proofpoint. | observe IT
a division of Proofpoint

STEP 2:

A Guide to Setting Up Your Insider Threat Management Programme

proofpoint.com

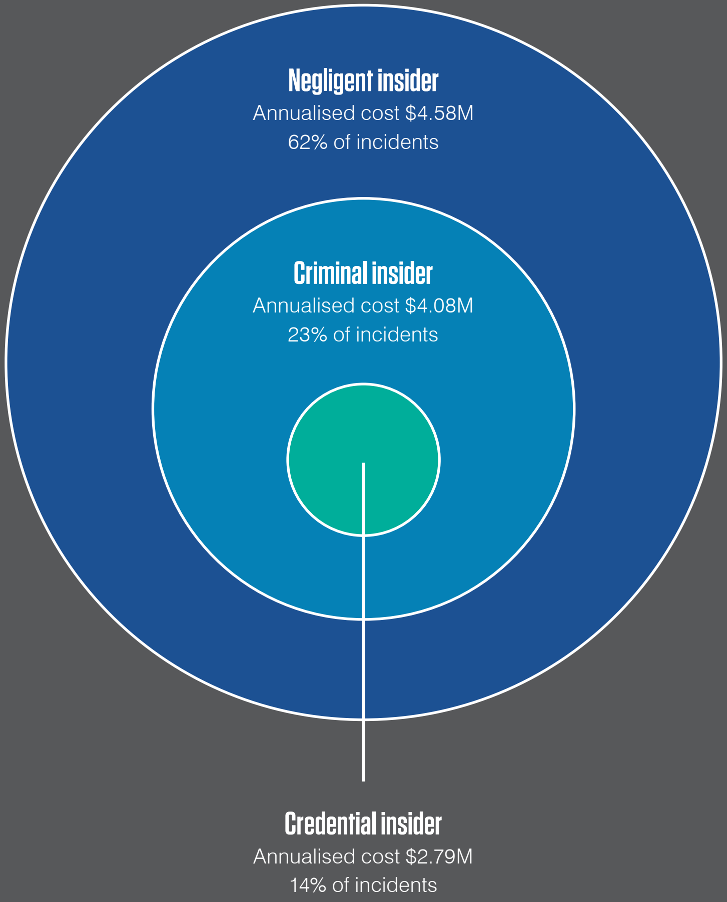


Figure 1: Cost of insider threats

WHAT ARE INSIDER THREATS?

Insider threats are one of the fastest growing categories of risk across organisations today. According to Ponemon Institute's 2020 Cost of Insider Threats: Global Report, the average cost of insider threats increased by 31% in two years to hit $11.45 million. Moreover, the frequency of insider-caused incidents jumped by 47% across the same timeframe.

But not all insider threats are created equal. They can range from negligence to credential theft to malicious activity. And each type of threat comes with a different price tag and consequences. (Figure 1 breaks down the three main types of insider threats.)

Companies have long been aware of the insider threat problem. But few are dedicating the resources or executive attention they need to actually reduce their risk. Others may be ready to make that commitment but just don't know where to start. Wherever you are in this journey, we're here to help.

This e-book explains:

- What it takes to set up an insider threat management programme (ITMP)
- How to measure success
- Best practices for scaling from an initial operating capability to a full and robust ITMP

[1] Ponemon 2020 Global Cost of Insider Threats Global Report

SECTION 1

Getting Started with an Insider Threat Management Programme

Think of insider threat management as a holistic focus on managing the risks that insiders pose to your corporate assets.

It starts with a strong foundation: a unified mission that breaks down the traditional silos between "security" (personnel-focused) and "InfoSec" (network-focused IT). Successful ITMPs are truly cross-functional. This effort should involve not just your security and IT departments but also legal, HR, line of business leaders, executives, and more.

