



INSIDER THREATS:

A guide to understanding, detecting
and preventing insider security incidents

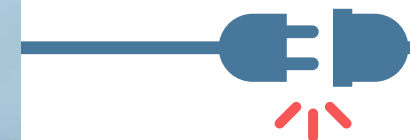
Introduction

Insider threats are a growing concern for business owners and IT experts. According to Verizon's 2020 Data Breach Investigations Report, **30 percent of data breaches directly involved internal actors**¹. Security threats that originate from within an organization are often the hardest to detect and prevent, especially since an insider has the trust and knowledge of infrastructure systems and data assets as well as authorized access to both.

Despite a 47 percent increase in insider threat incidents over the last two years, most organizations **don't have proper security systems** in place to detect or prevent insider incidents².



The goal of this eBook is to help you understand what insider threats are and explain the severity of the risks, costs and consequences these threats can inflict on your business. You will also get guidance on how to identify common indicators and warning signs as well as the security controls and strategies you need to prevent or mitigate the risks and impacts of insider incidents.



1. <https://enterprise.verizon.com/resources/reports/dbir/>

2. <https://www.observeit.com/cost-of-insider-threats/>

What Is an Insider Threat?

An insider threat is a security breach risk situation posed by people from within an organization. An insider can be a current or former employee, or a third party such as a business partner or contractor, who has authorized access to sensitive information and can divulge, modify or delete data records.

Based on the insider's intent, insider threats are often broadly classified into malicious or criminal insiders and unwitting or negligent insiders. Malicious insider threats are intentional, where the insider misuses privilege, trust and knowledge to disclose information for financial or personal gain. Negligent insider threats are unintentional in nature and are caused due to carelessness or human error.



Who Are Potential Insiders?

Anyone who has authorized or privileged access or insider knowledge about a company's infrastructure, operations, cybersecurity practices or data, is a potential insider threat.

They could be, current or former:

- 💀 Business owners or employees
- 💀 Contractors/sub-contractors
- 💀 Partners
- 💀 Vendors

Over 60 percent of insider incidents are caused by negligent employees or contractors,

23 percent by criminal/malicious insiders and 14 percent as a result of credential theft³.



Types of Insider Threats:



Malicious Insider:

The perpetrator could be a disgruntled employee or anyone with malicious intent who exploits their position and privilege to disclose sensitive information for personal or financial benefits, or to deliberately sabotage the company.



Negligent Insider:

A regular employee or an unintentional participant whose carelessness leads to a security incident. Many organizations fail to recognize this threat until it's too late.

Collusive Insider:

This type of insider has links with external bad actors whose motive is to compromise sensitive data or steal trade secrets or intellectual property by gaining access into the organization.

Third-Party Insider:

This type of insider could be a business associate, contractor or vendor who has some level of access to an organization's network and information. They may not be a direct threat but have access to unsecure systems or devices that could easily be exploited by cybercriminals.



Common Motivations Behind Insider Threats

The reasons behind insider threats vary. Here are some common motivations behind these threats:

a. Money/Greed:

Financial gain can be a huge motivator for malicious insiders. Whether it's customer information or trade secrets, data is an asset. For a malicious insider with access to an organization's network and information, this is an easy opportunity to make a quick buck.



b. Espionage:

Sometimes referred to as industrial espionage, economic espionage or corporate spying. It is the act of obtaining sensitive information or trade secrets and sharing it with another party for commercial or financial purposes.

c. Strategic/Competitive Advantage:

An organization could plant a mole in its competitor's company to obtain proprietary or customer information to gain a competitive edge. It could also be an insider sharing classified information to another competitor for personal gain or a departing employee taking confidential documents or customer lists to impress a new employer.

d. Revenge:

A disgruntled employee or a former employee who joins a competitor can deliberately or unwittingly disclose trade secrets.

e. Ideological/Political/Religious Agenda:

These insiders can be influenced by emotions or extremist moral or religious beliefs. They could also be primarily driven by national pride or have unique political objectives.

Why Your Organization Needs to Take Insider Threats Seriously

Since insider threats originate from within an organization, they are hard to detect and defend against, making them very dangerous. Unlike external actors who need access to penetrate an organization, an insider has legitimate access to a company's network and systems. An insider with bad intent can exploit these authorizations and easily bypass security measures to expose confidential information and compromise an organization.

Primary Asset Targets for Insiders

An insider can divulge sensitive data either deliberately or accidentally, which can be damaging and costly for an organization if it falls into the wrong hands. Some of the primary asset targets for insiders include:

- 💀 Critical operational or programming data for business
- 💀 Private customer or employee data
- 💀 IP or trade secrets
- 💀 Financial data

Global research shows that, on average, 17 percent of all sensitive files of a company are accessible to every employee⁴



4. <https://www.varonis.com/blog/data-risk-report-highlights-2019/>

Most Common Consequences and Costs of an Insider Attack



Apart from data and revenue loss, insider attacks can have a devastating impact on an organization.

Some of the common consequences of insider attacks include:

Loss of Critical Business and Customer Data:

An insider event can put critical business and customer data at risk, which can lead to lost confidence, negative reviews or credential theft.



Disclosure of Trade Secrets:

Losing intellectual property, such as trade secrets, blueprints or designs, can lead to a competitive disadvantage. A business rival can leverage the stolen information to get ahead of the competition.

Financial Costs and Losses:

Insider security incidents can result in significant revenue loss.



The total average cost of insider-related incidents is \$11.45 million – a 31 percent increase over the previous two years³.

Reputation and Brand Damage:

Diminished reputation is a long-term consequence of an insider attack. One successful insider incident can damage even the best of brands and reputations.

