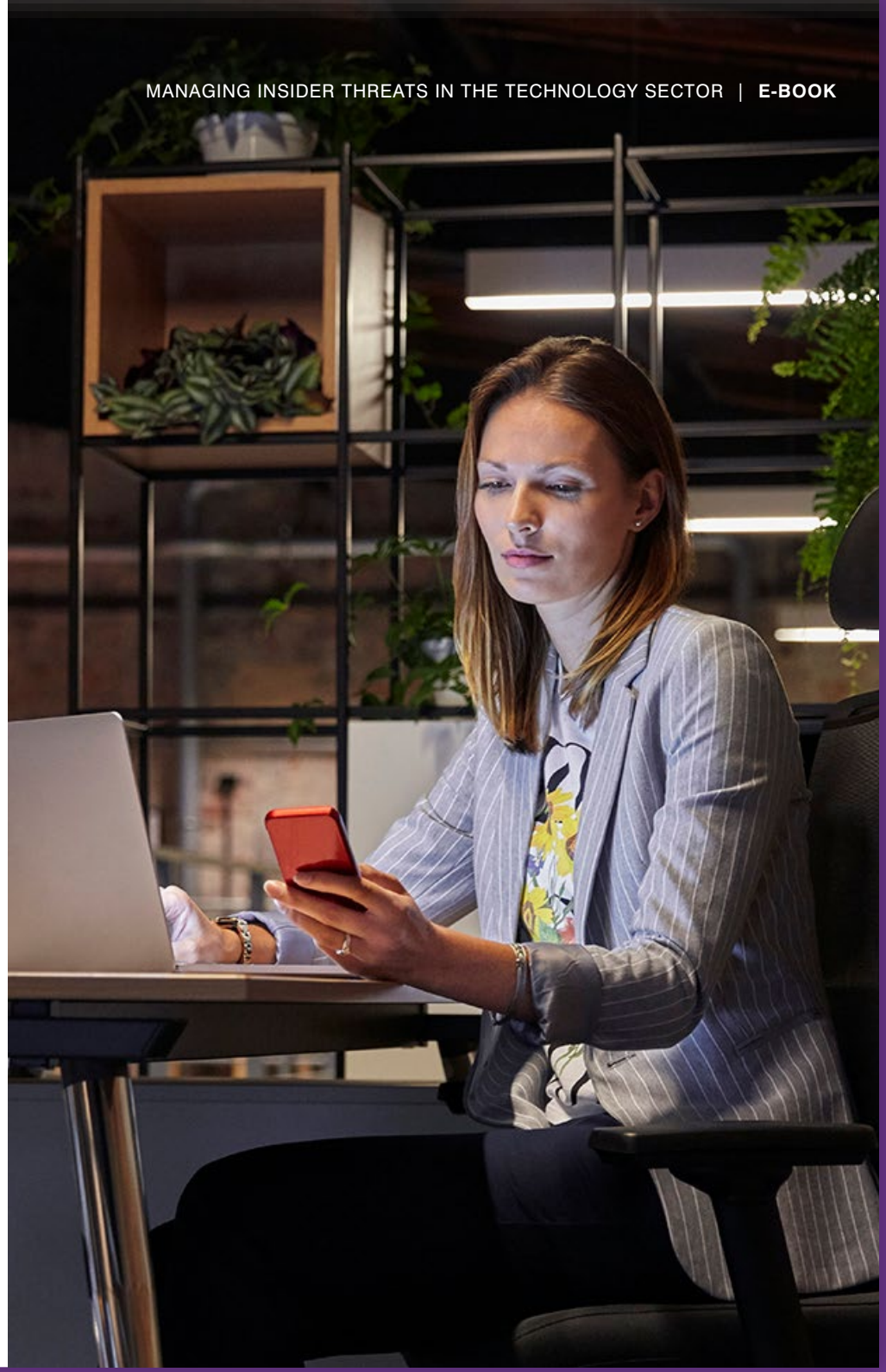
proofpoint.

Managing Insider Threats in the Technology Sector

A Guide to Securing Your Intellectual Property and Competitive Advantage



From 2018 to 2020, the total annualized cost of insider threats in the technology and software industry rose 67% to $12.3 million.[1]

Introduction

For modern technology companies, innovation is a team effort. It often entails collaborating with others throughout the organization and with outside partners and vendors. And they all have varying levels of insider access to valuable data.

Technology firms must manage and protect all kinds of sensitive information, including:

- Source code
- Product designs
- Patents
- Proprietary processes
- Trade secrets
- Contracts
- Customer data

That's getting harder in an era of remote work. Today, your extended team may include outside contractors, consultants, vendors and global supply chains.

Not surprisingly, most companies have deployed defenses to reduce the risk of cyber threats entering their environment. But what about the threats that are already inside? Whether a result of malicious, negligent or compromised users, these insider threats also pose serious business risks.

