exabeam®

INSIDER RISK MANAGEMENT

Adapting to the Evolving Security Landscape

SHAWN M. THOMPSON, ESQ.

SHAWN M. THOMPSON, ESQ.

MR. THOMPSON IS THE FOUNDER AND CEO OF ITMG (ITMG.CO), the leading insider risk management service provider to the private sector. He possesses over 20 years' experience investigating, prosecuting, and managing insider threats and is widely sought after for his unique expertise. He is a former federal prosecutor and senior government official who held executive positions with several agencies, including the FBI, NSA, and DNI. As a seasoned risk management professional, experienced prosecutor, credentialed special agent, and trained analyst, his cybersecurity 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.

TABLE OF CONTENTS

FOREWORD

TODAY, IT IS INCREASINGLY DIFFICULT FOR ORGANIZATIONS TO SECURE THEIR CRITICAL ASSETS.

As the workforce continues to evolve with employees working remotely, storing information in the cloud, and a global workforce, corporate data can be accessed from almost anywhere, instantly. Leaving critical assets susceptible to being accessed, downloaded and stolen within seconds, and without raising suspicion.

Why Is This Important?

Insider threats comprise the majority of security incidents impacting an organization. Insider attacks involve malicious and negligent activity against an organization that comes from people within. The usual suspects are employees or contractors with access to an organization's network, applications, or databases. The term is most commonly used to describe illicit or damaging online actions.

While most often associated with stealing information, any action that could negatively impact an organization falls into the insider threat category. These include sabotage, fraud, and espionage. A disgruntled or recently terminated employee might, for example, shut down or lock critical systems in a deliberate attempt to damage the business or reputation of an organization.

Typically, insiders carry out their plans via abuse of access rights – both physical and online. In its simplest form, employees or contractors may search file shares looking for sensitive information that is not properly secured via system access controls. In the case of a compromised insider, the attacker may try what is known as privilege escalation, which is taking advantage of system or application flaws to gain access to resources they do not have permission to access.

Different Motivations and Behaviors

Organizations can spot or predict insider threats by observing user behavior in the workplace and online. Being proactive may allow you to catch potential malicious insiders before they exfiltrate proprietary information or disrupt operations.

Some risk signs in the workplace that should be heeded include an employee's interest in matters outside the scope of their duties, working odd hours without authorization, and excessive negative commentary about the organization. User behaviors that fall outside the norm of usual behavior patterns of an employee and their peer group can be indicative of an emerging threat.

Behaviors are not limited to users. Entities, laptops, computers, devices, and routers that demonstrate unusual behavior are also a harbinger of possible breaches. An unsecured port, a port that's never been used or excessive activity are some of the behaviors that are associated with entities.

There's a solution. Organizations can protect their networks and reputation from breaches and damage. Some companies have seen tremendous success using new and emerging technology to protect their environments. This shows that with the right implementation, they, and you, can get in front of threats.

FOR MORE INFORMATION ON HOW EXABEAM CAN HELP YOU DETECT POTENTIAL THREATS BEFORE THEY MAKE HEADLINE NEWS VISIT EXABEAM.COM.

INTRODUCTION

INSIDER RISK[1] MANAGEMENT IS AN OFTEN DISCUSSED, YET LARGELY MISUNDERSTOOD, TOPIC.

Most security practitioners view the insider threat problem through a pure threat lens (e.g. *all employees are threats*), yet others see it as a compliance exercise (e.g. *addressing NIST and ISOO gaps*). The key and real value, however, is to view insider threat as a risk management problem and see it in the context of asset impacts, vulnerabilities, and threats. In so doing, the organization can gain proper insight into its true risk posture. The purpose of this book is to provide necessary thought leadership on best practices for managing insider threats through the application of a defined *insider risk management* model.

This book is divided into three sections. Section One frames the insider threat problem, highlighting the prevalence and impact of insider threats and common management challenges. Section Two defines the backdrop and context within which security managers must deal with the problem of managing insider risk. This section will explore the changing mindsets of insiders, and how the changing employee culture and workplace environment create a security tinderbox. Section Three focuses on solutions and strategies for effectively managing insider risk, including practical strategies for improving any insider risk management program.

[1] The terms "insider risk" and "insider threat" will be used throughout this book to accurately describe the context and nature of the given topic. While risk is different from threat, as will be discussed, the latter is used colloquially to describe all efforts to manage insider impacts. As such, the terms will be used interchangeably to reflect the generally understood meaning and common usage of each.

Section 1

—

THE PROBLEM

The bedrock principle is that insider threat is about people.
People with different roles and interactions within the organization.
People who are interconnected and who comprise an organizational ecosystem.
Most importantly, people who can impact an organization in multiple ways.
This section explores the problem of insider threat, defining key terms
and challenges and exploring the scope of the problem itself.

INSIDER RISK MANAGEMENT – MORE THAN JUST A THREAT

INSIDER RISK MANAGEMENT OR "INSIDER THREAT MANAGEMENT," IS OFTEN THE ELEPHANT IN THE ROOM.

The topic itself is so taboo in some organizations that the terms are "softened" to descriptions such as "insider trust," "employee enablement," and "employee loyalty." While there is nothing wrong with these descriptors (it matters not what the program is called but the substance that underlies it), employing such euphemisms tends to distract and detract from the true objective – risk management.

Threats from insiders (employees, contractors, partners, etc.) must be understood in the proper context. Most "experts" simply focus on the threat itself (i.e. the actions of insiders that cause harm). This, however, is shortsighted and results in a purely reactive security posture. This focus must be able to build and deliver an actionable program that encompasses asset impacts, the vulnerabilities to those assets, and the threats posed.

Risk management is an aggregation of the assessment of harm to a given asset, taking into account the likelihood that a particular threat could exploit a known vulnerability. Risk management is a discipline that is applied to a wide range of domains including financial risk management, security risk management, cyber risk management, etc. At its core, regardless of the domain to which it is applied, risk management includes some information on asset impacts, vulnerabilities, and threats. Removing one of the three elements from the equation, removes the ability to conduct proper risk management. Too often the terms risk and threat are used interchangeably, which leads to a mischaracterization of the problem itself. This then leads to asking the wrong questions and pointing the ship in the wrong direction. Threat is an *element* of risk. Threat does not equal risk and simply conducting a threat assessment is not, in itself, managing *risk*. Risk comprises three elements: impact, vulnerability, and threat.

For example, conducting a traditional NIST or ISOO assessment where controls are examined and gaps identified and scored is a "vulnerability" assessment. Likewise, conducting a review to determine the most likely threat actors and their relative capabilities to attack is a "threat" assessment. Moreover, conducting a business impact assessment or a more tailored assessment to determine the level of harm to the organization if an asset were to be compromised is an "impact" assessment. The parts (impact, vulnerability and threat) are individually valuable, but must be combined to represent and capture true risk.

THE RISK OF APPLYING TRADITIONAL "RISK" MODELS TO INSIDER THREAT

IMAGINE SPENDING MILLIONS OF DOLLARS ON "SECURING" YOUR COMPANY ONLY TO DISCOVER THAT AN EMPLOYEE TOOK YOUR CROWN JEWELS TO A COMPETITOR.

The impacts are devastating. Millions of dollars in R&D lost, reputation is tarnished, and your business goodwill suffers. This is, unfortunately, not an uncommon occurrence and one that occurs despite the billions of dollars spent on traditional security. So why do these types of compromises continue to occur?

Misplaced Threat Focus and False Assumption

Traditional security focuses on external threats yet many breaches succeed simply by exploiting basic security laws (unpatched software, factory server password settings, etc.) and the social engineering of insiders. Moreover, a significant amount of breaches are intentionally facilitated by trusted insiders themselves. Thus, focusing only on the outside hacker misses the mark because insiders, through poor security practices, negligence, or intentional misconduct, are the weak link in the cybersecurity chain.

In addition, traditional security falsely assumes that insider threats cannot be prevented. As such, most controls and resources are dedicated to detecting network threats only, which loses sight of the real problem – employee behavior. As a result, the cycle of compromises and breaches continues.

SOLUTION – FOCUS ON INSIDER THREATS

- Roughly two-thirds of all security events are caused by insiders.[2]
- Employees are the most cited culprits of security incidents.[3]
- The great majority of intellectual property theft is committed by insiders.[4]

Risk Is Largely Misunderstood

Traditional security risk management views risk in several ill-defined ways. The first is that risk equals threat. The second is that risk equals vulnerability. A third position defines risk as threat plus vulnerability. The problem with these views is that they fail to properly combine the three essential components of risk – impact, threat, and vulnerability.

SOLUTION – PROPERLY DEFINE RISK

True risk is the likelihood that a given asset can be compromised by an identified threat by exploiting a current vulnerability. The asset is the key component of risk since it is the particular asset whose compromise could have deleterious effects on your business. Stated another way, without a defined impact to an asset, there is no risk. Similarly, if there is no threat or vulnerability there is also no risk to an asset. It is, therefore, the combination of all three that define and capture the true risk posed to an asset.

Traditional Assessments - Wrong Questions and Wrong Problem

Traditionally, security managers have relied on NIST, COBIT, and ISOO frameworks for measuring "risk." These frameworks, however, only provide a way to assess network-centric organizational risk, not insider risk.

They are vulnerability models and do little to inform an organization about specific asset risks. Thus, a security manager seeking to protect critical assets will be left with many unanswered questions.

SOLUTION – APPLY AN ASSET-FOCUSED INSIDER RISK MODEL

Effective security requires an effective security risk model that assesses and manages risk by focusing on insiders' interaction with critical assets. All threats are not equal, nor are all vulnerabilities and assets. Effective risk management requires risk prioritization. First, assets must be properly identified and impacts determined. Second, specific threats and vulnerabilities related to each asset must be identified. Third, risks to each asset must be properly measured. Lastly, mitigation strategies must be developed. Through this method, an organization can more effectively apply security measures in the most efficient and cost-effective manner leading to an enhanced security risk posture.

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

[3] Kaspersky – The Human Threat in IT Security (2018), Verizon DBIR (2019), IBM X-Force Threat Intelligence Index 2018

[4] The Commission on the Theft of American Intellectual Property (IP Commission, http://www.ipcommission.org/ U.S. Department of Commerce, Intellectual Property of the U.S. Economy (2016)

CHALLENGES – YOU'RE NOT ALONE

THIS SECTION WILL IDENTIFY THE MAJOR CHALLENGES TO MANAGING INSIDER RISK AND PROPOSE PRACTICAL SOLUTIONS TO OVERCOMING THEM.

Who's the Boss?

As the saying goes, "a house divided against itself cannot stand." Similarly, an insider threat program (ITP) without a clearly-defined leader will also fail. Too often companies neglect to appoint a leader out of a "team approach" mentality or out of deference to current management fiefdoms. The result of putting everyone in charge is that no one is in charge.

This doesn't require an insider threat "czar" with total control and veto authority over all things related to security and risk management. What is required, however, is an individual who is ultimately responsible for fostering collaboration across functions, bolstering capabilities, and measuring and reporting progress to leadership. The government refers to this role as the "senior official" responsible for managing insider threat. In corporate America, this official may be any of the following: CRO, CSO, CISO, or CAO.

CHIEF RISK OFFICER

The CRO *may* be the best person to lead the ITP. This largely depends, however, on the scope and role of the CRO. Some CROs focus only on the strategic risk of the company. They set organizational risk tolerances and may develop methodologies for capturing and measuring risk postures. In this model, the operational risk is still "owned" by the operational leaders (CSO, CISO, business units, etc.). CROs that fall into this category are not well positioned to lead an ITP because they lack the visibility and operational granularity required for an ITP. Other CROs, however, focus on both the strategic and operational risk of the company. They not only set organizational risk tolerances, but also are involved in measuring, managing, and improving the operational risk posture of the organization.

CROs in this group are well positioned to lead the ITP. They will often have the necessary high-level authority (report to CEO, Audit Committee, etc.) and by virtue of their scope, will also have the necessary relationships across all functions of the organization (business units, legal, HR, CSO, CISO, etc.). While the "ownership" of the risk itself may still be the purview of the operational leaders, CROs in this group will often have joint responsibility and reporting requirements. This will make them a vested and empowered leader ideally suited to lead a cross functional program like an ITP.

CHIEF SECURITY OFFICER

A logical choice to lead the ITP is the CSO. They often have existing working relationships across the organization, including legal, HR, risk, and cyber. This grants them the necessary perspective and influence to foster collaboration on improving insider threat capabilities. Some CSOs, however, lack a comfortable understanding of the technical aspects of insider threat management and may not feel empowered to lead the ITP. For example, insider threat tools are often owned by the CISO and thus are responsible for the testing, implementation, and maintenance of each tool. This can be a heavy lift in both human capital and financial resources. As such, CISOs are and need to be heavily engaged in any ITP. This fact notwithstanding, CSOs can still be effective by creating solid working relationships and workflows between functional organizations, including the CISO, and leveraging the collective expertise of all groups.

CHIEF INFORMATION SECURITY OFFICER

The traditional choice to lead the ITP is the CISO. Insider threat has been traditionally viewed as a subset of cybersecurity. As such, CISOs are the logical choice to lead any efforts designed to manage threats to the organization – internal or external. This view is changing, however, as insider threat is a unique discipline that encompasses a broad range of security, HR, cyber, and legal disciplines. CISOs are also, almost exclusively, focused on "digital" security or data-centric security. Insider threat is by definition a human problem, not a data problem. As a result, CISOs may unduly limit the scope of an ITP by virtue of the scope of their role and function. Moreover, CISOs that report to the CIO (which is common) arguably have a natural conflict of interest.

