Devolutions

THE STATE OF IT SECURITY IN SMBs 2024/2025

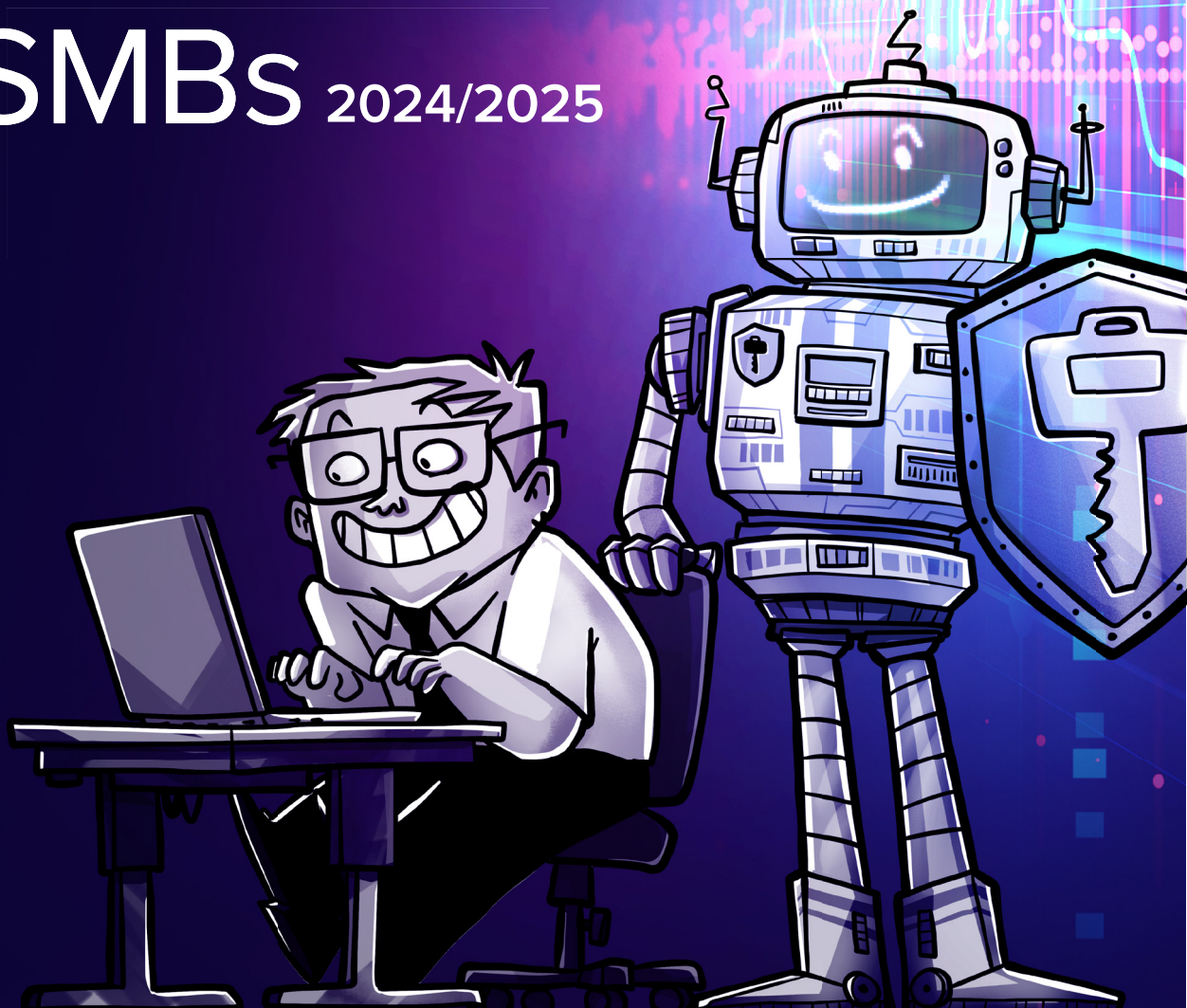


Table of contents

Introduction

1 **PAGE 5**
Confidence vs. Capability Gap

2 **PAGE 10**
Manual PAM Still Dominates

3 **PAGE 16**
AI Is Coming, But Most Aren't Ready

4 **PAGE 22**
Budgets Are Growing, But Still Too Low

5 **PAGE 28**
Insider Threats: A Known Risk, But Rarely Addressed

6 **PAGE 34**
Training Still Isn't Standard

Conclusion

Future Outlook

Recommendations

Contact Us

The Big Picture: While confidence is high and budgets are rising, real posture still lags.

And some of the most effective defenses are still missing in too many organizations.

In today's threat landscape, **small and medium-sized businesses (SMBs) are no longer off the radar** — they're on the front lines. From phishing scams and ransomware to insider threats and cloud misconfigurations, cyberattacks now strike organizations of all sizes, in all sectors, with growing sophistication and financial impact. In fact, our survey indicates that **43% of SMBs faced at least one cyberattack** in the past year.

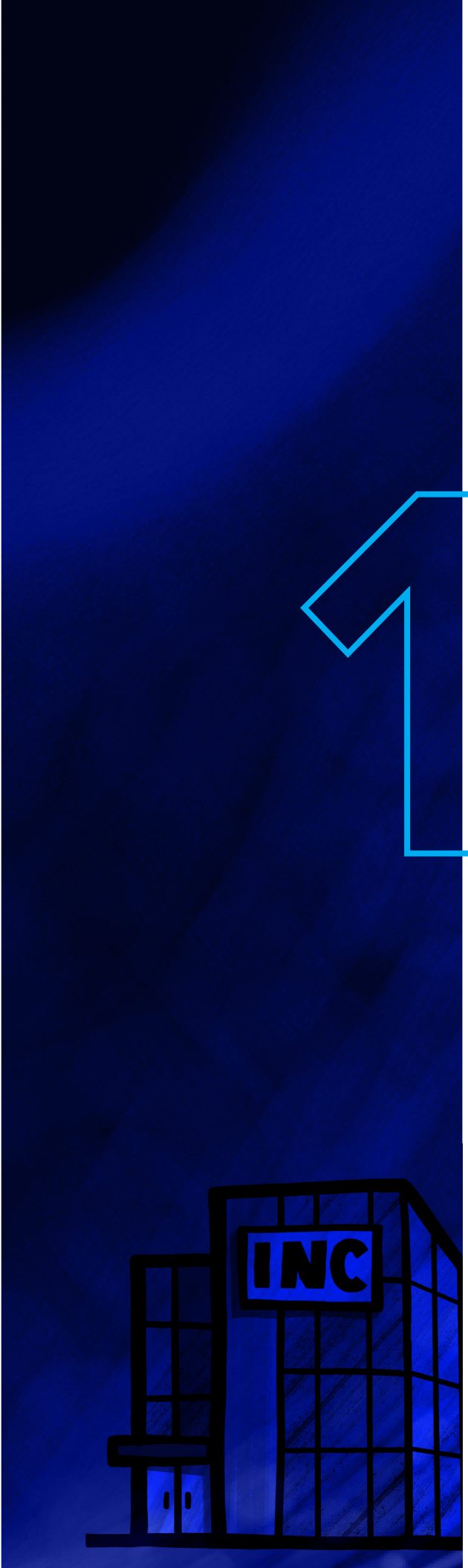
To better understand how SMBs are responding to this new normal, **Devolutions conducted its largest-ever global cybersecurity survey,** collecting responses from 445 professionals across IT, security, and executive leadership roles. This year's results shine a spotlight on six areas that reveal how far SMBs have come — and how far they still have to go.

