Innovations
LEARNING SERIES

Modern Blueprint to Insider Threat Management

Taking a People-Centric Approach to Implementing Your Insider Threat Management (ITM) Program

Lawrence Miller

POWERED BY
ActualTech MEDIA

BROUGHT TO YOU BY
proofpoint.

Innovations
LEARNING SERIES

Modern Blueprint to Insider Threat Management

EXPRESS EDITION

By Lawrence Miller

PUBLISHER'S ACKNOWLEDGEMENTS

EDITORIAL DIRECTOR

Keith Ward

DIRECTOR OF CONTENT DELIVERY

Wendy Hernandez

CREATIVE DIRECTOR

Olivia Thomson

SENIOR DIRECTOR OF CONTENT

Katie Mohr

PARTNER AND VP OF CONTENT

James Green

ABOUT THE AUTHOR

Lawrence Miller, CISSP, has worked in information security and technology management for more than 25 years. He received his MBA in Supply Chain Management from Indiana University and has earned numerous technical and professional certifications throughout his career. He is currently working as an IT security solutions consultant. He has previously worked as the Vice President of IT for a major Verizon reseller, director of IT and e-commerce for a retail merchandising company, and IT operations manager for a top 100 U.S. law firm. He served as a Chief Petty Officer in the U.S. Navy and is the author of more than 200 books on various topics including information security, cloud, unified communications and collaboration, storage, 5G, and the Internet of Things.

ENTERING THE JUNGLE

Introduction: What Is an Insider Threat? 7

Chapter 1: Recognizing the Insider Threat 8

The Nature of Work Is Changing 9

Understanding Your People Perimeter 11

Preventing Data Loss 13

Exploring Common Business Use Cases 14

Check Yourself: Recognizing the Insider Threat 20

Chapter 2: Setting Up Your Insider Threat Management Program 22

Effectively Managing Insider Threats 22

Getting Started with an Insider Threat Management Program 25

Developing and Scaling Up Your Operating Capability 26

Driving Success with an Insider Threat Management Framework 30

Check Yourself: Setting Up Your Insider Threat Management Program 32

Chapter 3: Implementing an Insider Threat Management Platform 35

Taking a People-Centric Approach to Data Loss Prevention and Insider Risk Management 35

Threat Detection and Analytics 39

Privacy and Compliance 40

Key Capabilities 42

Check Yourself: Implementing an Insider Threat Management Platform 43

Wrapping Up 44

CALLOUTS USED IN THIS BOOK

THE 101

This is where we turn when we want to provide foundational knowledge for the subject at hand.

OFF THE BEATEN PATH

This is a special place where you go to discover insight into topics that may be outside the main subject but that are still important and relevant.

BRIGHT IDEA

When we have incredible thoughts (at least in our heads!), we express them through eloquent phrasing in the Bright Idea section.

DEEP DIVE

Takes you into the deep, dark depths of a particular topic.

EXECUTIVE CORNER

It’s not all tech all the time! This is where we discuss items of strategic interest to business leaders.

ICONS USED IN THIS BOOK

DEFINITION

Defines a word, phrase, or concept.

KNOWLEDGE CHECK

Tests your knowledge of what you’ve read.

PAY ATTENTION

We want to make sure you see this!

GPS

We’ll help you navigate your knowledge to the right place.

WATCH OUT!

Make sure you read this so you don’t make a critical error!

TIP

A helpful piece of advice based on what you’ve read.

What Is an Insider Threat?

Welcome to the Innovations Learning Series: Modern Blueprint for Insider Threat Management, Express Edition!

What is an insider threat? An insider threat occurs when someone with authorized access to critical information or systems misuses that access—either accidentally or maliciously. This can result in data loss, legal liability, financial consequences, reputation damage and more.

And even though insider threat incidents are becoming increasingly prevalent, and valuable information and trade secrets are at stake, many organizations don't understand the nature of these threats or how to detect and prevent them.

This eBook will help you recognize the insider threat, set up a successful insider threat management program, and implement a robust insider threat management platform for your organization.

Let's get started!

CHAPTER 1

Recognizing the Insider Threat

Most organizations today spend significant time and resources detecting and mitigating external threats. Yet few make the same investment in addressing internal threats. This is often because organizations don't know what insider threats look like—let alone how to tackle them.

And herein lies one of the first challenges associated with mitigating insider threat risks: insider threats are not always malicious. Many insider threat incidents are due to negligence by well-meaning people who accidentally leak confidential or sensitive data. And other insider threat incidents stem from compromised users who unwittingly fall victim to credential theft or malware that infects and takes control of their devices.

An *insider* refers to employees, independent contractors and consultants, third-party contractors, supply chain partners and service providers, among others. The definition of an insider has expanded significantly in recent years as a result of businesses becoming more digitally and globally interconnected.

In this chapter, we'll explore how the changing nature of work contributes to an increase in insider threats, how the traditional network perimeter has evolved, how data loss occurs, and which insider threat use cases are most relevant to organizations like yours.

The Nature of Work Is Changing

The modern digital workplace has evolved; more people work from anywhere and access data from everywhere more than ever before. As enterprises increasingly adopt a work-from-home (WFH) or work-from-anywhere (WFA) model—particularly in the wake of the global pandemic—the traditional notion of a network perimeter has all but disappeared.

Organizations must address greater cyber risks from sophisticated external threats, as well as negligent, compromised, or malicious insiders. Organizations also need to be cognizant of the complex data privacy and protection regulations, such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standards (PCI DSS), that have strict rules governing how data is used, processed, and stored.

According to the Proofpoint *2021 Voice of the CISO Report*, 58% of chief information security officers (CISOs) believe that even though employees understand their role in protecting against cybersecurity threats, they also pose the biggest risk.

