How Accidental Insider Breaches are Becoming the Biggest Security Threat as Technology Advances

Preventative steps to ensure your company stays secure.

While various dangerous cyber attacks frequently make headlines, most workplace data breaches are unintentional, caused by end-users who fail to follow company security policy or try to get around it.

Accidental insider threats are more difficult to avoid and detect since the individual doesn't have a malicious thought behind the action. Additionally, that person often needs access to the organization's network to execute its job.

This article will dive deep into this type of insider threat indirectly caused by employees, partners, or people associated with your business.

The state of current accidental insider attacks in the world

Negligent insiders are the root cause of **56% of incidents**. At the same time, credential thefts have almost doubled. According to the latest insider threat global report published by Proofpoint, they are the costliest to remediate, at an average of over **$800,000 per incident**.

Internal data breaches that happened in the past few years

Every year, the number of insider assaults has increased due to various causes and factors. Between 2018 and 2020, the statistics show the number went from 3200 to 4700 per year. About 60 percent of firms now experience 30 or more insider assaults each year due to the rise in insider threats.

Accidental causes seem to be the majority cause of all these incidents. The statistics show that 55% of the organizations identify that threats happen by mistake when employees reveal sensitive information without being aware of any cybersecurity measure of protection.

The same study shows that organizations today are spending +60% more resources than before to combat this type of threat. The harm grows more prominent as the company grows and becomes more sensitive through multiple negligent actions happening constantly.

Accidental Insider threats are becoming more frequent

External threats aren't the only fear of tech companies today, but the real danger sometimes comes from the inside. The negligent behavior of employees or compromised users left unchecked brings companies a high and growing risk.

As we saw earlier, insider cyber attacks are becoming more and more powerful, and the number of accidental incidents is rising. The 2022 Cost of Insider Threats: Global Report reveals that:

- There are now +40% more insider threats compared to the previous two years
- Accidents and negligent behavior is the most common cause of cyber incidents
- Financial and professional services have the highest average activity costs
- The bigger the organization, the bigger the costs per incident are

With the ongoing rise of insider threats comes the job of enhancing cybersecurity to combat such risks. Insider threat cybersecurity is becoming increasingly expensive.

What is the best strategy for protecting your company against accidental insider threats?

rInsider threats are becoming more common and happening through human errors in more and more companies. This is why we reached out to a few companies and see how they are protecting themselves against this type of cyberattack.

More education is needed for threat prevention.

“The best way to protect your company against accidental insider threats is to educate your employees and create a security-first work culture.

When your employees aren't informed about the risks that can come from various actions, you're constantly going to be subjected to threats and risks from one or many of your employees, causing major negative impacts for your business. By educating them, they'll know how to behave, what to look out for and avoid, and what procedures need to be followed in order to maintain a safe work environment.

Of course, this information needs to coincide with technology and protocols that will help you to protect your business. We've been focusing on security for many years, meaning our employees know exactly what to do and what not to do. In addition, when we hire new employees, security is an important part of the onboarding process. This keeps security at the top of each employee's mind from the get-go."

Says Josh Wright, CEO of CellPhoneDeal**.**

Increase the number of tests and internal training.

"Human error is now, and likely always will be, the biggest source of data breaches and security problems at any organization. In my experience, the best way to combat this is with drills, more drills, and even more drills than that. Doing a phishing test is the most basic of basics and can be incredibly revealing – who fell for it? To what extent? Did it happen more than once? Is there a trend for what data got leaked during the test? The more you learn about your internal vulnerabilities, the more you can prepare for the future by strengthening data protocols and scheduling additional training for the particularly susceptible.

That said, it is most definitely possible to take it over the top and annoy your people enough that they cry foul. That's why my recommendation would be to rotate testing and training around departments rather than doing it for everyone all at once – give people a break and upskill where possible."

Adds Dragos Badea, CEO at Yarooms**.**

Better access management is the way to go.

"One of the best ways to prevent accidental insider threats to your company is implementing an access management system. Access management simply refers to the way you segment areas of your company and what is accessible by certain employees. By restricting access to certain data, software, etc., you create a protective barrier whereby internal threats will be restricted.

This reduces risk within your company as well as makes it harder for threats that are caused internally to spread to other areas of the business. You can't just stop at having implemented the access management system either; you also need to monitor it and ensure procedures are being followed correctly in order to keep your business safe."

Advise Us Sean Nguyen, Director at Internet Advisor**.**

Monitor employee behavior in real-time

“When we think of insider threats, we automatically think of aggrieved employees with malicious intentions instead of employees posing a threat due to ignorance and negligence. But it can be both the cases and third-party contractors or vendors that have access to the organization’s security. Some warning signs of a possible breach can include disgruntled behavior towards colleagues, violation of policies and protocols, use of unauthorized devices, and downloading huge amounts of data, especially when it’s not associated with their job.

The best strategy for protecting against these insider threats is to monitor employee behavior in real-time to predict abnormal behavior related to potential data theft, potential sabotage, or misuse. Enforcing security policies that limit access to personal data and specify who can reach what data under which circumstances. And also providing security awareness training to get rid of any vulnerable links by minimizing human error.“

Shares Ben Richardson, Senior Software Engineer, at SecureW2**.**

Create a data security policy for your company

“I feel that prioritizing security through multiple best practices, protocols, and procedures and then articulating these in a policy is the greatest way to avoid being a breach victim.

I recommend that data transit be kept to a bare minimum. Only move data from one device to another if it is essential. Removable media can readily misplace, putting all of the data on it at risk. Also, change your passwords frequently to keep them unpredictable and difficult to hack. Symbols and numerals are excellent choices.”

Adds Amy Bos, Founder of MediumChat**.**

SmartVault

Built with bank-level security, SmartVault offers a cloud-based document management system and client portal designed to help you reduce costs, raise productivity and employee happiness, stay in compliance, and deliver higher levels of service.

SCHEDULE A DEMO

smartvault.com