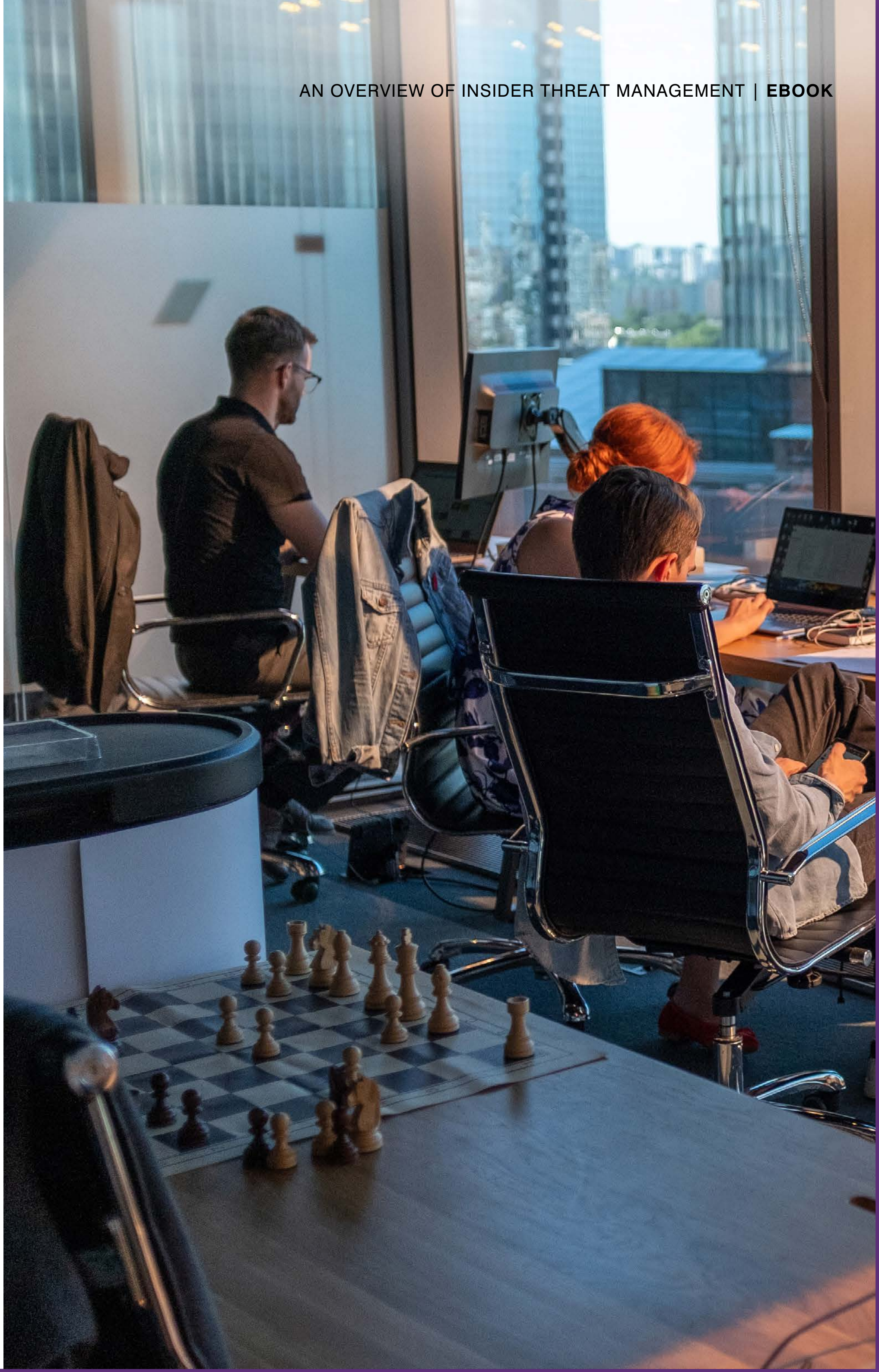
proofpoint. | observe IT
a division of Proofpoint

AN OVERVIEW OF INSIDER THREAT MANAGEMENT | **EBOOK**



STEP 1:

An Overview of Insider Threat Management

proofpoint.com

The number of insider-caused cybersecurity incidents has increased by a whopping 47% since 2018, according to Ponemon.

