

The enemy within:

An insider threat management handbook



Table of Contents

1. Introduction	1
2. What is an insider threat?	2
3. Dangers of an insider threat	3
3.1 Breaches can go undetected for long periods of time	4
3.2 The breadth and scale of insider threats can be enormous	4
3.3 Preventing insider threats is difficult	4
4. What are the different types of insider threats?	5
4.1 The malicious insider	5
4.2 The negligent or careless insider	5
4.3 The third-party insider	6
5. Indicators of an insider threat	7
5.1 Behavioral indicators of an insider threat	7
5.2 High-risk system indicators of an insider threat	8
5.2.1 Excessive orphaned files or user accounts	8
5.2.2 Presence of shadow IT	8
5.2.3 Inappropriate level of authentication	8
5.2.4 Excessive "access denied" readings	9
5.2.5 Data exfiltration	9
The malicious insider threat kill chain	9
6. Ten best practices to fight insider threats	10
6.1 Establish baseline behavior for both individuals and networks	10
6.2 Provide the least amount of privilege possible	10
6.3 Run periodic, organization-wide risk assessments	10
6.4 Educate your end users	11
6.5 Implement strict password and account management policies	11
6.6 Deprovision orphaned user accounts	11
6.7 Prevent logic bombs from executing	11
6.8 Enforce active remediation	12
6.9 Scrutinize your remote access policies	12
6.10 Audit, monitor, and record all access attempts	12
7. Insider threat statistics	13

1. Introduction

“

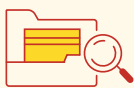
**If you know neither
the enemy nor yourself,
you will succumb in
every battle. ”**

Sun Tzu _____

The greatest threats to any organization today typically come from the employees and partners it trusts the most. Insider threats present organizations with a unique problem, as they could be intentional attacks carried out by malicious actors or unintentional mistakes from well-meaning employees. This e-book is designed to identify and explain the various indicators of insider threats, as well as the latest trends and practices used to prevent insider threats and mitigate their effects.

2. What is an insider threat?

An insider threat is any unauthorized or unintended security threat to an organization's data or information systems that originates from an individual operating inside the organization. The insider doesn't necessarily need to be a current employee—they could be a contractor, or a temporary or former employee. Insider threats can lead to data theft, data misuse, sabotage, espionage, and fraud, as well as compromise of an organization's data integrity, availability, confidentiality, and more.



According to Verizon's **2017 Data Breach Investigations Report**, insider threats are more prevalent in the healthcare industry than outsider threats. **Sixty-eight percent of protected health information (PHI) data loss incidents from 2016 to 2017 involved insiders.**

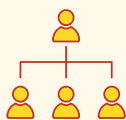


According to Trend Micro's **Cybercrime and Other Threats Faced by the Healthcare Industry** report, a full set of PHI from a deceased person can be sold on the dark web for at least **\$1,000.**

3. Dangers of an insider threat

Some of the largest security incidents that have ever occurred—including the Equifax, Fedex, and National Security Agency (NSA) breaches—were data theft events perpetrated by an insider. Understanding the motives behind an insider attack, the potential indicators of an impending insider attack, and preparing for the consequences of one is essential for any organization.

The factors below explain why insider threats are one of the most



According to Protenus' **2017 Breach Barometer Annual Report**, it takes an **organization 308 days** on average to **identify a breach**.



According to Protenus' **Q1 2018 Breach Barometer** report, the PHI of 1,129,744 healthcare members was exposed, stolen, or viewed by unauthorized individuals in the first quarter of 2018.

3.1



Breaches can go undetected for long periods of time

According to Ponemon Institute's [2018 Cost of Insider Threats: Global](#) report, it takes on average more than two months to contain an insider threat. The longer it takes to discover an incident after it occurs, the longer it takes to assess the damage inflicted, apprehend the individuals involved, and take additional reactive measures to prevent future incidents.

3.2



The breadth and scale of insider threats can be enormous

Security vulnerabilities can arise from almost anybody and from anywhere. Be it a disgruntled employee, a sloppy user, a masquerading data thief, or a partner lacking the necessary security measures, the variance of insider threats is what makes every department in every organization vulnerable to an insider attack.

3.3



Preventing insider threats is difficult

Not all internal incidents are intentional—more often than not they're caused by a user's inattentiveness or sloppiness. This makes it difficult to have a holistic solution that detects both intentional and unintentional security incidents. Besides, many malicious insiders enter legitimate credentials on their own machines using privileges that were already granted to them, making it even more challenging to detect and thwart ongoing attacks.

4. What are the different types of insider threats?

Insider threats come in all shapes and sizes, but they most commonly fall under one of three categories:

- **Malicious insiders**
- **Negligent or careless users**
- **Third-party contractors**

4.1



The malicious insider

Malicious insiders deliberately undermine an organization's security systems. Whether they're a disgruntled employee or a criminal agent, these individuals use their legitimate or stolen credentials to access the organization's systems with the intent to disrupt, steal, or misuse IT systems or data.