The mandate of the CIO is to ensure the confidentiality, integrity, and availability of information (i.e. make sure employees can do their jobs). This mandate isn't always in alignment with the security needs pertaining to insider threat, which may result in funding for insider threat being delayed or limited at the expense of other CIO priorities.

CHIEF ADMINISTRATIVE OFFICER/GENERAL COUNSEL/HUMAN RESOURCES

While not the traditional leaders of an ITP, senior executives in this group may become the de facto leaders by virtue of how the organization is structured. In some organizations, the Chief Administrative Officer (CAO) is a dual-hatted role that may also be the General Counsel or Chief of HR. In these scenarios, some security functions may also report up to the CAO. Thus, many of the ITP functions and responsibilities may flow up to the CAO. The CAO will often have the ear of other top executives and as a result can be a strong enabler of the ITP. This governance structure may work as long as the CAO is supported by a strong group of senior security leaders. Without strong senior and mid-level managers, this model will lack the direction and subject-matter expertise required to properly develop, implement, and sustain an ITP.

Messaging

Messaging or "telling the story" is arguably the number one success factor for an ITP, above obtaining executive buy-in and governance. The reason is that before buy-in or governance can be achieved, decision-makers need to hear and understand the purpose and the need for an ITP. This is no simple task. Every organization has a unique culture, leadership styles, and corporate environment that needs to be understood to craft a proper message. In addition, the form of the message can be as important or more important than the substance. For example, if your leadership prefers in person briefings, sending them a 25-page strategy document alone will not suffice. Likewise, spending time on an elaborate PowerPoint may be a waste of time, if they only want to hear from you in person. Still others may want the slides! The point is to do your homework and determine how leadership wants the message to be delivered.

Forming a relationship with your communications team is always a good first step. They will know and understand how best to deliver an impactful message. Messaging is not, however, only a vertical exercise.

While this should be your first focus, it is equally important to deliver your message across functions and to the entire workforce. Here again, your relationship with your communications team will pay dividends. The message must be tailored to your audience and aligned with specific objectives.

Losing the Balance

To promote a proactive strategy, certain methods are required to ensure that the organization has the ability to respond to actions that pose harm. In this context, privacy policies must not be overly restrictive but must strike the proper balance between protecting employees without unnecessarily restricting legitimate and tailored security efforts. Similarly, security must be customized and pursue a least restrictive means methodology to strike the proper balance between protecting the organization's assets without unnecessarily impacting legitimate privacy interests of employees. ITP policies and procedures must be mutually developed and coordinated between the ITP and legal and privacy personnel to ensure a proper balancing of equities.

Lack of Program Definition

Insider risk management processes and governance structures have been traditionally defined within the context of investigative processes. This has led to a myopic and narrow focus on *responding* to known threats and events. While *investigative* processes and procedures are often better defined and supported with a clear governance structure enabled by policies and procedures, "insider threat" is much more than responding to security alerts or investigating anomalous behavior. As a result, many essential Insider Threat Program components are not included in current security risk management governance structures.

Lack of Knowledge of Critical Assets

The most basic function of an insider risk management program is to protect the assets that provide the organization with its competitive advantage. This requires a complete understanding of critical assets. An asset is something with potential value to an organization and for which the organization would suffer harm if the asset were compromised. Critical assets can be both physical and digital and can include facilities, systems, equipment, and technology. A complete understanding of critical assets (both physical and digital) is essential in defending against threats, both internal and external, that will often target the organization's critical assets.

INSIDERS ARE THREATS

FROM A BUSINESS RISK PERSPECTIVE, IT MATTERS NOT WHETHER THE HARM WAS CAUSED BY OUTSIDERS, INSIDERS, NEGLIGENCE, ORGANIZED CRIME, OR A NATION-STATE.

What matters is that harm was in fact caused that negatively impacted the organization. The bottom-line is that threats from both outsiders and insiders must be properly managed to adequately protect your organization. That said, insider threat is often overlooked or simply mitigated as an "HR problem" without formally addressing the root cause of the problem itself. Understanding the true nature of each is necessary to manage the greatest amount risk at an acceptable cost.

What We Know

Insider threat is a growing problem.[5] Insider threat incidents are on the rise, with most organizations experiencing more incidents within the last year.[6] Organizations are not prepared to prevent, detect, or manage insider threats,[7] but they are increasingly implementing controls to manage them.[8]

Employees continue to be the biggest threat to corporations[9] and cause twice as much damage as external threats.[10] Research suggests that two-thirds of all security events are caused by insiders and a large percentage of these are caused by insiders leaving the organization.[12] The great majority of these, however, are caused by unintentional insider threats[13] that are difficult to detect because traditional security devices and solutions are primarily designed for detecting malicious activities.

Nature of the Threat

Hackers by nature are disruptors. They seek to gain access to your systems to deny service and impact operations (e.g. denial of service attacks, ransomware, etc.). They also may seek personally identifiable information to sell on the Dark Web. Hackers by definition have one way in and one way out – through your network (leveraging credentials of insiders notwithstanding). They have limited ingress and egress opportunities. Conversely, insiders have multiple ingress and egress opportunities and often target sensitive information (trade secrets, IP, business plans, etc.) to use for their personal benefit. Insiders may also seek to disrupt the business (e.g. sabotage), leak information, commit fraud, or engage in workplace violence. The insider threat vector is, therefore, much greater than the outsider.

---

[5] V2018 Insider Threat Report, Cybersecurity Insiders

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

[7] Netwrix 2018 Cloud Security Report; 2018 Insider Threat Report, Cybersecurity Insiders

[8] 2018 Insider Threat Report, Cybersecurity Insiders

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

[10] CERT Insider Threat Center

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

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

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

Perception v. Reality

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

PANDORA'S BOX – NOW IT'S A PARTY

PROPERLY ADDRESSING THE INSIDER THREAT PROBLEM REQUIRES AN UNDERSTANDING OF WHY INSIDER THREAT IS AN ELUSIVE, DIFFICULT, AND EVOLVING PROBLEM.

This section will highlight the risk changes that organizations face which will allow for a clearer security direction moving forward.

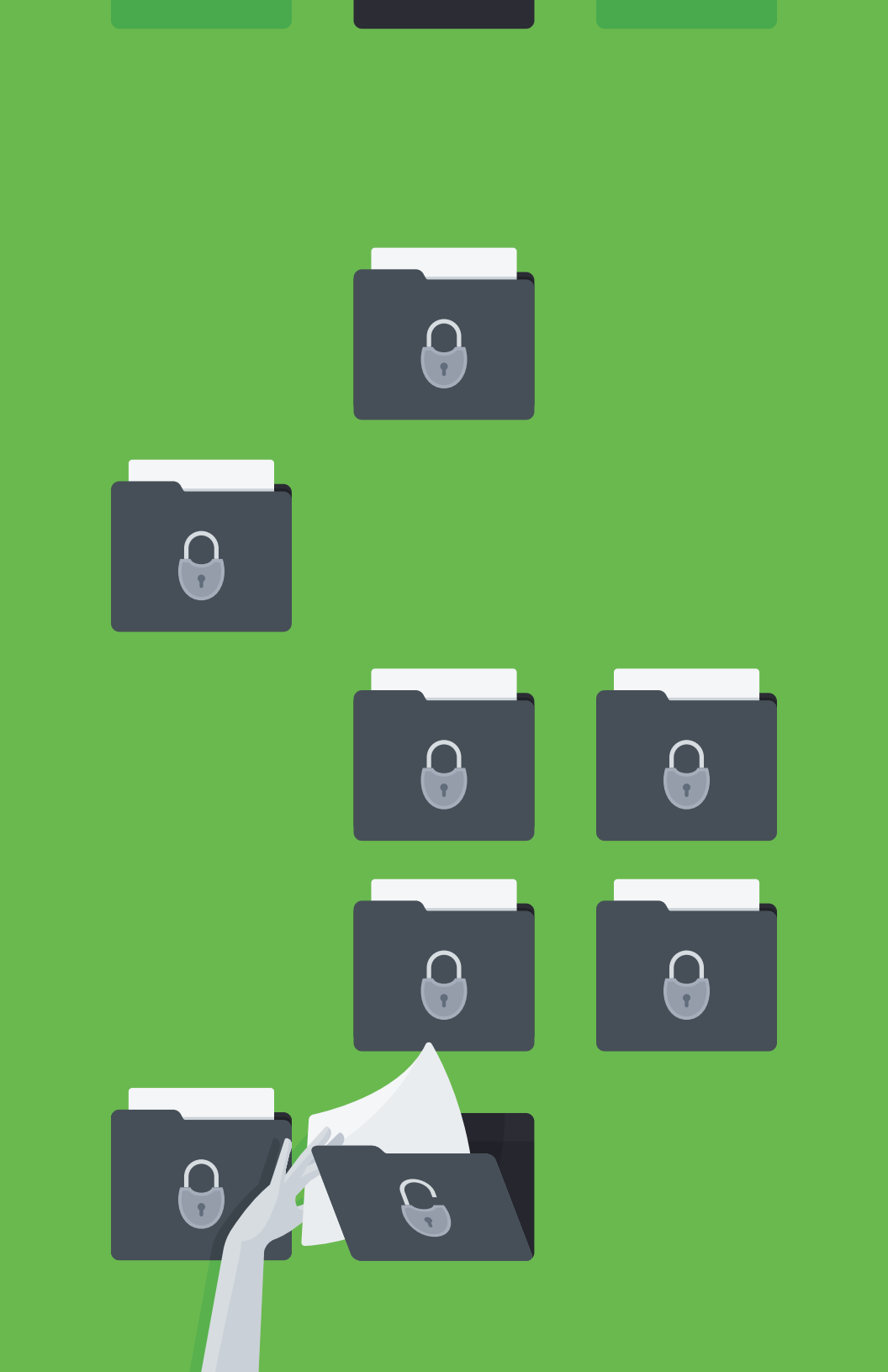
Managing insider risk is a security nightmare. The security manager's task is to protect corporate assets from the very people who are granted legitimate access – insiders. These insiders may access information at the office or at home, on a corporate device or a personal one, on a corporately-managed network or in the cloud or, in most cases, all of the above. In addition to these "opportunities" to steal corporate secrets, insiders may have various "motivations," including greed, unmet expectations, revenge, etc. Last but not least, insiders may be "triggered" to steal sensitive data by leaving for a new job, being denied a promotion, being transferred or reassigned, or being fired.

This "powder-keg" of a threat becomes even more challenging by the lack of tools and restrictions placed on security managers to deal with insider threats. For example, corporations are very deferential to any potential privacy impacts on employees – real or imagined.

This leads to an uphill battle for any security manager seeking to implement tools that can monitor employee behavior or otherwise identify behaviors indicative of insider threat.

Beyond tools, the nature of insider threats requires a cross-functional program from across the organization. Collaboration and sharing between HR, CSO, CISO, CRO, business units, and legal is necessary to manage insider threats. This also is hampered by perceptions on privacy and when combined with the inherent stove-piping that exists in many organizations, the security manager is quickly hand-tied.

In today's workplace, we give more access to insiders, on more devices and networks, without providing the resources necessary for the security manager to properly manage the resultant risk.



Section 2

—

THE CONTEXT

Employee loyalty is declining, and privacy often trumps security. Consequently, organizations need to build resilient security programs that evolve from a “trust but verify” to a more “zero-trust” security model. This requires an understanding of the insider threat context and environment. From Hansen to Snowden, this section will arm the reader with an understanding of the “new breed” of insiders, how they think, different personas, common insider threat events, and insider risk management trends.

PREVALENCE AND IMPACT – HOUSTON . . . WE HAVE A PROBLEM

TOO OFTEN, ORGANIZATIONS FAIL TO PROPERLY DEFINE THE PROBLEM.

Resultantly, their security efforts (strategies, objectives, and tools) miss the mark. Insider threat is more than an employee intentionally stealing IP. It covers both intentional and unintentional threats and includes a range of personas and events, including fraud, sabotage, theft, unauthorized disclosures, and workplace violence.

How an organization defines insider threat will dictate the parameters of their insider risk management program. Failing to properly define insider threat causes ambiguity of objectives, roles, and responsibilities. This confusion and lack of direction inevitably leads to disagreements over roles and funding, which ultimately leads to apathy and the demise of the program itself. A best practice first step is to capture and define the scope of the program by determining which personas and event types the organization seeks to address.

INSIDER THREAT PERSONAS

Leakers

Leakers represent the newest breed of insider threats. Historically, organizations could generally rely on the loyalty of its employees. It was not uncommon for employees to work for an organization their entire career. As a result, employees tended to protect their organization and develop a deep sense of loyalty to it, which inhibited actions such as leaking that could cause damage to the organization. This model, however, has drastically changed. Employees today no longer feel the same sense of loyalty. This is due to several reasons, including the nature of the workforce, the increased job switching, and evolving corporate environments. This has resulted in a workforce that is less stable, committed, and content with the status quo.