Fortunately, adopting an insider threat management (ITM) strategy can reduce your risk and keep you focused on what you do best: creating great products and services.

This e-book explains how to manage insider threats without disrupting the open, collaborative culture so vital to innovation. We'll explore a people-centric approach to insider threat management. You'll learn how to balance organizational agility, data security and user privacy.

[1] Ponemon. "2020 Cost of Insider Threats Global Report." February 2020.

SECTION 1

Insider Threats in Today's Dynamic Technology Sector

3/4 of insider threat incidents happened by accident or user compromise.[2]

Every business must protect sensitive information and confidential business practices, including:

- Customer information
- Trade secrets
- Sales and marketing competitive information
- Intellectual property

This is especially critical for technology firms. The typical software company has source code that serves as the "secret recipe" of its entire product line. Life science firms create drug formulations worth hundreds of millions of dollars. And medical device makers' design breakthroughs can provide an edge in a highly competitive market.

Like other industries, the technology sector is moving to distributed workforces and extended supply chains. At the same time, it relies more and more on cloud-based platforms shared by a wider range of users. In a typical enterprise, it isn't just employees with access to sensitive data. Contractors, gig economy workers, service providers and remote employees may also have access.

Suddenly, defining an "insider" isn't so simple.

Defining what constitutes a "threat" isn't much easier. ITM isn't just about detecting malicious users. Not every insider threat is a greedy insider looking for a payout or disgruntled worker seeking revenge. Many risks stem from negligent and compromised users who unwittingly pose as insider threats.

[2] Ponemon Institute. "2020 Cost of Insider Threat Global Report." February 2020.

SECTION 2

The Who and What of Insider Risk

Insider risk should be a major focus of any digital-driven businesses.

But where should they start? The first step in building a modern insider threat program is to understand the *"who"* and the *"what"* of insider risk:

- Who to be concerned about
- What to protect

Who to be concerned about

Managing insider threats starts with deciding which of your users pose the biggest risk. Every company and use case is unique. But here are some common categories of users to consider.

Non-employee users. Contractors, service providers, gig economy workers, consultants and partners may access your IT infrastructure. Any of them can pose a potential risk.

Privileged-access users. Some workers need access to protected infrastructure and information to manage these critical systems. Examples include:

- IT and database administrators
- Engineering team members
- Managed software or service providers
- Penetration or QA testers

High-risk employees. Some users may be deemed a high risk by human resources based on factors such as:

- Behavior
- Job changes
- Performance or disciplinary issues
- Flight risk

Technical users. Unlike any other industry, the technology sector has a high concentration of technical employees. Malicious insiders with technical know-how can use their skills to:

- Create unauthorized accounts
- Change the intended behavior of code
- Open security vulnerabilities
- Modify critical data

Remote workers. A far greater portion of the global workforce is now working remotely. Working from anywhere while connected to the corporate network can increase the risk of security gaps. These include:

- Data leakage
- Credential theft
- System compromise

It's not just about malicious users

The term "insider threat" is commonly associated with users who show malicious intent. They may be motivated by financial gain, revenge or foreign allegiances. But negligent and compromised users are actually a much more common cause of insider breaches.

Negligent users are those acting outside of sanctioned processes. They unwittingly expose your infrastructure or data and increase risk.

Compromised users are those whose accounts are under the control of outside attackers. Some are compromised through social engineering. Others are simply victims of account takeover through no fault of their own.

In any case, negligent and criminal users are usually your biggest insider risk.

Negligent Insiders

$307K
Per incident

4.58M
Cost to organizations

Criminal Insiders

$756K
Per incident

4.08M
Cost to organizations

Credential Insiders

$871K
Per incident

2.79M
Cost to organizations

Ponemon 2020 Cost of Insider Threats Global Report

What to protect

Technology companies rely on their IP, confidential practices and other trade secrets for a competitive edge. They also need to comply with a range of data privacy and industry regulations. Here are some of their highest priority concerns:

Intellectual property. IP is the highest value target for malicious insiders. A common scenario: a privileged or technical user steals IP and takes it to a competitor.

Compliance. The technology, life sciences and medical device sectors are subject to a wide range of compliance mandates. These rules govern how firms protect data, information and the integrity of their processes. Compliance gaps can lead to major penalties.

Service disruption. Attackers with insider access can damage or disrupt customer and employee-facing services. Downtime can mean lost revenue, opportunity and trust.

Sensitive data. Many technology companies store sensitive customer data or other critical information. Their success hinges on keeping that data secure.

Brand damage. Technology brands are built on trust with their customers, employees and stakeholders. When security breaches occur, especially when caused by insiders, this trust is violated. That hurts your brand and reputation.