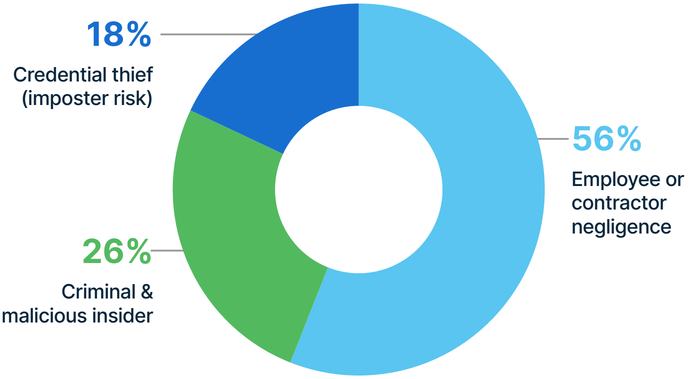


Figure 1: Frequency of negligent, compromised and malicious insider threats (Source: Ponemon Institute 2022 Cost of Insider Threats Global Report)

Insider threats are typically categorized as follows (see **Figure 1**):

- **Negligent**: User mistakes that unintentionally create risks. According to the Ponemon Institute 2022 *Cost of Insider Threats Report*, negligent insiders are responsible for 56% of all insider threat incidents, at an approximate cost of $485,000 per incident and an average annual total cost of $6.6 million.

- **Compromised**: Users that have been successfully targeted by social engineering or malware to steal their login credentials and/or take control of their devices. According to Ponemon, compromised insiders are responsible for 18% of all insider threat incidents, at an approximate cost of $805,000 per incident and an average annual total cost of $4.6 million. Worth noting is that the cost of credential theft to organizations increased 65% from $2.79 million in 2020 to $4.6 million in 2022, illustrating that compromised insiders may now be the greatest insider threat risk to organizations.

- **Malicious**: Users who intentionally cause damage or steal from an organization, usually motivated by greed, revenge, or a sense of entitlement. According to Ponemon, malicious insiders are responsible for 26% of all insider threat incidents, at an approximate cost of $648,000 per incident and an average annual total cost of $4.1 million.

Over the past two years, cybersecurity incidents caused by insider threats have increased by 44% to an average annual cost of $15.38 million per organization according to Ponemon. Some real-world examples of insider threats include:

- **Negligent:** U.S. soldiers trying to memorize the security protocols around nuclear weapons protections unknowingly leaked a significant amount of sensitive information over an eight-year period by using an unsecured flashcard learning app.

- **Compromised:** A cybercriminal group led by a Florida adolescent coerced a Twitter employee to give up credentials for corporate administrative tools. This led to takeovers of verified accounts used in a Bitcoin-promotion scam that stole $117,000 from customers.

- **Malicious:** A ConocoPhillips employee created fraudulent invoices to trick the oil giant into paying a friend's business more than $3 million. The actions were part of a larger embezzlement scheme that totaled nearly $7.3 million.

Understanding Your People Perimeter

Once a mainstay of cybersecurity, perimeter-based security strategies are no longer sufficient to protect an organization's sensitive applications and data in today's WFA world. Several recent trends that have driven work—and its associated data—beyond traditional network perimeters include:

- Greater workforce mobility, including WFH and WFA remote work models

- Widespread adoption of Software-as-a-Service (SaaS) and cloud-based file sharing

- Growing reliance on independent and third-party contractors and consultants, supply chain partners, and service providers

In short, people—not workplaces—are the new perimeter. Thus, robust insider threat management (ITM) requires organizations to understand how their people work with data and develop a people-centric strategy to prevent data loss from insider threats.

Know Your People

Not all insiders are created equal. Some pose more risk to the organization than others.

Therefore, when looking at how to address insider threats, you must be able to assess risk, based on dynamics relevant to your business. Soon-to-depart employees or contractors, highly visible executives, human resources and finance employees with access to sensitive data, and IT administrators with privileged access may constitute a high-risk insider for your business.

Another category to define are Very Attacked People™ (VAPs). These are high-value users that threat actors repeatedly target, hoping to find a way into the organization. These targets vary by business and industry. What they have in common is their risk: they are worth pursuing, because the opportunity is commensurately great.

Know Your Data

Once you understand the people who need to be protected, look at your data and consider:

- Which data is sensitive or valuable?
- Where does that data reside and how is it used?
- Who has access to it and who should have access?

Next, assess the devices and applications that are used to interact with this data and get work done. All these devices and applications should be viewed as valves from which data could leak. Your insider threat management program (ITMP) should close as many of these valves as possible and monitor anything that cannot be closed completely.

Preventing Data Loss

Data loss, whether negligent or malicious, can occur through many common channels, including:

- **Cloud and web apps:** SaaS and web-based applications often contain sensitive information. Even when approved for use (or sanctioned) by the organization, these applications can introduce risks. However, many organizations have no tools to prevent (or even detect) unauthorized, unapproved, or unsanctioned "shadow IT" applications that may create unacceptable security and compliance risks.
- **Cloud storage:** These easy-to-use services, including file transfer protocol (FTP) sharing sites, are often used by teams and individuals to collaborate and share files with minimal IT or security oversight.
- **Developer tools:** Application developers often use web-based hosting sites for version control. These sites make it easier for developers to collaborate but can also lead to leaks of trade secrets and proprietary source code.
- **Email:** Malicious insiders might steal sensitive or valuable data by forwarding it to a personal email account.
- **Mobile devices:** Smartphones can boost productivity but also pose a threat to an organization's data with their recording, camera, storage, and email client capabilities.
- **Printed copies:** Although this storage medium is less common today, printed hard copies of sensitive documents can be a major source of data leaks and need to be tracked, managed, protected, and properly destroyed like any other data.

- **Removable media:** USB storage devices ("thumb drives") and SD cards containing sensitive information can be easily lost or stolen and malicious users can use them to exfiltrate data or infect devices with malware.
- **Screen capture and screen sharing software:** Screen capture software (such as Snagit and Snip-it) and screen sharing capabilities in collaboration platforms (such as Cisco WebEx, Microsoft Teams, and Zoom) can be used to surreptitiously obtain unauthorized images of sensitive information.
- **Social media:** Unauthorized use of social media makes it easy—whether maliciously or negligently—to post sensitive information on sites such as Facebook, LinkedIn, and Twitter.

Exploring Common Business Use Cases

Certain business scenarios make organizations more vulnerable to insider threats. These common scenarios often result in higher risks of data loss from insiders.

Remote Employees, Contractors, and Third-Party Vendors

Whether through remote employees, third-party contractors, or executives and sales teams always on the move, every modern organization is dispersed and mobile today. Remote collaboration on sensitive assets heightens the risk of negligent mistakes and malicious behavior. It can be difficult for organizations that have relied on perimeter-based security solutions to retain control of sensitive data as the physical boundaries of the traditional office disappear, especially as employees adapt to new ways of working.

