Insider Threats on the Rise, Warns Drip7

2024 began with the Mother Of All Breaches (MOAB), with 26 Billion records accessed. Insider threats have been up 47% in the last two years and increasing.

SPOKANE, WA, UNITED STATES, February 27, 2024 /EINPresswire.com/ -- What is an insider threat? It is the possibility of an insider using their access to an organization to harm that organization. This could be an employee, subcontractor, vendor, or former employee. The harm could be intentional and malicious or unintentional.

Insider threats have emerged as a growing security concern. Insider threats have increased 47% in the last two years, according to Trellix's 2024 Threat Prediction.[1]

> Build a company culture where employees feel responsible to protect the organization with best practices, such as access to information, document control, and phishing identification"
>
> *Heather Stratford, Drip7 Founder and CEO*

A joint study by Stanford University Professor Jeff Hancock and security firm Tessian has found that 88 percent of data breach incidents are caused by employee mistakes. Similar research by IBM Security puts the number at 95 percent.[2] Mastercard reports that 52% of SMEs reported a cyber attack last year. The unintentional incidents can be addressed by better and more frequent training.[3]

56% of insider incidents are caused by negligence, according to Ponemon. Most often, people ignore best practices when it comes to protecting information.[4]

"Build a company culture where employees feel responsible for protecting the organization with best practices, such as access to information, document control, and phishing identification," stated Heather Stratford, Founder and CEO of Drip7.

Recent trends reveal that close to 60% of cybersecurity attacks can be traced to company

insiders who have access to confidential data.[5]

Incidents of former disgruntled employees causing harm have made the news. So far in 2024, over 34,000 employees have been laid off among more than 140 tech companies, according to layoffs.fyi. Some of the big names this year include Snap, which owns Snapchat, Zoom, PayPal, Salesforce, Microsoft, eBay, TikTok, Wayfair, Google, Discord, Audible and Rent the Runway.[6] This does not include layoffs in other industries or medium-to-small businesses.

Business leaders surveyed by Resume Builder found that 38% of those surveyed think layoffs in their organization are likely this year. The reasons range from the impact of AI to concerns of a recession.

Not all organizations initiating layoffs have off-boarding practices to reduce the insider threat risk.

In the last year, 61% of companies have reported an insider threat.[7]

Prevention needs to be a combination of technology and training. The technology needs to consider internal threats, not just external forces seeking to breach firewalls.

Organizations would benefit from a mindset of enlisting the employees as a line of defense and giving them training in best practices to prevent breaches. This addresses unintentional insider threats.

New hires and transfers between internal offices need to have onboard training to understand all the dos and don’ts to keep the organization safe and how to apply policies and procedures in day-to-day operations.

This includes understanding phishing, spear phishing, social engineering, and company policies on access controls, handling of documents, and privacy of personal information. Microlearning with small bits of information presented as frequently as daily helps keep this important information top-of-mind.

An example of an unintentional breach is when the private details of 36,000 Boeing employees, in hidden columns, were put at risk after a Boeing employee emailed an Excel spreadsheet containing the data to his spouse, who is not a Boeing employee, to ask for help formatting the document.[8]

Intentional threats require wise use of technology and manager training in what to look for. When an employee is terminated, for whatever reason, off-boarding is a key time the organization is vulnerable. IT, Security, and HR teams need to coordinate the off-boarding process. Together they can create a checklist of access on apps, platforms, etc, to address in the off-boarding and establish not only what to address but when.[9]

The top insider threat actors, according to Finances Online are:
Privileged IT users
Managers with access to sensitive information
Contractors and Consultants
Employees[10]

The most common insider threat is caused by negligent employees, at 62%. Malicious insiders are the least common at 14%.[11] Bloomberg reported on an ex-Apple employee who was sentenced to jail for stealing trade secrets.[12]

Privacy is crucial for individuals to safeguard their personal information and data, while security measures aim to protect them from harm. However, security often requires access to private information, which can create a conflict with the right to privacy.[13] Privacy vs security is a delicate balance, particularly when defending an organization from insider threats.

2024 has brought the “Mother Of All Breaches”, (MOAB). 26 Billion - that is not a typo - that is B for Billion records were accessed. There are likely duplicates but the scale is beyond all past incidents.[14] It speaks to the need to have unique passwords for each account access.

Loan Depot, the 5th largest retail mortgage lender, had a cyber attack in 2024 with the sensitive information of 16 million plus clients exposed.[15]

Marriott had the distinction of having one of the largest data breaches until MOAB. Personal data and guest information of almost 400 million guests were accessed, including eight million credit card records. Three years later, they had another significant breach with the personal information of over five million guests accessed.[16]

With employees gaining access to more and more in an organization to improve efficiency, the risks of insider threats increase. In 2024 specifically, with more layoffs and increased adoption of AI, the potential for malicious insider threats will increase. This is not the time to stick your head in the sand and wait to see what develops. Now is the time to prepare for each aspect of insider threats due to ignorance, negligence, or malicious intent.

[1] https://cybermagazine.com/articles/navigating-the-threat-landscape-in-2024
[2] https://securitytoday.com/articles/2022/07/30/just-why-are-so-many-cyber-breaches-due-to-human-error.aspx#:~:text=A%20joint%20study%20by%20Stanford,the%20number%20at%2095%20percent.
[3] https://www.mastercard.us/en-us/business/overview/safety-and-security/trust-center.html
[4] https://www.circadianrisk.com/resources/blog/what-can-you-expect-insider-threats-to-look-like-in-2024
[5] https://www.forbes.com/sites/forbestechcouncil/2023/01/31/three-ways-organizations-can-

improve-their-cybersecurity-posture-without-spending-money/?sh=675bf0e0335e
[6] https://www.nasdaq.com/articles/will-2024-be-a-big-year-for-job-cuts#:~:text=But%20so%20far%20in%202024,Audible%20and%20Rent%20the%20Runway
[7] https://financesonline.com/insider-threat-statistics/
[8] https://www.code42.com/resources/infographics/insider-threat-examples-in-real-life
[9] https://www.code42.com/resources/infographics/tips-for-including-security-in-employee-offboarding
[10] https://financesonline.com/insider-threat-statistics/
[11] https://financesonline.com/insider-threat-statistics/
[12] https://www.bloomberg.com/news/articles/2024-02-14/ex-apple-engineer-sentenced-to-4-months-for-trade-secrets-theft
[13] https://www.diplomacy.edu/blog/how-can-we-balance-security-and-privacy-in-the-digital-world/#:~:text=Privacy%20is%20crucial%20for%20individuals,with%20the%20right%20to%20privacy.
[14] https://cybernews.com/security/billions-passwords-credentials-leaked-mother-of-all-breaches/
[15] https://www.forbes.com/advisor/mortgages/loan-depot-mortgage-cyberattack-update/#:~:text=Mortgage%20firm%20loanDepot%20now%20says,million%20consumers%20in%20its%20systems
[16] https://techcrunch.com/2020/03/31/marriott-hotels-breached-again/

Deb McFadden
Drip7
+ +1 203 856-4046
PR@drip7.com
Visit us on social media:
Facebook
Twitter
LinkedIn
Instagram
