SmartVault

Stop and Spot Insider Breaches

5 Tips for Ensuring the Internal Security of Your Business

Introduction

Protecting Against the Most Common Problems

Insider threats and data breaches are among the most common problems companies encounter in protecting sensitive data. According to a recent Insider Threat Report, insider threats have increased in frequency and cost in the past two pandemic years.

Indeed, there are multiple layers of protection available to use, and for some companies, they are already in place. However, the number of internal data breaches has doubled since 2020, and there are more risks associated with negligent employees who have been working from home.

What is an Insider Threat?

Insider threats refer to any potential security or data breach that a company has through employees, business partners, contractors, or any other internal user who has access to internal resources. The company1s access permissions, documents, and other critical assets are a potential threat if the company data is stolen through their personal computer or access controls.

The costs of internal cyber-attacks are high, and they can reflect upon a company in various ways, such as:

- Disrupt ion of services
- Technology
- Direct or indirect labor
- Process changes
- Cash outlays
- Revenue losses
- Overhead

The Definition of an Insider Threat in Cybersecurity

The Cybersecurity and Infrastructure Security Agency defines insider threats as a situation where a current or former employee, contractor, or partner creates the opportunity, directly or indirectly, for others to access sensitive information and damage the organization. Depending on their role in the organization, and the type of access they have to login credentials, documents, and other types of data, they create vulnerabilities and security risks for the organization.

Once stolen through an insider security breach, third-party cybercriminals can use the data for espionage, sabotage, unauthorized disclosure of information to the public, or direct action on this data to damage its resources or make it disappear.

Two Common Reasons Behind Insider Attacks

01

Malicious insider threats
This is the direct action of an internal user who is leaking sensitive information deliberately, with the end goal of damaging the organization. A disgruntled employee can work as an individual or unite their forces with competitors or other cybercriminals.

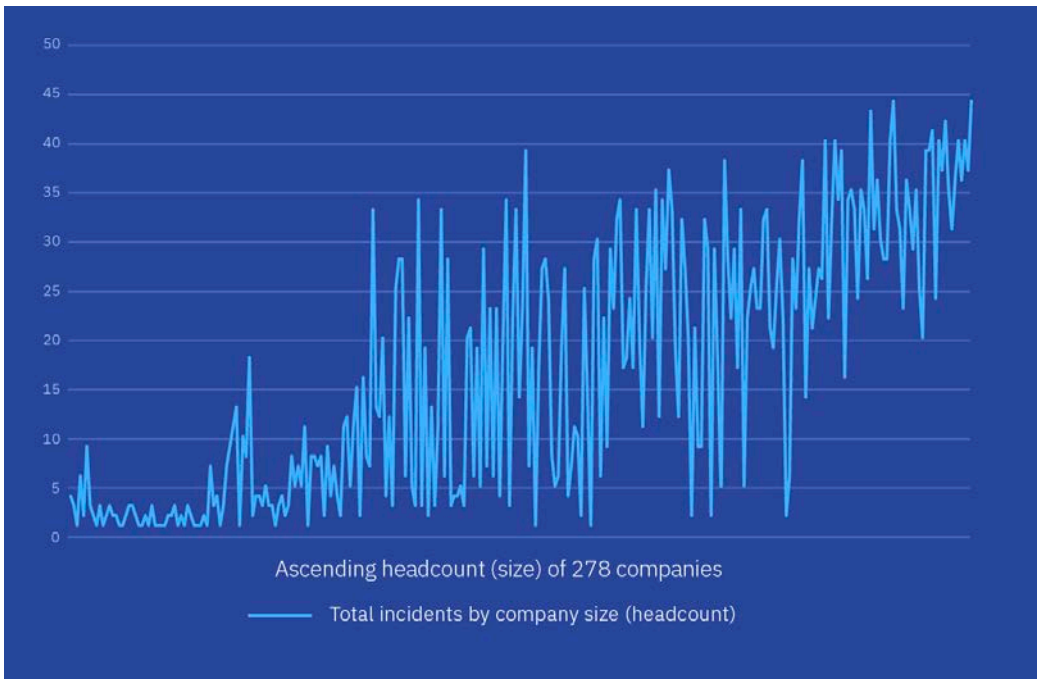
02

Negligent internal actions
These are situations when employees or people associated with the company create potential insider threats through careless behavior. Sending sensitive information to the wrong person, storing sensitive data on your browser, logging into company accounts from unsecured devices or networks, leaving your personal computer unattended, and losing devices are user behaviors that are an endpoint with a potential internal threat.

Types of Insider Threats

Let's take a look at other data breaches. We discover that the larger the organization, the more insider incidents there are, with financial organizations being the top area of attack.

Insider incidents in ascending order by headcount (size)



Source: Insider Threat Report 2022

This figure shows the distribution of insider incidents in ascending order by headcount or size of the participating companies. As can be seen, the upward slope suggests that the frequency of insider incidents is positively correlated with organizational size. The correlation is most salient for larger-sized companies.

If we look at the two categories mentioned above, we discover that they break down even further into six types of insider threats.

- Negligent workers
- Departing employees
- Security evaders
- Malicious insiders
- Inside agents
- Third-party partners

Insider threats and breaches examples

Cybersecurity professionals work around the clock to resolve new issues breaking security controls, but the main category of vulnerabilities remains - the company's employees.

Let's explore some of the most well-known internal data loss breaches and how their security teams managed to create an insider threat prevention to deter such situations!

Bank of America

Back in 2011, a former employee of the Bank of America sold a batch of customer data points containing sensitive information, such as names, addresses, birth dates, and PINs, to cybercriminals who committed fraud and identity theft.