Consequently, employees may take actions that harm organizations because they are protesting the organization itself, a specific action, or to obtain personal notoriety at the expense of the organization.

THERE ARE FOUR TYPES OF LEAKERS:

- **CONSCIENTIOUS OBJECTOR:** An individual who opposes an organization's purpose, actions, or philosophies
- **SYMPATHIZER:** Person who knowingly misuses an organization's systems to attack others in support of an external cause, but with harmless intent to the organization itself
- **ACTIVIST:** Highly motivated supporter of a cause
- **SELF-AGGRANDIZER:** Seeks publicity and acknowledgment

Careless

Careless insiders are often overlooked in most research and academic activity and are often not even included in the definition of insider threat itself. This is a major flaw, however, as unintentional insider threats represent the largest group of insider threats. Most research suggests that 50 to 75% of insider threat events are caused by careless insiders. It is important to include this group in the definition of insider threats for this reason. Moreover, security controls and training can directly and positively impact the occurrence of this type of threat. Research suggests that implementing dynamic education processes that seek to inform users in near real time of their policy or procedure violations, can decrease future occurrences by 75%.

THERE ARE TWO TYPES OF CARELESS INSIDERS:

- **RECKLESS:** Person who knowingly and deliberately circumvents safeguards for expediency but does not intend harm or serious consequences.
- **NEGLIGENT:** Person who carelessly or unknowingly misuses systems or compromises assets, this includes victims of phishing scams.

Disgruntled

Disgruntled individuals represent the largest group of insider threats. These individuals have experienced certain triggers that have impacted their current view of the organization itself or their particular role in the organization. These individuals may also be the most difficult to identify based on the ubiquitous nature of the underlying causes themselves. All employees will experience certain events whether at work or in their personal life that may impact their work productivity, morale, or outlook. The truly disgruntled employee, however, allows these events to manifest themselves into hostility towards the organization by serving as triggers to harmful actions. An unhappy individual who feels unfulfilled later loses the previous connection to the organization.

THERE ARE GENERALLY THREE CATEGORIES OR CAUSES OF DISGRUNTLEMENT IN EMPLOYEES:

- **UNMET EXPECTATIONS:** Individuals who feel they have been *passed over for promotion, denied a bonus,* or removed from responsibilities may be disgruntled and unsatisfied at work.
- **WORK EVENT:** Individuals who experience certain work events may also become disgruntled. Work events might also include such things as *being denied promotion and bonuses* but also include such things as work conflicts, HR issues, or unstable work environments caused by harassment, job or role changes, or larger organizational changes such as a merger or acquisition, reduction in force, or management changes.
- **LIFE EVENT:** Individuals who experience certain life events may also become disgruntled. Life events include money problems, divorce, crime, drugs, alcohol, and depression.

Opportunist

An opportunist is an individual who seeks to better themselves at the expense of the current organization. These individuals are not necessarily seeking to harm the organization itself but are seeking to better themselves through the advancement and creation of a new opportunity.

Profit is not the primary motivating factor such as for the thief. Here, the opportunist is generally entrepreneurial in spirit and seeks to advance themselves through new ventures or positions. While these individuals do not necessarily seek to harm the organization or to maximize immediate profit to themselves, each is a real and axiomatic consequence of their actions.

OPPORTUNISTS FALL INTO THREE CATEGORIES:

- **NEW JOB WITHIN THE COMPANY:** These individuals are unhappy with their current work role or job function. They seek to obtain a different position within the company itself. This may be within the current division or department or with a new division within the company. These individuals do not seek to harm the company but will often circumvent security controls and measures to gain access to information that will better themselves for a new position. This might include accessing employee profiles, databases of sensitive projects, or unlawfully accessing or using credentials of other employees.
- **START A NEW COMPANY:** These individuals seek personal gain by obtaining an advantage by co-opting company information, using company resources, or using company time to work on their new venture. These individuals may seek sensitive or proprietary information to use in their new venture or they may simply want to gain competitive advantage by collecting customer information, pricing information, and strategy information pertaining to new product releases or customer acquisition strategies.
- **JOIN A COMPETITOR:** These individuals are similar to those who seek to start their own company. However, this group tends to seek sensitive intellectual property that they perceive to be of value to a competitor.

Thief

A thief is an individual solely motivated by profit. Thieves are distinguished by opportunists in several ways. The first is that these individuals do not seek to start their own company or to work for a competitor. Second is that these individuals will steal anything of value to include intellectual property, personally identifiable information, health information, financial information,

or other valuable data. These individuals also, in addition to information theft, will steal tangible corporate property — computers, supplies, electronic devices, or other corporate owned assets — for their own gain. These individuals tend to be lower-level employees and are often involved with outside conspirators to whom they sell the information or assets for personal gain. For example, they may sell health information to an organized crime syndicate for identity theft.

Conspirators

Conspirators seek to harm the organization by any means necessary. This may include attacks on an organization's employees, information systems, facilities, or the reputation and goodwill of the organization itself. These individuals have specific and defined purposes for acting. Profit is generally not the motive but an ancillary benefit of the damaging actions themselves. For example, a competitor may seek to damage the reputation and goodwill of an organization for the primary reason of harming that organization. The competitor, however, will inevitably receive some ancillary benefits to any reduction in profits of the organization itself.

THERE ARE FOUR MAIN TYPES OF CONSPIRATORS:

- **COMPETITOR:** Business adversary who competes for customers, revenues, public exposure, or resources
- **NATION-STATE:** State-sponsored attacker with significant resources, and able to affect a major disruption on a national scale
- **ORGANIZED CRIME:** A crime syndicate with significant resources and attack skills
- **TERRORIST:** A person who relies on physical violence or extreme acts to support a socio-political agenda

INSIDER THREAT EVENTS

Leak (Unauthorized Disclosure)

Leaking of intellectual property or data on the part of the insider. Leaks may be caused by carelessness, unfamiliarity with or circumvention of information security protocols, or be intentional.

EXAMPLES INCLUDE:

- Unwittingly providing information in a phishing attack
- Talking about sensitive matters to a person without appropriate clearance
- Leaving sensitive documents to others
- Posting confidential details to social media sites

Misuse

Broadly encompasses any insider use of enterprise resources in ways that bypass or ignore safety or security protocols; violate enterprise policies; are unrelated to the insider's job; are illegal; or otherwise potentially harm the enterprise, intentionally or unintentionally.

EXAMPLES INCLUDE:

- Using an enterprise server inappropriately for personal gain
- Using the enterprise printer to print hundreds of wedding invitations
- Downloading pirated movies onto an enterprise laptop

Fraud

Using insider access to divert enterprise financial resources to oneself. In short, stealing money from the company.

EXAMPLES INCLUDE:

- Influencing others to use a supplier with whom the insider has an existing financial relationship
- Expense report fraud
- Use of controlled, non-public information for insider trading

Physical Theft

Stealing physical property, as opposed to intangibles such as money or intellectual property.

EXAMPLES INCLUDE:

- Stealing valuable inventory
- "Borrowing" a laptop or other corporate device

Violence

Physical harm to others. This category ranges from minor incidents to more serious scenarios.

EXAMPLES INCLUDE:

- Violence or the threat of violence used to coerce employees
- Angry employee punching their supervisor
- General threats against the organization or people

Sabotage

Intentional destruction of enterprise resources so they can't be used. Or the deliberate introduction of malware or a security vulnerability into a product an enterprise develops.

EXAMPLES INCLUDE:

- Breaking a component in a critical machine
- Contaminating a clean room
- Installing a logic bomb in enterprise software
- Misconfiguring a product to cause failure
- Inserting malware in software drivers downloadable from the company website

Intellectual Property Theft

Stealing information or IP, such as software or business data. The threat agent takes unprotected information and copies it (the enterprise retains access to the data) or physically retains it (the enterprise loses access to the data). This is similar to espionage, but the scope, sophistication, and motivation are different.

EXAMPLES INCLUDE:

- Prior to leaving the enterprise, an employee downloads design files to take to a new employer

Corporate Espionage

Systematic and targeted extraction of corporate information by a trusted insider that gives the attacker a strategic economic or public relations advantage. Espionage may bring to mind sophisticated government spies, but most of the people who engage in corporate espionage are average insiders who are engaged by an outside organization to complete a relatively specific task.

EXAMPLES INCLUDE:

- An employee sells product prototypes to a competitor
- A person sends specific, confidential personnel files to a handler
- An employee receives taskings to target specific information

NOT YOUR FATHER'S INSIDER - THE CHANGING MINDSET

TRADITIONALLY, INSIDERS WERE GENERALLY LOYAL TO THE ORGANIZATION FOR WHICH THEY WORKED.

For example, many "baby boomers" likely worked for only one or two employers for their entire career and they changed employers only out of necessity (relocation, promotion, family circumstances, etc.).[14] As a consequence, they developed a high degree of respect for the organization which translated into loyalty (i.e. putting the interests of the employer above their own). Comparatively, today's insiders are likely to have a half-dozen or more employers during their careers.[15] They can aptly be described as opportunists – generally holding a "grass is greener" viewpoint – and change jobs searching for something different, not always out of necessity. This results in a lack of loyalty to any particular organization.

For today's insiders, loyalty begins and ends with the insider's personal self-interest. Once the organization no longer serves the interest of the insider (promotion, continued increase in self-worth, etc.), loyalty ceases to exist. At this stage loyalty, as a natural buffer and governor on employee conduct, no longer serves to protect the organization from unauthorized, and at times unlawful, behaviors. Self-interest is the dominating and motivating factor, not the employer's interest.

In addition to opportunists, this lack of loyalty has spawned another more virulent mindset – the leaker. The leaker mindset is different from opportunists (those simply focused on self-interest) in that leakers also focus on what they view as the public's interest, as so defined to align with their own self-interests. Leakers will not only steal your information for their own interests, but also for their warped definition of the public's interest (i.e. "the public needs to know because I decided").

This changing mindset is of most consequence when employees leave the organization.

Leavers are the greatest risk to any organization as this is the time when insiders are most likely to take information. The problem for organizations is that, as stated, there are more people leaving organizations than ever before. Today, employees stay on average four years. Millennials and technical employees, however, average only two years.[16]

WHAT'S YOURS IS EVERYONE'S - THE CHANGING CULTURE

TODAY'S 24-HOUR NEWS CYCLE CREATES A "FIRST TO PRINT" PHILOSOPHY THAT ENCOURAGES INFORMATION DISSEMINATION AND COLLECTION.

Both were historically done by recognized news services and the reporters who supported them. Print and television media controlled what we read and saw and thus the "media" were aptly described as the "Fourth Estate" – wielding power and influence akin to the three branches of government. Today, however, the Fourth Estate is a fragmented collection of disparate media platforms, mediums, organizations, and individuals. Information collection and dissemination is now not only carried out by traditional journalists, but now by bloggers, YouTubers, and anyone with a Twitter or other social media account.

This journalistic shift has impacted the way information is collected and disseminated. Today, organizations such as Wikileaks have influenced a generation of disaffected individuals and provided not only a medium and outlet to disclose information, but also the motivation and philosophical purpose.

[14] US Department of Labor, Bureau of Labor Statistics, USDL-18-1500 (September 2018)
[15] Id.
[16] US Department of Labor, Bureau of Labor Statistics, USDL-18-1500 (September 2018)

For example, Wikileaks not only seeks to print sensitive information from corporations and governments, it also purposely encourages insiders to actively collect and steal such information. This is a profound change from traditional reporting.

There has always been a fine line, at times both ambiguous and vague, between receiving information illegally obtained and reporting on that information (see the New York Times reporting on Pentagon Papers case and subsequent Supreme Court ruling). At what point does a reporter become an "aider and abettor" of criminal activity and cease acting as a journalist? This question may someday be answered with clarity by the Supreme Court with the recent indictment of Wikileaks founder Julian Assange.

This shift has created a new "leaker mindset" where the collection of information and dissemination of it are now closer to the source than ever before. Sites such as Wikileaks have empowered individuals to steal and disseminate classified information (e.g. Bradley Manning and Edward Snowden) and to raise the specter that it is their duty to do so – for the "greater good." This mindset is not, however, limited to government-classified information leaks, as Wikileaks has spawned a plethora of damaging leaks in the private sector as well.

Regardless of the harm or benefit of leaking certain information, the fact remains that today organizations face a changing culture that not only influences but encourages the leaking (i.e. stealing) of sensitive information. This emboldens individuals to take information and disclose it to the detriment of the organization.

[17] https://globalworkplaceanalytics.com/telecommuting-statistics

THE 24/7 INSIDER – THE CHANGING ENVIRONMENT

THE CORPORATE WORKPLACE IS RAPIDLY CHANGING.

Traditional norms of working at a physical location are becoming obsolete and working remotely is the new norm. Employees are no longer confined to corporate offices, facilities, or even devices. This new paradigm has numerous benefits to both the employer and employee (cost, flexibility, morale, etc.). This new model also, however, creates new challenges for managing insider risk.

Data is the new endpoint. As the workplace evolves from the traditional physical office to remote and virtual workplaces, traditional means of managing insider risk are becoming obsolete and ineffective. This new "digital fence line" creates new threats and vulnerabilities to corporations. A new perimeter-less insider risk management approach to security is needed that shifts the priority to the insiders' interaction with data or the information object itself; in addition to the logical protection of devices or networks to safeguard data and monitor, audit and control people. The core concept is that the data object should be persistently protected and should remain so at rest and in motion, at all times, from data creation to consumption and through to destruction. The network perimeter status quo security approach has proven to be resource dependent and expensive to manage with limited protection results and serious consequences resulting from major data breaches. A new insider risk management model will allow corporations to adapt to the evolving workplace.