Common risky behaviors of remote workers include:

- Downloading files during irregular hours

- Sharing account credentials
- Installing unauthorized software
- Leaving credentials unprotected
- Logging on from different endpoints
- Sharing files with unauthorized users

To address these risky behaviors, consider the following tips:

- Use an ITM solution that enables third-party monitoring and helps ensure compliance with data privacy regulations
- Enforce security policies for remote workers and coach employees on best practices for following these policies when out of the office
- Explore the context of potential incidents to understand the user's motivations

BRIGHT IDEA

Le Figaro: A Newspaper Makes Headlines – But Not in a Good Way

French newspaper Le Figaro's accidental data leak—caused by a third-party hosting firm's poor security hygiene—exposed 7.4 billion records between February and April 2020.

Lessons Learned:

- Outside vendors must meet strict risk assessments before they are used to store or traffic valuable information about users.
- Attacks often morph from data theft to more complex and dangerous attacks that target internal systems, so having early warning systems in place is key.
- Database leaks are one of the most common insider threat types. Make sure yours are properly configured and that monitoring is in place to detect leaks.

Departing Employees

Departing employees are especially high-risk users. Though these users' motivations are often completely innocent, there is the chance that they can be malicious. For example, a departing employee may look to steal trade secrets and bring them to their new employer. They may use cloud storage services, personal email, or removable media to exfiltrate data. In some cases, organizations don't promptly disable access to corporate applications and systems even after termination, leaving the door open for former employees to access sensitive data.

EXECUTIVE CORNER

PPE Shipments Sabotaged During the COVID-19 Crisis

The fired ex-VP of finance at Georgia-based Stradis Healthcare deleted or altered more than 115,000 data records, disrupting shipments of personal protective equipment (PPE) during the early days of the U.S. pandemic response.

Lessons Learned:

- Creation of fake accounts is a key insider threat indicator that should be quickly flagged by security software and reviewed internally.
- Employees with a disciplinary history—especially those involving access and system abuse—should be flagged as high risk and monitored with extra caution. Revenge is a common motive for malicious insiders.
- Employees with a high level of privilege, such as a VP of finance, should also automatically receive more scrutiny to ensure they do not abuse their privileges.

To address the insider threat from departing employees, consider the following tips:

- Establish formal offboarding processes (with both HR and IT teams), including promptly disabling access to prevent unauthorized access to applications and systems
- Monitor activity for high-risk users who are preparing to leave the organization
- Collect contextual information (who did what, when, where, and why) to aid investigation after an insider threat incident

Virtual Applications and Desktops

Virtual desktop infrastructure (VDI) systems and applications are often used for remote access to critical systems and data. Misuse of virtual apps and VDIs is a common problem, made more difficult because manually monitoring remote access is impractical.

To address the insider threat from virtual apps and desktops, consider the following tips:

- Institute thorough background checks for third-party users, particularly those with privileged access
- Deploy an ITM solution to monitor user activity and detect system misuse within popular VDIs and virtual applications, such as Citrix Ready and VMware Horizon

Shadow IT

Even when organizations authorize the use of various IT applications and tools, people don’t always follow the rules. Whether they’re trying to get around a cumbersome process, looking for a shortcut, or avoiding technology that just doesn’t work, employees and other insiders often turn to “shadow IT” applications and infrastructure. The most common risk is data loss through cloud storage, web applications, or SaaS applications. Often, user access and privileges are too loosely controlled by IT, leading to unauthorized access to sensitive data.

To address the insider threat from shadow IT, consider the following tips:

- Limit the ability for employees and other insiders to download or access unsanctioned technology on corporate-owned devices, such as laptops and mobile devices
- Increase visibility into shadow IT by monitoring user activity and alerting the security team when something unusual or risky happens, or if data is found outside of approved environments
- Solicit feedback from employees about security, reinforce protocols with training, and listen to employees' experiences and complaints. People often circumvent technology in a misguided attempt to solve real IT challenges that inhibit their productivity.

Mergers and Acquisitions (M&A)

Managing data risks during the M&A process is a major challenge. Risk and compliance teams need to know who has interacted with sensitive information to ensure both parties are aware of the risks before the deal is closed.

And once the deal closes, it's critical to gain visibility into the varying degrees of employee security awareness and hygiene. Though it's a challenge to combine differing—and often conflicting—security policies across organizations, it may be even more challenging to control access privileges for administrators.

Complex personnel issues may also result directly from the M&A. For example, if employees depart voluntarily or are laid off, they might attempt to take sensitive information with them and disgruntled employees out for revenge might attempt to defraud the organization or its customers.

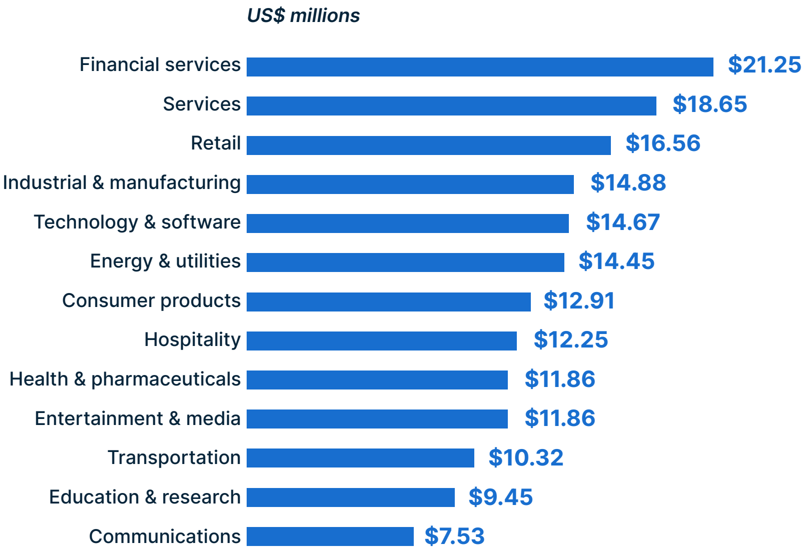


Figure 2: Annualized cost of insider threat activity, by industry (Source: Ponemon Institute 2022 Cost of Insider Threats Global Report)

To address the insider threat from mergers and acquisitions, consider the following tips:

- Detect data leakage from corporate locations (for example, private deal terms, trade secrets, undisclosed security events, and other information that's stored in files from customer relationship management, enterprise resource planning, or human resources systems)
- Issue alerts when privileged users try to get access to sensitive systems, use shared credentials, or install suspicious tools
- Monitor and collaborate closely with human resources to monitor potentially high-risk user groups

As shown in **Figure 2**, the annualized cost of insider threat activity differs across industries, and are highest in the financial services industry.