One of the victim1s data was used to order and cash checks from the bank. The criminal had all the calls forwarded to another cell phone so that the victim wouldn't be alerted. As a result, the victim lost over $20,000. Bank of America offered to reimburse the victims and had to spend $10M to resolve this data breach.

SunTrust Bank

The bank's client data was stolen by a former employee, back in 2018, including sensitive data, such as names, phone numbers, addresses, and account balance details. The file contained more than one million clients• data, but it wasn't reported as a data breach.

SunTrust informed their clients about the incident, and current status, including details about what type of data was stolen. The bank continued to work with external experts on raising protection forces for future cyberattacks.

Tesla's Autopilot

In 2019, the company filed a lawsuit against a former employee reporting that he stole sensitive data, including the source code for the Autopilot technology behind Tesla's cars. Tesla also noted that this particular employee joined one of their competitor companies.

The Importance of Fighting Against Insider Threats and Data Breaches

As we can see, insider threats carry a higher impact and cost because the specific category of privileged users targeted has direct, privileged access to downloading internal information. So, the people involved in these threats are directly connected with the company, having access to sensitive data behind the firewall or other IT security measures.

Advantages of protecting a company against insider threats

If you are building an insider threat detection program to fight this type of data security problem and attacks, you'll be able to identify potential risks in real-time. Some of the core benefits are:

- The detection of suspicious behavior immediately
- The identification of high-risk profiles and threats among employees
- The ongoing monitorization through behavior analytics and management of cyber threats
- Mapping common patterns to fine-tune the program in the long term
- Aligning the organization to the latest information security protocols
- Building a robust compliance control infrastructure for IT teams
- Having a quicker system for incident response
- Creating a unified authentication and access management for admins and other people involved

The negative consequences of an insider attack

As we identified earlier, the impact of an insider data breach brings a sizeable financial loss and damages the company's reputation. Besides these direct results, the attacker knows all your weak points, and your company can be threatened with higher attacks and a higher financial gain for him.

Compared to external threats, you're less likely to suspect poor behavior from your employees, so this is why most insider attacks are discovered after the attack has been made. The danger increases, especially if we talk about intellectual properties or highly regulated industries like healthcare or finance.

How to Prevent Insider Attacks in Your Company

Insider threats can cause severe damage to your company, indeed, but there are ways to protect yourself against them, so let's see what's the baseline where you can start:

- Secure the most critical assets first
- Prepare an incident response plan that will guide your efforts in case of an attack
- Improve or create higher security policies
- Safeguard current employees by investigating unusual activities
- Analyze existing employee rights with intellectual property
- Have a strong backup for all your internal data

Other Types of Security Threats

Insider data breaches are only one type of security threat that a company can face. There are more hidden ones waiting out there to harm your company, and some of the most common are:

- Installing malware, such as spyware, ransomware, viruses, and worms
- Emotet - one of the most destructive security threats that's a modular banking Trojan that acts as a downloader of other banking Trojans
- Denial of service (DoS) - is a type of cyber attack that floods a computer or a network with files that make it unable to respond to different types of requests
- Man in the middle (MITM) - when hackers enter into a two-party transaction or action, such as blocking web traffic or filtering and stealing data.
- Phishing attacks - are those using a fake communication channel and trying to trick you into opening their message and taking the desired action
- SQL injection is a type of attack that inserts malicious code into a server that uses SQL to make it release the information they hunt.
- Password attacks are when cybercriminals attack your password to access all your information. One of the most common actions is social engineering - a strategy that relies on human interaction and tricking people into breaking standard security practices.

5 Tips & Tricks to Help You Protect Your Business

Evaluate security policies and insider risks

Your IT security team carries a high responsibility to improve the company's efforts against insider threats. The process usually starts with evaluating your current critical assets and potential risks. This way, you ensure the baseline of what you already have.

The NIST Guide for Risk Assessment is an excellent resource to use as a starting point. This will help you identify the biggest threats to your organization, any potential vulnerabilities coming from internal sources, possible outcomes of internal attacks, and the probability of this to occur.

Raise internal awareness about malicious insider threats

Another step in improving your current efforts against internal threats is to raise awareness across all your organization about this type of attack. If you don't know where to start, we recommend the following steps:

- Review current access rights for employees and former employees
- Give people access only to the systems they need to perform their job
- Run a background check on employees, especially on those who need access to sensitive data
- Restrict the control to those who need sensitive data, and have a thorough process for new requests
- Send a company reminder to all your employees to let them know the information is being monitored
- Create and communicate a guide including best practices so that people know where to look for information
- Inform people through dedicated materials and security training

Build an insider threat program

A strong insider threat program keeps your organization protected, and all the action items should bring clear steps for your employees to follow, such as:

- A common password manager
- A dedicated network and system permissions for each role or department
- Restrictions against specific software that need sensitive information or to bypass security controls
- Best practices on how to protect company devices when you are using or not using them
- How to react in cases of insider threats through clear protocols to follow
- Ways to identify suspicious emails, phone calls, or other messages, even if they look like they are coming from other internal users

Monitor internal attacks and compromised assets

Monitoring insider threats can be difficult if you rely only on your internal team members or a single source of information.

Look for dedicated software solutions to help you monitor internal attacks or compromised assets. Effective solutions will help you analyze what's happening and where internal assets need more effort based on priorities. Imperva recommends machine learning applications or tools like UEBA - User and Event Behaviour Analytics for your security team1s threat detection, analysis, and alert communication.

Examine past internal insider threats and data breaches

Examining past data breaches, incidents, and other potential threats is always a learning lesson that will guide people to have better protection in the future. So, don't forget to include this step in your process!

Ready to see how SmartVault can help you increase cybersecurity?

Schedule a 15-minute demo with one of our document management experts or sign-up for a free 14-day trial today!

SCHEDULE A DEMO **START YOUR TRIAL**

SmartVault

www.smartvault.com