span

Insider Risk

E-BOOK

NEVEN

Zitek

CYBER SECURITY BUSINESS
SOLUTIONS DIRECTOR

January 2025

Insider risk

Insider risk is a threat or harm that comes from individuals within an organisation who have authorised access to its systems, networks, or data. These individuals - referred to as "insiders" - can either intentionally or unintentionally cause damage, data breaches, fraud, or other harmful activities impacting confidentiality, integrity, or even the availability of information and/or information systems.

Types of insider risk

Insider risk can be categorised into several types, depending on the nature of the threat.

Malicious Insider Threats:
Stealing sensitive or proprietary information, such as intellectual property, customer data, or financial records, often for resale, personal use, or to benefit a competitor. Deliberately causing damage to the organisation's systems, data, or infrastructure, such as deleting critical files, introducing malware, or disrupting services to hurt operations. Engaging in fraudulent activities like financial fraud, manipulation of records, or misappropriating company funds for personal gain.

Unintentional Insider Threats (Accidental Risk):
Unintentional mistakes such as sending sensitive information to the wrong recipient, misconfiguring security settings, or accidentally disclosing confidential data. Insiders losing company-issued devices like laptops, smartphones, or USB drives that contain sensitive data without proper data protection mechanisms such as encryption, which may then fall into unauthorised hands.

Negligent Insider Threats:
Using weak passwords, failing to update software, or neglecting to follow proper access controls, making it easier for malicious actors to exploit vulnerabilities. Failing to adhere to organisational security policies, like sharing passwords, leaving devices unattended, or bypassing security protocols in favour of convenience - such as “shadow IT” file sync services that enable users to sync business documents with computers and mobile devices accessible anywhere and anytime. When such unmanaged devices are compromised attackers gain access to sensitive corporate data without any knowledge of the impacted organisation. Not properly managing or disposing of sensitive information, such as leaving documents containing confidential data in public areas or failing to shred sensitive paper records.

Privilege Misuse:
An employee who has more access rights or privileges than necessary for their job, allowing them to access, modify, or delete sensitive data. An insider who uses their access to perform unauthorised actions, such as accessing data outside their role or circumventing security measures.

Social Engineering by Insiders:
An insider unintentionally sharing login credentials or other sensitive information after falling victim to a phishing attack, which is then exploited by an external attacker. Insiders who, due to a lack of training or awareness, are manipulated by attackers to provide unauthorised access to critical systems or data.

Compromised Insiders:
Attackers stealing or guessing an insider's login credentials, thereby using them to access sensitive data or systems. Insiders who are coerced or blackmailed by external parties into providing access to organisational resources or engaging in malicious activities.

Departing Employee Risks:
Departing employees taking sensitive data, intellectual property, or trade secrets when leaving the organisation, often to use in a new job or to benefit a competitor. Former employees may sabotage systems or data during their exit process, for example, by introducing malware or deleting crucial files. Employees who leave may still have access to company systems if proper offboarding processes aren't followed, posing a risk of unauthorised access or data leakage.

Consequence of insider risk

Insider risks can have significant consequences for organisations, especially if not managed properly. Here are main impacts:

Financial Losses
Insider threats can lead to direct financial losses through theft or fraud, and indirect costs related to resolving data breaches.

Business Disruption
Critical operations can be interrupted, leading to downtime and loss of productivity.

Regulatory Non-Compliance
Failing to manage insider risks can result in non-compliance with regulations, leading to fines and legal penalties.

Damage to Reputation
Incidents can harm an organisation's reputation, affecting customer trust and business relationships.

Loss of Competitive Advantage
Sensitive information, such as trade secrets, can be leaked, giving competitors an edge.

Employee Morale
Security incidents can create a stressful work environment, affecting overall employee morale and productivity.

How to manage insider risk

Managing insider risk is a critical aspect of maintaining organisational security, ensuring data protection, and safeguarding intellectual property. Given the wide range of potential consequences of insider threats, effective management involves a combination of proactive strategies, technological tools, policies, and a strong organisational culture.

Here are best practices to help manage insider risk:

1. Establish Clear Policies and Procedures

Information Asset inventory is a crucial step in insider risk management. It helps in understanding the importance and impact of information on business processes. Policies and technical measures should be designed to protect information in proportion to their value and impact on business processes.

Risk Assessment: Regularly assess the risks associated with each information asset. This includes identifying potential insider threats and vulnerabilities. Please remember that risks will change over time and that risk assessment is an ongoing activity.