This survey explores six key insights that matter most in 2025:

1. **The gap between confidence and actual preparedness**
2. **Persistent reliance on manual security practices like spreadsheets**
3. **AI adoption intent vs. reality**
4. **Budget growth that doesn't match risk levels**
5. **Insider threats that are recognized but under-addressed**
6. **Training programs that aren't keeping pace with the threats**

Each chapter breaks down what the data reveals, highlights contrasts across roles and sectors, and includes a striking visual + sector spotlight for fast understanding.

Our goal? To help SMBs benchmark their progress, spot their blind spots, and build a smarter, more secure future — without adding complexity they can't manage.



1 Confidence vs. capability gap

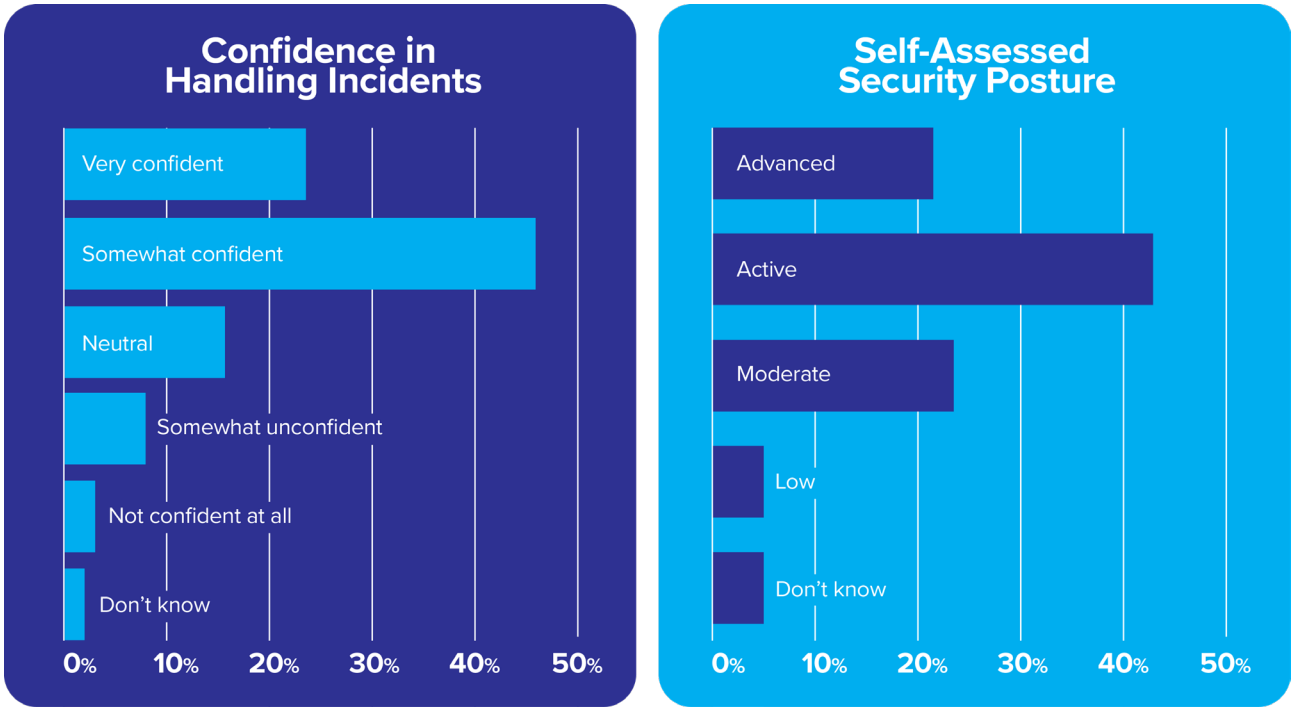
71% of SMBs feel confident in handling a major cybersecurity incident — but only **22%** say they have an advanced cybersecurity posture.

It's a striking mismatch — and one that's echoed across roles, regions, and sectors. This **confidence-capability gap** is one of the clearest signals from this year's survey: **most SMBs believe they're prepared**, yet very few have the structures, policies, and tools in place to truly withstand today's cyberthreats.

Compared to 2023, confidence among SMBs dropped from 80% to 71%, and self-reported advanced posture **slipped from 30% to 22%.** This suggests a growing awareness of risk — but not yet a corresponding leap in readiness.

Breakdown of Confidentce vs. Security posture

(2024-2025 Survey)



Role Breakdown: Who's Confident vs. Who's Actually Ready

This disconnect isn't just theoretical — it's operational. It impacts everything from breach response to executive oversight to vendor relationships.

When we break down responses by role, a clear pattern emerges: **the further a role is from the front lines, the higher the confidence** — but not necessarily the readiness.

Executives often feel secure, bolstered by dashboards, optimistic briefings, or cyber insurance — yet that confidence may overlook the friction and fragmentation happening on the ground. Security teams, involved in strategy and policy, sit between the two — aware of risk, but not always equipped to fix it.

Meanwhile, **IT professionals report the lowest confidence and the lowest posture.** They're closest to the day-to-day vulnerabilities: legacy systems, manual controls, and the real cost of underinvestment.

Role group	% Confident	% Advanced posture
C-level executives	82%	28%
Security professionals	76%	26%
IT / Employees	67%	19%

WHAT THIS SHOWS:

This is more than perception. It's a strategic misalignment — and one that can delay investment, suppress visibility, or foster dangerous assumptions.