WHAT ARE INSIDER THREATS?

Insider threats are on the rise. According to the 2020 Ponemon Cost of Insider Threats Global Report which uncovered a **47% increase in insider-caused cybersecurity incidents since 2018**. These incidents are costly, both in terms of reputation and finances—the **average annual cost for insider threats is now $11.45 million**, also according to Ponemon.

So, what is an insider threat? An insider threat occurs when someone with authorized access to critical information or systems misuses that access—either purposefully or accidentally—resulting in data loss, legal liability, financial consequences, reputational damage, and more.

Even though insider threat incidents are becoming increasingly prevalent, and valuable information and intellectual property are at stake, many organizations don't understand the causes of these threats, or how to detect and prevent them.

The first eBook in this series is intended to provide an introduction to insider threats, and why organizations need to take a people-centric approach to insider threat management (ITM) to protect their valuable information and intellectual property from the risk of insider threats.

KEY FINDINGS

In 2020 the average annual cost of an insider threats was

$11.45 million

77 DAYS

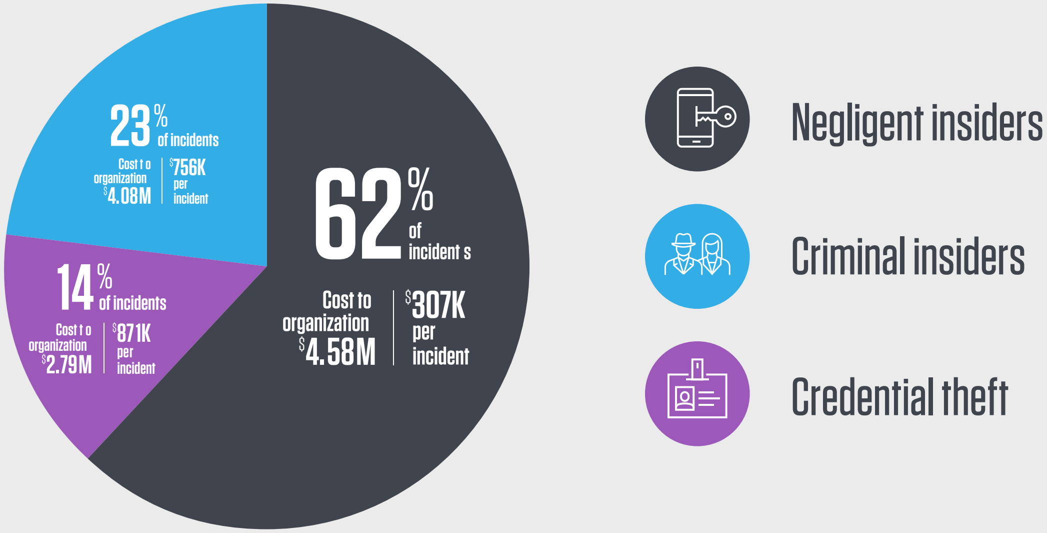
average time it takes to contain an insider incident

Since 2018 the cost of insider threats rose by

31%

Since 2018 insider-caused cybersecurity events have increased by

47%



Source: 2020 Ponemon Cost of Insider Threat report

SECTION 1

The Nature of Work is Changing

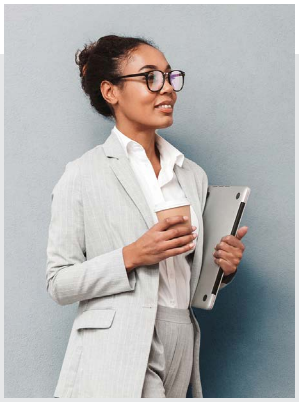
As companies embrace a more remote workforce and a digital-first work environment, the notion of a traditional network perimeter is a relic of a bygone era.

This change in workforce dynamics has created a unique set of cybersecurity challenges. Every organization faces pressure to maintain productivity and business continuity while complying with data-protection regulations and protecting from insider threats.

Who is an insider these days?

