

The No-Nonsense Guide to Insider Threat Management

The No-Nonsense Guide to Insider Threat Management

An insider threat incident occurs when someone with authorized access to critical information or systems misuses that access, either purposefully or accidentally, resulting in a negative outcome.

Recent research indicates that insider threat risks are on the rise. According to an independent report from The Ponemon Institute, all of the 159 organizations surveyed had at least one insider threat incident in the prior 12 months.¹ In fact, 25% of all security incidents² involve insiders.

Even though insider threat incidents are becoming increasingly prevalent, many organizations don't understand their causes, or how to detect and prevent them.

What's more, today's insider threats move faster and are more unpredictable than ever, which can present a challenge for many legacy security efforts.

This no-nonsense guide to insider threat management is intended to help get you up to speed, fast. Key takeaways include:

- The consumerization of IT and remote working — paired with the high margin for human error in the use of corporate applications — have caused a dramatic increase in insider threat risks in the last decade.
- Insider threats affect every industry in different ways, but across industries can cost organizations millions of dollars on an annual basis, or hundreds of thousands of dollars per incident.
- Employee and contractor mistakes cause two out of three insider threat incidents, which suggests the vast majority of insider threats can be prevented with the right strategy in place.
- Since people are at the center of every insider threat, putting people first is essential when creating an insider threat program. Think people, process, technology — in that order.

1. <https://www.observeit.com/cost-of-insider-threat/>

2. <https://www.verizonenterprise.com/verizon-insights-lab/dbir/>

Insider Threats: A History

If you've ever watched a true crime television show, you probably know that most crimes are perpetrated by someone the victim *knew* or *was close with*.

Did you know this also “applies” to security breaches and data leaks?



Insiders can expose an organization to any number of cybersecurity hazards thanks to their trustworthy status and access to sensitive data and systems.

According to a recent independent report from The Ponemon Institute³, insider threats of all types are increasing. Since 2016, the average number of incidents involving employee or contractor negligence has increased by 26 percent, and by 53 percent for criminal and malicious insiders. The average number of credential theft incidents has more than doubled over the past two years, increasing by 170 percent.

Even though insider threat risks are increasing now, they've been around for decades. Traditionally, the technological solutions most often used to prevent data exfiltration were DLP tools. These tools relied on IT or security professionals to correctly configure, deploy and fine-tune over time. In the early days of corporate IT use — when systems were centrally managed by the company, and technology use was limited to a subset of applications — these solutions were practical to implement and manage.

In the last five years alone, corporate IT use has dramatically changed. The consumerization of IT has led to end-users selecting the tools and technologies they want (both from a hardware and a software perspective). Remote work policies have given employees more freedom and flexibility, which has been a boon to productivity, but also difficult for IT to track. According to a study by Cisco⁴, 80 percent of end users' software is not cleared by IT.

Traditional DLP Tools

Traditional DLP agents can be challenging to manage in this type of environment, since they're focused on the data aspect of the equation, rather than the people aspect. First, DLPs can cause employees' applications to slow down or crash. Sophisticated end users have learned how to bypass these systems altogether, leading to an even riskier ecosystem for insider threats. Second, with unsanctioned IT use at an all-time high, it can be difficult for IT teams to even know where employees' data is located, or how it is being shared.

Modern insider threat management strategies focus on the people aspect of insider threats first, making an effort to understand users, create policies that fit employees' lives, and empower the proper use of technology on a regular, ongoing basis. By focusing on people rather than data alone, organizations can gain a more holistic view of what's happening — and prevent data exfiltration in the process.



3. <https://www.observeit.com/ponemon-report-cost-of-insider-threats/>

4. <https://blogs.cisco.com/cloud/the-shadow-it-dilemma>

Inside Jobs: A Snapshot of Notorious Insider Threats⁵

Rockwell & Boeing

1979-2006

Spies aren't just for TV and movies. Nation-state spying is a very real concern and one way that other countries can gain access to valuable trade secrets and intellectual property.

One example is man named Greg Chung, who spied for China when he worked at Rockwell and Boeing. From 1979 to 2006, Chung stole hundreds of boxes worth of documents related to military and spacecraft information. Given the length of time, it's practically impossible to know the dollar value or repercussions of this attack.

NSA & Edward Snowden

2012-2014

In quite possibly the most notorious top-secret document leak, Edward Snowden (according to US intelligence officials) downloaded up to 1.5 million files while he was employed as an NSA contractor, beginning in the late spring of 2012.

