TERAMIND

Tackling Insider Risk

The Path to Mitigation

It is becoming common for organizations of any nature to be violated by data breaches.

Breaches occur when an organization's security infrastructure is penetrated and sensitive data is accessed. The malicious path individuals take to penetrate an organization's data varies. Because of this variation, organizations must be open minded to different, evolving threats and be prepared for them.

19% of data breaches that occur are caused by individuals with inside access into a company.[1]

These negligent or malicious individuals are given the name Insider Threats. Insider Risk is the practice of proactively creating a culture that reduces the risk of an insider threat. An insider is any individual - contractor, employee, manager or CEO - that has access to sensitive company data, and they have the administrative rights to inflect changes on that data. An insider threat can steal, destroy or transfer data from an organization. They can take many different forms; which we will further explore in this paper.

Data breaches due to insider threats are ever-present, and many breaches that begin outside the organization are assisted by an insider. The silver lining is that organizations can stay ahead of these threats by using technology to track behavior changes that can indicate a positional shift in employees. Sentiment can be a strong indicator of shifts that might make someone vulnerable to being recruited by outside threat actors.

What is an Insider?

An insider, in the security world, refers to anyone who has privileged access to sensitive data inside your organization.

Four Types of Insider Threats

Let’s look further at the insider threats organizations must look for. **There are four types of insider threats that are commonly referred to in the cybersecurity world.**

The Oblivious Insider

Is any individual who has access to valuable company data. This insider is entirely unaware that their credentials may be compromised, leading the company to a breached state where an outsider may be doing reconnaissance or actively exfiltrating data via their account.

The Accidental Insider

Is an individual who is purposefully seeking to cause harm to an organization. A malicious insider comes in many forms. This insider has the purpose of malicious intent. This insider is simply trying to perform their job and may not realize they have accidentally exposed data, as in situations where S3 buckets are internet-facing and open to the public, but also contain sensitive data. Accidental insider activities can range from misconfigurations, to unknowing compliance violations, to succumbing to social engineering or phishing attempts.

The Malicious Insider

Is an individual who is purposefully seeking to cause harm to an organization. A malicious insider comes in many forms. This insider has the purpose of malicious intent. They may go through several hoops to reach their goal of destroying or stealing data. They may be a disgruntled employee destroying data as they leave or an employee who is secretly transferring sensitive data files offsite to make a profit on the darknet.

In 2023, a malicious insider at Tesla intentionally compromised of 75,000 internal employees' personally identifiable information (PII), among other sensitive data. The disgruntled employee leaked: [2]

- ✓ Employees' personal information (their names, addresses, phone numbers, and Social Security numbers)
- ✓ Customer bank details
- ✓ Production secrets
- ✓ Customer complaints about Tesla's Full Self-Driving (FSD) features

Finally, we have the professional insider.

This insider may be acting under the facade of a real employee while secretly compromising the organization. A professional insider may seek out an organization with vulnerabilities to target or simply search for vulnerabilities where they are employed. Once a malicious insider has obtained the data, they sell the data on darknet for profit.

In a massive "accidental insider" attack on MGM Hotel & Casino in 2023, it appears the a Help Desk agent changed credentials for hackers to gain access after a social engineering phone call. This led to a total shutdown of the organization's IT systems – AKA revenue streams – for days. [3]

Insider Attacks: Where's the Enemy?

Looking at the Verizon Data Breach Investigations Report for 2023, researchers found that **89% of privilege misuse cases were financially motivated, followed by a "grudge" at 13%.** [1]

That's over half of the attacks on sensitive data. These threats go undetected for months, because they can be perceived as everyday activity. For example, an employee might send data to a personal email or delete files once a week.

"Over a quarter (28%) of attacks involved insiders. The insider threat can be particularly difficult to guard against, it's hard to spot the signs if someone is using their legitimate access to your data for nefarious purposes." [4]

Furthermore, it may be difficult to prove an employee or vendor is guilty of suspicious activity without having concrete forensic evidence.

62% of employees involved in an insider attack were seeking to establish a second income from their employer's data. 29% of employees stole data to take with them to future jobs and 9% were looking to sabotage their company; the remaining employees were attributed to being negligent. [5]

The latter percentage of employees are acting destructive in nature, both with a purpose and/or carelessness. Data is being manipulated, stolen or breached either way.

Social Engineering is a process where threat actors dupe unsuspecting employees into becoming accidental insiders. **Social Engineering accounted for 17% of Breaches and 10% of all Incidents in 2023.** [1]

Insider threats – accidental or intentional – are not a matter of *if*, but *when*. Better to be prepared than caught off-balance, because awareness training alone has done little to nothing in stemming phishing and social engineering effectiveness over the years. [6]

Forward Progression: Insider Threat Mitigation

The first step in insider threat mitigation is becoming aware of all four types of threats and preparing mitigation methods for each. There are standard prevention tactics that organizations can use to combat the insider threat. Firewalls, antivirus software and backing up your data are not enough. They are simply the beginning framework.

Coupled with traditional security tools, other forms of data loss prevention tactics are not enough for the insider threat. Standard prevention tactics like performing employee background checks, implementing least privilege access for unnecessary areas and training employees on cyber threats are important.