Check Yourself: Recognizing the Insider Threat

In this chapter, we shared information to help you recognize the insider threat. Are you prepared to efficiently recognize an insider threat in your organization? Take a moment to test your knowledge.

1. True or False: The majority of insider threats are maliciously motivated.

FALSE. Though malicious insiders are certainly a type of insider threat organizations need to be prepared to recognize and respond to in a timely fashion to mitigate the impact on the organization, they are not the most common type of insider threat incident. Many insider threat incidents are actually the result of negligence by well-meaning people who accidentally leak confidential or sensitive data. And other insider threat incidents stem from compromised users who may fall victim to credential theft or malware that infects and takes control of their devices.

2. Is traditional perimeter-based security enough for today's modern workforce?

The short answer: No. People are the new perimeter in today's WFA world because, quite frankly, the traditional approach to perimeter-based security just won't cut it. Work no longer exists within an organization's four walls; from greater workforce mobility, to widespread adoption of Software-as-a-Service (SaaS) and cloud-based file sharing, to a growing reliance on independent and third-party vendors and partners, organizations need to be vigilant about data movement and usage.

3. What are the most common scenarios that can lead to greater data loss risk as a result of insider threat incidents?

There are many scenarios that are often associated with the highest data loss risk from insiders. These include:

- Remote employees, contractors, and third-party vendors
- Departing employees
- Virtual applications and desktops
- Shadow IT
- Mergers & Acquisitions

CHAPTER 2

Setting Up Your Insider Threat Management Program

Many companies are aware of the insider threat problem, but few dedicate the resources or executive attention required to actually reduce their risk. And some may be ready to make the commitment but don't know where to start.

Wherever you are in this journey, this chapter will provide insight into what it takes to set up and manage a successful Insider Threat Management Program (ITMP).

Effectively Managing Insider Threats

As we've previously discussed, traditional perimeter-based security is not sufficient since today's WFH and WFA models allow employees and third parties to access company information from wherever they choose to work. For this reason, the primary focus to effectively manage insider threats should be centered on user activity. It's all about how users are interacting with sensitive corporate data and assets rather than on monitoring and controlling a network perimeter. This is why it's so critical to build a people-centric security model. After all, data doesn't move itself; people move data (we'll get into this a bit deeper in Chapter 3).

So, what exactly is people-centric security? People-centric security means having complete visibility and context into how insiders are interacting with corporate data and assets. With visibility and context, security staff can more effectively conduct the three primary aspects of insider threat management:

- **Identify risky user behavior and sensitive data interaction.** As discussed in Chapter 1, understanding your people perimeter—that is, knowing your people and your data—is the first step to successful insider threat management. Simply put, you have to know what you're protecting (your data) and what threats you're protecting it from (your people, whether they're negligent, compromised, or malicious).
- **Detect and prevent insider security incidents and data loss.** The ability to detect, in as close to real-time as possible, when a user takes a risky action is critical, even if it doesn't reach the level of a full-blown "incident." Your detection efforts must strike a balance between delivering timely, actionable alerts and creating alert fatigue. To do this, your program must be able to fine-tune alert signals using a mix of real-world insider threat risk indicators and

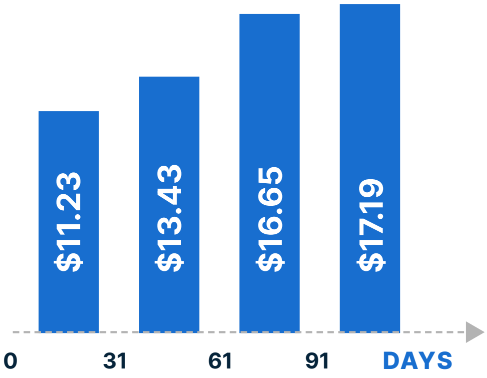


Figure 3: Average cost of insider threat activity by days to contain the incidents, in US$ millions (Source: Ponemon Institute 2022 Cost of Insider Threats Global Report)

organization-specific, unique alert dynamics. Prevention requires proactive user awareness and training and real-time controls, such as data loss prevention (DLP), to stop users from accidentally or intentionally compromising the security and privacy of sensitive data.

- **Respond quickly to insider security incidents and data loss.** The reality is that prevention is never 100% effective. When prevention fails, organizations need the ability to rapidly investigate, contain, and remediate incidents and data loss. The longer an insider threat or data loss incident persists, the more damage it can do—to both your reputation and your bottom line (see **Figure 3**). So, it's important to be able to respond quickly and appropriately. Also key is the ability of cross-functional teams, including security, IT, legal, human resources, executives and others, to work together.

EXECUTIVE CORNER

Balancing Legal Considerations and Company Culture

An ITMP requires you to increase oversight of insider activity around corporate data and assets, but it's important to do this in a way that complies with relevant laws and aligns with your corporate culture.

Legal issues can be challenging to navigate when building an ITMP, but don't let them stop you. The benefits of a successful ITMP far outweigh the struggles of meeting any legal requirements. In fact, certain laws and compliance requirements are best met through a holistic ITMP. From a legal and privacy standpoint, you are much better off implementing a well-designed ITMP than avoiding one due to concerns about potential legal hurdles.

Some of the most common issues that organizations encounter when building an ITMP include:

- **Consent:** Do you have consent to monitor your employees' digital activities? Do you need it?
- **Scope:** Whom will you monitor? Everyone? Only a subset of employees? Where, when, and how will you monitor them?
- **Agreements:** Do you have the necessary employment agreements in place?
- **Policies:** Do you have documented management support for the monitoring program?
- **Compliance:** Do you have a "watch the watchers" program in place to ensure employees or contractors tasked with monitoring don't abuse their privileges?

As you develop and expand your ITMP over time, review these questions with your legal team and other key stakeholders, including compliance staff, security experts, and executives. You can strike a healthy balance with legal considerations and company culture and still mitigate the risks posed by insider threats. It simply requires planning and preparation.