A successful ITMP requires all of these departments to work together toward common goal of decreasing organisational risk. It means having the ability to communicate clearly across technical and non-technical teams. It requires visibility into what insiders are doing with corporate resources. And it calls for a clear strategy to prevent and mitigate insider threats. ITMPs must include people, process, and technology—all working in close harmony.

Guiding principles:

Here are some guiding principles.

Designate an executive champion

Solidify support for your ITMP by designating a champion. The champion should help ensure that the organisation puts a priority on developing and operating the programme—and the resources needed to do both.

Identify a steering committee

Representation should extend beyond the traditional cybersecurity group. Be sure to include human resources, physical security and legal counsel (to address any ethical or privacy issues).

Build cross-functional working groups

Your larger working group (not just the steering committee) should include active legal counsel and privacy officers. This step helps ensure you have the right level of legal review and guidance 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 that the programme provides sufficient personal privacy and whistleblower protections. You can achieve this by anonymising user data and taking other precautions.

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. Some organisations have all of this in-house. But most can benefit from outside consultants with expertise forensics, legal issues, risk assessment, privacy, compliance, and other areas.

SECTION 2

Developing an Initial Operating Capability

Insider threats are a complex problem, and a full operating capability may take years to develop. But you can get immediate value by developing an initial operating capability (IOC), legally supported with documented policies and procedures, as illustrated in Figure 2.

An IOC is the minimum baseline capability. It includes governance, background checks, training, user activity monitoring, data management and investigation. Most organisations have the resources to manage these activities.

Guiding principles:

An effective IOC includes three broad categories of activities. Programmatic tasks are essential to running a programme. At the same time, some organisations should also consider added layers of threat management to address issues that arise from a dispersed structure. Finally, regular review can help improve the programme over time.

Programmatic tasks

- Establish the programme and direct functional managers to provide support.
- Describe the purpose of the programme—detecting, preventing, mitigating and responding to insider threats—in the context of the organisation's goals.
- Define and communicate which categories of workers are subject to the insider threat programme (such as employees, consultants, contractors and so on).
- Establish a programme office. You may want to include a centralised analysis and response "hub."
- Ensure that programme personnel have authorised access to insider threat-related information and data from across the organisation.
- Again, ensure legal, privacy, civil rights, civil liberties, and whistleblower protections issues are addressed.
- Mandate insider threat and general security awareness training.
- Define requirements to conduct independent assessments of whether the programme complies with guidelines and policies.

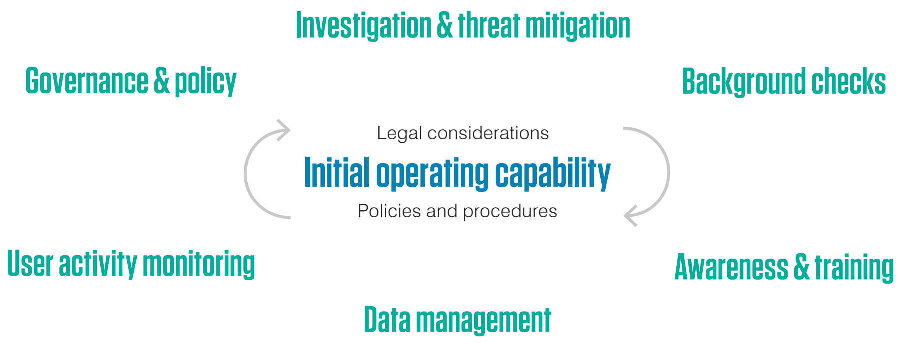


Figure 2: Insider threat management – initial operating capability

Added layers for dispersed organisations

Organisations that are hierarchical or regionally dispersed are at greater risk of having gaps in coverage. Geographically dispersed entities may need to draft the following layers to mitigate gaps:

- Policy
- Standard operating procedures
- Designated points of contact
- Established dedicated communication channels

Remote work, which is growing more common, and may require updates or changes to your ITMP. (We discuss these in detail in the first part of this e-book series.)

Regular review

Insider threat policies should be reviewed regularly. Incorporate lessons learned, ensure that the guidance is still effective and adapt to any changes to laws, policies, organisational structures or IT architecture.

