Guide

Guide to Proactive Insider Risk Management

QOHASH

In today's interconnected and data-driven world, organizations face a multitude of security risks, including those that originate from within. Insider risks, often overlooked or underestimated, can pose significant threats to the confidentiality, integrity, and availability of an organization's sensitive information and critical assets. From intentional malicious activities to accidental mishaps, insider incidents can result in financial losses, reputational damage, legal liabilities, and even the compromise of national security.

It is important to note that insider risk management is not a one-time endeavor but an ongoing process that requires regular assessment, adaptation, and improvement. By prioritizing insider risk management, organizations can not only protect their valuable assets but also foster a culture of trust, integrity, and accountability among their employees.

> **Companies that conduct a formal Insider Threat Program have 50% fewer chances of encountering a data breach.**
>
> (2022 Cost of Insider Threats Global Report, Ponemon)

The greatest asset an organization possesses can also pose the greatest risk. A fundamental factor behind insider threats lies in the very people who form an integral part of the system. Paradoxically, while most security tools focus on analyzing computer, network, or system data, they often overlook the crucial human element that can potentially unleash devastating consequences. According to IBM, insider threats are cybersecurity threats that originate with authorized users—employees, contractors, business partners—who intentionally or accidentally misuse their legitimate access, or have their accounts hijacked by cybercriminals.

According to the findings outlined in the Verizon 2021 Data Breach Investigations Report, insiders were found to be liable for approximately 22% of security breaches. The surge in Insider Threats is a cause for apprehension, given that such incidents come with hefty costs for organizations, leading to breaches that expose sensitive customer, client, and company data. Moreover, these types of threats are notoriously difficult to preempt. This guide aims to provide an all-encompassing set of strategies for the implementation of proactive measures in insider risk management processes.

Different Types of Insiders

Malicious Insiders: Malicious insiders are individuals who purposefully exploit their privileged access and misuse it to cause harm to the organization. Motivations behind their actions can vary, including revenge, financial gain, ideology, or even personal grudges. These individuals have valuable knowledge of the organization's systems, processes, and sensitive information, making them capable of executing devastating attacks. Malicious insiders may engage in unauthorized data access, theft, sabotage, or even intentionally leaking confidential information. Their actions can result in severe financial loss, reputational damage, or compromise of critical assets.

Compromised Insiders: Compromised insiders are individuals who unwittingly become a threat to the organization due to external factors. These individuals may have fallen victim to phishing attacks, social engineering, or other methods employed by external threat actors to gain control over their accounts, credentials, or devices. Once compromised, these insiders inadvertently facilitate unauthorized access to sensitive systems or data. Attackers exploit their compromised accounts to carry out malicious activities within the organization, often remaining undetected for extended periods. Compromised insiders can inadvertently trigger data breaches, install malware, or provide unauthorized access to external threat actors.

56% of incidents experienced by organizations were due to negligence, and the average annual cost to remediate the incident was $6.6 million.

(2022 Cost of Insider Threats Global Report, Ponemon)

Negligent Insiders: Negligent insiders, unlike the previous two categories, do not pose a threat out of malicious intent. Instead, their actions stem from **carelessness, lack of awareness, or disregard for security protocols and policies.** Negligent insiders may unknowingly cause harm through actions such as falling victim to phishing attacks, failing to apply software updates, mishandling sensitive data, or violating security policies. While their actions may not be intentional, the impact can be just as damaging. Negligent insiders often create vulnerabilities that can be exploited by external threat actors or inadvertently cause data breaches.

Impact of Insider Risks

Insider attacks have the potential to result in a myriad of detrimental consequences, spanning from non-compliance penalties to a loss of customer trust. Real-life cybersecurity incidents have demonstrated several common outcomes that organizations must be wary of.

Financial Losses: Insider attacks can have significant financial ramifications for organizations. This can result from various factors, such as the costs associated with investigating and remediating the incident, potential legal expenses, loss of business opportunities, and decreased productivity. Additionally, organizations may suffer financial losses due to theft of funds, unauthorized access to financial systems, or fraudulent activities carried out by malicious insiders.

Tarnished Business Reputation: Insider attacks can severely damage the reputation of an organization. News of a security breach caused by an insider can erode customer confidence and trust in the organization's ability to protect their sensitive information. The negative publicity and media coverage surrounding the incident can lead to customer attrition, difficulty acquiring new customers, and a long-lasting stigma associated with the organization's brand.

Regulatory Fines: Data protection regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), impose strict requirements on organizations for safeguarding customer data. In the event of an insider attack resulting in unauthorized access or exposure of customer data, regulatory bodies may levy substantial fines on the organization for non-compliance. These fines can be significant, further exacerbating the financial impact of the incident.

