The enemy within:
An insider threat management handbook
1. Introduction

2. What is an insider threat?

3. Dangers of an insider threat

   3.1 Breaches can go undetected for long periods of time
   3.2 The breadth and scale of insider threats can be enormous
   3.3 Preventing insider threats is difficult

4. What are the different types of insider threats?

   4.1 The malicious insider
   4.2 The negligent or careless insider
   4.3 The third-party insider

5. Indicators of an insider threat

   5.1 Behavioral indicators of an insider threat
   5.2 High-risk system indicators of an insider threat
      5.2.1 Excessive orphaned files or user accounts
      5.2.2 Presence of shadow IT
      5.2.3 Inappropriate level of authentication
      5.2.4 Excessive “access denied” readings
      5.2.5 Data exfiltration
   5.3 The malicious insider threat kill chain

6. Ten best practices to fight insider threats

   6.1 Establish baseline behavior for both individuals and networks
   6.2 Provide the least amount of privilege possible
   6.3 Run periodic, organization-wide risk assessments
   6.4 Educate your end users
   6.5 Implement strict password and account management policies
   6.6 Deprovision orphaned user accounts
   6.7 Prevent logic bombs from executing
   6.8 Enforce active remediation
   6.9 Scrutinize your remote access policies
   6.10 Audit, monitor, and record all access attempts

7. Insider threat statistics
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.
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 dangerous and persistent security issues organizations face.

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.
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](image-url)

<table>
<thead>
<tr>
<th>Traits</th>
<th>Demeanor</th>
<th>Goals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vindictive</td>
<td>Odd working hours</td>
<td>Revenge</td>
</tr>
<tr>
<td>Negligent</td>
<td>Financial stress</td>
<td>Financial gain</td>
</tr>
<tr>
<td>Overzealous</td>
<td>Dissatisfied with organizational policies</td>
<td>Espionage</td>
</tr>
<tr>
<td>Naive</td>
<td>Passed over for promotion</td>
<td>Hacktivism</td>
</tr>
<tr>
<td></td>
<td>Dismissed or fired; contract not renewed</td>
<td></td>
</tr>
</tbody>
</table>
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.

---

**The malicious insider threat kill chain**

- **Intention**
  
  An individual decides to steal or sabotage an organization’s IT system.

- **Reconnaissance**
  
  The target organization’s security systems are examined to identify weak spots.

- **Exploitation**
  
  Detected vulnerabilities are exploited to gain access to critical systems or data.

- **Exfiltration**
  
  The accumulated data is moved out of the organization’s perimeter.

- **Clean up**
  
  The individual erases all traces of the insider attack.

*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. Confining 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

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

DataSecurity Plus is a data visibility and security solution that offers data discovery, file storage analysis, and Windows file server auditing, alerting, and reporting features. Locate, analyze, and secure sensitive personal data in your files, folders, and shares from various insider and external threats. Gain visibility into data usage trends, file access patterns, volume of personal data in files, file permission changes, and more. DataSecurity Plus helps you meet multiple compliance regulations and generate clear, concise audit records as legal evidence.

Explore
DataSecurity Plus

Data discovery
Find, analyze, and track sensitive personal data—also known as personally identifiable information (PII)—stored in files, folders, or shares.
Learn more

File server auditing
Audit, monitor, report, and alert on all file accesses and modifications made in your file server environment in real time.
Learn more

Storage analysis
Analyze and identify redundant, outdated, and trivial data to declutter your file server and cut storage costs.
Learn more

$ Get Quote  Download
References


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