A recent study suggests that more than 40 percent of Americans telecommute part-time and some industries (finance, software, management) now have as much as one-third of their staff working remotely full-time.[17] Working remotely redefines the workplace. Employees are no longer confined to corporate offices, facilities, or even devices. Managing insider risk in the context of a physical corporate environment is difficult in itself, but the shift to a remote workforce and a "perimeter-less" workplace compounds these inherent challenges.

THE SECURITY TINDERBOX

THE CHANGES IN MINDSETS, CULTURE, AND ENVIRONMENTS CREATE A "SECURITY TINDERBOX" THAT IS PRIMED TO IGNITE (E.G. RESULT IN A COMPROMISE OF SENSITIVE INFORMATION AND HARM TO THE ORGANIZATION).

These changes continue to evolve and are additional burdens on today's security managers who are already faced with limited budgets, staff, and expertise to manage insider risk. While the majority of the aforementioned changes are out of the control of security managers, they can take certain steps to alleviate the effects and impacts of such changes.

1. IMPLEMENT AND ENFORCE A STRICT NEED-TO-KNOW POLICY

Giving employees more information than they need to know simply increases the chances of someone leaking or taking information when they leave the organization. A solid need-to-know policy will limit the unnecessary spread of information while controlling the individuals who have access. Need-to-know policies are often thought of as government-only policies designed to protect classified information. In reality, the same policies should be a part of any organization's information security program.

2. APPLY ROLE-BASED ACCESS CONTROL POLICIES

Giving employees more access to information than they need to do their job also increases the risk of compromise. Role-based or rule-based access policies allow an organization to enforce the need-to-know policy across the organization. Pre-defined access grants (e.g. need-to-know) for each organizational unit can be efficiently applied and enforced through a robust RBAC solution or similar access control paradigm (active directory, group policies, etc.).

3. EXAMINE INGRESS AND EGRESS METHODS

Giving employees more avenues and methods to access and egress sensitive data is a recipe for disaster. While the needs of the organization will dictate here, thought must be given to the scope and extent of such accesses. For example, is it necessary to grant all employees "admin access" to laptops? Should all employees be granted the ability to remotely log in to the network? Can such privileges be more finely tuned and limited in scope to create a stronger risk posture?

4. MONITOR INSIDER BEHAVIORS AND LIMIT DATA INTERACTIONS

Failing to properly monitor insider behaviors and limit data interactions significantly increases the organization's risk of compromise. Visibility is required to manage insider risk. This includes visibility into how insiders interact with data (e.g. data loss prevention), the level of network activity (e.g. user behavior analytics), and monitoring behaviors indicative of insider threat (e.g. user activity monitoring).

MANAGEMENT TRENDS

INSIDER RISK MANAGEMENT IS A DEVELOPING DISCIPLINE.

Organizations are only recently beginning to focus more attention on the management of insider threats and continue to explore solutions and tools that can assist in this effort. There are, however, several new trends that are of particular importance that are setting the stage for future ITP program standards.

FORMAL INSIDER THREAT PROGRAM

Many organizations are beginning to formalize their insider threat management efforts by creating Insider Threat Programs (ITP).[18] No longer is an ITP simply viewed as deploying a data loss prevention (DLP), security incident event monitoring (SIEM), or user activity monitoring (UAM) tool. A formal program requires a full spectrum approach and involves people, processes, and technology. A positive trend is to assign a program manager to align and develop the necessary cross-functional relationships. These positions are increasingly designated as Senior Vice Presidents or Executive Director level roles, which increase effectiveness and provide the necessary authority to effect change. Formalizing the ITP also involves capturing strategy, policies, and workflows relevant to the effective operation of an ITP. Organizations are discovering that effective collaboration across functions requires a common operating framework and understanding, which can only be effectuated through documenting and formalizing the ITP.

[18] Gartner 2019, Market Trends: *UEBA Providers Must Embrace Specialization.*

TRAINING, TRAINING, TRAINING

Traditional training programs that focused solely on cybersecurity awareness are now expanding to include insider threat topics. Specifically, these programs provide employees and managers an understanding of potential behavioral indicators and other common triggers of concern. In addition, information on how to avoid becoming a target or an unwitting insider threat is also an increasingly important component. Organizations have also started to weave their messaging for the ITP into their training programs. This provides a great opportunity to align the need and obtain support for the ITP while showing the demonstrated impacts and prevalence of insider threats to the organization.

OPERATIONAL HUBS

As organizations mature their programs, the need to centralize operations increases. The traditional stovepipe model where SOC analysts send alerts to investigators is inefficient at best. A centralized team or HUB made of up insider threat analysts and investigators promotes effective triaging and workflows. Dedicated teams also support the continued refinement of tool policies and rules that are needed for effective application.

EMAIL IS KING

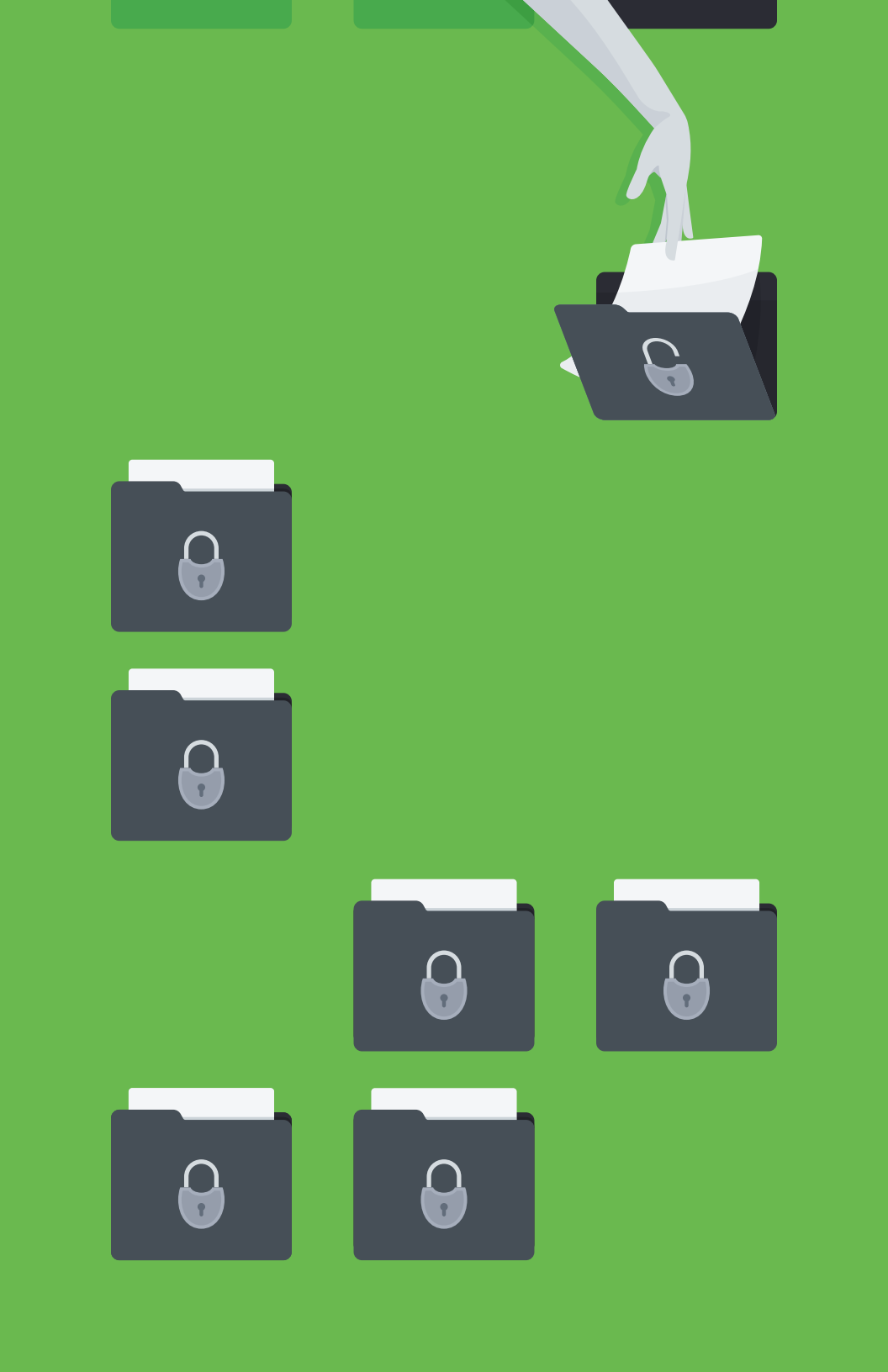
Email remains the largest threat vector for organizations and takes several forms including negligent emailing to unintended recipients, falling victim to phishing attacks, or deliberately sending sensitive files as attachments to unauthorized individuals. While the threat increases, solutions to mitigate remain elusive. Organizations are turning to a layered approach that incorporates a secure email platform and a data loss prevention strategy that incorporates tagging and classifying data to alert and block sensitive information from leaving the firewall.

BAD BREAKUPS

While email is the largest threat vector, the most significant threat indicator is when an employee leaves the organization. This holds regardless of the circumstances surrounding the departure. Research and case examples support the fact that even when employees leave on good terms, they often feel empowered to take sensitive information with them. It holds for senior executives the same as line employees. Once an employee has decided to leave, their loyalty appears to leave with them. Consequently, organizations are becoming increasingly focused on workflows and tools that can assist with identifying when an employee may leave the organization.

SOLUTIONS OVER TOOLS

Organizations are now demanding more robust insider threat solutions. This includes consulting and strategic advising on formalizing an insider threat program, how to leverage existing cybersecurity capabilities, and best practices for developing effective cross-functional collaboration. Tools alone are insufficient to properly manage the insider threat problem and companies are increasingly expecting more from tool providers – i.e. how to optimize the tool in their current environment.



Section 3

—

THE SOLUTION

Managing insider risk requires a full-spectrum solution. This includes incorporating technical and non-technical processes into a cross-functional insider risk management program. This section will define common insider risk management objectives, governance frameworks, and value-added metrics. Best practice will be explored and aligned with a proposed insider risk management model and milestone roadmap.

SETTING THE STAGE – WHO'S ON FIRST?

YOUR ORGANIZATION MAY BE A SMALL BUSINESS OR AN INDUSTRY AND MARKET LEADER.

Regardless, innovation likely drives all aspects of your organization's business operations. As such, your organization is also the target of competitors who seek to leverage your organization's innovations and human capital for their own corporate advancement. Consequently, protecting the organization's assets, intellectual property and human capital is a primary business objective. The organization's relationship with its employees and partner networks are integral in securing these assets. These relationships present different types of risk to the organization – business, financial, and security. The focus of this strategy is on "insider risk" or the harm posed by insiders to organization assets. Managing this risk requires an ecosystem of cross-functional components.

Define a Governance Structure

The ITP should be overseen by an Insider Threat Committee comprised of Chief Security Officer (CSO), Chief Information Security Officer (CISO), Chief Risk Officer (CRO) and legal and privacy leadership. Operational governance of the ITP should be managed by the CSO or CRO as ITP owner. An Insider Threat Working Group should serve as the cross-functional collaborative entity that will provide operational input to the creation and management of ITP components. Building a solid framework is essential and foundational to expanding capabilities.

Define the Program

Properly defining the components and functions that will be included in the ITP is a critical first step. Each organization will have different equities, needs, and organizational structures, however, the following notional framework[19] will create a solid foundation:

- Governance and Strategy
- Personnel Assurance
- Training and Awareness
- Asset Management – Crown Jewel Program
- Access Control
- Monitoring
- Analysis
- Investigation
- Insider Risk Assessment
- Oversight and Compliance

Define the Scope of the Insider Risk Management Efforts

As introduced in Chapter 1, an *insider* is anyone to whom authorized access to assets is granted and risk is the level of harm exposed to an asset.[20] *Insider risk* is therefore the level of potential harm that a particular insider or group of insiders poses to the organization's assets. Traditional "risk" models only focus on threat and ignore impact and vulnerability. Conversely, organizations should apply a true risk model – assessing asset impacts, threats, and vulnerabilities – that will promote a tailored and proactive application of resources on areas of greatest impact (e.g. focusing on those assets that would impact the organization the most if compromised), whether intentional or unintentional.

[19] Further discussed in The Roadmap section.

[20] Considering the likelihood that a threat can exploit a known vulnerability, multiplied by the expected impact to the organization.

There are three main categories of insider risk – *security, productivity,* and *compliance*. Security risks include harm to employees, negligent harm caused by employees, and intentional harm caused by employees. Harm to employees may be from external or internal actors, the former in the form of stolen credentials, phishing attacks, or targeted and harassing recruitment by competitors.

