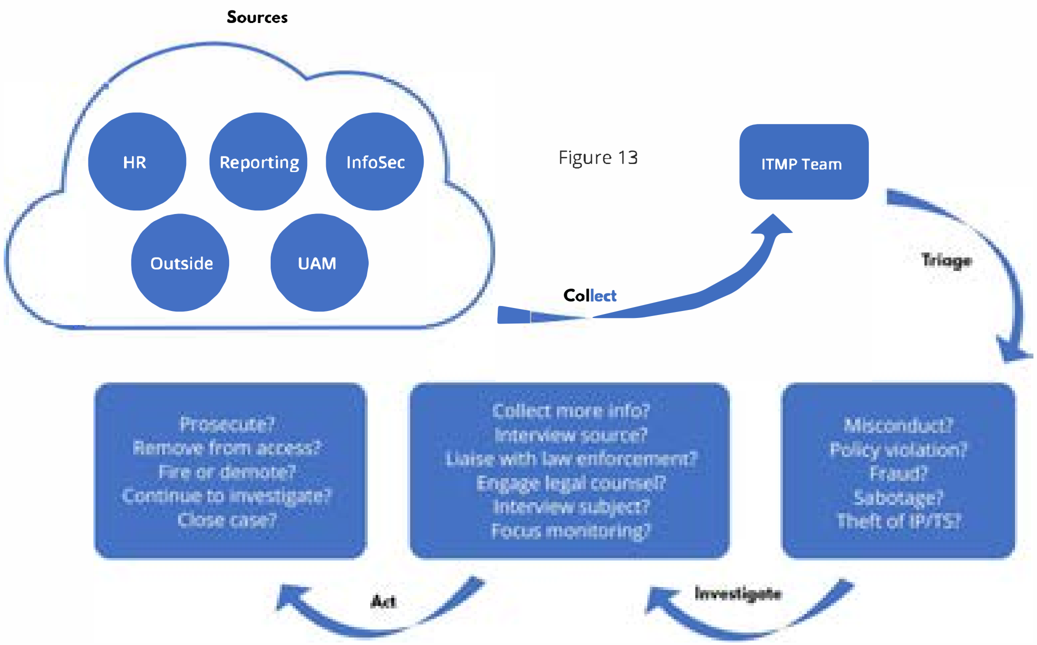


Figure 13

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, UAM, 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 usable by law enforcement. Seek help from outside experts early in the process if there is evidence of criminal activity.*

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, 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 Team.

Timeframe: This step should take approximately 1 week to complete.

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 O&C lead – An FTE 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.

CONCLUSION

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 stove-pipes. 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 regularly check the website InsiderThreatManagementProgram.com for updates and quarterly commentary on the topics discussed in this Guide. You are also encouraged to reach out to the authors and provide us with your feedback on how we can improve upon this Guide for future releases.

GABRIEL FRIEDLANDER

Founder and CTO
ObserveIT
gaby@observeit.com
www.observeit.com

About ObserveIT

ObserveIT is a lightweight endpoint solution that is focused on identifying and eliminating insider threats. ObserveIT identifies and eliminates insider threats with real-time security awareness, precise visibility and fast investigations.

SHAWN M. THOMPSON, ESQ.

Founder and President
Insider Threat Management Group
shawn@itmg.co
www.itmg.co

About ITMG

ITMG is a leader in providing tailored insider risk management advisory services to the private sector. ITMG’s line of services include Baseline Reviews, Insider Risk Assessments, Program Development and Enhancement, Insider Threat Law Consulting, Insider Threat Program Training, and Strategic Consulting.

APPENDIX A

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. Independent consultants can be an invaluable resource to help baseline your program and apply their subject matter expertise and experience-driven best practices.

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?
- 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 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 UAM policies and procedures in place?
- Do you have specific policies and procedures governing the collection, use, and dissemination of UAM data?

Data Analysis

- Do you have the ability to analyze insiders' interaction with 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?

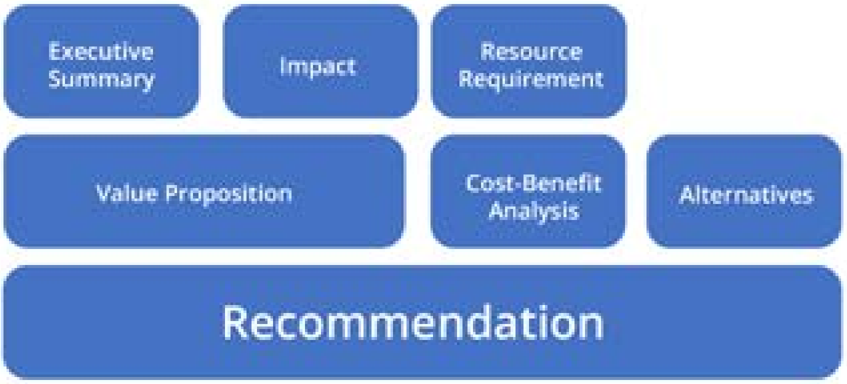
Insider Risk Assessment

- 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?