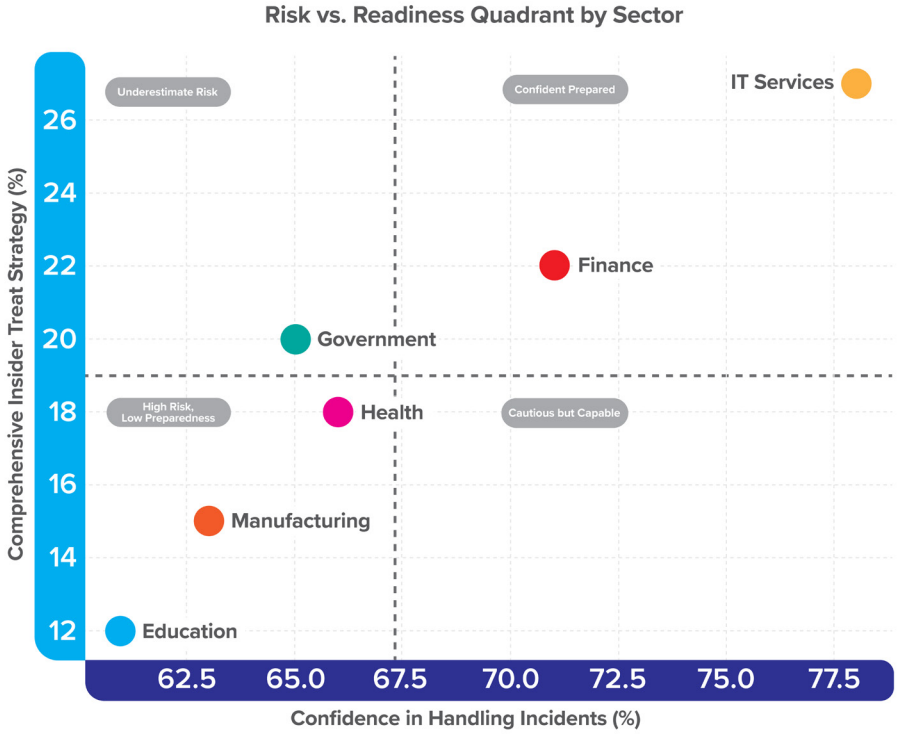
Risk vs. Readiness: A Sector-Level View

A deeper look at sector-level data shows this gap between confidence and preparedness isn't just about roles — it's **visible across industries**. Our sector-level quadrant analysis reveals an urgent truth: **some sectors are unknowingly overexposed**, while others are waking up to their gaps — but haven't closed them yet.

Sector Sidenote: Education

Confidence: 61%
Advanced posture: only 12%

"Confidence is not backed by maturity."
The education sector reports confidence levels near the average — but has one of the lowest posture ratings across all industries. In many cases, this reflects underfunding, legacy infrastructure, and lack of full-time security staff.



Why This Matters

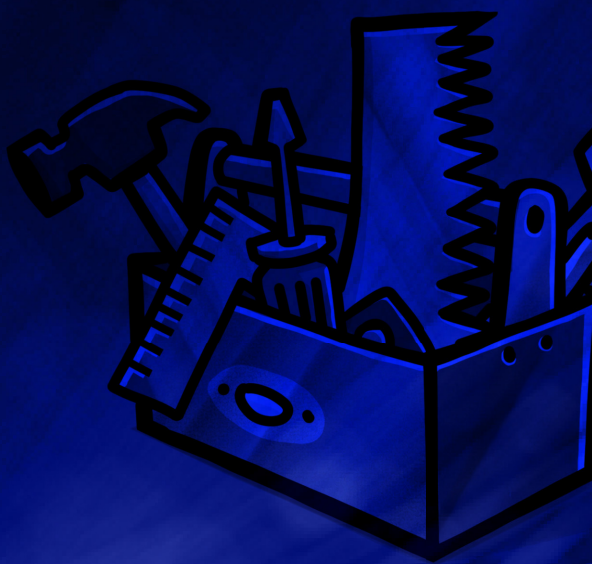
When confidence outpaces capability, critical risks are easy to overlook:

- Cyber insurance policies may not be comprehensive enough
- Leaders may underestimate the need for new tools or roles
- Teams may skip audits or incident simulations under the assumption they're covered

This isn't about reducing confidence — it's about realigning it with operational reality.

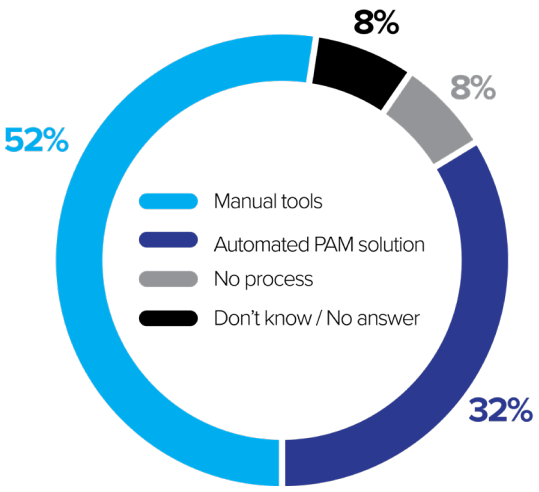
> Believing you're secure isn't enough anymore. In today's world, SMBs need to measure their posture honestly — and invest like it matters. Because it does.
>
> *David Hervieux, CEO, Devolutions*

2 Manual PAM still dominates



52% of SMBs still manage privileged access using manual processes — spreadsheets, vaults, or no formal system at all.

How SMBs manage Privileged Access
(2024)



Why SMBs don't have a PAM Solution

21%	Cost concerns	9%	Limited resources
14%	Lack of awareness	7%	Low priority
14%	Don't know	6%	Complexity
12%	No perceived need	3%	Integration concerns
12%	Alternative tools	3%	Other

Privileged Access Management (PAM) is one of the most critical pillars of cybersecurity — and one of the most neglected. Despite the rise in ransomware, insider threats, and zero-trust adoption, **most SMBs are still relying on basic, outdated methods to manage their most sensitive access.**

That reliance creates unnecessary risk. Manual processes introduce human error, obscure visibility, and delay revocation when people change roles or leave the company. And yet, the move to modern PAM isn't happening fast enough.

Despite the growing recognition of privileged access as a critical risk surface, the data reveals a concerning reality: **more than half of SMBs still rely on manual tools like spreadsheets or shared vaults to manage sensitive credentials.** Among those who haven't adopted a PAM solution, the barriers are more fundamental than technical — **cost, lack of awareness, and low perceived need** top the list.