Getting Started with an Insider Threat Management Program

Building a successful ITMP that reduces organizational risk requires a holistic, cross-functional effort that involves not just your IT and cybersecurity teams, but also legal, human resources, operations, line-of-business (LOB) leaders, executives, and many others. It requires clear and effective communication across technical and non-technical teams, visibility into what insiders are doing with corporate resources, and a clear strategy to prevent and mitigate insider threats. An ITMP must include people, processes, and technology—all working together in harmony.

Some important first steps include:

- **Designating an executive champion:** Solidify support for your ITMP by designating a champion. The champion should help ensure that the organization puts a priority on developing and operating the program—and that it allocates the resources needed to do so.

- **Identify a steering committee:** Representation should extend beyond the traditional cybersecurity group and include human resources, physical security and legal counsel, among others.

- **Build cross-functional working groups:** Your larger working group (not just the steering committee) should include legal counsel and privacy officers. This ensures you have the right level of legal review and guidance at every step in the process.

- **Ensure privacy by design:** ITMP personnel handle a huge amount of personally identifiable information (PII) and data about the individual conduct of employees and other insiders. So, work carefully to ensure the program provides sufficient personal privacy and whistleblower protections.

- **Assemble a complete team:** Insider threat personnel must have a solid understanding of cybersecurity, insider risk assessment, insider profiling, and security and privacy control architecture. If necessary, bring in outside consultants with expertise in forensics, legal issues, risk assessment, privacy, compliance and other areas.

Developing and Scaling Up Your Operating Capability

Insider threats are a complex problem, and a full operating capability may take time to develop. But you can get immediate value by developing an initial operating capability, legally supported with documented policies and procedures, as illustrated in **Figure 4**.

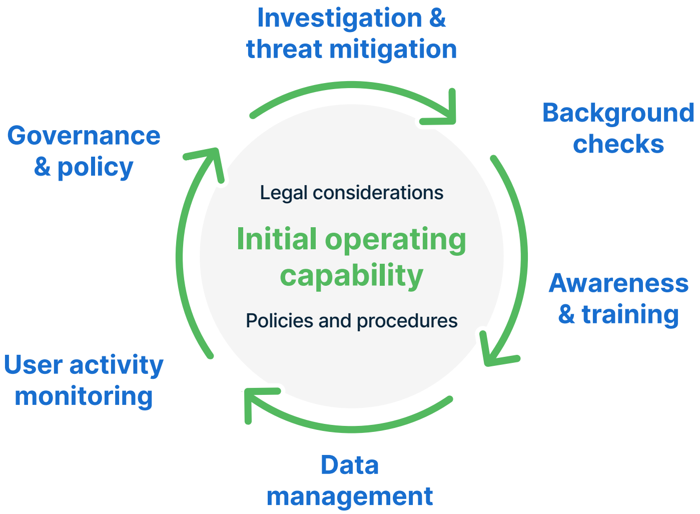


Figure 4: Insider threat management—initial operating capability

An effective initial operating capability includes three broad categories of activities:

Programmatic tasks: These tasks are essential to running an ITMP.

- Establish the program and appoint functional managers to provide support.
- Describe the purpose of the program—detecting, preventing, mitigating, and responding to insider threats—in the context of the organization's goals.
- Define and communicate which categories of workers are subject to the ITMP (such as employees, consultants, contractors, etc.).
- Establish a program office, which might include a centralized analysis and response hub.
- Ensure that program personnel have authorized access to insider threat-related information and data from across the organization.

- Address legal, privacy, civil rights, civil liberties, and whistleblower protection issues.
- Mandate insider threat and general security awareness training.
- Define requirements to conduct independent assessments of whether the program complies with guidelines and policies.

Added layers for dispersed organizations: Organizations that are hierarchical or regionally dispersed (including remote work) are at greater risk of gaps in coverage. Geographically dispersed entities might need to include the following layers to mitigate gaps:

- Policies
- Standard operating procedures
- Designated points of contact
- Dedicated communication channels

Regular review: Insider threat policies should be reviewed regularly. Incorporate lessons learned, ensure that the guidance is still effective, and adapt to any changes in laws, policies, organizational structure or IT architecture.

Beyond developing an initial operating capability, most organizations need to scale up over time to reach full operating capacity to maximize the effectiveness of their ITMP. This includes the following activities:

- **Personnel assurance:** Most organizations employ effective background investigation processes for full-time employees. Contract personnel and partners, however, often do not receive the same level of vetting. Onboarding training should be comprehensive. Visibility into employee behavior can often be enhanced through more formal collaboration between human resources and security.
- **Access control:** Even with effective access control processes and tools in place, some policies can create unnecessary vulnerabilities.

A common example is granting all users local administrative rights, by default, on organization-issued computers. Access control implementation is often too federated, with line managers solely responsible for a large part of data group creation and access grants.

- **Analysis:** Most large organizations deploy analytic resources to hunt for threats on the network and analyze log files with security information and event management (SIEM) solutions. But these efforts often suffer from a lack of datasets to analyze. Fully deploying user and data activity monitoring will foster greater analytic maturity, promote a more proactive insider threat strategy, and help track metrics.

- **Dynamic risk assessment:** Most organizations' insider threat assessment capabilities are limited to specific and narrowly defined use cases. At first they are ad hoc and reactive. A true insider threat capability requires a thorough understanding of the organization's critical asset threat factors, insider population, and existing vulnerabilities in certain types of data and systems. Once implemented, a mature insider threat assessment capability will enhance security awareness and support both reactive and proactive strategies, along with greater overall enterprise threat management.

- **Oversight:** Oversight of insider threat management functions and activities is typically shared between the chief security officer (CSO), chief information security officer (CISO), chief privacy officer (CPO), chief compliance officer (CCO) and legal counsel. A lack of a defined ITMP creates an activity-centric or issue-centric oversight model that is inefficient and lacks a strong sense of ownership. Clearly defined oversight fosters operational enablement and creates a more effective oversight and compliance framework.