The latter may take the form of a hostile work environment, sexual harassment, or workplace violence. All pose threats to the individual but also manifest as risks to the organization. Negligent harm caused by employees is the most prevalent risk. The great majority of employees are honest and loyal to the organization. However, due to unclear policies or lapses in judgment, they may place the organization at risk. Intentional harm caused by employees is the least likely but may also be the most damaging. Insiders with authorized access may not only compromise the organization's assets but may place the entire organization at risk. Productivity and compliance risks are functional in nature but include harm that results from failing to adhere to legal and regulatory guidelines, organizational policies, or failing to meet workforce expectations.

Leverage Existing Cybersecurity Capabilities

Most organizations have experienced a dramatic and positive shift in overall security posture over the last several years. This shift is likely, however, largely focused on network security controls and managing external threats. A byproduct has been the creation of several important functions that can be leveraged by the ITP. These functions will, however, need to be optimized, expanded, and tailored for the ITP. This strategic shift towards greater security risk management has led to a greater focus on managing insider risk. This has created positive momentum for the expansion of insider risk management capabilities, evidenced by both executive leadership support and current operational efforts. Most current capabilities are, however, entirely reactive and largely ad hoc. The existing functional components operate mostly independently with minimal formal collaboration.

Organizations should conduct an initial baseline capability assessment to understand their insider threat gaps and needs. This assessment should examine the entire organization and review existing cybersecurity capabilities. Identified gaps can then be mapped to requirements to build a workable roadmap. Most organizations will find that many of the resources needed to begin building an effective ITP already exist. The goal is to leverage those resources in a cross-functional manner to optimize value.

Define Privacy and Security Equities

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

GOALS AND OBJECTIVES – MEASURING CAPABILITY

METRICS ARE KEY TO MANAGING ANY ORGANIZATIONAL PROBLEM SET, INSIDER THREATS ARE NO DIFFERENT. MANY COMPANIES, HOWEVER, ASK THE WRONG QUESTIONS WHEN IT COMES TO MEASURING INSIDER THREAT AND SPECIFICALLY INSIDER THREAT MANAGEMENT CAPABILITIES.

The ITP should adopt an overarching theme to protect the organization's assets before they are compromised – in other words, to *proactively* manage insider risk. This theme should be supported by a series of specific goals and objectives to enhance excellence in four central domains or directives for an organization's ITP: Awareness, Understanding, Visibility, and Response.

Awareness

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

INSIDER POPULATION

The organization must have a clear picture of individuals and groups to whom access is given. The theme is to "verify then trust." This is first accomplished by continuing to strengthen existing pre-employment screening processes and procedures. Once granted access, threat assessment processes should continue to be enhanced and applied to properly assess reported threats. Organizations must have full knowledge of the number of employees, contractors, and business partners that have access to the organization's assets and to which assets they have access. Steps must also be taken to clearly identify different insider groups based on their level of access.

Logical insider groups, based on both physical and electronic access, should be created to foster proper threat and risk identification and measurement. For example, such groupings should include at the minimum: insiders with super-user access, privileged users, insiders with access to Crown Jewels, etc.

INSIDER ENABLEMENT

Insider buy-in is essential for an effective program. As such, the organization must provide insiders with resources to properly protect the organization's assets. This starts with clearly communicating workplace expectations and responsibilities at onboarding. Insiders must also be given awareness of the threats that the organization faces. To that end, insiders should be provided awareness training on insider threat personas, events, and behaviors as well as the prevalence and impacts such threats have had and can have on an organization.

TRANSPARENCY AND RESPONSIBILITY

An effective ITP requires a culture of transparency and responsibility both vertically and horizontally across organizations and functional components. Organizations should communicate the ITP to the workforce via a formal ITP policy that should broadly establish the overall purpose, objectives, structure, and oversight mechanisms. Insiders must also be made aware of their personal reporting processes and procedures. As insiders are granted authorized access, they should be informed of their duty to protect the organization's assets, to include fellow insiders, by understanding threat indicators and the mechanisms available to report such information to responsible officials in a secure and protected manner.

RISK WORKFLOWS

Relevant threat information must be incorporated into workflows that foster the identification and mitigation of behaviors that may adversely impact the organization. This should be an iterative process to continue to understand the organization's insider population for purposes of managing risk. Workflows should foster cross-functional collaboration to and from the ITP.

Understanding

Understanding refers to the need to know what is important to an organization by identifying and defining critical assets; developing granularity about those assets; prioritizing them based on impact to the organization; and developing processes and procedures that foster knowledge of asset workflows; and incorporating this knowledge into risk management processes.

CROWN JEWEL AND CRITICAL ASSET IDENTIFICATION

The organization must develop a formal program to iteratively identify and define critical assets and Crown Jewels. The former are those assets that if compromised would have an appreciable impact on the organization. The latter are those assets whose impact, if compromised, would be significant or catastrophic. Organizations should establish formal asset identification processes that capture relevant information including asset type, asset owner, authorized users, accesses, and locations. This process should be dynamic and repeatable to promote updating as needed.

PRIORITIZATION

The organization should develop an impact model that fosters the necessary prioritization based on the level of impact the asset would have on the organization if compromised. A repeatable methodology should be developed to assess impact and objectively rank assets based on impact levels.

MOVEMENT AND USE

The organization should develop processes and procedures that foster knowledge of asset workflows. Understanding asset movement and usage is an essential component to understanding risk. Paramount to this is understanding the asset user base and, most importantly, how users interact with assets.

RISK WORKFLOWS

Relevant asset information must be incorporated into workflows that foster the identification, measurement, and mitigation of risk. This should be an iterative process to continue to understand an organization's assets, asset users, and user interactions with those assets. Workflows should foster cross-functional collaboration to and from the ITP.

Visibility

Visibility refers to the need to monitor insider behaviors that are indicative of a threat to an organization's assets; monitor interactions of insiders with identified assets; log asset accesses and movements; and analyze behaviors, interactions, and logs to identify risk through iterative and repeatable methods.

INSIDER BEHAVIORS

Insider behaviors include both network and off-network information. This is important because both technical and non-technical methods are needed to properly discover insider threat behavior. Organizations should create and apply tailored threat ontologies to detect insider behavior indicative of threat. Ontologies should be incorporated and aligned with monitoring tools and methods to develop appropriate alerting policies. Identifying insider behavior requires multiple sources and methods to efficiently tailor threat methodologies. Sources and methods should be developed and coordinated with appropriate legal and privacy counsel.

ASSET INTERACTIONS

Asset interactions include how a user accesses, utilizes, stores, and disseminates the asset or information contained in the asset. This is important because it promotes a tailored application of threat methodologies, increasing effectiveness while promoting a balance between security and privacy equities.

Organizations should monitor insider interactions with identified assets and establish baselines using available technology to alert on unacceptable deviations.

ASSET ACCESS AND MOVEMENTS

A data-centric monitoring approach promotes efficiency throughout the risk management process. Focusing efforts on critical assets and those insiders with access, fosters the tailored implementation of monitoring tools. Obtaining visibility of asset actions is a necessary step to developing a tailored monitoring approach. Processes and procedures should be developed to dynamically obtain information on who, how, and when assets are accessed and moved.

CASE STUDY #1

CAN YOU SEE ME NOW?

CLIENT: GLOBAL PHARMACEUTICAL COMPANY WITH OPERATIONS IN OVER 100 COUNTRIES

Problem

Client has a well-deserved reputation for quality and excellence. As the market leader, the company must continue to protect the value of its products, operations, culture and reputation. Client, however, faces a clear and present danger that threatens to diminish this value. This danger stems from their trusted employees, contractors, and partner network (i.e. “insiders”). These insiders represent the greatest threat to Client’s value. The great majority of all of Client’s security incidents involve insiders, which include intentional, reckless, and negligent actions.

The largest vulnerability was Client’s lack of visibility and understanding of how their insiders accessed and interacted with critical business assets. This vulnerability dramatically increased the overall risk to the company’s critical assets. With no visibility the Client lacked the ability to make informed business decisions.

Solution

Client made an affirmative decision to implement a comprehensive risk management program that would protect corporate intellectual property and customer data worldwide.

THE PRIMARY OBJECTIVES WERE TWO-FOLD:

1) Classify normal user and machine behavior across a diverse environment and 2) Identify compromised credentials among a group of trusted employees.

Exabeam's next-generation Security Incident and Event Management (SIEM) was a key enabling technology to meet each objective. Exabeam's *Smart Timelines* offered sophisticated threat-hunting scenarios that provided automatically combined sequence, behavior, identification, and scope into a pre-processed object that would send an alert on identified threats. Client utilized the advanced analytic features to employ sophisticated threat-hunting scenarios.

Beyond meeting the identified objectives, Client incorporated the Exabeam toolset into its risk management program and applied it to multiple use cases (malicious insiders, compromised users, APT). By aggregating and collecting data from multiple sources (events and logs, netflows and packets, HR, user activity monitoring, external threat intelligence), Client was able to obtain the necessary visibility of insider behaviors and interactions to support effective risk management efforts.

RISK ANALYSIS – INSIDER RISK CENTER OF EXCELLENCE OR HUB

A risk model that identifies, measures, and analyzes threats, vulnerabilities, and impacts is necessary to understand and manage true risk to the organization. This model should be dynamic and capable of integrating and incorporating into new and existing ITP processes and workflows. An Insider Risk Center of Excellence or hub should be created and chartered to manage the alerting processes and thresholds. This Center should serve as the analytic hub responsible for creating risk, threat, impact, and vulnerability models to foster the understanding necessary for operational and programmatic action.

Response

Response refers to the need to develop an effective balance of employee and security equities by supporting a governance framework that oversees compliance with established guidelines; developing unified workflows that leverage the collective expertise of ITP components; and ensuring the ability to efficiently manage identified risks to organization assets.

OVERSIGHT AND COMPLIANCE

To promote effective oversight, operational parameters must be clearly identified, documented, and communicated to ITP personnel. A supporting governance framework should be established to oversee compliance with established guidelines. The Insider Threat Working Group, chaired by the Insider Threat Director, should manage the operational oversight mechanism, which should then develop formal metrics and communication plans with the Insider Threat Committee. In addition, quarterly compliance reports should be created and disseminated to legal and privacy stakeholders that summarize relevant information to be mutually defined by the ITP and legal.

UNIFIED WORKFLOWS

ITP component workflows must be integrated to be effective. To the extent possible, HR, CSO, and CISO workflows should be integrated as seamlessly as possible. This does not require a complete consolidation of all workflows, but an identification and integration of those that apply to the ITP. This unification will allow for all necessary asset, threat, and vulnerability information to be collected and analyzed to promote efficient insider risk management.

CASE STUDY #2

HIDING IN PLAIN SIGHT

CLIENT: GLOBAL ENGINEERING FIRM

Problem

Client experienced unusual file access and anomalous scraping activity on its network.

Solution

Exabeam's behavioral analysis identified unusual virtual machine (VM) creation activity and anomalous naming conventions for each of the VMs on the client's network. Combined with other anomalous activity, the machine and user were flagged as notable and escalated to analysts.

Analysts discovered the malware compromised machine was performing Pass the Hash[21] attacks to move laterally in the network. **The compromised machine was quarantined before it was able to exfiltrate data from the firm.**

[21] Pass the Hash is a hacking technique that allows an attacker to authenticate to a remote server or service by using the underlying hash protocol of a user's password, instead of the plain text password itself. Thereby replacing the need for stealing the actual password.

> Up to 60% of attacks involve lateral movement, but few products can detect it without loads of manual effort. Exabeam automatically detects lateral movement for early breach detection. Host-to-IP mapping and contextual enrichment build a true picture of all users and systems. Patented tracking follows attacks as they move through an organization and reconstructs the entire attack chain. Smart Timelines instantly visualize the entire incident including all affected users and systems and their activities.

MASTER MIND CONCEPT

Effective insider risk management requires the collective expertise of the entire organization. Stakeholders should unify to create processes and procedures to identify and manage risks to assets. Expertise should be sought and utilized from all resources and organizations within the organization's network. This concept should be implemented through the Insider Threat Working Group structure.

APPLES AND ORANGES

EFFECTIVE RISK MANAGEMENT REQUIRES INTEGRATION OF CROSS-FUNCTIONAL COMPONENTS AROUND A UNIFIED STRATEGY AND PURPOSE.

Too often threats are treated as separate and distinct categories. While there are clear differences requiring unique solutions, all threats to the organization must be managed under a full-spectrum risk management approach. This section will provide a model for successfully integrating insider risk management into existing physical and cybersecurity programs.

This strategy must be formally aligned with a defined risk management process. The strategic directives, goals, and objectives must be logically organized to achieve the goal of protecting assets.

Monitoring for threat information or identifying assets is of little value if not organized in a repeatable process that provides visibility and awareness of the organization's true risk. As synthesized below, the first step is to identify the elements of risk – asset impacts, threat, and vulnerability – and discover the supporting factors and indicators. The second step is to assess this information to place those indicators in the proper risk management context. The final step is to communicate risk information to ITP personnel and stakeholders to allow for actionable mitigation and proper executive oversight and support.

IDENTIFY

Assets

Asset identification is foundational to the ITP. A Crown Jewel Program Manager (PM) should be created and delegated responsibility for managing the organization's Crown Jewel Program. Asset information should be collected and securely maintained by the PM. The PM should work with business units to initially identify critical assets and thereafter update semi-annually, and as new critical assets are developed or identified. Critical asset identification should include sufficient information to be included in an insider risk registry process in support of a continued and repeatable methodological framework.