APPENDIX B: INSIDER THREAT MANAGEMENT PROGRAM BUSINESS CASE TEMPLATE



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?

III. Impact and Resource Requirements.

- For each solution define costs:
  - Human capital
  - Licenses
  - O&M
  - Equipment
  - Space

IV. Cost-Benefit Analysis and Alternatives.

- Why should your project be funded?
- Focus on value versus costs per sé (you need to guard against the bias that any security expenditure is simply 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
    - Create asset protection culture
    - More efficient decision-making
    - Early threat detection
    - Lower remediation costs
    - 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

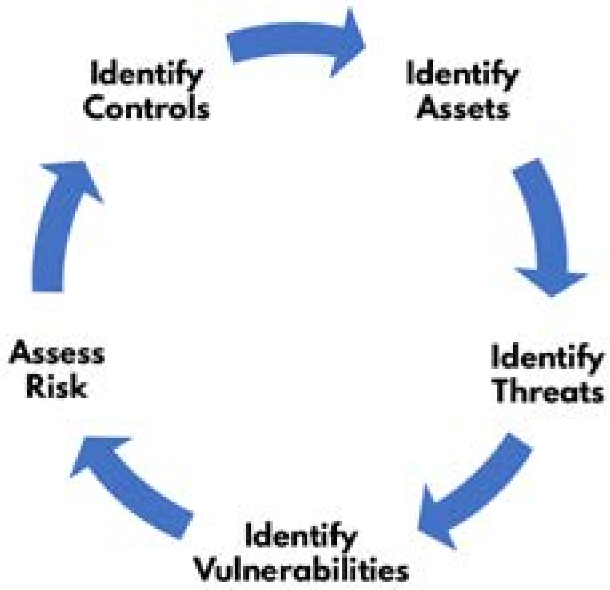
APPENDIX C: INSIDER RISK ASSESSMENT OUTLINE

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.

This five-step process is iterative vice 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 and presented to the client 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-related 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

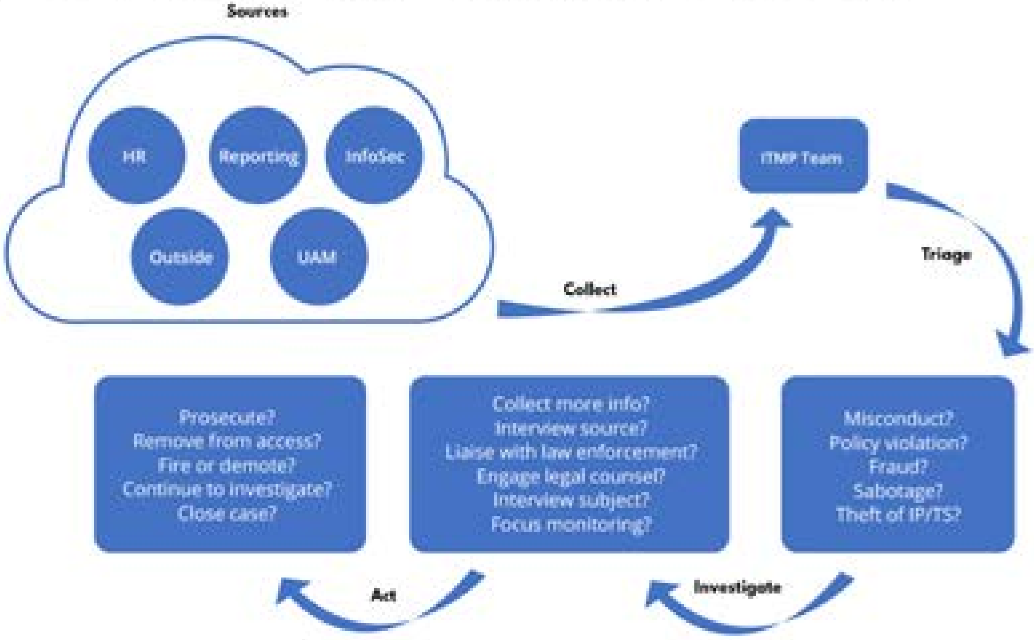
Step 4. Assess risk and determine priorities for asset protection

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

APPENDIX D: RESPONSE WORKFLOW



InfoSec Reporting Example Scenario

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

Triage: Insider Threat Team obtains additional information from InfoSec, HR and Management on whether the DLP 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, negligent, or within company policy?

Investigate: : The Insider Threat Team reports the DLP 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-up 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 DLP in order to exclude these type 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 results the Insider Threat Team will either close the case or consult with the legal department on necessary follow-up actions.