Devolutions

How SMBs can detect, stop & prevent insider threat attacks

JULY 2025

OVERVIEW

For several years, organizations have been advised, urged, and in some cases ordered by regulatory bodies and insurance companies to actively guard against cyber criminals. And while this warning continues, there is another — often neglected — danger on the cybersecurity battlefield that can be just as costly and disruptive as outside hackers: **insider threats**.

In this white paper, we take a deep dive about "the enemy within," and explore:

- **The definition of insider threats**
- **The impact of insider attacks**
- **Insider threats and small and mid-sized businesses (SMBs)**
- **Types of insider attacks**
- **Types of insider attack indicators**
- **7 strategies that help SMBs detect, stop & prevent insider attacks**

WHAT ARE INSIDER THREATS?

TechTarget defines an insider threat as a "**category of risk posed by those who have access to an organization's physical or digital assets.**"

It is important to add that "insiders" in this context do not exclusively refer to current employees. **It also includes interns, contractors, vendors, business partners, former employees, or any other individual who has (or had) authorized access to an organization's systems and networks.**

No, this does not instantly make all of these people suspects who are poised to steal data and commit identity theft! But it does highlight that the surface area for potential insider threats is enormous, and far larger than many organizations grasp. We look closer at these possible costs and consequences in the next section.

IMPACT OF INSIDER ATTACKS

When it comes to cybersecurity, many organizations focus exclusively (to varying degrees) on defending against hackers. This is vital, but it is not enough. **They must also actively guard against insider attacks.** Consider the following:

- The authors of Verizon's **2025 Data Breach Investigations Report 2025 Data Breach Investigations Report** state: "[W]e have seen many instances of insiders misusing their access for years before they are caught."
- IBM's **2024 Cost of a Data Breach Report** note that the average **cost of data breaches initiated by malicious insiders was $4.99M per incident.**
- Cybersecurity Insiders' 2024 Insider Threat Report point out that that **83% of organizations reported at least one insider attack in the last year.**

Furthermore, the impact of unmanaged insider threat risk goes beyond the (in some cases staggering) financial toll. **It can also create regulatory and insurance exposure, erode trust across teams and departments, damage reputation in the marketplace, and weaken and detection response posture.** While all of these consequences are severe, the last one is particularly worrisome. This is because once insiders "open the gates" to breach accounts and exfiltrate data, **they may forge a path for external cybercriminals to follow in the future, leading to even more costs and damage.**

INSIDER THREATS AND SMBS

In the Devolutions' State of IT Security in SMBs 2024/25 survey, **78% of SMBs said that they are "concerned" about insider threats.** This is a 45% jump from 2023, and certainly a step in the right direction since awareness is essential.

However, the Devolutions' survey also found that a whopping **82% of SMBs do not actively monitor for insider threat risks.** Even more concerning is that **28% of SMBs either have no plan to address insider threats, or they do not see it as a priority.**

The implication here is clear: **while most SMBs are aware of the problem, the vast majority are not translating this understanding into meaningful strategic action.** Unfortunately, the risk of insider threats will not resolve itself. On the contrary, it will only become more dangerous and costly in the future as the value of stolen data — either used by malicious insiders themselves, or sold on the dark web — rises.

Further in this white paper, we will explore proven and practical ways for SMBs to mitigate insider threat risk. First, let us look at the different types of insider threats, along with some risk indicators.

TYPES OF INSIDER ATTACKS

Generally, insider attack incidents fall into four broad categories: **malicious, accidental, negligent, and collusive.**

Malicious: Incidents are carried out by individuals who are aware that their actions will harm the organization. These individuals can be motivated by different factors, such as greed or personal grievances.

Accidental: Incidents are the result of honest (although perhaps grossly incompetent) mistakes. For example, an employee may click on an email link that they believed was safe, but turned out to be sent by hackers as part of a phishing campaign. Or a supplier may send a document to a third party, not realizing that it was confidential. While they are not deliberate, nevertheless accidental incidents can be extremely costly.

Negligent: Incidents are the result of a trusted individual knowingly breaking a rule (or perhaps multiple rules), but without the intention to cause a security breach. For example, an employee may choose to circumvent policy by storing sensitive corporate data in their personal cloud storage account (e.g., Google Drive, OneDrive, DropBox, etc.), because doing so is more convenient. Obviously, this is inexcusable, and could be grounds for termination, or even litigation. However, the key point is that the individual in question — while certainly careless and reckless — did not intend to harm the organization.

Collusive: Incidents are the result of an individual (or possibly a group of individuals) collaborating with external cybercriminal groups, in order to commit fraud, intellectual property theft, and/or espionage. Organizations are urged not to perceive collusive insider threats as "sensational," in the sense that only large high-profile multinational enterprises (think Fortune 100) need to actively guard against them, while SMBs with their relatively lower profile are out of harm's way. All organizations are at risk of collusive insider threats, regardless of size or sector. A survey by Bravura Security found that hackers approached 65% of executives or their employees to assist in ransomware attacks.