Vulnerabilities

A vulnerability, as an element of risk, is the susceptibility to harm or damage of a *particular asset.* Consequently, the level of vulnerability has a direct impact on the level of risk to an asset. Vulnerability is a combination of three factors – Ingress, Controls, and Egress. The ITP should assign an individual to be responsible for identifying and documenting the vulnerabilities of each critical asset group into an insider risk registry process in support of a continued and repeatable methodological framework.

Threats

A threat, as an element of risk, is the likelihood that an individual could use their authorized access, intentionally or unintentionally, to harm the organization.

A THREAT CONSISTS OF TWO FACTORS

1) The *ability* to do harm, which requires access and a means to egress 2) action.

- Ability is measured by examining the level of ingress and egress opportunities available to a particular user or group for a particular asset
- Action is measured by examining alerting behavior from several sources including: UAM tools, DLP tools, HR investigations, and security investigations

The ITP should assign an individual to be responsible for identifying and documenting the individuals who have access to critical assets and the level of ingress and egress opportunities. The ITP should also assign an individual to be responsible for identifying threat information from monitoring tools, for identifying and documenting threat information contained in Security investigation files and identifying and documenting threat information contained in HR investigation files.

CASE STUDY #3

DEPARTING EMPLOYEES = DEPARTING IP

CLIENT: GLOBAL SOFTWARE COMPANY

Problem

Client undertook a corporate restructuring program as a result of various mergers and acquisitions over several years. Part of this restructuring involved layoffs of a significant number of employees.

The execution of the layoffs was on a compressed time schedule that impacted HR's and IT's ability to effectively monitor and track exiting employees. Since departing employees pose the greatest threat to any organization, Client needed a solution to monitor and identify unauthorized exfiltration of corporate IP.

Solution

Client used Exabeam's Advanced Analytics to create a watchlist of exiting employees. Client identified over 10 employees attempting to leave with corporate data and used incident details to catalogue the exact list of downloaded files by each employee. HR then partnered with IT and legal to reduce severance packages of departing employees unless data was returned.

Exabeam provides greater ability to identify threats and vulnerabilities by increasing the speed to detect advanced threats such as insider threats, data exfiltration, and lateral movement. Insider threats and complex and unknown attacks are easily identified by using Exabeam on data from all existing security controls and data sources. Pre-built *Smart Timelines* automate incident investigations, including normal and abnormal behavior and lateral movement. Alert Prioritization elevates high risk alerts and incidents via risk scoring and behavioral analysis to focus analyst cycles where they matter most. Automated Incident Response via SOAR lowers MTTR, reduces human errors, and amplifies analyst productivity. **Customer estimates $450k in savings from this one round of layoffs.**

Assess

The goal of assessing insider risk is to provide clarity to stakeholders and decision-makers by identifying those insiders or insider groups that pose harm to the organization. This harm may be on a case-by-case perspective (i.e. a monitoring alert identifies an insider attempting to steal organization intellectual property) or on a programmatic level (i.e. an assessment identifies a capability deficiency).

The risk assessment process will support an understanding of both organizational risk and operational risk. The former provides an understanding of organization's insider risk management capability levels. The latter provides case specific alerting on actionable threats to the organization. This combination serves to provide the organization with a holistic insider risk management process that is both formal and repeatable, but also value-added both operationally and organizationally.

Communicate

To be effective, identified risk must be properly communicated to decision-makers. The ITP will promote organizational communication through the Insider Threat Working Group, which should be comprised of accountable officials for each of the ten ITP ecosystem components. Operational communication should be facilitated through the development of requirements to meet the directives, goals, and objectives of this strategy. The Insider Threat Center of Excellence or hub should serve as the primary entity for facilitating the identification, assessment, and communication of actionable information. Reporting processes and procedures should also be developed to provide necessary oversight of the ITP, which should include feedback to both the Insider Threat Committee and legal and privacy officials as necessary.

EYES WIDE OPEN

VISIBILITY IS KEY TO ANY SUCCESSFUL PROGRAM, YET IT REMAINS ELUSIVE DUE TO LEGAL, TECHNICAL, AND BUSINESS PROCESS CONSTRAINTS. THIS SECTION WILL DEFINE SOME INITIAL BASELINE DATA POINTS FOR PROPERLY MANAGING INSIDER THREATS AND BEST PRACTICES FOR OBTAINING VISIBILITY.

Asset Management

Data sprawl is an issue facing organizations of all types and sizes. Information is being stored in a wide variety of places within organizations. Identifying the "crown jewels" and developing governance processes is essential.

FORMULATE GROUND RULES

A continuous and systematic approach to managing data is required. Processes need to be put in place so that going forward, the crown jewels are immediately identified and properly protected.

ASSIGN CROWN JEWEL OWNERS

Once data hits a file share or data repository, its lineage tends to get lost. Every data element needs an owner who determines its importance to the business.

MAP DATA FLOWS

How data flows through a company's environment needs to be mapped. This includes documenting how the data is transformed as it passes through various systems, as the classification of data can easily change as it moves through the company. Once a process has been established for identifying an organization's crown jewels, appropriate levels of protection can be put in place to protect the assets.

Data Protection

Gone are the simpler times when basic file encryption was enough to secure data. Today's enterprises share files across an extended enterprise of vendors and partners and an increasing number of devices. Security controls must be applied to both digital and physical assets (including information and personnel) to ensure the ability to safeguard assets wherever they are accessed, used, transmitted, stored, or located.

PERSISTENT

Controls need to be persistently enforced. If a sensitive file is emailed, saved to a flash drive, stored in a cloud-based application, or transported anywhere else, security policies will remain in effect and data is protected.

TOP-DOWN POLICY ENFORCEMENT

Administrators need to enforce policies in a top-down manner, so corporate-wide policies can be applied consistently and cohesively across the enterprise, and down to the specific digital asset, device and user level.

GRANULAR

To maximize data separation efficiency, enterprises need to employ controls in a way that provides protection and insight at the lowest level possible, ensuring optimal security, data governance compliance and productivity.

Access Control

Identifying CJs and protecting assets is of little value if access to those assets is not properly managed. Two of the highest risk factors for insider threats are too many users with unnecessary access privileges and the increasing number of devices with access to sensitive data.

THE NON-HOSTILE THREAT

Most threats are unintentional. This illustrates the need for technical measurements, to limit accidents and negligent actions. Many organizations are still not in control of who has access to what and why.

THE NON-STATIC INSIDERS

Besides employees, most organizations also have temporary employees, contractors, and business partners who need access to the systems. These employees and insiders are non-static, moving across the organization throughout their lifetime at the business.

THE REMOTE EMPLOYEE

Working from home or while on the move poses a significant security threat for the organization. Systems become increasingly decentralized, which creates an open environment where data is even more difficult to protect. With many applications additionally moving to the cloud, workspaces are becoming virtualized, challenging overall security and compliance for organizations.

Basic Insider Risk Indicators and Best Practices

DOWNLOADING UNAUTHORIZED SOFTWARE MUST BE AN ALERT

While some downloads may be properly ascribed as mere “policy violations” and handled accordingly, others should be automatic alerts. For example, employees downloading encryption software should create an alert. There is no legitimate business need for an employee to download an encryption program as the purpose of encryption is to keep file contents from being viewed by the organization.

RECURRING THREAT EVENTS SHOULD PREDICATE ACTION

Organization divisions or units with a documented history of insider threat events should receive additional scrutiny such as enhanced monitoring or further vetting procedures.

SCREEN CAPTURE AND KEYLOGGING ARE NECESSARY INVESTIGATIVE TOOLS

While the thought of deploying agents and tools to log keystrokes of all employees all the time and to capture their screen activity is anathema to privacy officials, it's also impractical. That said, as an investigative tool it provides unique and singular intelligence not discoverable by other means. In many cases, the only way to discover an unauthorized exfiltration will be by watching the employee's screen activity.

SCRAPING IS A KEY INDICATOR

Scraping or gathering large amounts of files, is a common technique used by insiders who are preparing to leave the company. Scraping is also difficult to detect, because most of the files scraped are those to which the employee has legitimate access. The only practical way to detect scraping is through deviation alerting or establishing a baseline of activity and comparing it to similar core groupings.

LEAVING IS A KEY INDICATOR

Leaving is well documented as a key threat indicator. The difficult task is identifying this intention at the earliest possible time. An employee who submits their resignation, then begins to scrape information is an easier case. Presuming there are efficient workflows in place to notify security who is then properly enabled to deploy enhanced monitoring, there is a good chance of detecting misconduct. Most cases, however, are not clearly defined and require creative discovery methods. For example, the use of LinkedIn, Indeed, or any number of job sites, are primary sources of information that can provide insight to the ITP.

An increased use of these sites combined with a recent update of a resume, on a company device, could indicate their intention to leave.

REMOVING CREDENTIALS AND ACCESSES UPON TERMINATION

Access removal procedures are generally effective when terminations are handled by HR, such as when employees are removed for cause (e.g. violence, theft of IP, etc.). Procedures are less effective, however, when HR is not involved, e.g. when an employee voluntarily leaves. In these situations, access removal processes are less clear and not uniformly or efficiently employed. Improving access removal procedures for all insiders (employees and contractors), whether they are voluntarily or involuntarily separated, should be a critical priority.

CASE STUDY #4

CLOSING THE BACK DOOR

CLIENT: GLOBAL APPAREL COMPANY

Problem

Client experienced an increase in data theft from departing employees in cloud-based applications. The company's account termination processes were inefficient and represented a large vulnerability.

Solution

Client deployed Exabeam and identified anomalous GitHub access by terminated employees. Exabeam used feeds from the HR system to identify terminated employees and associated accounts. With Exabeam, Client was able to identify the unauthorized accesses and prevent further data loss.

Detecting advanced threats such as insider threats, data exfiltration, and lateral movement is a major challenge for all organizations.

Insider threats, complex and unknown attacks are more easily identified by using Exabeam on data from all existing security controls and data sources. Alert Prioritization elevates high risk alerts and incidents via risk scoring and behavioral analysis to focus analyst cycles where they matter most. Exabeam is designed around a risk-based approach to security management. By analyzing user behavior on networks and applying advanced analytics to detect anomalies, it automatically stitches relevant events together to pinpoint malicious indicators more easily and rapidly detect insider threats.

A NEW PARADIGM FOR THE PERIMETER-LESS WORKPLACE

A NEW PERIMETER-LESS INSIDER RISK MANAGEMENT APPROACH TO SECURITY IS NEEDED THAT SHIFTS THE PRIORITY TO THE INSIDERS' INTERACTION WITH DATA OR THE INFORMATION OBJECT ITSELF; IN ADDITION TO THE LOGICAL PROTECTION OF DEVICES OR NETWORKS TO SAFEGUARD DATA AND MONITOR, AUDIT AND CONTROL PEOPLE. THIS SECTION WILL PROPOSE A NEW MODEL FOR DEALING WITH THE "NEW" INSIDER THREAT.

Managing insider risk in the context of a physical corporate environment is difficult in itself, but the shift to a remote workforce and a "perimeter-less" workplace compounds these inherent challenges. There are four primary objectives of an insider risk management program – *awareness, understanding, visibility,* and *protection.* A perimeter-less workplace requires an adaptation and tailoring of traditional risk management methods.

Awareness

Awareness means developing a clear picture of your insider population, providing insiders with resources to properly protect assets, creating a culture of transparency and responsibility, and developing workflows that foster the identification and mitigation of aberrant behaviors.

In the traditional workplace, *training* is focused on best practices for operating in an office environment and how to spot aberrant behavior from coworkers and how to protect against common email attacks. Good workplace hygiene is emphasized (not leaving documents on printers, locking screens, badging into secure areas, etc.) and how to report information to managers. *Insider populations* are defined by those that have *physical* access to corporate offices and *workflows* are focused on identifying aberrant behaviors in the workplace.

By contrast, in the perimeter-less workplace, *training* must focus on the remote workplace and the unique environments involved. Here, proper hygiene for accessing corporate information (fake hot spots, spoofing, shoulder surfing in public spaces, etc.) must be emphasized as well as properly handling information outside of the office (printing, storage, transmitting). Use of file sharing sites, USBs, email security and device management (personal and corporate) are of particular importance in this environment. Reporting workflows must also adapt and utilize more hotlines to report suspicious activity to security. Here, *insider populations* must be understood from a virtual access standpoint since many employees may never step foot in the physical corporate facility. Lastly, *workflows* must incorporate methods and means to identify aberrant behavior outside of the workplace.

Understanding

Understanding involves focusing on what is important to the company by identifying and defining critical assets, developing granularity about those assets, prioritizing them based on impact, and developing processes and procedures that foster knowledge of asset workflows and incorporating this knowledge into a risk management framework.

In the traditional workplace, the focus is on the corporation as "asset holder" (on corporate devices, networks, physical locations). Workflows are mapped, if at all, to intra-office collaborations. Risk is therefore understood within the confines of the traditional corporate environment.

Once critical assets are identified, an understanding is required of who has access to those assets and how they are handled, stored and moved. For traditional workplaces, this is often an eye-opening exercise, with access to their critical resources often far wider than imagined.

By contrast, in the perimeter-less workplace, the insider is often the "asset holder" (storage on personal devices, USBs, file sharing sites, home office) and the spread of critical assets is even more pronounced. Working remotely, staff have a wide variety of mechanisms to handle and store assets.

