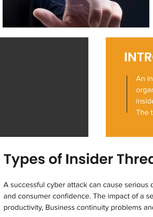
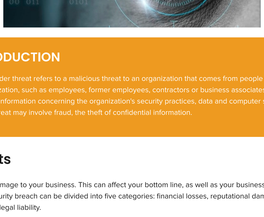
Skillmine
Technology • Consulting • Services

infosec
Miners

INSIDER THREAT





INTRODUCTION

An insider threat refers to a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems. The threat may involve fraud, the theft of confidential information.

Types of Insider Threats

A successful cyber attack can cause serious damage to your business. This can affect your bottom line, as well as your business' reputation and consumer confidence. The impact of a security breach can be divided into five categories: financial losses, reputational damage, Loss of productivity, Business continuity problems and legal liability.

Insider Type	Motivations	Example	Risks
Malicious	Making money or avenging a slight	Terminated employee plants a logic bomb to execute malicious code	Theft of core company intellectual property. Disruption of operations. Damage to company reputation.
Negligent	Ignorance or carelessness	Careless employee posts corporate data in public cloud container	Theft of core company intellectual property. Disruption of operations. Damage to company reputation.
Compromised	Oblivious to the risk they pose	An attacker uses compromised credentials to exfiltrate corporate data	Access to sensitive company systems or assets. Theft of core company intellectual property.

Source: keepnetlabs.com

Insider Threat Activities and Risk Factors

Threat Activities

Fraud: Covers stealing of a wide range of personal data, Including personal identification data, Financial Data, Billing Data etc.

Data Theft: The act of stealing information stored on computers, servers, or other devices with an intent to obtain confidential information.

System Sabotage: The act of intentionally exceeding or misusing an authorized level of access with an intention of harming an organization.

Risk Factors

Mismanaged Access: Insiders taking advantage of access to valuable data are involved in 15% of all data breaches.

Shadow IT: IT projects (like cloud services) that are managed outside of, and without the knowledge of, the IT department.

BYOD: Hacking, malware, and data leakage are the biggest BYOD security risks. Bad actors take advantage of unsecured devices, networks, and malicious apps to personal devices for company information.

Motivations for an Insider Attack

The underlying motivations of insiders are fraud (55%) and monetary gain (49%) the biggest factors that drive malicious insiders, followed by theft of intellectual property (44%). The ideal insider threat solution apprehends threats from all these vectors, including financial, personal and professional stressors as signs that a person is at risk or already an active insider threat

55% Fraud

49% Monetary gain

44% IP theft

Source: keepnetlabs.com

Average cost savings of implementing security tools and practices

- $3.4 million — User behavior analytics(UBA)
- $3.1 million — Privileged access management (PAM)
- $3 million — User training & awareness
- $2.8 million — Threat intelligence sharing
- $3.7 million — Strict third-party vetting procedures
- $2.7 million — Incident response management (IRM)
- $2.6 million — Employee monitoring & surveillance

* Data provided by 2020 cost of Insider Threats: Global Report by the Ponemon Institute

Source: ekransystem

Best Practices in Preventing and Detecting an Insider Threat

Employ risk assessments.
The organizations must employ risk assessment in an enterprise-wide landscape of information security, ascertaining their critical assets, and establishing a risk management procedure for defending those assets from both insiders and outsiders.

Implement division of duties and least privilege.
Separation of duties necessitates the implementation of least privilege: Authorizing people only for the resources they need to do their jobs.

Execute strict password and account management policies and practices.
Should your organization's computer accounts can be jeopardised, insider threats will have an occasion to bypass both manual and automated mechanisms, therefore adopt strict password and account management policies and practices.

Monitor your employee's online actions.
Monitoring the employees' online status is important to discover and examine suspicious insider actions before major severe outcomes arise.

Beware of the system administrators and privileged users.
Logging and monitoring should be performed by a combination of system administrators and privileged users. Therefore, extra attention must be applied to those users.

Actively shield against malicious code.
Privileged users like system administrators can array logic bombs or install other malicious code on the system or network. These types of attacks are difficult to detect ahead of time, still, practices can be realised for a speedy detection.

Apply layered defence against remote attacks.
Remote access policies and procedures must be created and executed very carefully since insiders tend to feel more confident and less restrained when they have little fear of examination by coworkers.

Monitor and respond to suspicious behaviour.
In addition to monitoring online actions, organizations should closely monitor other suspicious or disruptive behaviour by employees in the workplace.

Computer and network access management after employee termination.
When employment is terminated, it is important that the organization have a job termination procedure that disables all of the employee's access points to physical locations, networks, systems, applications, and data.

Execute secure backup and recovery methods.
It is important that organizations always think for the possibility of an attack or disruption and implement secure backup and recovery policies.

Create an insider threat control checklist or documentation.
Insider threat control checklist or documentation will help to secure your organization against vulnerabilities for an attack.

Possible Consequences of an Insider Attack

- Financial Losses
- Loss of customer's trust
- Ruined business reputation
- Regulatory fines
- Disclosure of trade secrets
- Falling share prices
- Compromise of customer's data

The cost of insider threats keeps rising

These expenditures continue to rise year after year.
Monitoring, investigation, escalation, incident response, containment, ex-post analysis, and remediation costs for a single insider threat occurrence increased from $513,000 to $756,760.

Source: Ponemon Institute 2018 & 2020 Cost of Insider Threats: Global Reports

2017: 8.76 million

2019: 11.45 million

Total average cost of insider threats

Conclusion

Security threats caused by insiders can happen to any company. And the consequences of insider-related breaches are often devastating. However, in most cases, it's possible to detect and stop insider attacks with the help of dedicated cybersecurity tools.

The following are today's largest cybersecurity issues, according to the most recent insider threat cybersecurity statistics:

- Preventing insider attacks is becoming more expensive.
- The most typical cause of a data leak is user error.
- Users with no privileges are just as harmful as those with privileges.
- Insider threat deterrence must take center stage in any cybersecurity strategy.

The biggest threat will come from where you least expect

-Myrna Soto

SKILLMINE CYBER SECURITY TEAM

Skillmine
Technology • Consulting • Services

India | KSA | UK | USA

#46/4, Novel Tech park, Kudlu Gate, Bangalore Karnataka-560 068

+91 9920663515

www.Skill-mine.com

info@Skill-mine.com