3. 2020 Cost of Insider Threats: Global Report

Some of the common consequences and costs of insider attacks include:



Loss of Customer Trust and Business:

This is perhaps the worst consequence of an insider attack. Although organizations can physically or operationally recover from an insider attack, regaining the trust of concerned customers and partners can be difficult.

Regulatory Compliance Violations and Fines:

An insider threat leading to disclosure of personal information can have serious consequences, including government fines, legal fees, lawsuits and in some cases, even imprisonment.

Loss in Market Value:

An insider threat can have a direct impact on market value.



For example, the Shopify data breach incident carried out by two members of its support team caused a 1.27 percent fall in Shopify's stock price⁵.

Loss of Productivity

From identification to remediation, an insider incident consumes a lot of time, which can lead to downtime and impact an organization's productivity.

5. <https://community.shopify.com/c/Shopify-Discussion/Incident-Update/m-p/888971/highlight/true#M197487>

Recent Insider Threat Incidents

Microsoft Security Incident **Exposes 250 Million Customer Records**

In December 2019, the Comparitech security research team discovered unsecured Microsoft databases that contained 250 million customer records collected over a period of 14 years⁶. These publicly accessible records included customer email and IP addresses, geographical locations, Microsoft support agent emails, case numbers and resolutions. The incident occurred due to the unintentional misconfiguration of security rules as a result of employee negligence.



Microsoft secured the servers within 24 hours after the leak was notified. Since the data did not contain any personally identifiable information and no malicious use of the data was detected, there were no serious consequences apart from Microsoft apologizing to its customers and reassuring them about their data security.

6. <https://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online/?sh=574b2d594d1b>

Recent Insider Threat Incidents

Hackers Attacked Twitter to Promote a Bitcoin Scam

In July 2020, hackers launched a successful phishing attack on Twitter employees and gained access to a Twitter administrator tool. They targeted 130 accounts and successfully gained access to 45, some of which included VIPs such as former President Barack Obama, billionaire businessmen Bill Gates, Elon Musk and Jeff Bezos, several renowned personalities, and popular company accounts like Apple and Uber⁷.



The compromised accounts were used to promote a Bitcoin scam that generated over **400 payments valued at \$121,000** from Twitter users. This insider threat incident caused a four percent drop in Twitter's stock price.

7. https://en.wikipedia.org/wiki/2020_Twitter_bitcoin_scam

Spotting Common Indicators or Warning Signs



Behavioral Indicators:

Although insider threats are difficult to identify and prevent, there are some common behavioral and digital signs that can help you recognize and stop them before they cause any damage.

- 💀 Dissatisfied employees, change in attitude, declining performance
- 💀 Ignores security practices or attempts unauthorized access to data
- 💀 Frequently in the office during unusual working hours
- 💀 Agitated or displays negative behavior towards colleagues
- 💀 Violates company policies
- 💀 Shows dissatisfaction towards work, talks about resigning or new opportunities



5. <https://community.shopify.com/c/Shopify-Discussion/Incident-Update/m-p/888971/highlight/true#M197487>

Spotting Common Indicators or Warning Signs



Digital/Network Indicators:

- 💀 Downloads, accesses or transfers unusually large amounts of data
- 💀 Attempts to access confidential data that's not related to one's job role
- 💀 Makes constant requests to gain access to tools and resources not required or associated with one's job functions
- 💀 Uses unauthorized storage devices like USB drives
- 💀 Collects or copies files from classified folders
- 💀 Emails confidential information outside the organization



5. <https://community.shopify.com/c/Shopify-Discussion/Incident-Update/m-p/888971/highlight/true#M197487>

Preventative Defensive Strategies

To err is human. **In fact, more than 80 percent of data breach incidents are generated by some form of human error¹.** Therefore, an insider threat management strategy and regular employee training are the best defense against these threats.

Here is a list of security controls and best practices that can help prevent and detect insider threats:



1. Regular Risk Assessments: Organizations must identify and evaluate the potential dangers of a security incident, determine its critical assets and implement appropriate risk management measures to protect those assets.



2. Require Identity Authentication: Implementing two-factor (2FA) or multifactor authentication (MFA) will fortify security controls by verifying user identity via multiple unique factors before granting access to systems or sensitive data records.



3. Access and Permission Management: Granting only the bare minimum user permissions or systems and data access required to perform a job reduces the risks of unauthorized access, especially those that can result from exposed or stolen privilege credentials.

Preventative Defensive Strategies

Here is a list of security controls and best practices that can help prevent and detect insider threats:



4. Security Awareness and Insider Threat Training: Organizations should periodically educate employees on data security, security policies and procedures, and common security threats.



5. Establish 'Baseline' Activities or Behaviors: Establish this within your organization to take advantage of automation and machine learning.



6. Ongoing/Continuous Monitoring: Monitoring employee online activity as well as any suspicious behavior can help detect threats and prevent security incidents from occurring.



7. Data Backup and Recovery Solutions: Organizations should implement efficient backup and recovery solutions to avoid costly downtime and severe consequences of insider threats.



PARTNER WITH AN IT AND CYBERSECURITY SPECIALIST

Insider threat incidents continue to rise, making every organization vulnerable. The unfortunate truth is that anyone with 'insider access or knowledge' poses a potentially serious threat to your business. This is why managing insider incidents all by yourself can be quite a challenge.

An IT and cybersecurity specialist, like a Managed Services Provider (MSP), can provide huge value and peace of mind for your business. They have the experience and specialized tools to not only help implement necessary security controls and employee training measures, but also detect and mitigate your exposure to insider threat risks.

To find out how you can efficiently mitigate and prevent insider threats to secure your organization's data, network and employees, contact us today!