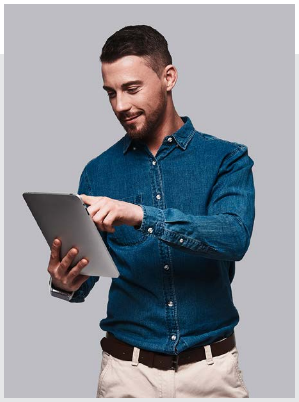
As businesses have become more digital and globally interconnected, the definition of an insider has expanded. Insiders can be:

Employees

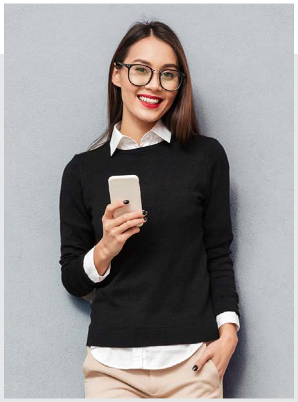


Independent contractors and consultants

Third-party contractors



Supply chain partners



Service providers

Not all insiders are created equal. Some pose more risk to the organization than others. This is why 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, contractors whose contracts are expiring, and anyone with a high level of privileged access may constitute a high-risk insider for your business. We'll discuss this in more depth below.

The impact of insider threats

According to the Ponemon report, the average annual cost of insider threats rose by 31% in two years to $11.45 million. The frequency of incidents spiked by 47% in the same time period.

According to the same study, insider threats typically have three main profiles:

Negligent insiders

Employees or contractors who make mistakes that unintentionally cause incidents.

Criminal and malicious insiders

those who intentionally cause damage to an organization from the inside.

Credential thieves

those who target insiders' login information to gain unauthorized access to applications and systems.

Of the three profiles, credential thieves caused the most damage per incident, costing organizations an average of $871,000 per incident. That's three times more per incident than a negligent insider. But, the frequency of credential theft was 14% of all incidents, which limited the average annual cost to $2.79 million per year.

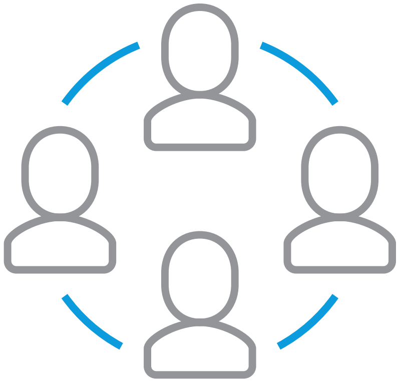
In contrast, negligent insiders accounted for 62% of all incidents, costing organizations the most in total per year: an average $4.58 million. And while criminal insiders dominate the headlines, their frequency was only 23% of all incidents. Still, at an average annual per-incident cost of $756,000, this group should not be ignored. Criminal insider incidents account for a total of $4.08 million in average losses per year.

Not just an IT problem anymore

In the past, cybersecurity was primarily an IT concern. Today, chief information security officers (CISOs) are called into boardrooms regularly. They are tasked with protecting information, data, and intellectual property. And, when a leak happens, they are responsible for uncovering and addressing the problem—which has often caused major financial and reputational damage. In short, CISOs have evolved from a technical role into having a frontline impact on the health, growth, and reputation of their organization.

SECTION 2

Understanding Your People Perimeter



Once a mainstay of cybersecurity, network perimeter strategies alone no longer work. Over the last five years, several forces have driven work outside of traditional perimeters, including:

- Growing reliance on independent contractors
- The rise of SaaS apps and products
- Cloud-based file sharing
- Workforce mobility

In short, people—not workplaces—are the new perimeter. This is why, to create a strong ITM program, companies must develop a strong understanding of how their people interact with data.

Know your people

The first step is to get a sense of your workforce. This goes beyond headcounts and payroll—it encompasses understanding who is in your organization and ranking their risk-levels.

Some people are at higher risk than others due to public visibility, such as c-level executives. Others may be high-risk because their role gives them carte blanche access to company systems.

Another category to define are Very Attacked People™ (VAPs). These users are high-value targets that cyber attackers approach over and over again, hoping to find a way into the organization. These targets will 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 ask:

- Which data is sensitive?
- Where does that data live?
- Who has access to it?
- Who should have access?

Next, assess the tools that employees are using to interact with this data and get their work done. What endpoints do you need to watch? Some of these tools may be physical, while others may be virtual. All of them can be seen as valves from which data could leak—and your insider threat management program (ITMP) should seek to close the valve as much as possible and monitor what cannot be shut off.