4.2



The negligent or careless insider

More often than not, it's a negligent employee who causes irreparable damage to an organization. For example, sloppy actions—such as clicking on a phishing mail, deleting a sensitive file, disregarding data share protocols, using an unsecured public network for accessing sensitive data, or using weak credentials—lead to leaked data or security vulnerabilities that criminals can take advantage of.

4.3



The third-party insider

Many third-party contractors, such as vendors, are provided with limited access to an organization's resources and data. If a third party's own network ends up being compromised, it may serve as a gateway into the systems of the organization that hired them.



According to the Ponemon Institute's **2018 Cost of Insider Threats: Global** report:

- Incidents involving stolen credentials are the most costly.
- A negligent insider is the root cause for most incidents.
- Organizational size and industry affect the cost per incident.
- The occurrence of each insider threat type is increasing.
- Employee or contractor negligence costs companies the most.
- On average, it takes more than two months to contain an insider incident.



According to **Cisco's 2018 Annual Cyber Security Report**, 53 percent of all attacks resulted in financial damage of more than \$500,000. These damages include lost revenue, customers, and opportunities, as well as out-of-pocket costs.



According to **Breach Level Index's statistics**, 71 data records are lost or stolen every second.

5. Indicators of an insider threat

Indicators of an insider threat can be split into two categories:

- Behavioral indicators
- Non-behavioral indicators




5.1



Behavioral indicators of an insider threat

Displaying one or more of the traits listed below does not necessarily mean that a person will carry out an attack, but just that an organization needs to monitor them more often. The high-risk behaviors below are commonly associated with insider threats.

Fig 1. Possible traits, demeanor, and goals of an insider

 Traits	 Demeanor	 Goals
Vindictive	Odd working hours	Revenge
Negligent	Financial stress	Financial gain
Overzealous	Dissatisfied with organizational policies	Espionage
Naive	Passed over for promotion	Hacktivism
	Dismissed or fired; contract not renewed	

5.2



High-risk system indicators of an insider threat

Other than behavioral indicators, there are multiple system vulnerabilities that a potential insider could take advantage of. Being aware of these early indicators could help organizations seal the exposure and take preemptive actions against potential insider attacks. Some of the indicators include:

5.2.1 ***Excessive orphaned files or user accounts***

Organizations open themselves up to insider attacks when they lack provisions for deleting or modifying files, folders, and user accounts when users change their role within the organization or leave altogether. Orphaned accounts provide a means for malicious actors to gain unauthorized access and perform data theft. If an orphaned account is a privileged one (e.g. a user account with administrative privileges to one or more systems, or a sysadmin's account), then the threat is exponentially greater.

5.2.2 ***Presence of shadow IT***

Shadow IT refers to the use of an organization's IT applications and other IT infrastructure without the knowledge of the organization's IT department. When an enterprise lacks information regarding which of its IT resources are being used, then managing and securing those resources becomes difficult. What's more, these resources could provide a channel through which malicious actors infiltrate the network.

5.2.3 ***Inappropriate levels of authentication***

Easy or weak authentication protocols, without the use of step-up or multi-factor authentication, embolden malicious actors in their endeavors. On the other hand, inappropriate levels of strong authentication can also cause multiple problems, including employees justifying the use of shadow IT. Access control measures should always reflect the sensitivity of the information that is being accessed.

5.2.4 **Excessive "access denied" readings**

Multiple failed access attempts to restricted critical IT resources clearly points to a potential insider attack. It's essential to monitor denied access attempts to IT resources that are beyond what's required for employees to perform their duties.

5.2.5 **Data exfiltration**

Unauthorized exfiltration of sensitive data is a red flag that can indicate the presence of a malicious insider. Downloading or acquiring copies of proprietary or critical information; using unauthorized business protocols to transmit data; and transferring data outside the organization are all strong indicators of an insider threat.