Driving Success with an Insider Threat Management Framework

Organizations should complete an ITMP implementation plan to guide the program and allocate resources. An effective ITMP framework includes foundational tasks and a mindset of continuous refinement and improvement in the following areas:

Programmatic tasks program planning: Use the implementation plan to set milestones and achieve the following programmatic tasks:

- Explaining program staffing and resourcing.
- Outlining the responsibilities for a program office.
- Delineating how information from various departments is provided to the insider threat hub.
- Outlining the organizational methodology to conduct self-assessments.
- Deciding whether to solicit outside assistance. Third parties may be beneficial to assist with legal concerns, for example.
- Determining the dates and milestones for initial operating capability and full operating capability.
- Formulating current and subsequent fiscal year budgets.
- Satisfying organizational reporting requirements.

Living documentation: Treat your implementation plan as a living document, subject to change as milestones are achieved or missed, or as risks evolve.

Work in progress: Policies and operating procedures are important parts of any ITMP, but don't delay approval of the implementation plan for the sake of completeness. Treat it as a work in progress.

Annual report format: Deliver your annual report in a format that suits your organization's unique culture.

Self-assessments: Perform periodic self-assessments, for example, before an implementation checkpoint, publication of the annual report, or independent oversight review/assessment.

DEEP DIVE

Measuring Return on Investment (ROI) to Define Success

Many businesses view security as a cost center. They might understand the importance of certain security investments, but rarely expect to see a return on that investment. Yet security ROI is real—especially when it comes to insider threats. Being able to prove ROI can help teams secure the resources needed to properly manage insider threat risk.

Building a successful ITMP requires investments in people, processes, and technology. To show the ROI of your organization's ITMP, you should measure and track the following primary areas:

Insider threat incidents: Measure how incident numbers change over time using insider threat metrics. Determine which prevention and mitigation tactics work best for your organization and where to focus future budget to improve results. Also track the average cost of investigation, containment, and remediation for incidents over time.

Aim for reductions in two key areas: the overall number of incidents and the cost of resolving each incident (by detecting and containing them earlier).

Customer acquisition and retention: A strong security posture, bolstered by an ITMP, may also drive revenue by demonstrating secure and compliant practices and building customer trust. These practices not only help maintain the current customer base but also win new deals. Your ITMP should align with security and compliance frameworks, such as the

General Data Protection Regulation (GDPR), System and Organization Controls (SOC) 2 and other industry-specific requirements. To prove ROI, track the number and volume of sales you secure that would not be possible without investing in insider threat management. Also note any customer retention statistics that can be directly tied to meeting and maintaining compliance and other security standards.

Reactive versus proactive spend: Most insider threats result from careless accidents or negligence. In other words, you can prevent many incidents with the right training and awareness. Spending money on these areas can bring about quick returns. That said, credential theft is the most expensive type of insider threat, so finding ways to prevent it or stop incidents driven by it has a dramatic impact on ROI.

Check Yourself: Setting Up Your Insider Threat Management Program

In this chapter, you learned some tips to set up your insider threat management program. Here are some questions to help you keep this information top of mind.

1. What are the five steps to follow to build a successful ITMP?

Building a successful ITMP requires a holistic, cross-functional effort. The five most important steps to start with include:

- Designating an executive champion
- Identifying a steering committee
- Building cross-functional working groups
- Ensuring privacy by design
- Assembling a complete team

2. What is people-centric security?

People-centric security means having complete visibility and context into how insiders are interacting with corporate data and assets. It's all about how users are interacting with sensitive corporate data and assets instead of monitoring and controlling a network perimeter. Gaining this visibility and context enables security staff to more effectively conduct the three primary aspects of insider threat management. These include:

- Identifying risky user behavior and sensitive data interaction
- Detecting and preventing insider security incidents and data loss
- Enabling faster response to mitigate security incidents and data loss

3. What does an effective ITMP implementation plan look like?

An effective ITMP implementation plan includes a framework that outlines foundational tasks that includes a mindset of continuous refinement and improvement. This extends to five primary areas:

- Programmatic tasks program planning
- Living documentation
- Work in progress
- Annual report format
- Self-assessments

4. How can you measure ROI on an ITMP?

Though security can often be seen as a cost center, security ROI (especially regarding mitigating insider threats) is very real. For example, the ability to measure how incident numbers change over time using insider threat metrics can help an organization determine which prevention and mitigation tactics work best, and where to focus future budget to improve results. Additionally, most insider threat incidents result from careless accidents or negligence. Investing in the right training and awareness can bring about quick returns.

CHAPTER 3

Implementing an Insider Threat Management Platform

Data doesn’t lose itself. People lose it. That’s why your endpoint data loss prevention and insider threat management solutions need to take a people-centric approach to preventing data loss at the endpoint and managing insider threats.

While other cybersecurity tools may provide useful data and context to support insider threat management activities, a purpose-built insider threat management platform and endpoint data loss prevention should be at the core of your ITMP.

This chapter explores the key elements, features, and capabilities of insider threat management platforms.

Taking a People-Centric Approach to Data Loss Prevention and Insider Risk Management

The fundamental technical challenge of protecting against insider threats stems from a simple fact: users are people. Their unique behavior is difficult to summarize or understand by just looking at log files. Sure, you might be able to collect data on every login, every transaction, and even every keystroke. But inferring the person’s intent from that data alone is tricky, if not impossible.

A people-centric approach to user risk analysis starts with aggregating and organizing data around each individual user. This is a key data construct. It enables far more efficient and accurate threat analysis and visualization than what you get with traditional security tools.

People-centric user-risk analysis consists of three key elements: user risk profiling, cross-channel visibility and context, and activity timelines.

User Risk Profiling

Every user has a unique risk profile. A major benefit of organizing data around a user is that you can focus attention on higher-risk users.

A user may pose higher risk based on these factors:

- **Alert history:** If a user repeatedly triggers alerts because of risky activity, they could score higher in your risk analysis.
- **Privilege levels:** Some users could be inherently riskier based on privileged access to data, systems, and resources.
- **HR watch list:** The human resources team may provide lists of at-risk employees that warrant special attention. Examples might include employees on performance plans and those who have recently given notice or whose contracts are about to expire.
- **Non-employees:** In today's workplace, many non-employees may have access to your data resources and infrastructure. Examples include third-party contractors, service providers, and supply-chain partners.
- **Very Attacked People™:** Some employees could be more frequent targets of email phishing campaigns or more advanced threats. You may need to monitor their activity more closely for signs of account compromise.