SECTION 3

Preventing Data Loss

Top vectors for data exfiltration

Data exfiltration can occur through many common threat vectors, either accidentally or maliciously. The most common channels through which data loss occurs are:

Removable media

Removable media is a common way for data to leave an organization. With removable media such as USB keys, sophisticated technical users can intentionally introduce malware onto company machines or equally business users can leave with important files.

Hard copies

While it may not seem as common as it used to be before laptops and smartphones, physical data can still be a major cause of data leaks. For organizations that frequently print and keep hard copies of critical sensitive documents, keeping track can be a major challenge.

Cloud storage

Team usage of cloud storage services is on the rise. These services are often used by both employees and outside contractors with minimal IT or security team oversight, making it difficult to secure their usage.

Personal email

Personal email accounts are often accessed by insiders to intentionally bypass corporate systems.

Mobile devices

Mobile devices can give workers a major productivity boost. They also pose a threat to organizations' data because of their multi-purpose use as recording devices, cameras, and storage devices.

Cloud applications

Cloud applications often contain sensitive documents and information. These apps can present risks even when organizations approve them. But many companies also have "shadow IT," which is created when users try to find ways around policies with unapproved apps and services.

Social media

Unauthorized use of social media is a big concern for security teams. It's easy for an employee to post leaks of sensitive corporate information on sites such as Facebook, Twitter, and LinkedIn, whether intentionally or unintentionally.

Developer tools

Technical users often access web-based hosting sites for version control of code. These sites make it easier for developers to collaborate but can also cause IP and proprietary source code leaks.

Screen clipping & screen sharing

Unauthorized screen clipping and screen sharing services can easily be used to exfiltrate data. Regularly accessing these sites—or other unauthorized software—could be an indicator of a potential insider threat.

FTP sharing sites

Many organizations prohibit the use of File Transfer Protocol (FTP) sharing sites. But because they're so easy to use, they're common causes of data leakage.

SECTION 4

Common Business Use Cases

Certain business scenarios make organizations more vulnerable to insider threats. Oftentimes, these scenarios can result in higher risks of data loss from insiders.

Use case: mergers & acquisitions (M&A)

Managing data risks during the M&A process is a major challenge. Cybersecurity is important during due diligence. Leaks of sensitive information could hurt the deal. For example, risk and compliance teams need to know who has interacted with sensitive documents, so that both parties can be aware of the risks before the deal is closed.

After a merger or acquisition is completed, new employees may have varying degrees of security awareness and hygiene. Combining differing—and often conflicting—security policies across organizations is challenging. Perhaps even more difficult is controlling access privileges of administrators. Complex personnel issues may result directly from the M&A. For example, if employees depart voluntarily or are laid off, they may attempt to take sensitive information with them to new jobs. Disgruntled employees out for revenge may attempt to defraud the organization or its customers.

The solutions

- Detect data leakage from corporate locations (e.g., private deal terms, IP, undisclosed security events or other files from CRM, ERP, HR systems or code.)
- Alert on privileged users accessing sensitive systems as root, using shared credentials or installing suspicious tools.
- Monitor and collaborate closely with HR on potentially high-risk user populations.

Use case: shadow IT

While many organizations have official, company-sanctioned IT tools and infrastructure, people don't always follow the rules. Whether they're trying to get around a cumbersome process, looking for a shortcut, or avoiding tech that just doesn't work, employees and other insiders often turn to "shadow IT" infrastructure and apps.

According to the 2019 Verizon Data Breach Investigations Report, one of the top forms of misuse from approved users was unapproved workarounds—in other words, people cause breaches by trying to circumvent protocols.

The most common risk is data loss through cloud storage, web apps or SaaS apps. Often user access and privileges are too loosely controlled by the IT team, leading to the potential for sensitive data and documents to be accessed by those outside the organization.

The solution

- 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—people often circumvent technology in a misguided attempt to solve real IT obstacles.

Use case: virtual apps and desktops

Virtual desktop infrastructure (VDI) systems and applications are often used by third-party IT consultancies to access user machines remotely. Misuse of virtual apps and VDIs is a common problem. These otherwise trusted users can sometimes become malicious insiders and abuse their privileges to access sensitive data remotely on employee machines. Ideally, IT teams would manually watch screen recordings in case of mistakes or misuse in VDIs. In reality, this manual effort is impractical, if not impossible.