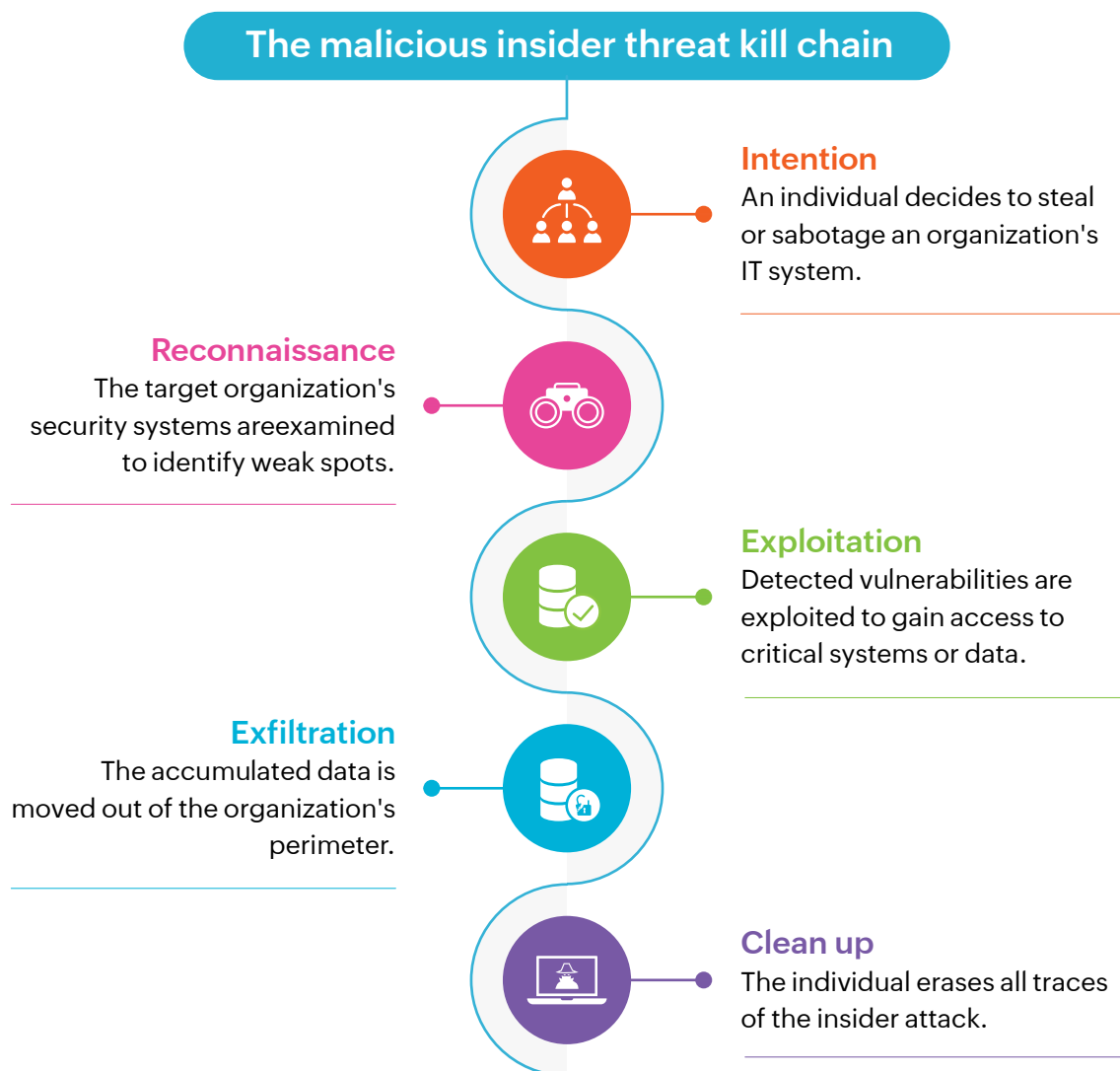


Fig 2. The insider threat kill chain.

6. Ten best practices to fight insider threats

6.1



Establish baseline behavior for both individuals and networks

Consistently record and monitor the normal pattern for employees' baseline behavior so you have something to compare sudden or unusual activity with. Analyze the net volume of file transfer across your network, total access attempts to your most critical files, and other critical access points for easier detection of abnormalities.

6.2



Provide the least amount of privilege possible

Restrict the presence of overexposed files, folders, and shares. Use a robust access management system to prevent unwarranted access and reduce the number of access points through which malicious actors can easily exploit your organization's data.

6.3



Run periodic, organization-wide risk assessments

Determine the type of data your organization processes, how critical the data is, where it's stored, and who has access to it. An inventory of your organization's data and other relevant details helps establish the type of security and access control measures needed. Also, all third-party vendors working with your organization should conduct risk assessments to thoroughly investigate their security posture and keep your organization safe.

6.4



Educate your end users

Regularly train your employees on how to spot and avoid common insider attack scenarios such as phishing emails and malvertisements. Educate and caution your employees about the consequences of violating organizational policies and procedures.

6.5



Implement strict password and account management policies

Deploy multi-factor or step-up authentication and enforce strong password policies to fortify your organization's network. Additionally, lock out users from their sessions after a fixed period of inactivity to prevent malicious actors from misusing abandoned systems in the middle of a session.

6.6



Deprovision orphaned user accounts

Closely monitor employees and third parties for suspicious behavior when they're nearing the end of their service. Disable each of their access points to the organization's various physical and IT resources immediately after they exit the organization.