Compromised Customer Data: Insider attacks can result in the unauthorized access, theft, or exposure of customer data. This sensitive information may include personally identifiable information (PII), payment card details, login credentials, or other confidential data. The compromised customer data can be exploited for a variety of malicious activities, such as identity theft, financial fraud, or targeted phishing campaigns, leading to substantial harm to the affected individuals and potential legal liabilities for the organization.

Loss of Customer Trust: Perhaps one of the most significant consequences of insider attacks is the erosion of customer trust. Customers place their faith in organizations to safeguard their sensitive information. When insiders breach that trust, customers may feel betrayed and choose to take their business elsewhere. Rebuilding customer trust after a security incident can be a challenging and lengthy process, requiring transparent communication, enhanced security measures, and proactive efforts to demonstrate a renewed commitment to data protection.

Understanding the Risks

Insider attacks pose a heightened level of danger due to three critical factors:

1. Insiders often do not engage in malicious actions, making it significantly more challenging to identify harmful insider activities compared to external attacks.

2. Insiders possess intricate knowledge of an organization's cybersecurity vulnerabilities, enabling them to exploit these weaknesses effectively.

3. Insiders are intimately aware of the location and nature of sensitive data within the organization, granting them the ability to target and exploit these valuable assets. Insiders can easily exploit their privileged access where the same access that enables them to do their work also grants them direct access to data they can exploit or leak if they have malicious intent.

These combined factors make insider threats a formidable challenge to detect and mitigate effectively in comparison to external attacks.

Understanding the Signs

While harder to prevent, it is imperative for organizations to possess the ability to discern atypical behaviors that could signal an insider threat. Presented below are five key behaviors that may serve as signs of insider risk:

Unusual Access Patterns: Keep a vigilant eye on employees who access files, systems, or sensitive information beyond their regular working hours or unrelated to their job responsibilities. Maintaining meticulous monitoring of access controls and promptly addressing sudden alterations in permissions for files or folders containing sensitive information is crucial.

Unexplained Data Modifications: Remain vigilant for unexplained or unauthorized alterations made to critical data or files by individuals who possess access privileges. Unauthorized changes may indicate insider tampering or attempts to conceal illicit activities. Even seemingly minor acts such as file renaming might serve as tactics to hide the gradual accumulation of sensitive information.

Unusual Data Flow: Be attentive to anomalies in data flow, such as excessive file downloads or uploads, particularly to external or unauthorized destinations. Instances of suspicious activity between corporate and personal networks, clouds, or accounts should be scrutinized. Questioning the motive behind an employee sending a copy of a critical document to their personal email address is essential.

Hostile and Planned Departure: Exercise caution when encountering employees who exhibit hostility or express resentment toward the organization, colleagues, or management during their departure process or shortly before leaving. Conversely, individuals planning their departure might conceal risky behavior and move critical data while maintaining a low profile. It is essential to have a robust off boarding process that allows retrospective analysis of an employee’s data movement.

Inconsistent Work Patterns: Pay heed to individuals who demonstrate inconsistent work patterns, such as working irregular hours or engaging in activities beyond their usual scope shortly before departing from the organization. These irregular behaviors might indicate an employee preparing to carry out malicious actions or exploit vulnerabilities. While a single policy deviation might not be cause for alarm, it is the accumulation of such behavior that can ultimately prove costly for the company in the long run.

Understanding the Motives

Insider incidents can stem from various motives, each driven by different factors and circumstances. While motives can vary depending on the individual and the organization, here are some common reasons behind insider incidents:

Financial Gain: One of the most prevalent motives is financial benefit. Insiders may commit acts such as embezzlement, fraud, or intellectual property theft to gain personal financial advantage. This could involve stealing funds, misusing company credit cards, or leaking proprietary information to competitors for monetary rewards.

Revenge or Resentment: Disgruntled employees who feel mistreated, overlooked, or wronged by the organization may seek revenge as a motive. These individuals may sabotage systems, delete critical data, or leak sensitive information to tarnish the organization's reputation or cause financial harm.

Personal Curiosity or Thrill-seeking: Certain insiders may act out of curiosity, seeking unauthorized access to systems or data for personal enjoyment or thrill. They may exploit their technical skills to explore sensitive information without malicious intent but still cause potential harm by breaching security protocols.

Accidental or Negligent Actions: Not all insider incidents are intentional. Negligence, lack of awareness, or inadequate training can lead employees to make mistakes that result in data breaches or system disruptions. Accidental disclosure of sensitive information or falling victim to phishing attacks are common examples of unintentional insider incidents.