This suggests a major disconnect: even as cyberthreats evolve, many organizations either don't understand what PAM is, or don't realize how vulnerable their current practices leave them. It's not just a tooling gap — it's a visibility and education gap.

Role Breakdown: Who's Using Manual PAM — and Why

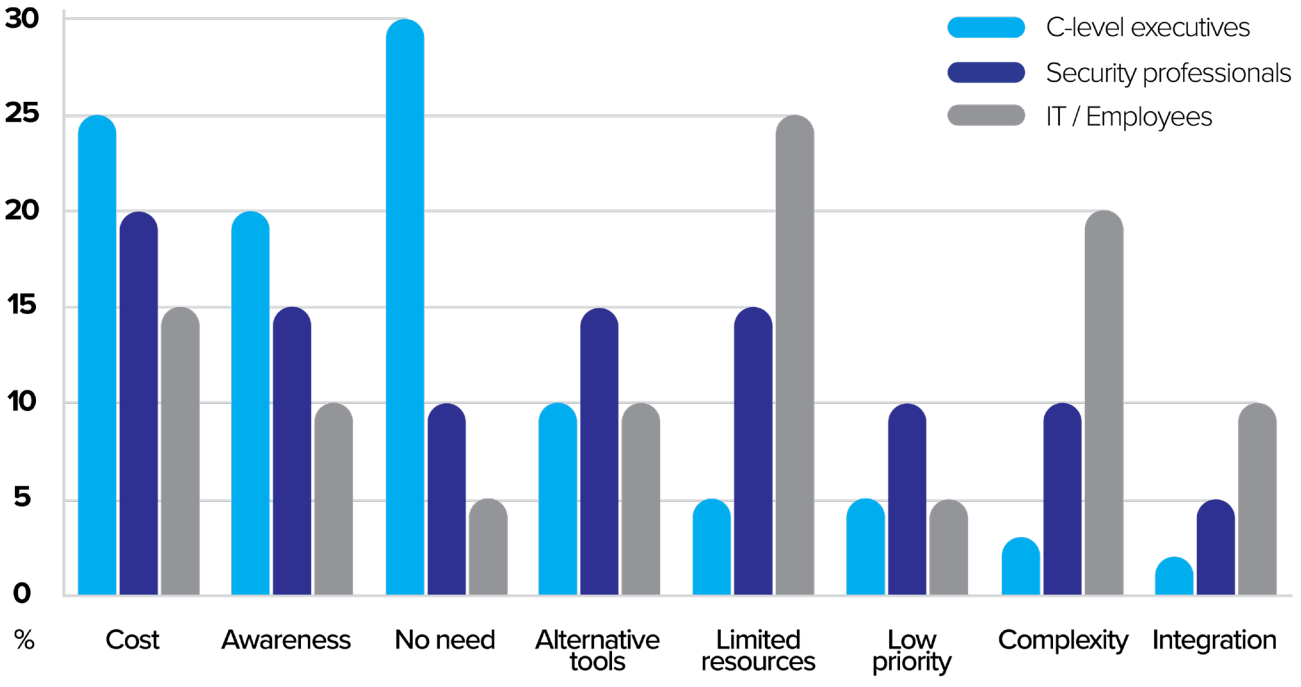
PAM adoption isn't just about buying software. It's about understanding who's affected, what's blocking them, and how to remove those barriers.

Role group	% Using Manual PAM
C-level executives	44%
Security professionals	49%
IT / Employees	55%

This chart reveals a deeper truth behind manual PAM persistence: **each role experiences different blockers.**

- **C-Level leaders** often cite lack of awareness or perceived need, believing vaults or basic policies are sufficient. For them, PAM is often a checkbox — not a system.
- **Security professionals** face a mix of strategic and technical barriers. They know PAM is important, but must balance cost, internal resistance, and incomplete rollouts.
- **IT employees**, closest to the systems and risks, report the heaviest friction. Limited resources, integration issues, and tool complexity are everyday realities — and they're the ones still managing accounts manually.

Estimated PAM adoption barriers by role group



WHAT THIS SHOWS:

Adoption rates highlight regional gaps in securing privileged accounts.

Sector Sidenote: Finance
Manual PAM use: 51%

"Legacy friction and integration hesitancy." The finance sector — highly targeted, heavily regulated — still sees over half of respondents using manual tools to manage privileged accounts. Complexity, cost sensitivity, and integration fears with core systems often delay full PAM rollout — even where risk is highest.

"PAM Adoption: Netherlands Leads, USA Lags."

A deeper look at sector-level data shows this Privileged Access Management (PAM) adoption remains highly uneven across regions. In the Netherlands, around **25%** of SMBs have deployed a PAM solution — reflecting a strong push toward securing privileged accounts.

Meanwhile, in the USA, **more than 50%** of organizations still rely on manual methods like spreadsheets and vaults. This disparity shows that while awareness of privileged access risks is rising globally, **true adoption and maturity are still heavily influenced by geography.**

Why This Matters

Manual PAM is the perfect example of a known problem that persists anyway. The barriers are familiar:

- Cost and licensing models
- Integration with legacy infrastructure
- Low perceived need outside compliance events

But so are the consequences:

- Lost visibility into who has access to what
- Delayed deprovisioning of risky or dormant accounts
- Untraceable use of privileged credentials

The longer this issue is deferred, the more deeply risk gets embedded into the organization's operations.

Despite increased awareness of access-related risks, **manual PAM use has actually grown since 2023** — from 45% to 52%. Meanwhile, automated adoption has barely moved. This suggests that many SMBs are either **unable to implement PAM at scale, or are checking the box without full deployment.** The blockers highlighted by role groups — from cost and complexity to lack of internal resources — help explain why progress has stalled.

