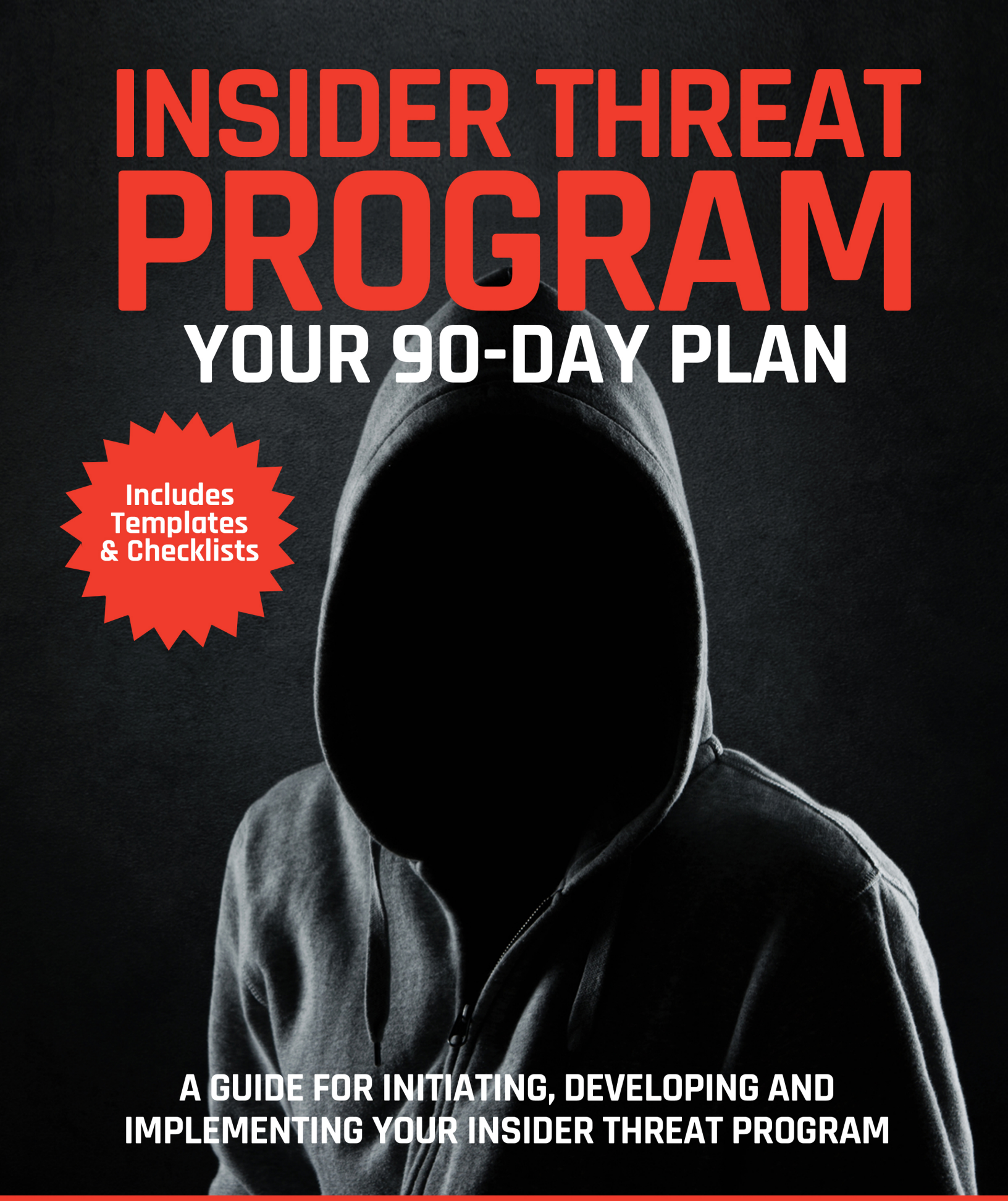
INSIDER THREAT PROGRAM

YOUR 90-DAY PLAN

Includes Templates & Checklists



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

Shawn M. Thompson, Esq.

Gabriel Friedlander

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.