The solution

- Institute thorough background checks for third-party privileged users.
- Deploy an ITM solution to monitor user activity and detect system misuse within popular VDIs and virtual applications used by IT contractors, such as Citrix Ready and VMWare Horizon.

Use case: departing employees

Often, departing employees are considered high-risk users. In fact, almost 70% of employees exfiltrate data on their way out. Sometimes these users' motivations are completely innocent. More often than not, they're malicious. For example, a departing employee may look to steal trade secrets and bring them to their new employer.

They may use common insider threat vectors, such as removable media, print jobs, personal email, or cloud applications to exfiltrate data. Or, in some cases, organizations do not turn off access to corporate applications and systems even after termination, which leaves an open door for employees to continue to access sensitive data after they've left.

The solution

- Establish formal offboarding processes (with both HR and IT teams), including disabling access to prevent unauthorized access to applications and systems.
- Monitor activity for high-risk users who are leaving the organization.
- Collect context into who did what, when, where and why. This can speed up the investigation process in the event of an insider threat incident.

Use case: remote employees, contractors, and third-party vendors

Every organization is mobile now. Whether it's work-from-home employees, third-party contractors, or executives and sales teams always on the move. As teams collaborate remotely on sensitive assets, the risks of security mistakes and malicious insider behavior are equally heightened. It can be difficult for organizations that have relied on perimeter-based security solutions to retain control, as the boundaries of the traditional office disappear.

Common risky behaviors of remote workers include:

- Downloading files during irregular hours
- Sharing account credentials
- Installing unauthorized software
- Leaving credentials unprotected
- Logging on from unusual endpoints
- Sharing files with unauthorized users

The solution:

- Use an ITM solution that enables third-party monitoring, while staying compliant 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.
- Gain context into potential incidents to understand the user's motivations.

SECTION 5

Industry-Specific Threats & Concerns

INDUSTRY	KEY ISSUES	DID YOU KNOW?
Financial Services	• Fraud and monetary losses • Disclosure of confidential customer and/or account data • Destabilization of critical infrastructure	The financial services industry accrued the highest average insider threat annual costs at $14.5 million.[1]
Telecommunications	• Disruption of critical communications infrastructure • Theft of personally identifiable information • Corporate espionage • Denial of service (DoS) attacks	67% of attacks targeted at the information industry are financially motivated.[2]
Technical Services	• Intellectual property theft • Disruption of IT operations • Customer data leaks • Network and systems disruption	50% of breaches in the technical and professional services industry involved credential loss.[2]
Healthcare	• Theft or misuse of protected health information • Theft of misuse of electronic healthcare records • Insurance and financial fraud	76% of all insider incidents in the healthcare industry were caused by fraud.[3]

INDUSTRY	KEY ISSUES	DID YOU KNOW?
Government	• Theft or abuse of constituent information • Fraud and misuse of public funding • Compromised defense systems • Leaked intelligence	16% of all breaches target public sector organizations.[2]
Retail	• Theft of customer data, including identity theft and financial records • Loss of customer trust • Compromised point of sale systems	The average data breach costs a retail organization $172 per stolen record.[4]
Manufacturing	• Intellectual property theft • Nation-state threats • Loss of valuable data including customer information, product roadmaps and more	Manufacturing experiences more espionage-related breaches (27%) than any industry.[2]
Energy & Utilities	• Lack of security awareness and software maturity • Financial and career pressures • Geographically dispersed workforces	The energy sector has the fourth highest annualized cost of dealing with insider threats in the U.S. at $11.54 million.[2]

[1] 2020 Ponemon Institute Cost of Insider Threats.

[2] 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.

[3] Carnegie Mellon University Insider Threats in Healthcare (part 7 of 9: Industry Threats Across Industry Sectors).

[4] RetailDive 5 Numbers to know about retail cybersecurity.

CONCLUSION AND NEXT STEPS

Protection Starts with People

While insider threats present a financial and reputational risk to organizations, they can be addressed successfully as part of a broader security strategy. The key is to invest in people, processes, and tools that are focused specifically on insider threats and that center people at the heart of the strategy.

As our world has become more complex and technologically dependent, the vectors for security threats have increased. In this context, organizations should fit their ITM into a seamless and integrated security program that focuses on their biggest asset, and potentially biggest risk: people.

LEARN MORE

For more information visit proofpoint.com.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity 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.

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.