SECTION 3

Develop an Insider Threat Management Framework to Drive Success

Organisations should complete an ITMP implementation plan as a mechanism to establish the programme and allocate resources. Every year after the plan is approved, have the programme's senior manager submit an annual report to the executive team. The report should document:

- What the programme accomplished that year
- What resources were allocated to it
- Insider threat risks it identified
- Recommendations and goals for improving the programme
- Major challenges.

Guiding principles for an ITM framework:

An effective ITM framework includes foundational tasks and a mindset of continuous refinement and improvement.

Programmatic tasks programme planning

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

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

Living documentation

Most organisations treat their implementation plans as living documents—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 ITM programme. But don't delay approval of the implementation plan for the sake of completeness. Treat it as a work in progress.

Annual report formal

You can deliver your annual report as a lengthy document, two-page summaries or PowerPoint briefing. The format depends on your organisation's unique culture.

Self-assessments

A key tool for programmes is a self-assessment regime. This is typically conducted before an implementation checkpoint, publication of the annual report, or independent oversight review/assessment.

SECTION 4

Balance Legal Considerations and Company Culture with Policy Needs

Legal issues inevitably arise when attempting to implement an insider threat management programme or solution. The nature of an ITMP is that it 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, your corporate culture and promises made to people who work for the organisation.

Legal issues can be tricky to navigate when building an ITMP. 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 rules 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 fears about potential legal hurdles.

Here are the most common issues that organisations encounter when building an IMTP:

- **Consent.** Do you have consent to monitor your employees? Do you need it?
- **Scope.** Whom will you monitor? Everyone? Only a subset of employees? Where and when will you monitor them?
- **Agreements**. Do you have the necessary employment agreements in place?
- **Policies.** Do you have documented support for the monitoring programme?
- **Compliance.** Do you have a "watch the watchers" programme in place, to ensure those tasked with monitoring do not abuse their privileges?

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

SECTION 5

Effectively Manage Insider Threats: What it Takes

We've outlined some of the programmatic aspects of setting up an ITMP. Now let's talk about the capabilities that your technology and team need to properly defend against these unique and common threats.

The key is building a capability to support a people-centric security model. The focus should be on user activity. It's all about how users are interacting with sensitive corporate data and assets rather than on monitoring a technology or network perimeter—which for most organisations no longer exists.

People-centric security means having complete visibility and context into how insiders are interacting with corporate data and assets. Visibility and context enables organisations to better conduct the three primary aspects of insider threat management.

Detection

This is the ability to detect, in as close to real-time as possible, when a user takes a risky action—even if it doesn't reach the level of a full-blown "incident." Your detection efforts must strike the right balance between timely, actionable alerts and the risk of alert fatigue. Your programme must be able to fine-tune alert signals using a mix of real-world insider threat risk indicators and organisation-specific unique alert dynamics.

Response

This is the ability to investigate and respond to real incidents in a streamlined and organised fashion. The longer an insider threat incident persists, the more damage it can do—to your reputation and bottom line. So it's important to be able to respond quickly and appropriately. Also, key is the ability to work cross-functionally across teams ranging from security and IT to legal, HR, c-suite and more.

Prevention

This is the ability to stop a user from accidentally or intentionally violating security policy using user education, real-time reminders, and blocking when necessary. You've heard the phrase "an ounce of prevention is worth a pound of cure." This is never truer than with insider threats.

To effectively manage insider threats, organisations must become adept at preventing, detecting and responding to insider threats. Those that can do all three in a coordinated and streamlined fashion stand the best chance of decreasing their risk.