BRIGHT IDEA

See Something, Say Something: Tips to Help Raise Employee Awareness and Reduce Insider Threat Risk

Data doesn't lose itself. People lose it. That's why you need a people-centric approach to managing insider threats and preventing data loss. So, it makes sense that proactive and engaging employee awareness training and education should be an integral component of your insider threat management and data loss prevention program. Here are some helpful tips to get you started with an awareness program for your organization:

- **Gamification:** In much the same way that IT has successfully raised awareness of email phishing threats with regular, interactive employee phishing simulations, make your insider threat management program fun and engaging for your employees.
- **Use different channels:** Email blasts aren't much of a blast. Consider other channels to get your message out, including short videos, intranet postings, text messages and others.
- **Remember the three pillars of insider security (consistency, visibility and transparency):** Incorporate these principles in your awareness program to help your employees recognize and report insider threats without feeling like a "snitch."

Cross-Channel Visibility and Context

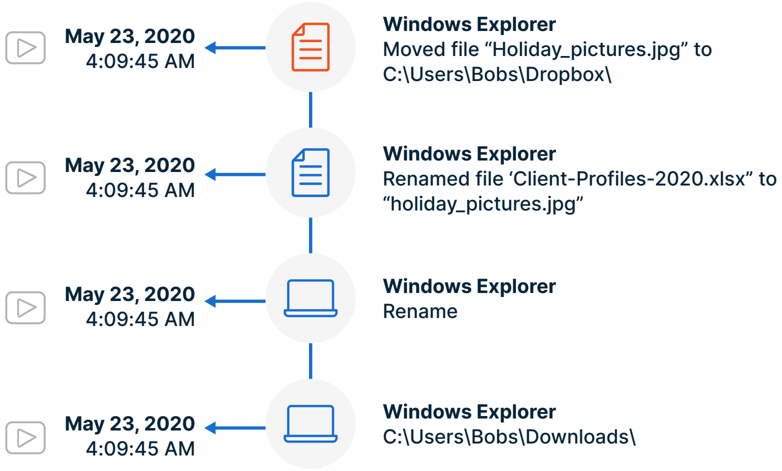
Insider threat management platforms aggregate data on user activity and how they interact with key files, infrastructure, and resources. Full endpoint visibility is critical to getting an accurate picture of user risk. But you need more than just visibility. Context is critical to understanding the risks around user activity, the data they interact with, and the threats they face. For a unified view of all their digital activity in the workplace, you also need know how users interact with:

- Physical and virtual resources
- Cloud applications
- File-sharing services
- Social media
- Email

Activity Timelines

The final critical element to people-centric user risk analysis is visualizing users' activity data. This analysis should include activity for multiple applications across multiple environments over time. Think of the mass of data created from a single user session. Now multiply that for every user and every session in your environment. Leveraging a visual element is key to making sense of it all.

It's easy to understand why a timeline (such as the one shown in **Figure 5**) would be valuable during an incident investigation.



May 23, 2020
4:09:45 AM

Windows Explorer
Moved file "Holiday_pictures.jpg" to
C:\Users\Bobs\Dropbox\

May 23, 2020
4:09:45 AM

Windows Explorer
Renamed file 'Client-Profiles-2020.xlsx" to
"holiday_pictures.jpg"

May 23, 2020
4:09:45 AM

Windows Explorer
Rename

May 23, 2020
4:09:45 AM

Windows Explorer
C:\Users\Bobs\Downloads\

Figure 5: An example of an activity timeline visualization

But it can also be useful for preventative activities, such as alerting. You can use timelines of user-activity data to trigger scenario-based alerts or anomaly detection algorithms. And a visual depiction of the data can help threat analysts more easily and efficiently interpret the context behind an alert.

You need context to understand and respond to insider risk. Having full visibility into each user's activity with data and technology resources, visualized on a timeline, provides insight you just can't get from reading activity logs. Together, user risk profiling, cross-channel visualization, and activity timelines can help security teams analyze insider risks in much more advanced and effective ways. They are what make a people-centric approach so powerful.

Threat Detection and Analytics

A people-centric approach to insider threat management organizes data created by user activity and augments it with key context. Every ITMP should start by analyzing the primary risks to the organization.

Regardless of the unique risks that apply to your organization, every threat-detection regime should include the following few key elements:

- **Policy-based rules:** A central feature of insider threat management platforms consists of automated actions triggered by defined scenarios. Policy-based rules define what scenarios should trigger an automated action and what that action should be. Insider threat management platforms enable security teams to define policy-based rules that include logic and data attributes around user actions, data context, threat context and user profile.

- **Threat scenarios:** When using a policy-based rules engine, you can build generalized libraries of predefined threat scenarios. Security teams can draw on these to quickly deploy a baseline ITMP.

- **Anomaly detection:** Organizations collect massive amounts of data from firewalls, network gateways, and endpoints and are now applying artificial intelligence (AI) and machine learning (ML) to this data to proactively identify potential threats. The people-centric data paradigm organizes user data in a correlated fashion. This approach helps detect behavioral anomalies more efficiently, whether you use AI/ML algorithms or custom policy-based rules that trigger insider threat alerts.

- **Threat hunting:** Teams using a people-centric insider threat management solution can also apply powerful search, filtering, and data visualization tools to proactively search for insider threats. Threat hunting is a common and successful cybersecurity strategy. Analysts search through network data to identify threats that are otherwise evading security measures. You can apply the same process to data on user activities.

Privacy and Compliance

Privacy is critical in every organization, but security and control can be at odds with privacy—especially when it comes to insider threat management. Every organization has a unique privacy culture and is subject to specific compliance requirements. Insider threat management platforms must be flexible enough for your organization to deploy in line with its distinct privacy and regulatory mandates and culture. Here are several key features that support an organization's unique needs:

- **Exclusion:** Forbid employees from using company-issued devices for personal activities, including online banking, shopping, insurance, and personal email is tricky. To accommodate this reality, define activities that are excluded from monitoring to help prevent alert fatigue.
- **Anonymization:** Another key privacy utility is anonymizing users in the monitoring process. With anonymization, analysts can see

the full detail of a user activity, even if that person is on a watchlist, but all the user's PII is shielded.

- **Role-based and attribute-based controls (RBAC/ABAC):** RBAC and ABAC are critical in efficiently deploying insider threat management privacy policies and workflows that support user privacy. By using human resources systems or Lightweight Directory Access Protocol (LDAP)/Active Directory integrations, you can apply policies using standardized RBAC/ABAC rules. This integration ensures that your policies are consistent in real time.