Three Ways Privileged Users Become Insider Threats

According to Computer Emergency Response Team (CERT), a third of insiders in the technology sector abused their privileged access. Here are three warning signs to look out for.

1. **Escalating privileges or giving access to untrusted users.** You may begin to detect users granting themselves (or others) access to restricted areas of the network. In many cases, they may log into systems with a low-privilege account to find coding errors or design flaws to exploit. From there, they escalate their privileges and gain more access. If these insider threats succeed, they can:
    - Create new system users
    - Access files
    - Authorize network activity
    - Change system settings
2. **Abusing administrator privileges.** Many organizations restrict admin access to prevent the risks inherent in granting powerful root-level control. But sometimes, an admin may need temporary root-level permissions to run some commands and scripts. In those cases, they may use the sudo ("superuser do") command in Unix and Linux. Sudo gives admins temporary root-level permissions to do their jobs without needing full root access. But sudo is a powerful command that comes with big security downside: admins can abuse it for all kinds of risky and malicious acts.
3. **General negligence with admin credentials.** Most insider threat incidents are caused by employee or contractor negligence. Sometimes, these mistakes can be even more costly than malicious incidents. Privileged users can become major risks if they grow careless about general security hygiene, such as password management. Examples that may increase the risk of a breach include:
    - Neglecting to regularly change admin passwords
    - Sharing admin credentials through insecure systems

Many organizations have also accidentally included admin credentials in code they submit to sites such as GitHub.

SECTION 3

How Insider Threat Management Technology Can Help

ITM helps security teams get a handle on this unique threat vector. It combines elements of Data Loss Prevention (DLP) and User Behavior Analytics (UBA) to reduce risk in three key ways:

Identifying user risk

Detection of risky user access to assets alone will not protect against insider threats. Falling back to manual correlation of disparate logs from your applications is too difficult and slow.

With Proofpoint ITM, you get granular visibility into user access and activity on applications, files, data, servers, desktops and virtual environments across Windows, Mac and Linux/UNIX platforms. Detect data exfiltration, unauthorized access and activity, risky application usage and negligent behavior in real-time.

Protect from data loss

Most technology companies have data they must protect to stay competitive and in business - intellectual property, customer data, regulated information and more. Quickly identifying and preventing users from accidentally exposing or maliciously exfiltrating sensitive data is a core function of a modern ITM solution.

With Proofpoint ITM, you can set pop-up notifications to deter or set prevention rules to block users from moving files in a risky manner. Warning messages turn potential negligent or accidental behavior into a teachable moment. In the case of obvious malicious behavior, stricter action such as prevention of the data movement is appropriate.

Accelerate incident response

The cost of insider threats hinges on the time and cost of responding to incidents. Modern ITM solutions help security teams reduce those costs by 56%, on average.[3] More focused detection, easy to understand context as evidence lead to faster response and cheaper insider threat programs.

With Proofpoint ITM, respond quickly with timeline-based and screenshot evidence of user activity before, during, and after an incident. Integrate our telemetry with existing security tools and workflows. Customize user and data activity collected based on compliance and privacy requirements and anonymize users' data to protect their identity.

[3] ESG Analyzing the Economic Benefits of Proofpoint Insider Threat Management 2020 Report

SECTION 4

Real-World Insider Threat Scenarios

Insider threats at software companies

Gaining visibility into out-of-policy user activity

A large software company was dealing with thousands of policy exceptions yet had no real-time visibility around technology usage.

One department allowed USB device usage. Another gave users access to non-corporate cloud applications. The team needed a targeted way to detect and respond to risky activity without locking down the company's open culture.

Best practices to balance detection with user privacy while protecting your sensitive data:

- Conduct regular and targeted security awareness training that incorporates real-world threats and tactics.
- Invest in lightweight endpoint solutions that detect risky user behavior and data movement in real time and provide incident response workflows to speed up insider investigations.
- Collaborate with your HR, legal, compliance and IT teams on data collection of user and file activity, risky behavior detection policies and incident response workflows for insider threats.
- Warn and educate users when they make a mistake or before they attempt something malicious.

Insider threats in life sciences

Protect data associated with intellectual property

The CISO of a global life sciences company learned the hard way about her team's data-loss blind spots after a fired worker was suspected of IP theft.

She and the team had spent months working on data discovery, classification and policy creation to locate and protect the company's valuable data. But the organization's IP was always in flux and hard to classify. When a recently terminated employee was suspected of stealing crucial IP, it took three weeks to determine what actually happened. The security team had to manually correlate logs from the data loss prevention tool, application firewall and the user's endpoint. Only afterward could the CISO provide details to the board of directors. The delay caused senior executives and the board to question the company's ability to stop similar incidents.