6.7



Prevent logic bombs from executing

A logic bomb is a piece of malicious code hidden within a script that becomes active when a particular condition—such as a specific date, time, or launch of an application—is satisfied. Clear segmentation of duties and code reviews could help deter malicious actors from setting off a logic bomb.

6.8



Enforce active remediation

Using active remediation techniques, such as USB blocking, strong email filtering, and pop-ups asking for authorization when accessing critical files, helps build your organization's defense against unintentional insider attacks.

6.9



Scrutinize your remote access policies

Design and implement remote access policies with extra scrutiny to ensure that only trusted employees and partners are provided access. Confine remote access only to devices issued by your organization. Monitor and control remote access from all endpoints, especially mobile devices.

6.10



Audit, monitor, and record all access attempts

Capture and record every file access and transfer. Analyze and create a baseline for user and network behavior to easily detect deviations from the regular pattern.



Gartner forecasts worldwide information security spending to exceed \$124 billion in 2019, showing a growth of 8.4 percent from 2018.

7. Insider threat statistics

Industry	Organization	Type of attack	Method	Consequence	Others
Healthcare	Anthem	Negligent, inattentive-insider	Phishing email	May have exposed personal health information of more than 78.8 million individuals	Anthem spent over \$260 million on security measures post-breach
Engineering	Omega Engineering	Malicious insider	Deployed a logic bomb	Damage cost the organization \$10 million	Primary motive was revenge for being let go
Manufacturing	Toyota	Malicious insider	Infiltrated through old work credential	Stole critical personal data and beta testing data, and sabotaged 13 applications	The orphaned user account wasn't deprovisioned
Government	FBI	Malicious insider	Data exfiltrated in thumb drives using remote access	20,000 files or more exfiltrated	Primary motive was hacktivism
Technology	Facebook and Google	Negligent, inattentive insider	Whaling, a type of phishing scheme	More than \$100 million stolen	Primary motive was hacktivism
Energy	Tesla	Malicious insider	Malicious code	Made changes to Tesla's manufacturing operating system and exported sensitive Tesla data to third parties	Primary motive was hacktivism

DataSecurity Plus

ManageEngine DataSecurity Plus is a unified data visibility and security platform. It audits file changes in real time, triggers instant responses to critical events, shuts down ransomware intrusions, and helps organizations comply with numerous IT regulations. It analyzes file storage and security permissions, deletes junk files, and detects security vulnerabilities. Users can assess the risks associated with sensitive data storage by locating and classifying files containing personally identifiable information (PII), payment card information (PCI), and electronic protected health information (ePHI). It also prevents data leaks via USBs, email, printers, and web applications; monitors file integrity; and audits cloud application usage. Together, these capabilities ensure the all-round protection of data at rest, data in use, and data in motion.

To explore these features and see DataSecurity Plus in action, [check out the online demo](#). To learn more about DataSecurity Plus, visit www.datasecurityplus.com.

↓ Download free trial

\$ Get a quote

Explore DataSecurity Plus' capabilities



File server auditing

Audit and report on file accesses and modifications, with real-time alerts and automated responses for critical file activities.

[Learn more](#)



File analysis

Analyze file security and storage, manage junk files, optimize disk space usage, and identify permission vulnerabilities.

[Learn more](#)



Data risk assessment

Discover and classify files containing sensitive data such as PII, PCI, and ePHI by combining content inspection and contextual analysis.

[Learn more](#)



Data leak prevention

Detect and disrupt data leaks via USBs, email, web applications, and printers; monitor endpoint file activity; and more.

[Learn more](#)



Cloud protection

Track enterprise web traffic and enforce policies to block the use of inappropriate, risky, or malicious web applications.

[Learn more](#)

Our Products

AD360 | Log360 | ADAudit Plus | EventLog Analyzer

Exchange Reporter Plus | SharePoint Manager Plus

References

<https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf>

<https://www.trendmicro.com/content/dam/trendmicro/global/en/security-intelligence/research/reports/wp-cybercrime-&-other-threats-faced-by-the-healthcare-industry.pdf>

https://cdn2.hubspot.net/hubfs/2331613/Press_Releases/Breach%20Barometer%202017%20Annual%20Report%20-%20Press%20Release%20-%20Jan%202018.pdf

https://cdn2.hubspot.net/hubfs/2331613/Press_Releases/Q1%202018%20Breach%20Barometer-%20Press%20Release.pdf

<https://www.verizon.com/about/news/ransomware-still-top-cybersecurity-threat-warns-verizon-2018-data-breach-investigations-report>

<https://protenus.com/breach-barometer-report>

<https://www.databreaches.net/>

<https://heimdalsecurity.com/blog/insider-threat/>

https://images.idgesg.net/assets/2017/08/idg_presentation_cybercrime_07202017_final_compressed.pdf

<https://www.nbcnews.com/news/world/how-snowden-did-it-flna8C11003160>