Risk models now must include threats and vulnerabilities concomitant with operating outside of the corporate environment. Classification of possible "asset holders" is therefore broadened to whatever is available in home offices. This can include personal computers, tablets, phones, and removable media. The ever-growing use of IoT devices further complicates this process. Moreover, when considering critical data in transit, remote workers are far more likely to use alternate means and devices in transmitting organizational data. As such, inter-office workflows must be catalogued as an elemental part of identifying the threats and vulnerabilities outside of the traditional corporate environment.

Visibility

Visibility involves monitoring insider behaviors that are indicative of a threat to corporate assets (network and off-network), monitoring interactions of insiders with identified assets, logging asset accesses and movements, and analyzing behaviors, interactions, and logs to identify risk.

In the traditional workplace, visibility is limited to corporate-owned devices and networks and behaviors at the corporate facility.

By contrast, the perimeter-less workplace must include visibility on personal devices, behavior outside of the corporate facility (open source data sources), and understanding how data assets are moved, transferred, and stored outside of corporate networks.

To counter the loss of visibility into the ways that staff store, transmit and work on data, organizations need governance and workflows that enable the tracking of the flow of data and assets outside of the corporate network and domains. These policies and procedures may restrict remote staff to the use of specific devices or enterprise mobility management tools that compel a standardized process that can be comprehensively monitored. Such tools allow an organization to integrate all mobile devices into a management framework that includes security, identity, application, and content management.

To counter the loss of *visibility* into staff behavior, alternate means for the early identification of employee warning signs are required. Such mechanisms will allow the organization to respond with the right degree of engagement, assistance, support and discipline. Open source data can provide insight into individuals' behavioral stressors and actions and can help employers continuously examine an employee's potential threat to an organization. Continuous evaluation of open source data can help assess employees working at customer locations or home, whose changes in behavior are less visible to colleagues and managers. Used properly, this data can help recognize behaviors unobservable by technical monitoring and provide early warnings to possible risk.

OPEN SOURCE INFORMATION includes financial data (bankruptcies, credit reports, liens, etc.). These may indicate unexplained affluence and financial difficulties. Law enforcement data (arrests, convictions, protective orders, etc.) may indicate unpredictability, volatility, and an inability to follow laws. Social media postings may reflect unusually negative (and even violent) sentiments toward an employer, colleagues, public personas, family members and former partners.

Protection

Security controls must be applied to both digital and physical assets (including information and personnel) to ensure the ability to safeguard assets wherever they are accessed, used, transmitted, stored, or located.

In the traditional workplace, the focus is on the device and human endpoint. Controls are designed to alert on events (post-action) and are limited to the corporate perimeter (network and physical). By contrast, in the perimeter-less workplace, data is the new endpoint. The focus must be on the digital asset itself as the new perimeter. Controls must be designed to manage access (pre-event) and invoke object-level end-to-end encryption.

The perimeter-less workplace requires persistent, data-centric encryption that goes beyond the end point and traditional authentication approaches. To properly manage insider risk in the perimeter-less workplace, security teams need to augment protection mechanisms with additional security layers that focus on data in a more granular, persistent and dynamic fashion. This means being able to encrypt any digital asset regardless of source application, format or device OS.

THERE ARE THREE PRIMARY "PROTECTION" REQUIREMENTS FOR THE NEW PERIMETER-LESS WORKPLACE:

- **PERSISTENT.** Encryption needs to be enforced persistently. If a sensitive file is emailed, saved to a flash drive, stored in a cloud-based application, or transported anywhere else, security policies will remain in effect and data is protected.
- **TOP-DOWN POLICY ENFORCEMENT.** Administrators need to enforce policies in a top-down manner so corporate-wide policies can be applied consistently and cohesively across the enterprise and down to the specific digital asset, device and user level.
- **GRANULAR.** To maximize data separation efficiency, enterprises need to employ encryption in a way that provides protection and insight at the lowest level possible, ensuring optimal security, data governance compliance and productivity.

The new perimeter-less workplace requires a new insider risk management paradigm. By adapting and redefining models for risk awareness, understanding, visibility, and data-centric persistent asset protection, organizations can develop effective programs to confidently manage insider risk both inside and outside the traditional corporate environment.

LEARNING TO CRAWL – BUILDING A WINNING STRATEGY

ORGANIZATIONS FACE A CHANGING RISK ENVIRONMENT AND NEW COMPETITIVE CHALLENGES AND THE CONSTANT NEED TO BETTER PROTECT THOSE EQUITIES.

Most organizations also have insider risk management capabilities that are best described as "nascent" resulting in a high risk of compromise to the organization's assets. Most have numerous insider risk management capability deficiencies, including the lack of a formal insider risk management strategy. This strategy is, however, the bedrock of an organization's Insider Threat Management Program (ITP).

The Approach

The insider threat strategy should treat the organization as a single entity with an ecosystem of functional components. The core strengths of any organization are grounded in its commitment to excellence and its talented workforce and network of employees, contractors, and business partners. This network presents different types of risk to the organization – business, financial, and security. The focus of the strategy is on "insider risk" or the harm posed by insiders – those granted access – to the organization's assets. Managing this risk requires an ecosystem of cross-functional components.

The plan should also focus on the ecosystem, rather than the particular components or parts that compose it. The strategy should propose organization-wide goals and actions that transcend the boundaries of particular entities or business units.

It should take advantage of its distributed strengths while also reinforcing those strengths and facilitating the "bottom-up" innovation and expertise of each component. The relationship of insider risk management to the management of the broader enterprise risk of the organization should be an ongoing and dynamic interchange.

The challenges and opportunities of an organization's changing business environment require the need for enhanced corporate capacity to act as a unit, that is, to chart strategic directions and mobilize functional risk management components around business objectives. For example, an organization will set certain revenue goals. This growth will require a significant increase in the number of insiders – employees, contractors, and partners – which will also increase the level of risk and the need to properly manage it. This challenge also presents an opportunity to increase significantly the organization's insider risk management capabilities. The growing costs of research and development, human capital management, and brand protection require an institutional response to insider risk management that sets priorities and ensures that support is cost effective. The traditional myopic view of "security" as a pure cost center creates a need to rethink how the organization fulfills its duty to protect its assets and change the paradigm. Insider risk management is a business enabler that will enhance an organization's enduring commitment to innovation and people. Corporate-wide strategies and tactics will help the organization meet these challenges.

The Aspiration

The strategic plan should put forth an overarching aspiration for the organization: to manage the greatest amount of risk at an acceptable cost while intelligently balancing employee and security equities. Having an overarching aspiration for the organization is important for the one-ecosystem theme of the plan.

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

Strategic Directives

The strategy should adopt a foundational theme of protecting the organization's assets before they are compromised – in other words, to proactively manage risk. This theme should be supported by a series of specific goals and objectives to enhance excellence in four central domains or directions for organization's Insider Threat Management Program (ITP): Awareness, Understanding, Visibility, and Response.

The **Awareness** directive emphasizes the importance of developing a clear picture of an organization's insider population by ensuring a trusted workforce, providing insiders with resources to properly protect organization's assets, creating a culture of transparency and responsibility, and developing workflows that foster the identification and mitigation of behaviors that may adversely impact the organization.

The **Understanding** directive focuses on the need to know what is important to an organization by identifying and defining critical assets, developing granularity about those assets, prioritizing them based on impact to the organization, developing processes and procedures that foster knowledge of asset workflows, and incorporating this knowledge into a risk management framework.

The **Visibility** directive recognizes the need to monitor insider behaviors that are indicative of a threat to an organization's assets, monitor interactions of insiders with identified assets, log asset accesses and movements, and analyze behaviors, interactions, and logs to identify risk.

The **Response** directive fosters an effective and proper balance of employee and security equities by supporting a governance framework that effectively oversees compliance with established guidelines, developing unified workflows that leverage the collective expertise of ITP components, and ensuring the ability to efficiently manage identified risks to an organization's assets.

Business Enablement

An insider risk strategy is more than managing and mitigating harm to an organization, it's about business enablement.

AS A BUSINESS ENABLER, AN INSIDER RISK STRATEGY PROMOTES AND ENABLES:

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

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

THE MODEL

THE FOUR PRECEDING STRATEGIC DIRECTIVES ARE SUPPORTED THROUGH THREE PRIMARY GOALS – BUILD A FRAMEWORK, ENHANCE CAPABILITIES, AND OPTIMIZE OPERATIONS.

Build a Framework

The first strategic goal is to build a framework that supports effective insider risk management. A framework establishes a foundation of structures, processes, and procedures. The framework should be supported through the development and continued enhancement of the following objectives. First, develop an ITP governance and organizational structure, then define the program and how it will be governed. Second, develop an ITP implementation plan to support the implementation of objectives. Third, develop ITP policies and procedures; defining parameters and workflows. Fourth, establish ITP roles and responsibilities; accountable personnel foster program efficiency. Fifth, identify and communicate legal and regulatory parameters to ITP stakeholders and personnel. Sixth, develop a formal Critical Asset Management Program that supports the Understanding directive and promotes robust risk management practices. Seventh, expand the use of monitoring tools to support the visibility directive and obtain the necessary understanding of risky behaviors and asset interactions.

Enhance Capabilities

The second strategic goal is to enhance the organization's insider risk management capabilities. Leveraging existing and creating new capabilities will be the lifeblood of an organization's ITP. Capabilities should be supported through the development and continued enhancement of the following objectives. First, strengthen sharing and collaboration between HR and security, ensuring threat information is conveyed in a timely manner. Second, develop a formal Insider Risk Assessment policy; clear and targeted risk models will promote effective identification and mitigation practices.

Third, create an Insider Risk Center of Excellence; to foster visibility and support response efforts. Fourth, employ a "verify then trust" model that ensures proper vetting of all personnel granted access to organization assets. Fifth, create feedback mechanisms for effective oversight to promote ITP legitimacy and continued program viability. Sixth, expand the proactive use of monitoring tools; reactive deployments alone are insufficient.

Optimize Operations

The third strategic goal is to optimize operations by maturing the organization's ITP framework and capabilities and focusing on results-driven measurables. Operations should be optimized through the development and continued enhancement of the following objectives. First, ensuring full understanding and visibility of Crown Jewels, and expanding this list as capabilities increase. Second, ensuring full awareness, understanding, and visibility of the riskiest insiders to foster optimal asset protection. Third, expand training programs to include awareness and operational training to both the workforce and ITP personnel. Fourth, foster employee engagement and messaging to promote awareness and obtain necessary buy-in and understanding of asset protection equities. Fifth, mature the insider risk assessment process to provide a total knowledge outlook of organizational insider risk and to support ITP response measures. Sixth, expand analytic resources to fully understand threat behaviors and to efficiently support mitigation processes.

THE ROADMAP

EACH GOAL IS FURTHER SUPPORTED BY VARIOUS OBJECTIVES THAT INDIVIDUALLY AND COLLECTIVELY ALSO SUPPORT THE FOUR STRATEGIC DIRECTIVES.

This Directive-Goal-Objective approach establishes a logical methodology upon which detailed implementation plans can be subsequently developed. In this context, requirements and tasks can be efficiently created since ITP directives, goals and objectives have been clearly established and communicated.

Build a Framework

Building a framework includes defining the ITP functional components, establishing governance structures, defining roles and responsibilities, and creating supporting policies and procedures. A clear and operationally focused framework is necessary to effectively enable ITP operations.

BROAD OBJECTIVES THAT SUPPORT THIS GOAL INCLUDE:

ALIGN THE INSIDER RISK MANAGEMENT STRATEGY AND POLICY WITH BUSINESS OBJECTIVES

To be effective, an insider risk management strategy must be aligned with business objectives. To foster this alignment and become a business enabler requires the collaboration of several functional components that make up the Insider Threat Management Ecosystem. The strategy and policy shape these components and define the organization's approach to managing insider risk and develop the foundation for creating requirements to address business objectives, regulations and laws, and current risk operating environment. These directives, goals, and objectives guide all activities related to insider risk management.

The current model for most organizations is purely reactive and focused on investigative measures.

A new model must clearly define a proactive strategy that involves a paradigm shift for people, processes, and technology applications, as well as the policies and legal frameworks that support them. As a definitional matter, "insider risk" must be independently defined and categorized to encompass the unique characteristics and management challenges. While part of "cyber risk" in a broad sense, including insider risk as a cyber risk, creates blind spots and ignores the unique characteristics and broader impact of insider threats. "Cyber risk" connotes risks emanating from networks and the digital realm and thus result in network or technology solutions to manage them. "Insider risk," however, is much more than network security and involves a range of human behaviors, characteristics, and personas that include network behavior, but also involves off-network behaviors and broader physical and personnel security issues not captured by a focus on network security.

Organizations must develop the strategies and policies to manage insider risk to organizational operations, assets, and individuals; implement the risk management strategy consistently across the organization; and update the risk management strategy as required to address organizational changes. The ITP should strive to align insider risk management processes with strategic, operational, and budgetary planning processes. Leveraging the Insider Threat Committee as part of the governance structure will facilitate the consistent application of the risk management strategy across the organization's entire ecosystem.