Modern PAM doesn't have to be complex or costly — but it does need to be real. If SMBs want to protect what matters most, they have to move away from good intentions and toward **automated, auditable access control.**

> The human is often the weakest link — and spreadsheets don't make us stronger.
>
> *Maurice Côté, VP Product, Devolutions*

3 AI is coming, but most aren't ready

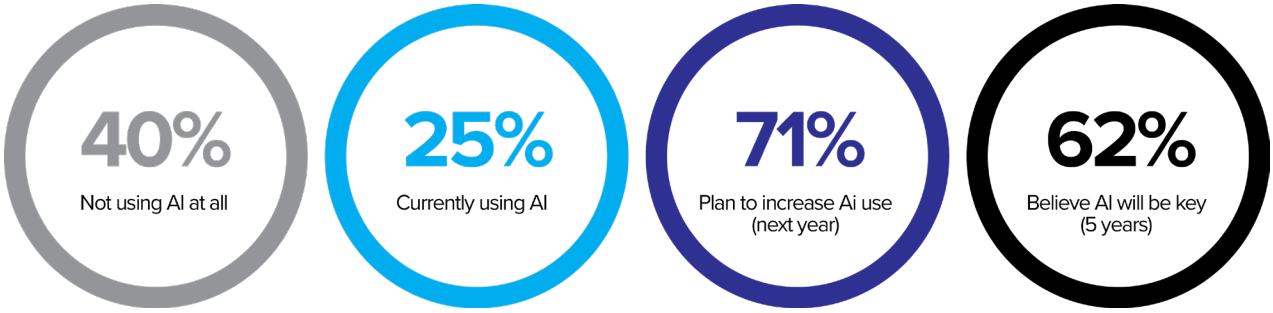
71% of SMBs say they plan to increase their use of AI in cybersecurity — yet **40%** aren't using it at all today.

Artificial Intelligence is no longer just a buzzword — it's becoming a core component of modern cybersecurity. From automated threat detection and anomaly spotting to predictive analysis and behavior-based access control, **AI promises faster, smarter, and more scalable defense.**

But promise and practice are two very different things.

Despite the enthusiasm, our survey shows a persistent adoption gap. **Most SMBs want to use AI — but many simply aren't ready.** Whether due to cost, lack of internal expertise, privacy concerns, or a fear of over-reliance, nearly half still haven't taken the leap.

The gap between belief and action couldn't be clearer. **Only 25% of SMBs are currently using AI in their cybersecurity efforts, while 40% haven't started at all. Yet, 71% plan to increase their use within the next year, and 62% believe AI will be a critical part of their strategy within five years.** This signals a strong strategic appetite for AI — but one that **hasn't yet translated into widespread operational adoption.**



Role Breakdown: Optimism vs. Action

AI is exciting — but for many SMBs, it's still out of reach due to capability gaps.

Just like in other areas, **C-Level leaders are the most optimistic,** with 80% saying AI will play a significant role. But **IT and security staff** are more reserved — and for good reason.

They're the ones evaluating integration, managing compatibility, and addressing false positives. They **see the effort it takes** to go from AI concept to real operational value.

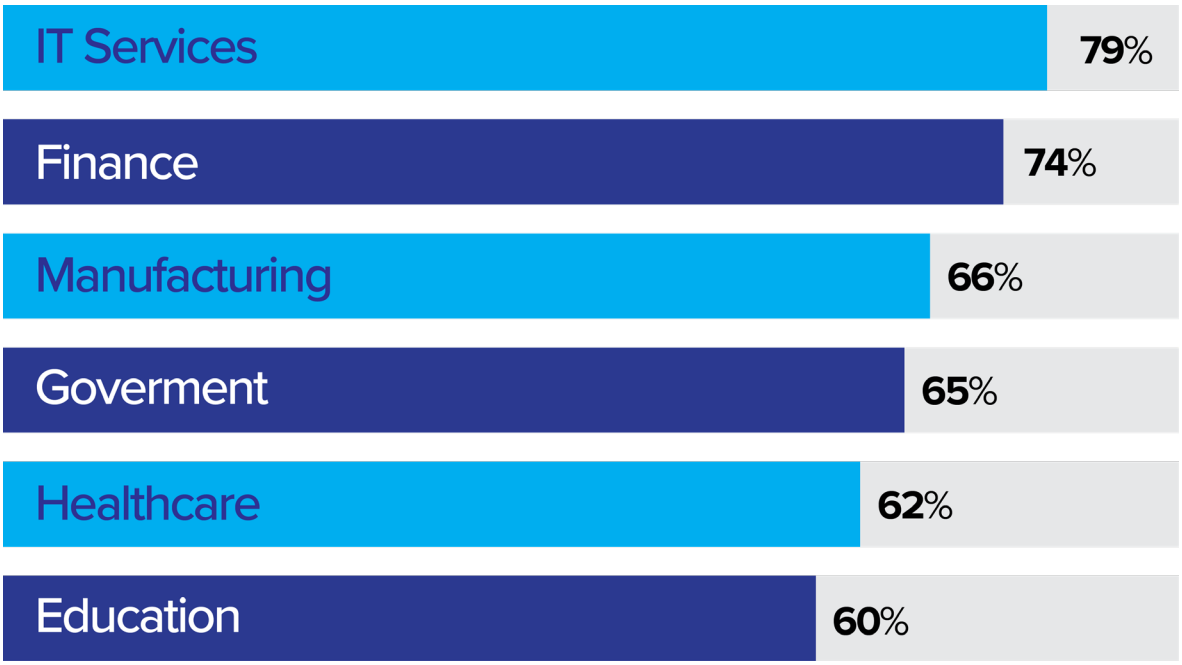
Role group	% Planning to use AI
C-level executives	80%
Security professionals	74%
IT / Employees	67%

WHAT THIS SHOWS:

Sector Sidenote: Healthcare

Planned AI usage: 62%
– one of the lowest in the survey

"In a high-risk environment, AI is still seen as complex."
The healthcare sector, while increasingly digitized, remains cautious toward AI – citing concerns over data privacy, regulation, and operational disruption. This highlights a deeper challenge: AI readiness requires more than belief – it requires infrastructure, alignment, and trust. Healthcare's hesitation reflects deeper fears across the board: 49% of all respondents worry about cyberattacks on AI systems, and 43% are concerned about data privacy.



Planned AI usage (Next 12 months)

Why This Matters

AI tools are rapidly becoming more accessible — but implementation is where most SMBs fall short.

Key concerns from the survey:

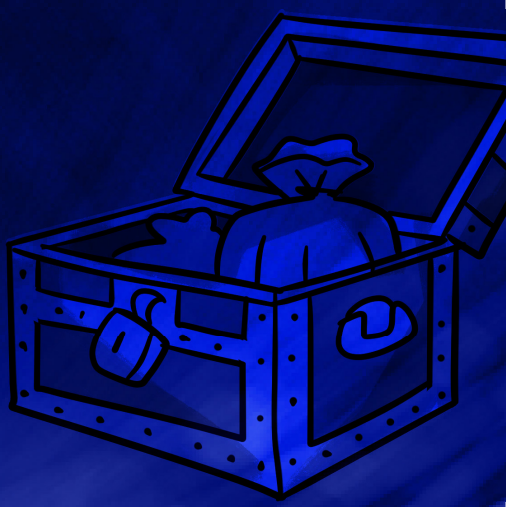
- **49% worry about cyberattacks on AI systems**
- **46% fear over-reliance**
- **43% cite data privacy issues**
- **31% mention cost as a barrier**

This paints a picture of an audience that's **open-minded but cautious** — ready to embrace automation, but wary of creating new blind spots. As our CISO Martin Lemay said last year: "Artificial intelligence (AI) is a major and promising advancement, deserving a place in human history. However, like fire, its use requires caution and discernment. Devoid of ethical awareness and not free from flaws, AI relies on vast amounts of data, which can be misused. Therefore, it is vital to establish appropriate governance and stringent data legislation to prevent abuse."