However, the effectiveness of all of these tactics fluctuate. An employee with a clean background check can evolve into a criminal. Least privilege access policies can become ineffective; if an employee uses someone else's computer or accesses another's credentials. There is no guarantee that employees will abide by the policies, techniques and tools explained in any training sessions. Further, changes in workflow or structure can lead to a disgruntled employee that can potentially become an insider.

Modern day technology advancements have led us to a much more comprehensive and effective way to mitigate the insider threat. Now, organizations can identify threats to their sensitive data by using monitoring detection and behavioral analytics software.

Monitoring software operates through machine learning and behavioral analytics, once the software is deployed it will identify organizational trends. From here, a profile of normal behavior is established. Any trend variation or unusual activity will be noted.

This technology is a progressive and proactive approach to insider threat mitigation. It allows automated detection and alerts to be delivered in real-time to the admin. Threats are detected quicker and forensic evidence of the breach can be provided.

Data can be used for training methods, or an employee can be stopped in mid-action from performing a bad data hygiene practice. The training benefits of monitoring software are not to be understated. Using interactive, real examples of what to do vs what not to do is the content that needs to appear in training sessions rather than a slideshow.

The findings from monitoring software are impactful for privileged access training as well; those users have extensive access to sensitive data. It is pertinent to keep privileged access users current in training to stay on top of threat trends and risk mitigation.

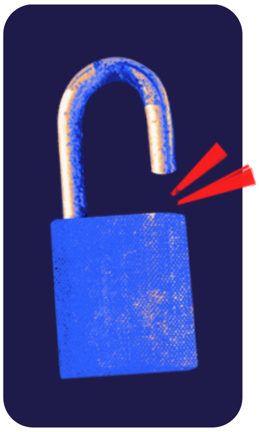
Employers can monitor file transfers, emails and behavioral trends to determine if an insider is stealing sensitive data. Through an anomaly detection feature, when an employee performs an undesirable action - categorized by the administrator - notification is swift and detailed. Some changes recorded are: a shift in working hours (working at times when nobody else is), a decrease in productivity, missing deadlines or meetings or completing tasks outside of their regular duties. [7]

A comprehensive dashboard compiles all activity monitored within the organization, whether employee or third party vendor related.

Let's refer back to our four insiders with examples of how user analytics and monitoring can prevent each of these scenarios.

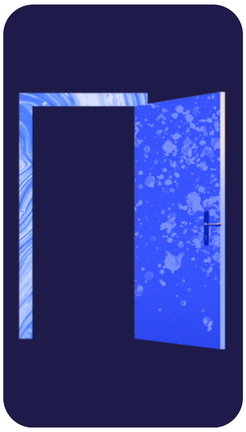
The Oblivious Insider

Has opened a seemingly typical vendor email detailing that the employee must update credentials. Through email monitoring, the employer can identify the dangerous email and halt the interaction.



The Accidental Insider

Who carelessly breezes past security measures has clicked on an infected link. Monitoring software will alert to the link as well as allow the employer to locate the source of the link and perform any necessary damage control.



The Malicious Insider

Was just fired and is searching for data to destroy. Monitoring software will alert you to any files that are being tampered with allowing you to intervene.

The Professional Insider

Is attempting to exploit a company vulnerability to steal data for profit. Advanced DLP coupled with monitoring software provides data visibility, allowing you to view and halt any data transfers.

Teramind software offers organizations the threat detection, monitoring and security measures necessary to arm themselves against the influx of insider threats coming our way.

Works Cited

1. Verizon DBIR 2023: Seal, Tara. (2018). Infosecurity Magazine. Insider Threats Responsible for 43% of Data Breaches. Retrieved from https://www.infosecurity-magazine.com/news/insider-threats-reponsible- for-43/.

2. Kohen, Isaac. Hackernoon. (Nov. 27, 2023). (March 22, 2018). 5 Examples of Insider Threat-Caused Breaches that Illustrate the Scope of the Problem. Retrieved from https://hackernoon.com/data-breach-what-teslas-biggest-insider-threat-in-2023-can-teach-us-going-into-2024

3. Murphy, Margi. Bloomberg Media (Oct. 3, 2023). Murphy, Margi. Bloomberg Media (Oct. 3, 2023). Ashford, Warwick. (August 15, 2016). Computer Weekly. Sage Data Breach Underlines Insider Threat. Retrieved from https://www.computerweekly.com/news/450302518/Sage-data-breach- underlines-insider-threat.

4. Verizon. 2018 Data Breach Investigations Security Report. 2018. Verizon Enterprise. Retrieved from https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_x g.pdf.

5. Townsend, Kevin. Security Week, (July 19, 2023): https://www.securityweek.com/security-awareness-training-isnt-working-how-can-we-improve-it/#:~:text="Security%20awareness%20programs%20can%20sometimes,time%20to%20stop%20an%20attack."

6. Thudium, Megan. (September 4, 2017). IT Security Central. 4 Different Types of Insider Attacks. Retrieved from https://itsecuritycentral.teramind.co/2017/09/04/4-different-types-of- insider-attacks-infographic/.

7. https://www.teramind.co/solutions/insider-threat-detection

TERAMIND

Request Your Custom Demo Now

Get a Demo