Access Controls: Implement strict access controls based on the principle of least privilege. Ensure that employees only have access to the information necessary for their roles. Note that data classification provides the foundation for implementing effective access controls, ensuring that data is protected according to its value and sensitivity.

Code of Conduct: Create clear policies regarding acceptable behaviour, confidentiality, and security standards. Ensure that employees understand their responsibilities concerning data and information security.

Insider Threat Policy: Develop a specific policy for managing insider threats, detailing the procedures for detecting, reporting, and responding to suspicious behaviour or incidents.

2. Employee Awareness and Training In Span Cyber Security Centre

span | Cyber Security Center

Ongoing Security Training: Regularly educate employees about cybersecurity risks, social engineering tactics, and how to recognise and report suspicious activity. This should include specific training on insider threats and how they can be detected early.

Behavioural Training: Teach employees about the importance of ethical behaviour, company values, and the potential consequences of engaging in or overlooking insider threats.

Phishing and Social Engineering Simulations: Conduct regular phishing tests and simulations to teach employees how to spot phishing emails and other common social engineering tactics used to exploit insiders.

3. Implement Strong Access Controls

Least Privilege: Limit access to sensitive systems, data, and information to those who need it for their role, and ensure access is reviewed regularly.

Multi-Factor Authentication (MFA): Require MFA for accessing critical systems to add an additional layer of security beyond just passwords.

Separation of Duties: Ensure that critical tasks require multiple individuals to complete, reducing the risk of one insider having too much control over a process.

Regular Access Audits: Conduct periodic reviews of who has access to what and remove access for employees who no longer require it.

4. Monitor and Analyse User Activity

User Behaviour Analytics (UBA): Use UBA tools to monitor and analyse user behaviour for signs of unusual or risky activity. These tools can help detect potential insider threats by identifying deviations from normal patterns.

Logging and Auditing: Implement robust logging to track activities, such as access to sensitive data and systems. Regularly audit logs to detect any suspicious or unauthorised actions.

Real-Time Monitoring with Span Security Operations Centre: Use real-time monitoring systems that can immediately alert security teams about any anomalies or suspicious activities, such as accessing unauthorised files or data transfers.

5. Create a Strong Incident Response Plan

Rapid Detection and Response: Develop a response plan that ensures quick detection, containment, and mitigation of insider threats. The plan should clearly outline steps for investigating incidents and handling legal, regulatory, and PR ramifications.

Reporting Mechanisms: Encourage employees to report suspicious activity anonymously. Establish a clear and confidential reporting process for employees to alert management about potential insider threats.

Incident Simulations: Regularly run security incident drills to ensure the team is prepared for real-world scenarios. Practice responding to insider threats, data breaches, and other security incidents.

6. Leverage Technology Solutions

Data Loss Prevention (DLP): Implement DLP tools to monitor and restrict the movement of sensitive information across networks and endpoints. This can help prevent unauthorised data transfers by insiders.
Endpoint Detection and Response (EDR): Use EDR tools to monitor and respond to suspicious activity on devices, such as laptops, smartphones, or workstations, that could be exploited by insiders.
Encryption: Encrypt sensitive data both at rest and in transit to ensure that even if data is accessed or stolen, it remains protected.

Digital Rights Management (DRM): Use DRM tools to prevent the unauthorised distribution of sensitive content, such as intellectual property or trade secrets.

7. Monitor and Control External Access

Third-Party Risk Management: Assess the security practices of third-party vendors or contractors who have access to your systems and sensitive data. Make sure they adhere to the same security standards as your internal teams.

Privileged Access Management (PAM): Control and monitor external contractors and third-party users with privileged access to critical systems. Ensure that access is temporary and limited to specific tasks.

By combining these practices into a cohesive insider risk management program, organisations can significantly reduce the likelihood and impact of insider threats, helping safeguard their assets, reputation, and long-term success.

How Span can help with establishing insider risk management?

Starting to manage insider risk is essential to protect your organisation from potential threats like data theft, fraud, or unintentional leaks. We can help by conducting a comprehensive risk assessment to identify vulnerabilities, developing clear policies for data handling and acceptable use, and ensuring these policies align with industry standards. We also provide customised employee training to raise awareness about insider threats and their role in prevention.

Additionally, we can assist with implementing strong access controls, provide real-time monitoring, and build an effective incident response plan to quickly address any security breaches.

Partnering with us will help you create a robust insider risk management strategy and improve your overall security. Encourage a culture where employees feel comfortable reporting suspicious behaviour without fear of retaliation. Finally, continuously assess and update your insider risk management strategies to adapt to new threats and changes in your organisation.

Contact us at: info@span.security