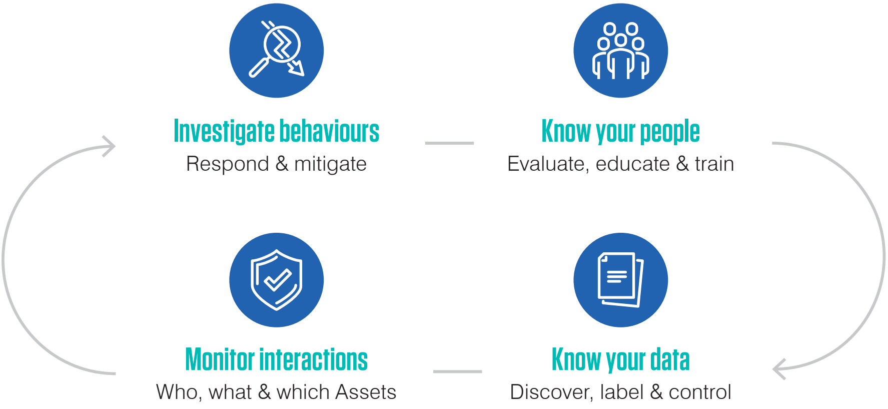
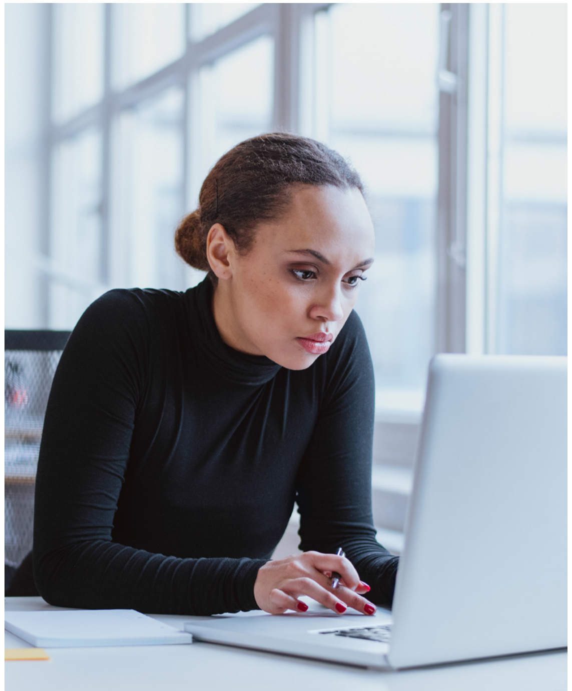


Figure 4: How to effectively manage insider threats

SECTION 6

Implement an Insider Threat Management Platform



Insider threat technical solutions come in many varieties. Some are network security tools re-branded as "insider threat tools." Others are simply aggregators of network log data. In the next e-book in this series, we cover insider threat management and cybersecurity tools in detail. We explain the limitations of traditional tools when it comes to defending the "people perimeter."

No technical solution on the market meets all of the important insider threat management aspects described in section 5. All leave gaps that must be filled by other solutions—or worse, simply go unmitigated, increasing business risks.

One of the best options to address insider threats is a purpose-built insider threat management platform. These tools are designed to look "inward"—not outward as many security tools on the market today. Insider threat management tools can complement one or more of the legacy tools described in the next e-book. In some cases, a dedicated ITM platform can support a standalone approach to detecting and mitigating insider threats.

The Proofpoint ObserveIT Insider Threat Management Platform offers comprehensive user and data visibility, rich analytics, proactive detection, and rapid response.

ObserveIT allows the organisation to gain comprehensive visibility and context by monitoring the actions and behaviours of users. Monitoring includes actions that signal a potential behavioural or workflow issue, such as keyword usage or files accessed. Someone using a co-worker's login credentials is one example. Visiting suspicious websites could be another.

In the fourth of this e-book series, we explain in greater detail the role and value of a dedicated ITM Platform such as Proofpoint ObserveIT.

SECTION 7

Measure Return on Investment to Define Success

Many businesses view security as a cost center. They may understand the importance of certain security investments, but they rarely expect to see a return on that investment. But 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 people, processes, and technology. But as the Ponemon 2020 Cost of Insider Threats Report illustrates, prevention and rapid detection and response will save real money in the long run. Let's look at this in more detail.