TYPES OF INSIDER ATTACK INDICATORS

Some types of cyberattacks are unmistakable. For example, victims of ransomware attacks do not have to speculate on whether they are under siege: the clear (and terrifying) evidence is right in front of them, complete with payment demand and rapidly-approaching deadline.

Conversely, attacks carried out by insiders are typically much more insidious and tougher to detect, because they happen behind-the-scenes; in some cases, persisting for months, or even years. Below are some signs that an insider attack could be under way or imminent:

Privilege escalation: An employee has escalated their access privileges (if they are able to do so on their own), or has requested more access, without a clear business justification.

Abnormal system access: An employee starts accessing resources to which they have access (so privilege escalation is not necessary), but the reason for their activities is unclear. For example, an employee who works on the sales team begins accessing databases and systems used by the finance team. While this could be legitimate, it might be an indication that something untoward is taking place (or is about to happen).

Abnormal data exfiltration: An employee is suddenly downloading sensitive data, and this is inconsistent with their past activities, or the activities performed by colleagues/peers in a similar role. An example is a departing employee who copies sensitive data, which could be used for personal gain or to assist them in their next job (we look closer at how to de-provision exiting employees in the next section).

Sequence of questionable activities: An employee performs activities that, in themselves, are not necessarily unusual. However, the sequence (and also possibly the speed) at which they are carried out raises questions. For example, an employee renames a file, and then downloads it to a personal device. This could indicate that the employee is knowingly breaking the rules in order to get the file (although their motive may be unclear and requires further investigation).

Attitude changes: This is the least "black-and-white" sign of a potential insider attack on the list, but it could also be the most revealing. An employee who inexplicably starts behaving in a covert and secretive manner — or on the other extreme, in an intimidating and threatening way — could be carrying out an insider attack. Keep in mind that in some cases individuals may be coerced or blackmailed by cybercriminal gangs, which can trigger very unusual and unpredictable behavior shifts.

Before moving on to what SMBs can do to reduce the risk of insider threats, it must be added that, in all but the most blatantly obvious cases (i.e., an employee is caught "red-handed" accessing prohibited accounts or stealing sensitive data), these signs are only potential indications that something untoward could be going on behind-the-scenes. They raise questions that must be answered in a diligent, documented, and discrete manner.

7 STRATEGIES THAT HELP SMBS DETECT, STOP & PREVENT INSIDER ATTACK

So far, we have looked at what insider threats are, who carries them out, and what they can look like from the outside. Now, let us pivot and explore seven seven strategies that can help SMBs significantly reduce their risk of being victimized by an insider attack.

1. Create a comprehensive insider strategy

As we noted earlier, according to the Devolutions' State of IT Security in SMBs 2024/25 survey, insider threat awareness among SMBs has increased year-over-year from 33% to 78%. However, during the same period, the **proportion of SMBs with a comprehensive insider threat strategy only increased marginally from 15% to 20%.**

Many SMBs are adopting tools and measures that strengthen their cybersecurity profile, such as privileged access management (PAM) and multifactor authentication (MFA). **Yet without trying these elements into a broader insider threat strategy, they remain highly exposed.**

SMBs need to close the gap between awareness and action by aligning policy, with monitoring and onboarding/offboarding (more on this in the next strategy). Further, they need to integrate these into their PAM and training flows, and incorporate it into their overall incident response plan so that everyone knows what to do, when, and in what order in the aftermath of a breach (however caused). **SMBs are cautioned that treating insider threats like edge cases is a mistake.** Treating them as inevitabilities — and knowing how to reduce the risk and effectively respond vs. frenetically react to incidents — is wise.

2. De-provision departing employees

Today, the average employee will have 12 job changes during their career (and many will have even more). Why is this relevant in a white paper about preventing insider threats? It is because of this next, far more chilling statistic: a survey from Beyond Identity found that **1 in 4 ex-employees still retained access accounts from past jobs — including former IT staff and managers who had access to privileged accounts.**

Granted, we can assume that the vast majority of these former employees do not represent an insider threat. However, it only takes one greedy, aggrieved, or compromised individual to launch a successful cyberattack.

In addition, there is the possibility that these former employees could be victimized by a cyberattack. As a result, the login credentials that they used for previous workplaces could fall into the hands of hackers if they were stored in a spreadsheet, browser, poorly-protected password manager, etc.

The mandate for SMBs is clear: **close this gap by establishing a standard process for employee departures.** At a minimum, the process should include the following core activities:

- Immediately change the employee's password(s) so they cannot log in. If there is a legitimate reason for them to do so, then they can make a formal request.
- Disable or lock all accounts. Disabling accounts is best, since this eliminates the possibility of future access. However, it may be necessary to lock accounts until the data can be archived elsewhere (after which the accounts should be disabled).
- Change all passwords on shared privileged accounts. These include (but are not limited to) domain administrator accounts, local administrator accounts, emergency access accounts, application accounts, system accounts, and domain service accounts. Forrester researchers estimate that 74% of all data breaches involve compromised privileged credentials.