From 2013-2014, Snowden's whistleblowing efforts led to series of striking reports from journalists, exposing the NSA's surveillance tactics used on US and foreign citizens, world leaders, companies, and governments.

Anthem

2016-2017

In April 2017, Anthem discovered that an employee had been stealing and misusing Medicaid member data since as early as July 2016.

The employee at fault had emailed a file containing data regarding Anthem members to his own personal email address. The data included Medicare ID numbers, Social Security numbers, Health Plan ID numbers, names of members, and other sensitive information for more than 18,000 people. The employee was removed and placed under investigation.

Google & Uber

2017-2018

In 2017, Waymo (Google's self-driving car project) sued Otto (a company acquired by Uber) for patent infringement and stolen trade secrets. The lawsuit alleged that Otto founder Anthony Levandowski downloaded more than 14,000 confidential and proprietary files from Waymo before he resigned, concealing his activities from his employer.

According to the lawsuit, these files contained information for a LiDAR circuit board design system patented by Waymo, that measures distance using lasers to create a 3D map of a vehicle's surroundings. Waymo learned of the alleged infringement when it was copied on an email from a LiDAR component vendor. The lawsuit was settled for \$245 million in 2018.

5. Aggregated from various news stories, appendix at end of Guide (see Appendix on Page 12)

Why Focus on Insider Threats Now?

Any high-growth company has more projects than hours in the day. With so many competing priorities, why focus on insider threats now? Simply put, threats like the ones listed above are becoming more common and more costly. According to independent research performed by The Ponemon Institute⁶, the average annual cost of an insider threat per company is \$8.76 million.

In addition, as cited above, insider threat risk potential is increasing with a rise in use of applications that are not sanctioned by IT. Combine these factors with the nearly 3.9 million Americans⁷ who reported they worked from

home in 2018, a 115% jump in just three years. As more employees access corporate systems outside of work, the margin for error has increased dramatically.








The cost and cause of insider threats can vary dramatically depending on the industry and size of the company. Therefore, it's crucial to learn about the security issues specific to companies like yours in order to prevent them. Here's just a snapshot of industry-specific concerns, keeping in mind there are many more affected industries beyond the ones we've listed below.



6. <https://www.observeit.com/ponemon-report-cost-of-insider-threats/>

7. <https://smallbiztrends.com/2018/04/2018-remote-work-statistics.html>

Industry-Specific Threats & Concerns⁸

Industry	Key Issues	Did you know?
Financial Services 	<ul style="list-style-type: none"> • Fraud and monetary losses • Disclosure of confidential customer and/or account data • Destabilization of critical infrastructure 	24% of breaches target financial organizations.
Telecommunications 	<ul style="list-style-type: none"> • Disruption of critical communications infrastructure • Theft of personally identifiable information • Corporate espionage • Denial of service attacks 	75% of attacks targeted at the information industry are financially motivated.
Technical Services 	<ul style="list-style-type: none"> • Intellectual property theft • Disruption of IT operations • Customer data leaks • Network and systems disruption 	Technical services companies power the modern world and are often hit with insider attacks as a result.
Healthcare 	<ul style="list-style-type: none"> • Theft or misuse of protected health information • Theft or misuse of electronic healthcare records • Insurance and financial fraud 	Healthcare is the only industry where insider threats outnumber external threats. 56% of the sector's breaches are caused by insider threat actors, while 43% are caused by external risks.
Government 	<ul style="list-style-type: none"> • Theft or abuse of constituent information • Fraud and misuse of public funding • Compromised defense systems • Leaked intelligence 	12% of all breaches target public sector organizations.
Retail 	<ul style="list-style-type: none"> • 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 \$172⁹ per stolen record.
Education 	<ul style="list-style-type: none"> • Tampering or loss of student records • Identity theft or loss of personally identifiable information • Financial loss for both institutions and students 	The number of lost, stolen, or compromised records increased 164 percent in the first 6 months of 2017, compared to the second half of 2016. ¹⁰

8. <https://www.verizonenterprise.com/verizon-insights-lab/dbir/>

9. <https://www.retaildive.com/news/5-numbers-to-know-about-retail-cybersecurity/435682/>

10. <https://edtechmagazine.com/higher/article/2017/12/education-sector-data-breaches-skyrocket-2017>

Top Causes of Insider Threats

An insider threat incident can impact any company, no matter the industry or location. Despite this range of variability, it turns out that many of these incidents have common causes.