To show ROI of Insider Threat Management Programmes, organisations should measure and track three primary areas:

Insider threat incidents

To demonstrate ROI, measure how incident numbers change over time using insider threat metrics. Determine which prevention and mitigation tactics work best for your organisation 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 catching them earlier). A purpose-built insider threat management platform such as Proofpoint ObserveIT makes it easier to track these numbers while helping the organisation decrease insider threat-related costs over time.

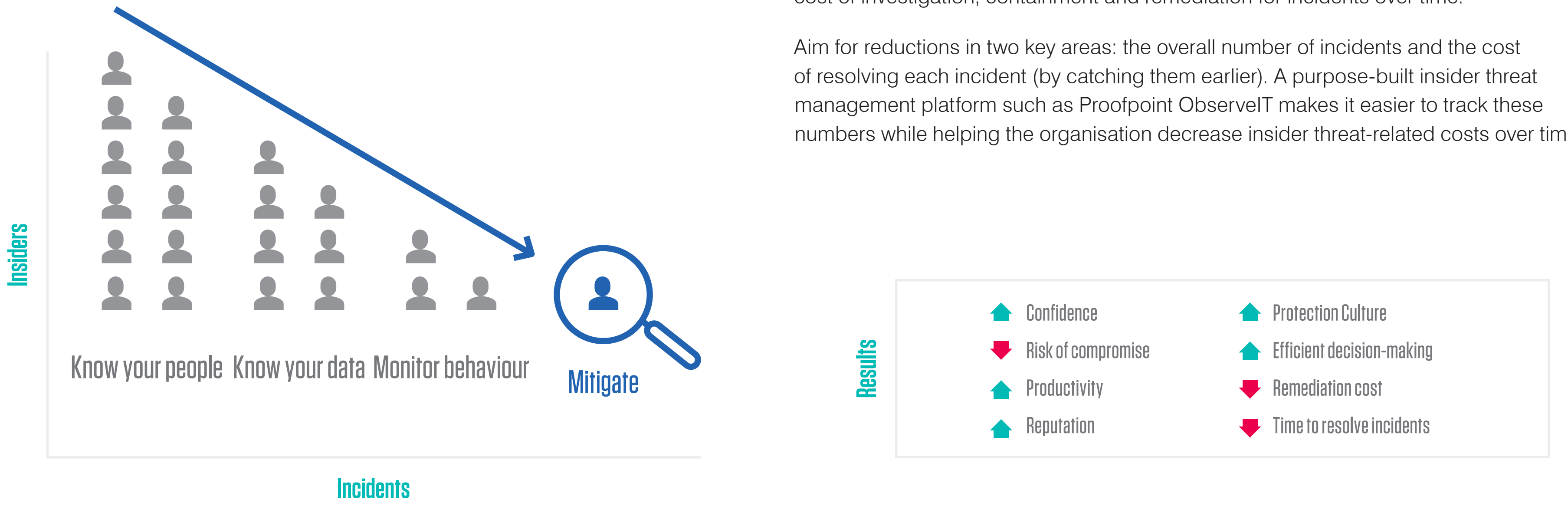


Figure 5: Insider threat management programme – ROI

Customer acquisition and retention

A strong security posture, bolstered by an ITMP, may also drive revenue by demonstrating secure and compliant practices. These practices not only help maintain the current customer base but also win new deals.

As discussed throughout this series, your insider threat programme should meet security and compliance frameworks such as GDPR, SOC 2, and other industry-specific regulations. To prove ROI, track the number and amount 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 vs. proactive spend

Most insider threats result from 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 will have a dramatic impact on ROI.

