THE ENEMY **WITHIN**

You've locked down your firewalls and hardened every endpoint so no one gets in. But the enemy doesn't need to infiltrate—they're already inside.

The damage from insider threats, inflicted from within an organization's defenses, can be even more severe than attacks from outside the perimeter. Insiders—or users— are a ticking time bomb that is unpredictable, underestimated, and potentially absolutely devastating.

Two thousand twenty-four statistics suggest insider threats count for 35% of all data breaches†, yet only 30% of CISOs rank insider threats as a major concern. It's a risk that's growing—insider breaches accounted for just 20% of the total in 2023—but is largely being swept aside in favor of louder and more obvious digital hazards.

> **"Poorly configured access to critical resources can be a powerful source of accidental sabotage**

THREATLOCKER TIP

Use ThreatLocker Storage Control and Unified Audit to control data access and instantly view all activity.

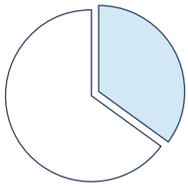
Insider threats first

If anything, insider activities should be at the top of the cybersecurity list, given that their varied and unknowable nature makes them so dangerous. This hazard exists outside of the archetype of the shadowy hacker, and can emerge from anywhere. Security professionals must be ready for anything, from the innocent to the malicious, and consider every user as a potential trojan horse. While active attacks are in the minority, accounting for only 27% of the total number of threats, employees or contractors working with malice are some of the most dangerous.

They might use their system access to deliberately steal data, install malware, or sabotage critical systems. External attackers, rival businesses, or criminal syndicates might also coerce those with legitimate access credentials to steal sensitive information or perform acts of fraud or espionage. A user doesn't even need to know they've been compromised; account credentials delivered to malicious hands through phishing attacks, shoulder surfing, or careless actions turn employees into unknowing accomplices.

The people problem

Psychologist B.F. Skinner wrote in 1969's Contingencies of Reinforcement that "the real problem is not whether machines think but whether men do." Skinner's words predated the modern information society, but they ring truer than ever today. When one looks along the lines of negligence—the re-used passwords, the accidental attachments,



2024 STATISTICS SUGGEST
INSIDER THREATS ACCOUNT FOR 35 %
OF ALL DATA BREACHES

the overworked and under-vigilant worker falling prey to attacks—that quote comes into focus. And it does not only apply to users. Oversight on the part of administrators and poorly configured access to critical resources, can be a powerful source of accidental sabotage.

It is vital that administrators do not ignore the explosion in potential attack surfaces that the modern hybrid environment provides. A planted USB drive, "lost" near an office and plugged in by a well-meaning employee, is a classic and not-quite apocryphal way of malicious software making itself into the bounds of the network perimeter. But there is so much more to contend with today: the IoT devices which have fallen behind in their update schedule, providing a backdoor for attackers; the messaging apps, from personal software like WhatsApp to corporate-sponsored platforms like Slack, which relax employees and may stop them thinking twice about sharing files they shouldn't; the advanced espionage hardware, imperceptible USB keyloggers, data sniffers, or compromised Wi-Fi networks which sneak past traditional defenses.

Each of these, and countless more, serve as a reminder that modern security is not just about building and maintaining an impenetrable digital fortress. When one's business consists of a thousand potential Trojan horses, it is as important to build behavioral awareness, operational vigilance, and an ingrained security culture that works to prevent potential insider attacks from ever happening willingly or accidentally.

On the defensive

A Zero Trust mentality forms a large part of these countermeasures. The point here, after all, is that no user, and no access, is inherently trustworthy. Strict access controls, identity verification and least-privilege policies go a long way to eliminating the possibility of insider attacks.

Administrators also need visibility. Behavioral analytics can detect suspicious behavior early, allowing it to be stopped before it turns into an attack. Anomalous logins, unusual file transfers, and excessive data downloads may all be indicators of espionage and can all be made visible to security personnel without compromising privacy.

> **"On the ground, the key is buy-in from workers and executives alike. Cybersecurity is not only an IT issue; it's a boardroom issue**

On the ground, the key is buy-in from workers and executives alike. Cybersecurity is not only an IT issue; it's a boardroom issue. Clear policies built around well-defined accountability structures encourage appropriate action from above, while regular training and clear messaging can ensure employees in the firing line remain hyper-aware.

The new cybersecurity posture

The solution to insider threats boils down to preparing for the inevitable. No strategy is bulletproof; Zero Trust behavior will minimize the impact, but it must go together with complex risk assessments, regular attack simulations, and well-formulated incident response plans. This is a case of safeguarding against human nature itself, outsmarting an enemy one cannot possibly know before they make a move. When the enemy is already within your walls, you can't let your guard down for a second.