Best practices to protect intellectual property and remove data-loss blind spots:

- Detect movement of IP by high-risk users in real time.
- Update and simplify acceptable-use and intellectual property policies. Your people should be able to easily understand and learn them.
- Provide contextual intelligence that ties all data movement to the users involved. Correlate users' actions before and after the data movement.

Insider threats at medical device companies

Protecting valuable data and IP from third parties

An international medical device company needed to integrate with outside partners without creating needless security and compliance risks.

The company worked with hundreds of third-party vendors, contractors and partners for R&D and throughout its supply chain. These critical partners needed access to sensitive product development and internal company data.

At the same time, the CISO was rightly concerned that the natural churn of partners and its own workforce posed an insider risk. It wasn't clear how many users had insider access to company data—or whether they should. She wanted greater visibility and control over what was being shared and when.

Best practices to secure third-party access and stay compliant:

- Get visibility into the user activity of vendors, suppliers and contractors as they work on your critical applications, servers and IP.
- Retain a detailed audit trail of their activity for at least a year. Global supply chain compliance requirements may require longer retention windows.
- Get endpoint-based screen capture before and after third parties commit malicious or accidental actions. These provide irrefutable evidence of wrongdoing or negligence.

Conclusions and Recommendations

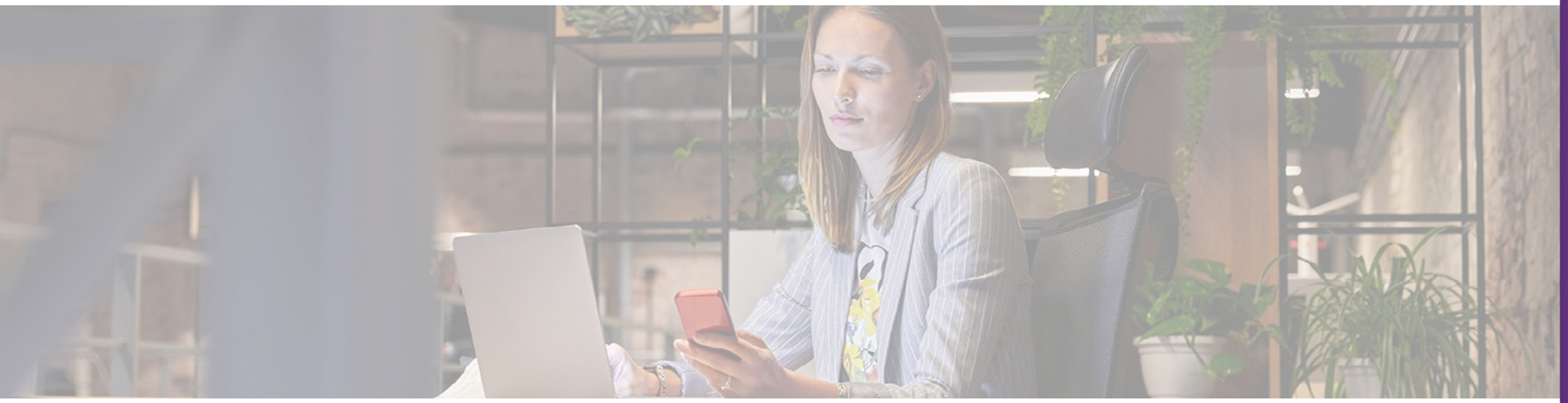
Why Proofpoint: Best Practices ITM from a Trusted Advisor

Proofpoint ITM helps protect against IP data loss from malicious, negligent and compromised users. We take a people-centric approach that is focused on visibility, detection and response—without hurting endpoint performance.

- **Context-based user risk analysis.** Get real-time visibility across app and browser usage, server access, desktop activity, data and file interaction, email usage and exfiltration vectors. We can instantly correlate user activity, data interaction and system usage in an easy-to-view timeline.
- **Protection of user privacy.** Protect your assets while complying with organizational, cultural and industry privacy standards. Exclude personal applications from monitoring. User anonymization enables first-line analysts to monitor and initiate response without seeing the user's identity.
- **Insider threat detection.** Hunt for risky behaviors before they become real insider threats. Easily correlate detection of unauthorized activity and access. Stop risky accidental actions, system misuse and out-of-policy data movement. Our comprehensive library of insider threat alerts helps you respond in real time.
- **Incident response workflows.** Choose from graduated response options. With ITM, you can warn or educate users, alert security, proactively log users off and even close applications. Collect evidence in real-time across all the apps, platforms and devices they use. Collaborate with other stakeholders such as HR and legal with easy-to-understand screen captures and timelines. Synchronize our intelligence with your Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) systems for complete incident response.

Take our insider threat risk assessment today.

Get a personalized report on your program maturity and share it with colleagues.



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**.

proofpoint.

0512-004-01-01 02/21