A valuable way to measure and demonstrate the ROI of your insider threat programme is to track costs over time in the areas of reactive vs. proactive efforts. Here are some examples:

Proactive costs

- Monitoring and surveillance
- User education and training
- Security awareness programmes
- Personnel
- Real-time policy reminders

Reactive costs

- Investigation
- Escalation
- Incident response
- Remediation
- Ex-post analysis

Generally, proactive insider threat efforts cost far less than reactive ones. Demonstrating that you are spending your money on proactive efforts to reduce or avoid surprise reactive costs down the road can also help make the ROI case. On the reactive side, demonstrating that you are decreasing the amount of time it takes to investigate and remediate incidents will help prove that you are reducing costs on that end of the equation, too.

Well-designed ITMPs decrease the number and cost of incidents, increase sales, and shift the balance from costly reactive measures to cost-effective proactive efforts. These programmes should be viewed as an investment with significant return potential—if they are managed properly. For many organisations, an ITMP can produce the biggest security ROI.

SECTION 8

Scale Up Your ITMP to Full Operating Capability

We've already covered the importance and value of getting started as soon as possible by developing an initial operating capacity for managing insider threats. But most organisations do need to scale up over time and reach full operating capacity (FOC) to truly manage insider threat risk.

Naturally, FOC will require more resources to implement the remaining ecosystem components. FOC includes all the initial operating capability components, plus personnel assurance, access control, analysis, dynamic risk assessment, and oversight.

Personnel assurance

Most organisations 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 behaviour can often be enhanced through more formal collaboration between HR and security.

Access control

Access control processes and tools are effective. But implementing some policies can create unnecessary vulnerabilities. A common example is granting all users local administrative rights, by default, on organisation-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 organisations deploy analytic resources to hunt for threats on the network and analyse log files with SIEM solutions. But these efforts often suffer from a lack of datasets to analyse. Fully deploying user and data activity monitoring will foster greater analytic maturity. They'll also promote a more proactive insider threat strategy and help track the metrics outlines in section 7.

Dynamic risk assessment

Most organisations' insider threat assessment capabilities are limited to specific and narrowly defined use cases. They might be better described as ad hoc and reactionary. A true insider threat capability requires a thorough understanding of each of the following:

- The organisation's critical asset threat factors
- The organisation's insider population
- The existing vulnerabilities of certain types of data and systems

(We cover these in detail in the next e-book in this series.) Once implemented, a mature insider threat assessment capability will enhance security awareness. And it will support both reactive and proactive strategies, along with greater enterprise threat management overall.

Oversight

Oversight of insider threat management functions and activities are typically shared between the CSO, CISO, CPO and legal. A lack of a defined ITMP creates an activity- or issue-centric oversight model that is inefficient and lacks a strong sense of ownership. That's why organisations need a clearly defined ITMP with established roles and responsibilities. Clearly defined oversight fosters operational enablement and creates a more effective oversight and compliance framework.

CONCLUSION AND NEXT STEPS

How Proofpoint Can Help

As the leading purpose-built solution on the market, the Proofpoint ObserveIT Insider Threat Management Platform protects against data loss, malicious acts, and brand damage from insiders acting maliciously, negligently, or unknowingly.

ObserveIT correlates user activity and data movement. By connecting these dots, we empower security teams to quickly identify user risk, detect risky activity in near real time, and respond to insider-led data breaches. Most organisations lack internal insider threat expertise and would benefit from objective third-party insider threat management professional services. These services can provide the visibility and justification needed to develop, implement, and sustain an effective strategic insider threat programme as described in this e-book.

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

[2] 2020 Ponemon Institute Cost of Insider Threats.

LEARN MORE

For more information visit proofpoint.com.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organisations' 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 organisations 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.

LEGAL DISLAIMER

This document does not represent legal interpretaion on corporate regulation and policy. Whilst efforts have been made to ensure maximum accuracy, this document does not substitute for the regulation. Only the regulation and its official interpretation can provide complete and definitive information regarding requirements. This document does not bind ObserveIT, a division of Proofpoint, and does not create any rights, benefits or defenses, substantive or procedural, that are enforceable by any party in any manner.

proofpoint.