Employee Negligence – Many breaches are caused when employees inadvertently share sensitive data. From accidentally clicking on a phishing email, to using out-of-policy software that exposes an organization to unnecessary risk, two out of three¹¹ insider threat incidents happen because of mistakes. Employees may be misunderstanding regulatory compliance requirements, company policies, or overall security best-practices.

For example, have you ever walked past a colleague's desk when the person isn't there and seen their screen lit up? Unsecured devices are a leading cause of accidental insider threats.



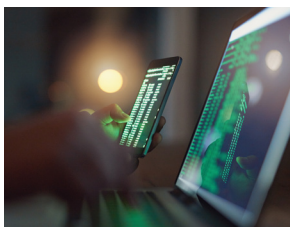
Vendors and Contractors – The importance of vendor monitoring can't be overlooked. Consultants, agencies, and other third party workers can pose a huge security risk. These workers need access to systems to do their projects, and they'll likely be given that access from their points of contact at your organization. However, because they work outside of the company, they may not follow the same security policies as your own workers. This inconsistency can open up an organization to potential vulnerabilities, which is why third party monitoring is so crucial.



Cybersecurity Policies – Your own cybersecurity efforts may actually be working against you. If your policies are putting up too many barriers or creating extra work, employees will find workarounds. What's a better solution? Keep an open dialogue, generate buy-in, and proactively share best practices with users. Most of all, listen to employees and work with them to create policies that protect the company — but don't hinder their ability to do their jobs.



Credential Thieves – Credential theft or impostor risk is the most costly¹² type of insider threat, averaging \$649,000 per incident. While remote login accounts and cloud software improve efficiency and communication, the chance that unauthorized users will exploit their access privileges increases dramatically. Using weak passwords, or recycling passwords across multiple services (as more than half¹³ of people admit to doing), make a credential thief's job that much easier.



Criminal or Malicious Users – When you're investigating or reconstructing an insider threat or trying to get ahead of bad behaviors, it's important to understand the intent of your users. Privileged or highly technical insiders could be exploiting their level of access to exfiltrate data from the organization. Malicious employees and state-sponsored insiders require much different security strategies.

11. <https://www.observeit.com/cost-of-insider-threat/>

12. <https://www.observeit.com/cost-of-insider-threat>

13. <https://www.darkreading.com/informationweek-home/password-reuse-abounds-new-survey-shows/d/d-id/1331689>

Behaviors to Watch

With insider threat risks on the rise, it's important to know the top behaviors that cause insider data loss.



Removable Media

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



Hard Copies

While it may not seem as common as it used to be before laptops and smartphones, physical data is still a major cause of data leaks. Keeping track of hard copies of critical company data can become a major problem.



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 are a reality of every organization today and can give workers a major productivity boost. However, 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 can cause data exfiltration as these applications often contain sensitive documents and information. Some users may also access "Shadow IT" applications that are outside of corporate policy.



Social Media

Unauthorized use of social media is a big concern for security teams. It's relatively easy for an employee to post leaks of sensitive corporate information — it's only a click away.



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 intellectual property and proprietary source code leaks.



Screen Clipping & Screen Sharing

Many users try to find ways around IT policies with unapproved software or applications. Unauthorized screen clipping and screen sharing services can easily be used to exfiltrate data. If users are regularly accessing these sites (or other unauthorized software), it could be an indicator of a potential insider threat.



FTP Sharing Sites

Many organizations prohibit the use of FTP sharing sites, but because of their ease of use, they're common causes of data leakage.

How to Detect & Prevent Insider Threats

Detecting a real insider threat can be difficult, because understanding trending user activity and intent requires context. There are many different ways to gather contextual activity data, but the last thing that anyone wants to do is add more layers to a security setup, increasing the burden on both the security team and users.

Below are some best practices for designing an effective insider threat management strategy that encompasses detection, prevention, and investigation/incident response. We recommend a holistic approach that balances people, process, and technology.



DETECTION



Identify trends in user activity (and investigate risky behavior)

Getting more insight into the actions taken by employees and vendors will provide the needed context to know whether a behavior requires further investigation. To protect users' privacy, anonymize this information whenever possible.