3. Enforce the principle of least privilege (POLP)

A proven and practical way for SMBs to reduce their exposure to insider threat risk (as well as those stemming from outside the organization) is by implementing POLP. This is a policy in which users — which includes employees, contractors, interns, and anyone else who legitimately requires access to accounts and systems — are only given the amount of access they need to carry out their jobs.

To establish and enforce POLP, SMBs should carry out the following activities:

- Make least privilege the default starting point, and add higher-level access as needed through analysis and in consultation with users.
- If temporary privileged access is required, use one-time-use credentials. These are granted at the last moment, and then revoked immediately after use. This approach (called "privilege bracketing") can be used for individual users, as well as processes and systems.
- Separate administrator accounts from standard accounts.
- Separate higher-level system functions from lower-level system functions.

- Automatically track all login attempts (including unsuccessful ones) and activity. It is critical to have full visibility and see precisely what users are doing.
- Regularly audit user privileges to ensure that access is appropriate.
- Have the ability to automatically revoke privileged access in the event of an emergency.

BONUS TIP: With **Devolutions Hub Business**, SMBs can centralize account access and enforce POLP — while still empowering their teams to work fast. In addition, Devolutions' **Remote Desktop Manager** and **Devolutions PAM** enable SMBs to configure and implement granular access controls that support POLP.

4. Establish a zero trust framework

The guiding principle of zero trust is "never trust, always verify." Every user, device, and application must be authenticated and authorized before access is granted — regardless of physical location. This approach restricts the ability of malicious insiders to obtain and maintain unauthorized access to sensitive systems and networks.

To establish a zero trust framework SMBs should implement the following:

- Replace unauthenticated legacy services and systems with cloud technologies. Among other security advantages, migrating to the cloud helps pave the way for passwordless authentication in the workplace, such as passkeys (see the Bonus Tip below for more advice on implementing passkeys).
- Design zero trust architecture based on how data moves across the network, and how users and apps access sensitive information.
- Verify trust upon access to any network resource by using MFA in real-time.
- Extend identity controls to the endpoint to recognize and validate all devices.
- Organize users by group/role to support device policies.
- Leverage automatic de-provisioning, along with the capacity to wipe, lock and un-enroll lost or stolen devices.
- Regularly update end user rights based on changes to roles/jobs, as well as changes to prevailing security policies and compliance requirements.

BONUS TIP: At Devolutions, we've embraced passkeys by integrating them into our products and services. The **Devolutions Workspace browser extension** allows users to store passkeys in the cloud-hosted **Devolutions Hub Business**, or self-hosted **Devolutions Server** advanced data sources and **Devolutions Hub Personal**.

5. Implement advanced monitoring solutions

As noted earlier, by their nature insider attacks are often tougher to detect than external attacks. **Advanced monitoring solutions give SMBs a significant advantage in the fight.** For example, tools such as User and Entity Behavior Analytics (UEBA) use machine learning algorithms and behavioral analytics to monitor user activity, and automatically flag anomalies that could point to potential insider threat activity.

6. Regular conduct security audits

Regular security audits verify if current solutions and practices are effectively mitigating insider threat risks. **These assessments must be comprehensive rather than superficial, and cover elements such as policies, permissions, and access controls.** It is also critical to review the incident response plan (which as mentioned should cover how to respond to insider threats), and update it accordingly.

7. Provide employee training

According to Cybersecurity Ventures' 2024 Insider Threat Report, 32% of respondents said that a lack of training and awareness was a major driver behind insider attacks. And this does not only relate to breaches caused by accidents or negligence. Ongoing cybersecurity training helps cultivate a "security culture." **When individuals know that the organization prioritizes IT security, then they are more likely to be diligent in this area, and less likely to break the rules knowingly or accidentally.**

THE FINAL WORD

The cyberthreat landscape is not restricted to defending against outside hackers. **Like larger enterprises, SMBs must also address and mitigate the risk of internal threats, regardless of whether attacks are (or could be) caused by accident, negligence, or malicious intent.** Being proactive and implementing the strategies highlighted in this white paper could go a long way to determining whether the journey ahead for SMBs is smooth and successful, or chaotic and costly.

DEVOLUTIONS: ON YOUR TEAM AND BY YOUR SIDE

At Devolutions, we offer multiple solutions — including those highlighted in this white paper — that help SMBs protect their data, assets, and reputation from the damage inflicted by insider attacks.

All of our solutions are easy-to-use, scaleable, affordable, and designed specifically for SMBs that need to establish strong cybersecurity, but without compromising efficiency or productivity.

To learn more, contact Devolutions today at sales@devolutions.net. Learn how we can help your SMB fight back against insider threats, while you strengthen your overall cybersecurity profile.