DEVELOP AN ITP ECOSYSTEM STRUCTURE

An effective ITP is a coordinated collaboration of cross-functional components with a unified vision and defined roles and responsibilities. Most frameworks, however, consist of separate and siloed functional components. Insider risk itself lacks definition of both scope and functionality, resulting in ambiguous roles and responsibilities. Current "insider risk management" processes and governance structures have been largely defined within the context of investigative processes. This has led to a myopic and narrow focus on *responding* to known threats and events. As a result, many essential ITP components are not included in the risk management governance structure.

A FORMAL ITP INCLUDES STRATEGY, DIRECTIVES, AUTHORITIES, GOALS, OBJECTIVES, GOVERNANCE, AND BUDGETARY AUTHORITIES SUPPORTING THE FOLLOWING COMPONENTS AND MISSION STATEMENTS:

- **GOVERNANCE AND STRATEGY:** The organization's ecosystem, structure, objectives, policies, and procedures are defined, and regulatory, legal, and operational requirements are understood and inform the management of insider risk.
- **PERSONNEL ASSURANCE:** The organization ensures a trusted workforce by fully vetting employees prior to granting them access to assets and by implementing procedures to alert on behavior indicative of insider threat once onboard.
- **TRAINING AND AWARENESS:** Insiders are provided with threat awareness education and are adequately trained to perform their insider risk-related duties and responsibilities consistent with related policies, procedures, and agreements. Workforce is trained on expectations, codes of conduct, conflict resolution processes, and policies and procedures supporting each.
- **ASSET MANAGEMENT – CROWN JEWEL PROGRAM:** The organization's assets are identified, prioritized, and managed consistent with the organization's insider risk strategy.
- **ACCESS CONTROL:** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
- **MONITORING:** Employees and assets are monitored to obtain visibility for purposes of uncovering actions that are indicative of threat and may negatively impact the organization.
- **ANALYSIS:** Analysis is conducted to identify behaviors and interactions that may be indicative of threat. Data is analyzed across multiple platforms and sources and capable of providing actionable alerts.
- **INVESTIGATION:** Behaviors, actions, and insider threat indicators are examined and fully explored to determine the level of threat. Identified threats are mitigated in accordance with established policies, existing business objectives, risk tolerance and legal parameters.
- **INSIDER RISK ASSESSMENT:** The organization's priorities, asset impacts, vulnerabilities, and threats are identified and used to measure insider risk to support business operations and security resource allocations.

- **OVERSIGHT AND COMPLIANCE:** Insider risk management personnel, processes, and procedures are formally managed and reviewed for compliance with established legal, privacy, policy, and regulatory requirements.

ESTABLISH NEW ITP ROLES AND RESPONSIBILITIES

As a cross-functional program, the ITP requires programmatic collaboration across several divisions and components. To foster this collaboration, each ITP component should be assigned a "component owner" (CO) who should have primary responsibility over their assigned component. This includes ensuring that component objectives are met, and requirements and tasks are created to mature component capabilities. Each CO should also be a member of the Insider Threat Working Group.

To manage this collaboration, a new Insider Threat Director (ITD) role should be created to serve as the focal point and the single point of communication to the Insider Threat Committee for all ITP related equities. The ITD should chair the Insider Threat Working Group and report to the CSO or CRO as ITP owner. This will allow the ITD to operate with the necessary ability to reach across components and effectuate value-added decision-making.

CLARIFY LEGAL AND REGULATORY PARAMETERS

Legal and privacy parameters must be clearly defined and communicated to the ITP. Clear legal and privacy parameters will positively impact the organization's insider risk management capabilities by enabling the effective implementation of affirmative insider risk management controls and capabilities, both proactive and reactive. These parameters will include a wide array of issues pertaining to employee monitoring, data protection, and employee investigations. They must, however, enable the ITP to collect, monitor, and analyze relevant information on organization-owned networks, devices, facilities, and authorized users of the same. The ITP should work closely with legal and privacy to communicate requirements and develop suitable parameters that effectively balance security and privacy equities.

DEVELOP A FORMAL CRITICAL ASSET MANAGEMENT PROGRAM

Organizations should develop a formal program to iteratively identify and define critical assets and Crown Jewels. The former are those assets that if compromised would have an appreciable impact on the organization. The latter are those assets whose impact, if compromised, would be significant or catastrophic. Current asset identification methods are manual and labor intensive. Organizations should identify technology to scan its ecosystem and identify Crown Jewels. This will support the overall Asset Management Program but will also enhance business units' understanding of their Crown Jewels which will allow them to more efficiently control and grant access. A designated program manager should be assigned responsibility over the continued identification, impact assessment, and collection of asset details (cataloguing of owners, user accesses, and ingress and egress methods). The program manager should be a member of IR-WG and the component owner of the Asset Management component. The objective is to ensure that critical assets are properly identified, catalogued, and their impact assessed as part of the broader Insider Threat Strategy.

DEVELOP AN ITP IMPLEMENTATION PLAN AND PROCESS

Efficient program development requires formal processes and procedures to support the implementation of ITP goals, objectives, and priorities. This plan should serve as the internal playbook for the ITP team and provide detailed guidelines for developing the capabilities to prevent, detect, and mitigate insider threat actors and events.

Enhance Capabilities

Enhancing the organization's ITP capabilities includes strengthening processes and expanding insider risk management operations, focusing on developing greater assessment and analytic capabilities, and integrating more proactive deployments of monitoring tools.

BROAD OBJECTIVES THAT SUPPORT THIS GOAL INCLUDE:

FULLY LEVERAGE MONITORING AND ANALYSIS TOOLS

Monitoring and analysis tools are designed to obtain visibility and understanding of actions and behaviors of assets and insiders on organization-owned networks and devices. Visibility and Understanding are primary directives of this strategy and integral to an effective ITP. Without either, an organization will remain critically susceptible to compromise. There are three general tool capabilities that provide such visibility and understanding – User Activity Monitoring (UAM), User and Entity Behavior Analytics (UEBA), and Data Loss Prevention (DLP). UAM tools are designed for continuous passive monitoring to collect a rich source of information such as video, keystrokes, file captures, etc., when a policy is violated it provides analysts context around the user's behavior. UAM tools must be deployed to continuously monitor user activity on the endpoint for actions and behaviors indicative of insider threat. UEBA tools are designed to integrate and analyze disparate data sources, including UAM and DLP, to identify patterns and behaviors and provide alerts of concerning activities. DLP tools are designed to look for specific attributes such as key words and file types, and take actions based on the rule set (can notify user, block, or block and notify). UAM, UEBA, and DLP must be used in parallel to provide a complete picture of both asset and insider actions and behaviors. *Fully leveraging* is herein defined as deploying monitoring and analysis tools to allow for full visibility of an organization's critical assets, insider behaviors, and insider interactions with those assets.

STRENGTHEN SHARING BETWEEN HR AND CSO

HR plays an integral role in insider risk management. As the organization charged with managing and processing employee onboarding, issue resolution, and off-boarding, HR is uniquely positioned to provide visibility regarding information indicative of insider threat. HR must continue to refine and streamline processes and procedures to share all insider threat information with the CSO. HR and CSO should seek solutions that integrate existing case management systems to allow the sharing and access of relevant threat information in a timely manner.

The CSO should also be incorporated into the termination workflow as this is a period of high risk to the organization. Notice should be provided at the earliest possible moment to give security sufficient time to conduct due diligence checks and make informed risk-based decisions. Automated mechanisms should be explored to send automatic alerts or notifications to notify the Security of relevant personnel actions.

DEVELOP A FORMAL INSIDER RISK ASSESSMENT POLICY

To promote robust insider risk management, a formal insider risk assessment policy must be created to define and address the purpose, scope, roles, and responsibilities. Monitoring and analysis efforts will be of limited value unless they are incorporated into a logical process to identify, assess, and communicate risk to ITP personnel and stakeholders. A formal policy will not only promote effective insider risk management but will also serve as a business-enabling tool that can be leveraged by leadership to better understand business risk and resource allocations.

CREATE AN INSIDER RISK CENTER OF EXCELLENCE

The Insider Risk Center of Excellence (COE) will serve as the analytic focal point of the ITP. The CSO should lead the COE and build up human resources to support the increased monitoring, analysis, and investigations that will result from the growth of the ITP. To be operationally effective, the ITP will need dedicated management, SME, analyst, and investigator support.

ENSURE PRE-ACCESS VETTING OF ALL PERSONNEL

Vetting of personnel is a foundational element to an effective ITP and supports the Awareness directive of this strategy. All personnel, regardless of status (employee, contractor, partner, etc.) should be subject to vetting prior to being granted access to organization assets. Most organizations only vet their full-time employees. For example, in many organizations, contractors are not subjected to the same background check procedures as full-time employees. Contractors are, however, often granted very sensitive access and can cause grave impacts to organization business value and operations.

Organizations should create a vetting program for all insiders, including contractors, who are granted access to organization information networks or when given organization-owned devices for use during their employment. Organizations should leverage existing and efficient background check processes for full-time employees to fully vet contractors.

Optimize Operations

Optimizing ITP operations involves maturing capabilities and achieving certain program effectiveness milestones. These include meeting certain risk coverage and monitoring criteria, expanding training programs, developing greater employee engagement, and more effective messaging regarding insider risk management.

BROAD OBJECTIVES THAT SUPPORT THIS GOAL INCLUDE:

ENSURE FULL UNDERSTANDING AND VISIBILITY OF CROWN JEWELS

Complete coverage of all assets is not necessary for effective risk management. A tailored approach as discussed, will allow for the greatest amount of risk to be managed at the lowest cost. Crown Jewels, as a subset of an organization's critical assets, represent those assets that if compromised would cause the organization the greatest amount of harm. Accordingly, the ITP must seek to obtain full awareness, understanding, and visibility of the Crown Jewels to allow for effective risk management.

ENSURE FULL AWARENESS, UNDERSTANDING, AND VISIBILITY OF RISKIEST INSIDERS

As with Crown Jewels, complete coverage of all employees, contractors, and business partners is not necessary for effective risk management. Here also, a tailored approach focused on those insiders that pose the greatest risk to an organization, promotes effective risk management by applying a least intrusive means methodology. This should include ensuring that monitoring tools are fully leveraged to support obtaining the necessary visibility on high-risk insiders.

EXPAND TRAINING PROGRAMS

Employees must be informed of the importance and methods needed to protect sensitive organization assets. While existing campaigns may provide information regarding proper security measures, this alone is insufficient to provide adequate awareness. These programs must be expanded and include additional required training for all employees. Training should define "insider threat," and explore the degree to which insider threats can impact mission and business equities. Training should also explore the different types of insider threat personas and how they can be used to better understand mission and business harm. Effective security training requires continuous and ongoing education and awareness campaigns. Security campaigns should be continually updated and expanded to ensure employees are engaged and informed of current security threats and practices.

FOSTER GREATER INSIDER ENGAGEMENT AND IMPROVE MESSAGING

An effective ITP requires the active involvement of employees, contractors, and partners. Insiders are the first line of protection against harm to the organization. Active involvement begins with properly engaging insiders at onboarding or, in the case of contractors and partners, at the start of an engagement, and educating them about workplace expectations and responsibilities. A solid policy structure is necessary to reinforce and deliver this message. Insider must be partners in the ITP and understand their responsibilities as employees and contractors to safeguard and protect assets. Insiders must also be provided clarity on proper and expected security practices and best practices for protecting sensitive information. Organizations should ensure policies and controls provide concise and coherent documentation, including the reasoning behind the policy, as well as consistent and regular employee training on the policies and their justification, implementation, and enforcement.

ORGANIZATIONS SHOULD BE PARTICULARLY CLEAR ON POLICIES REGARDING:

- Acceptable use and safeguarding of the systems, information, and resources
- Use of privileged or administrator accounts
- Ownership of information created as a work product
- BYOD and removable media usage
- Network and user activity monitoring

DEVELOP EFFECTIVE METRICS

A framework must be created for assessing progress that emphasizes the importance of (a) multiple measures for a given directive, goal, or objective, (b) combining quantitative metrics and qualitative indicators, and (c) minimizing the staff time devoted to such measurements. Such metrics need to be supplemented with qualitative assessments by independent experts to annually review the Insider Threat Management Program. Program maturation requires the ability to measure the effectiveness of developed capabilities, processes, and procedures. This plan specifies a core set of metrics for assessing organizational progress toward key priorities.

SPECIFIC METRICS MUST BE DEVELOPED TO UNDERSTAND, MEASURE, AND EXPAND ON THE FOLLOWING EFFECTIVENESS MARKERS:

- ITP capability levels
- Organizational risk levels
- Component capability levels
- Component development efforts
- Asset group risk levels
- Insider group threat levels
- Crown Jewel coverage levels
- Coverage levels of highest risk insiders
- Monitoring coverage levels
- Quality of monitoring alerts
- Alert response time
- Threats identified and mitigated

AUTHOR'S NOTE

ITMG was formed in 2014 to help companies successfully manage insider risk. In that time, we've been fortunate to have experienced and directly contributed to the growth of insider risk management as a separate and unique security discipline. As organizations continue to expand and formalize Insider Threat Programs, the need for qualified and experienced risk management professionals will undoubtedly increase. It is our hope that this book will contribute to this body of knowledge and support the continued growth of the insider risk management profession.

Shawn Thompson

Founder and CEO

ITMG

exabeam®

EXABEAM.COM