Keep an eye on file, passwords and folder activity:

Keep in mind that certain endpoint activity can also be indicative of malicious intent, or the possibility that credentials have been compromised or misused. For example, investigate logins to unauthorized servers or from unauthorized clients, as well as risk indicators around file, folder, and password activity.



Look to the web

Monitor for suspicious internet behavior, including browsing unauthorized content, contaminated websites with high security risks, or copyright-violating websites. Include policy violations such as running peer-to-peer file-sharing sites, webmail or instant messaging services on company servers; accessing the dark web; clicking links to phishing websites; and searching the web for information on malicious software.



Don't forget advanced technical users

Set up real-time alerts for when users intentionally use malicious tools or software, tap into sensitive admin tools or configurations, delete users or information from sensitive directories, hide information by tampering with log files or passwords, or attempt to gain higher access privileges to systems.

How to Detect & Prevent Insider Threats



INVESTIGATION & INCIDENT RESPONSE



Be prepared

Many organizations aren't prepared with a detailed incident response plan before an incident takes place, leaving them scrambling after an incident occurs. Prepping a playbook with a chain of command, and even going through an attack simulation, will smooth the incident response process and decrease the overall response time dramatically.



Investigate user activity

Knowing precisely what a trusted employee or contractor was up to, what happened and whether it was repeated is crucial. Not all insider threat incidents are malicious, but there is only one way to know for sure: investigating trending activity by viewing a step-by-step, click-by-click log or session video recording of an insider's actions.



Keep key stakeholders apprised

An incident response doesn't just involve the security team. A wide variety of stakeholders need to be kept in the loop, including key C-level executives, as well as HR, compliance, communications, and customer service leaders. With compliance regulations such as GDPR, teams can take swift action to ensure that breach disclosure protocols are being followed.



How to Detect & Prevent Insider Threats



PREVENTION



Understand your users

People are the most critical aspect of establishing a proactive insider threat management strategy that prevents good users from making bad decisions. Understanding the intent of insider threats is important, because it allows you to get ahead of risky behavior and problem-solve.

Consider starting an open dialogue with your trusted insiders to understand their needs (and potential problems), and supplement it with the right tools to monitor activity. Trust and understanding are key components to any cybersecurity effort!



Modify restrictive policies

Communication is the first step to mitigating risk of unintentional insider threats. Learn more about your users, and see if they are experiencing bottlenecks with your current data leakage prevention tools or policies — or circumventing them altogether for efficiency's sake. Then, see if there is a way to take a more “hands-off” approach.



Look for coachable moments

If an employee does something “risky” or out-of-policy, try to embrace it as a teaching moment. Give them the benefit of the doubt, depending on the situation. The incident could have been caused by a misunderstanding of policy, overzealous (or confusing policy), or simply not paying attention. Then, re-explain the policy and use an example-based rationale to ensure they understand why it was created in the first place.



Anticipate moments of intentional threat

Of course, not all insider threat incidents are accidental. Try to anticipate the people and events that could lead to an incident and create a game plan to mitigate the actual attack from happening. For example, a disgruntled former employee may have systems access and knowledge that you wouldn't want shared beyond the walls of your office. In this case, removing access to data and systems upon termination can lessen the chance of a data leak.

Next Steps

Today's technological advancements — like cloud-based software, mobile devices, and VPNs — make it easier than ever to collaborate with colleagues. Unfortunately, these tools also increase risk, as more and more people now have access to systems and data. To make sure that your security approach is successful in preventing insider threat attacks:

- **Work closely with your users** to develop a system they understand, and is convenient for them to adhere to.
- **Understand how technology can help** you detect insider threats and be proactive about protecting users on an ongoing basis.
- **Know how to paint the picture of an incident** by having visibility into who, when, and how users are accessing and sharing data.
- **Be prepared** with the right teams and processes in place to address an insider threat incident when it happens.

Insider threat solutions like ObserveIT can help your organization identify and eliminate threats before they take off and have harmful consequences.

Visit **observeit.com** to learn more
or click **here** to try it for free.

5. Page 4 Appendix

Chung: <https://www.newyorker.com/magazine/2014/05/05/a-new-kind-of-spy>

Snowden: <http://www.businessinsider.com/snowden-leaks-timeline-2016-9>

Anthem: <https://www.cnn.com/2017/07/31/new-anthem-data-breach-by-contractor-affects-more-than-18000-enrollees.html>

Google/Uber: <https://www.theverge.com/2018/2/9/16995254/waymo-uber-lawsuit-trial-settlement>