Compared to 2023, AI sentiment hasn't shifted dramatically. While the percentage of SMBs planning to use AI rose slightly (from 69% to 71%), and non-users dropped modestly (from 44% to 40%), there was **no meaningful leap in actual adoption. This suggests that while belief in AI continues to grow,** most organizations are still navigating foundational readiness — from tools and training to trust and integration.

> AI won't replace your cybersecurity team — but it will expose the cracks in your posture faster than ever. SMBs that treat AI as a partner, not a plugin, will be the ones who thrive.
>
> *David Hervieux, CEO, Devolutions*

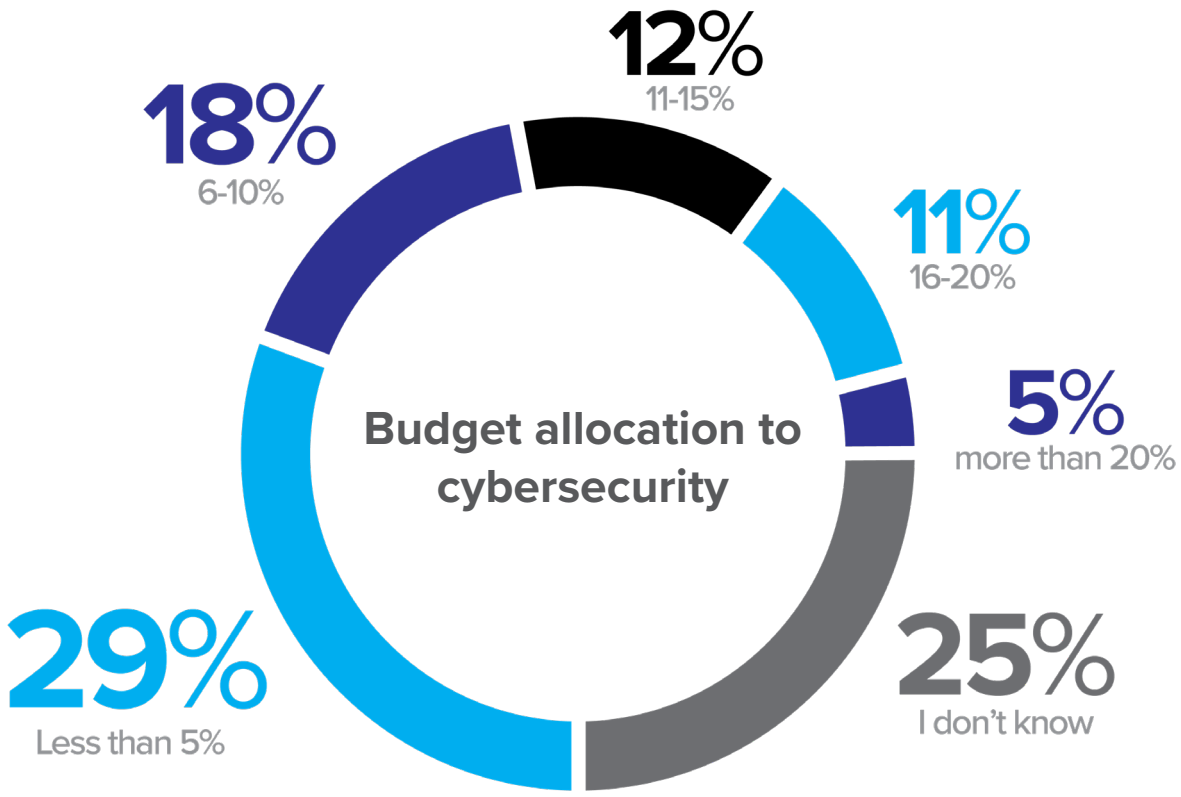
4 Budgets are growing, but still too low



63% of SMBs increased cybersecurity spending in 2024 — yet **29%** still allocate less than **5%** of their IT budget to it.

SMBs are spending more on cybersecurity — but not enough. Budgets are climbing, awareness is rising, and most leaders agree that cybersecurity is more important than ever. And yet, the data shows a concerning plateau: **too many organizations still underfund their security efforts relative to their risk exposure.**

That tension — between **budget optimism** and **budget reality** — is what defines this insight.



Role Breakdown: Who's spending... and who's still struggling?

55% still cite lack of budget as a blocker — despite rising spend. Visibility and prioritization matter just as much as dollars.

Role group	% Who increased budget
C-level executives	67%
Security professionals	64%
IT / Employees	61%

While leaders report rising budgets — and in some cases, they're driving that change — IT and security teams continue to flag resource shortages, deferred upgrades, and implementation gaps. If more money is being spent, but teams still feel constrained, the issue isn't just budget — it's how and where that budget is applied.

hese blockers confirm what IT and security teams have been saying: increased budget doesn't always mean empowered execution. While 63% of SMBs say they've increased cybersecurity spending, 55% still cite lack of budget as a top obstacle, and nearly half face skill gaps. Add to that low visibility into trends, weak prioritization, and performance blind spots — and it's no surprise that many teams feel like they're working harder without getting ahead.

What's holding SMBs back from advancing cybersecurity?