Insider Risk Management Framework

An insider risk management framework serves as a structured plan to identify, assess, manage, and mitigate risks that originate from within an organization. A robust framework is designed to guard against both accidental and malicious insider threats and aligns with the organization's broader information security and risk management strategies. The following will delve into the goals and objectives of an insider risk management framework, the core elements of a robust framework, and discuss the role of technology in managing insider risks.

Goals and Objectives

The primary goal of an insider risk management framework is to establish an effective system of processes, controls, and technologies that safeguard the organization's critical assets and data from potential insider threats. The objectives of a robust insider risk management framework often include:

Detecting and Preventing Insider Threats: The framework should enable the organization to identify potential insider threats before they can cause harm and implement countermeasures to prevent security incidents.

Risk Assessment and Analysis: The framework should facilitate the assessment of insider risk, including identifying potential sources of risk, measuring the possible impact, and prioritizing risks based on their severity.

Compliance with Regulations: Many industries have regulations that mandate certain levels of data protection and privacy. The framework should ensure the organization meets these regulatory requirements.

Promoting a Security-Conscious Culture: Beyond technical controls, the framework should promote a culture where all employees are aware of the importance of information security and their role in protecting the organization's assets.

Core Elements of a Robust Framework

A robust insider risk management framework includes several critical elements:

Policy and Procedures: The framework should start with clear policies and procedures that define acceptable and unacceptable behavior, outline the responsibilities of different roles, and provide guidance on how to respond to potential insider threats.

Risk Assessment: Regular risk assessments should be carried out to identify and prioritize potential sources of insider risk. This includes background checks during recruitment and ongoing behavioral analysis during employment.

Training and Awareness: Employees should be regularly trained on the importance of information security, how to handle sensitive data appropriately, and how to recognize and report potential security threats.

Access Controls: The principle of least privilege should be adopted, ensuring that employees have only the access they need to perform their jobs and nothing more. Access should be regularly reviewed and immediately revoked when no longer required.

Monitoring and Response: The framework should include systems for monitoring user behavior, detecting potential security incidents, and responding effectively when incidents occur.

Technology and Tools: Technology plays a vital role in an insider risk management framework, to not only detect and prevent insider threats but also to automate processes and provide actionable intelligence.

Select your Insider Risk Management Tool

Technology should be used in conjunction with a strong organizational culture, clear policies and procedures, regular training, and effective governance mechanisms. Only through a balanced, holistic approach can organizations effectively manage the complex and evolving challenge of insider risk. When selecting an insider risk management tool, the following features should be considered.

Proactive Approach vs Reactive Approach to Insider Risk Management

The overarching goal of any risk management strategy should ideally be incident prevention rather than merely having an incident remediation plan. The power of real-time alerts regarding risky behavior provides teams with the opportunity to act preemptively, averting potential incidents before they transpire.

To effectively counter insider threats, having constant visibility and control over insider activities is paramount. This allows organizations to adopt a proactive stance in safeguarding against insider threats, emphasizing prevention over reaction. By doing so, potential risks can be identified and neutralized before they escalate into serious incidents, enhancing the overall security posture of the organization.

Risk Quantification: It's indispensable for information security teams to have proactive indicators and benchmarks that enable them to monitor and measure risk as it escalates. These quantifiable metrics provide a clear understanding of threat levels and the possible impact in real-world scenarios, allowing teams to prioritize and manage risks effectively.

Data Element Tracking: Traditional approaches to risk assessment, such as merely observing file activity - a feature provided by 99% of the tools available in the market - are no longer adequate. A single file might contain thousands of data elements, each holding potential risk. A comprehensive assessment of risk necessitates deep visibility into the granular data within each file, enabling a more accurate determination of potential vulnerabilities and risks.

Historical Record of Data Movement: When an incident takes place, swift response is crucial. Keeping track of data elements enables a comprehensive historical record of data movement among employees. This feature eradicates the need for time-consuming manual investigations, providing a faster, more efficient way to trace data movement and locate potential security breaches.

Intelligence Dashboard: An efficient insider risk management tool should feature an intelligence dashboard that surfaces actionable insights. A centralized view of quantified risk across various business segments is essential. This dashboard should not only provide an overview of the risk landscape but also deliver actionable intelligence that can be used to drive risk mitigation strategies, ensuring a proactive approach to risk management.

About Qohash

Qohash is a leader in data security software development, delivering innovative and user-friendly security technologies that provide businesses with visibility and control over their sensitive customer data. Since its founding in 2018, Qohash has rapidly scaled its operations to offer solutions that empower organizations to maintain continuous oversight of their security posture. Currently available in the U.S. and Canada, Qohash's mission is to protect the world's most sensitive data.

To learn more about Qohash's insider risk management capabilities, visit qohash.com