- **Supporting audit compliance:** Countless data breaches have exposed personal information, and many of these were enabled by insiders, whether directly or through compromised accounts. As a result, governments have issued laws, mandates, and guidance for safeguarding this data. Many require organizations to maintain an audit capability of key employees and business processes that interact with sensitive data. Insider threat management platforms can provide the visibility into user activity and data interaction to support such mandates. They can also help proactively detect potential violations to support compliance efforts.

- **Staying consistent with privacy compliance:** Insider threat management platforms can collect significant amounts of personal information on the users being monitored. This information is subject to any data privacy regulations that apply to the region in which the data is captured, stored, or analyzed. Insider threat management platforms must be flexible enough to stay consistent with new and changing laws.

Key Capabilities

Insider threat management platforms, like all modern cybersecurity tools, should be built with modern software architectures to support enterprise-class deployment. They also need to include advanced features critical for successful deployment.

Here are some key capabilities to look for in an insider threat management platform:

- **SaaS Deployment:** The ability to deploy a pure software-as-a-service (SaaS) offering built on a modern, cloud-native architecture provides the flexibility and scalability organizations require.
- **Extensibility:** By its nature, insider threat management must integrate with a broad range of other systems, including human resources, security information and event management (SIEM), security orchestration, automation, and response (SOAR), data stores, and IT service management platforms.
- **Scalability:** Insider threat management platforms should efficiently support small organizations, subsets of larger ones, and full enterprise deployments under a single instance.
- **Agent performance:** Insider threat management platforms rely on lightweight endpoint agents for the collection of data. Agents must capture all required data reliably and they must run locally on each device without impeding performance or causing system crashes.
- **Analytics:** Insider threat management platforms must analyze massive amounts of data to provide actionable insights. To realize the full value of advanced analytics, your solution should use a powerful backend technology, such as ElasticSearch.
- **Unified:** Insider threat management is a key component of the broader security mandate of protecting people and information. It is critical to have a comprehensive view of users' digital activity in the workplace across different channels.

Check Yourself: Implementing an Insider Threat Management Platform

In the previous two chapters, you learned how to recognize insider threats and how to set up your ITMP. In this chapter, you learned how to implement an ITMP. Test your knowledge of effective implementation tips.

1. Why is user risk profiling an important part of an effective implementation of an ITMP?

Every user has a unique risk profile, which can be influenced by a number of factors. Effectively assigning users with a risk profile enables more efficient and accurate threat analysis because the security team can focus their attention on the high-risk users.

2. What are the four elements that every threat-detection regime should include?

Though every organization has its own unique risks, the four elements that every organization should have in their threat-detection regime includes:

- Policy-based rules
- Threat scenarios
- Anomaly detection
- Threat hunting

3. How can organizations navigate privacy and compliance with an ITMP?

Though security and control can be at odds with privacy, it doesn't mean privacy and security can't coexist. Insider threat management platforms must be flexible enough for your organization to deploy in line with its distinct privacy and regulatory mandates and culture. A key privacy utility is anonymizing users in the monitoring process. This ensures that analysts can see the full detail of a user activity, but all the user's PII is shielded.

Wrapping Up

In this Innovations Express Guide, we've shared how the changing nature of work has shaped the insider threat landscape, requiring a people-centric approach to insider threat management in order to prevent data loss and reduce organizational risk. You've learned how to get started on the journey of insider threat management by building an initial operating capability for your insider threat management program and scaling it up to full operating capability. And, you've learned about the most important elements to look for in an insider threat management platform, including key features and capabilities.

THE 101

Insider Threat Management Checklist

Protecting your organization from insider threats requires the right balance of people, processes, and technology. Use the following checklist to help you strike that balance.

□ **Are your users undertaking risky actions such as data exfiltration, privilege abuse, or application misuse?** Do you have visibility to:

- Address remote work risks for employees and contractors. Identify and protect sensitive customer data or intellectual property.
- Manage data risk associated with leavers and joiners.
- Support mergers and acquisitions.

□ **Are you able to detect negligent behavior, compromised users and malicious insiders?** Can you:

- Track and monitor risky user activity across all technology channels, including network, email, endpoint, removable media, and web and cloud applications?
- Track and monitor sensitive data and file interaction by users to identify insider threats?
- Track and monitor contractors, suppliers, and other third-party vendors using your systems?
- Have a regular process to identify your organization's critical and sensitive assets?

□ **Are you able to prevent data loss across many common threat vectors?** Does your current set up provide:

- Visibility into user behavior, threat insights, and data movement?
- Policies and controls in place to protect sensitive data and critical intellectual property from exfiltration?
- Context to discern malicious, compromised, and negligent users?

□ **When an insider incident occurs, are you able to rapidly investigate and respond to mitigate the risk?**

- Do you incorporate insider threat awareness into your security training for all employees?
- How often are you able to identify the user in user-driven incidents?
- How quickly are you able to resolve user-driven investigations?

□ **Insider threat management is a team sport.** Do you have the following in place:

- Appropriate representation from different departments and teams across the organization?
- Clearly defined roles and responsibilities for your ITMP?

- Team members with the necessary skills, training and access?

□ **Are the right governance and metrics in place?** Do you have:

- An insider threat management program already in place?
- Track and report on all three types of insider threats (negligent, compromised, and malicious)?
- Defined metrics for the insider threat management program?

□ **Are you able to balance user privacy, compliance and organization security?**

- Does your insider threat management program meet your legal authorities' concerns, your privacy culture, and civil rights in your jurisdiction?
- Do you have mechanisms to "watch the watchers"?

Take the Proofpoint Insider Risk Assessment today at https://www.proofpoint.com/us/learn-more/insider-threat-risk-assessment to assess your organization's insider threat readiness, see how you benchmark against your peers and walk away with an in-depth plan to improve your insider threat management maturity.

ABOUT PROOFPOINT

proofpoint®

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

ABOUT ACTUALTECH MEDIA

ActualTech
MEDIA

ActualTech Media is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.

If you're an IT marketer and you'd like your own custom Gorilla Guide® or Innovations Learning Series title for your company, please visit https://www.gorilla.guide/custom-solutions/