- **55%** Lack of budget
- **48%** Skill gaps
- **42%** Prioritizing of the other tech
- **25%** Low threat awareness
- **21%** Lack of perfornance metrics
- **20%** Belief current approach is adequate
- **17%** Low trend awareness
- **9%** Outsourcing uncertainly
- **9%** Not a priority

WHAT THIS SHOWS:

Sector Sidenote: Education

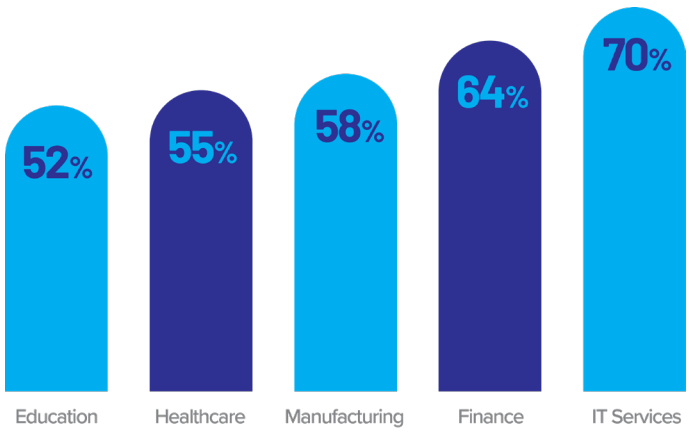
Only 52% increased cybersecurity budget in the past year — lowest of all tracked sectors

"Digitizing faster than they're securing."
In the education sector, digital transformation is moving fast — but security investment isn't keeping pace. Cloud adoption, remote access, and student privacy laws all raise the stakes, but many institutions are still operating **with outdated tooling and insufficient budget controls.**

"Cybersecurity Budgets: UK Invests Smarter, USA Plays Catch-Up."

When it comes to cybersecurity spending, the gap between strategy and execution becomes clear. In the UK, SMBs are showing stronger discipline, with a higher percentage allocating **more than 10%** of their IT budgets toward cybersecurity initiatives. In contrast, in the USA, while **63% of SMBs report increasing their budgets,** a large portion still allocate **less than 5%** of their overall IT spend to security. **Growth without strategic alignment risks reinforcing weak spots — not fixing them.**

Budget growth by sector



Why This Matters

More SMBs say they're spending more — but the underfunded majority hasn't moved much at all.

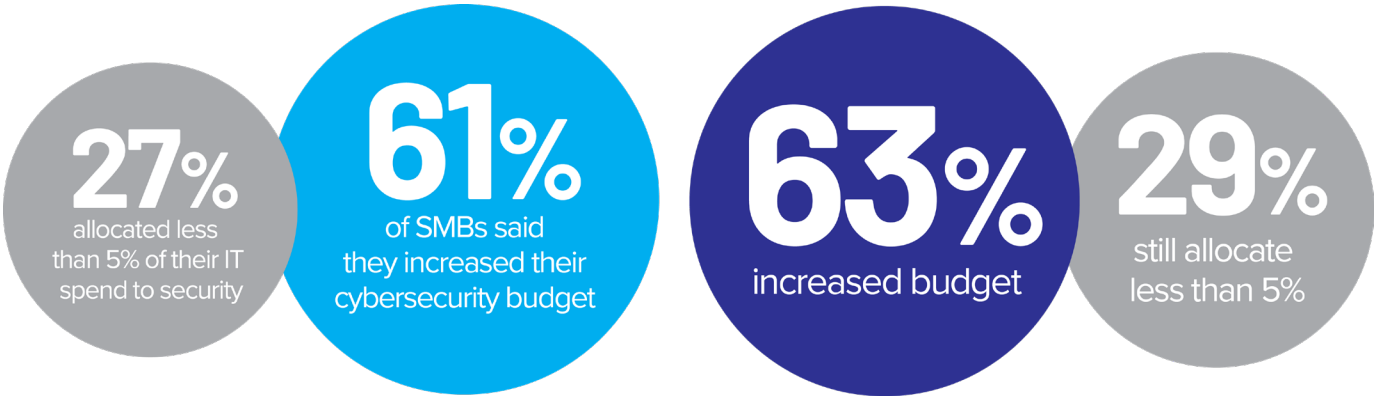
Security spend is often treated like insurance: easy to defer, hard to quantify — until something goes wrong. But in 2024, that mindset no longer holds.

Without proper investment:

- **PAM, AI, and training remain out of reach**
- **Shadow IT and unsecured endpoints multiply**
- **Talent retention and upskilling lag behind threat evolution**

Meanwhile, insurance providers, partners, and regulators are demanding more — and SMBs that don't evolve may find themselves disqualified or uninsurable.

Comparison to 2023: Budget vs Expectation



> Cybersecurity is no longer a technical cost — it's a business risk. And SMBs that treat it as an IT line item will find themselves unprepared for the demands ahead.
>
> *Simon Chalifoux, CIO, Devolutions*

5 Insider threats: a known risk, but rarely addressed

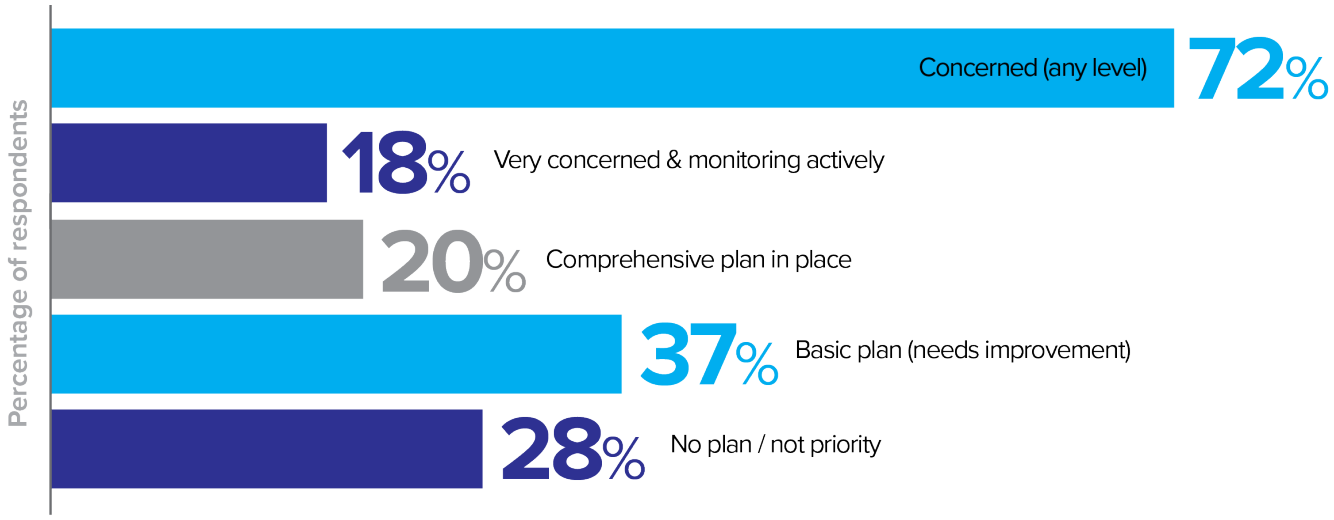
78% of SMBs are concerned about insider threats — but only **20%** have a comprehensive plan to manage them.