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.

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.

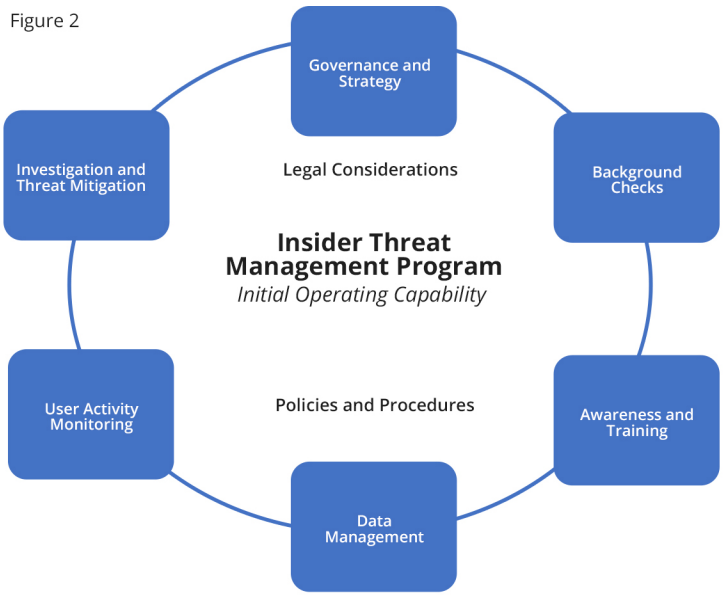
You Must Monitor Insiders' Behavior. Knowing how people behave within data, services, and applications is crucial in order to evaluate the risk and likelihood of an insider threat. Monitoring user behavior, coupled with full video captures of risky behavior, will provide unequivocal proof during the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

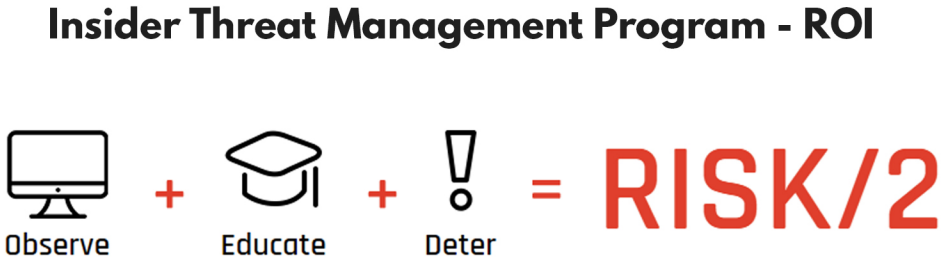
1 See Full Operating Capability discussion, page 19.

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



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.

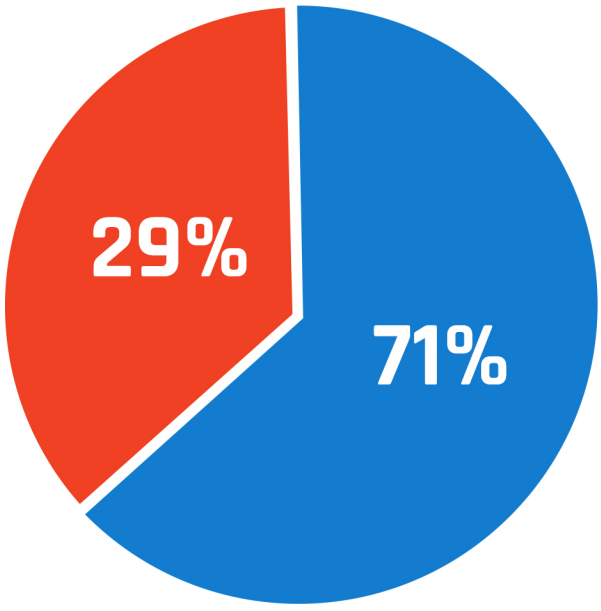
The Unintentional Insider Threat

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

[2] Experian 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



Malicious
Fraud/Data theft
Inappropriate access
Disgruntled employee

Unintentional
Misuse of systems
Honest mistakes
Cloud apps

* 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.

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.