Insider threats are a growing concern across every sector — and with good reason. Whether intentional (data theft, sabotage) or unintentional (misconfigurations, phishing clicks), insider-driven incidents are rising. But while awareness is high, **execution is lagging.**

This chapter exposes one of the starkest gaps in the entire survey: **most SMBs know insider threats are real — but few have done anything meaningful to address them.**

The gap between awareness and action is one of the starkest in the survey. **78% of SMBs are concerned, but only 20% have a plan — and just 18% actively monitor for insider risks.** A full 28% either have no plan or don't see it as a priority.

Insider threats: Awareness vs. Action



Role Breakdown: Awareness vs. Accountability

Insider risk isn't just a technology problem — it's a leadership and accountability gap.

Even among security professionals, **only 1 in 4** report having a mature insider threat strategy. C-Level execs tend to assume plans are in place — but IT teams often see the truth: partial policies, inconsistent enforcement, and weak tooling.

Role group	% With a real insider threat strategy
C-level executives	26%
Security professionals	24%
IT / Employees	17%

WHAT THIS SHOWS:

Sector	% Concerned	% With full strategy
Manufacturing	75%	15%
Education	77%	18%
Healthcare	79%	20%
Finance	83%	22%
IT Services	85%	27%

Sector Sidenote: Manufacturing

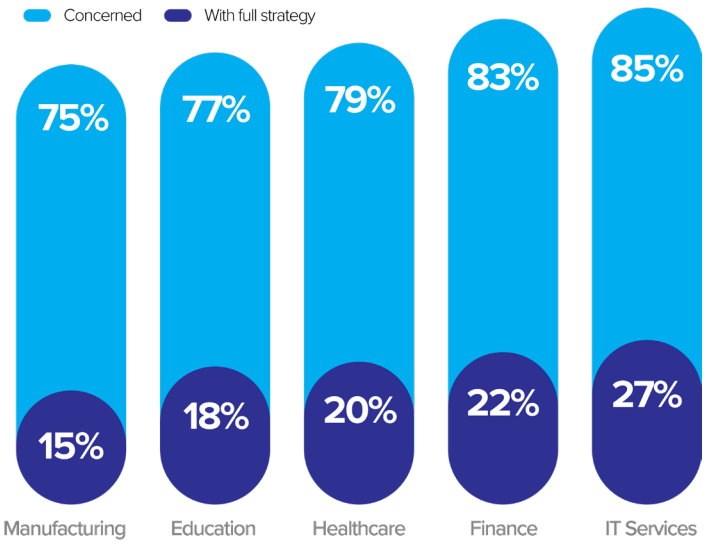
Only 15% of manufacturing organizations report having a full insider threat strategy.

"Awareness without structure."
Manufacturing is becoming more digitized — but many organizations are still operating with little visibility into user behavior, shared accounts, or third-party access. Insider threats are recognized, but response frameworks remain undeveloped.

Sector Summary: Awareness Outpaces Action

Every sector shows high concern — but no sector breaks 30% for full strategy adoption.

Insider threats: Concern vs. Strategy by sector



Why This Matters

Awareness has more than doubled — but actual strategy adoption has only crept forward. SMBs are thinking about insider threats more than ever — but they're still not acting.

Unlike ransomware or phishing, **insider threats often bypass traditional defenses.** They require visibility, context, and policy — not just technology. SMBs can't afford to treat them as afterthoughts. **It's time to move from passive concern to proactive planning.**

When unmanaged, insider risk:

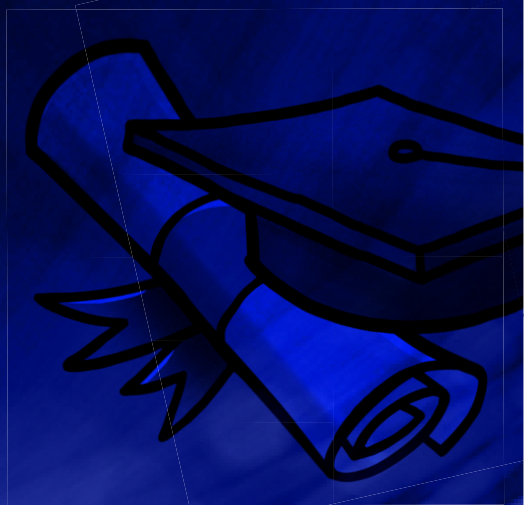
- **Weakens detection and response posture**
- **Creates regulatory and insurance exposure**
- **Erodes trust across teams and departments**

Many SMBs are adopting PAM, MFA, or training programs — but **without tying them into a broader insider strategy**, they're missing the point.

Compared to 2023, insider threat awareness has skyrocketed — from 33% last year to 78% in 2024. But despite this sharp rise in concern, the number of SMBs with a **comprehensive insider threat strategy** only increased marginally — from around **15% to just 20%**. The takeaway is clear: **more companies are talking about insider threats, but very few are actually doing anything about them.**

> You can't stop insider threats with a checklist.
>
> It takes visibility, culture, and trust — backed by policy.
>
> *Patrick Pilotte, CISO, Devolutions*

6 Training Still Isn’t Standard



Only 39% of SMBs offer continuous cybersecurity training — and 17% offer none at all.

Cybersecurity isn't just about tools — it's about people. And while awareness campaigns and phishing simulations have become more common, our survey shows that **most SMBs still lack a consistent, structured training program - and that's a problem.**

Because today, **the majority of breaches still involve human error** — whether it's clicking a malicious link, misconfiguring a system, or failing to report suspicious activity. And yet, nearly 1 in 5 SMBs don't provide any training at all.

Cybersecurity training by type

Role Breakdown: Who Gets Training — and Who Doesn't?

This isn't just a content problem — it's a perception problem. Training may exist, but it's often inconsistent, under-prioritized, or disconnected from day-to-day risk.

Training access — and perception — varies widely by role. **Nearly half of C-level executives (48%) believe ongoing cybersecurity training is in place**, but that number drops to **42% among security professionals** and just **35% among IT employees**.

This gap isn't just about availability — it's about **visibility**. Executives may believe training is happening because it's been mandated or budgeted. But on the ground, IT staff and technical teams **experience the inconsistency directly** — from missing modules to infrequent follow-ups or unclear expectations.

WHAT THIS SHOWS:

Sector Sidenote: Education

Only 29% of education-sector respondents say they offer continuous training.

"Security awareness should be foundational — especially in learning environments." Education systems manage large volumes of personal data, operate across hybrid access models, and face strict compliance obligations. And yet, **training often gets squeezed by budget, staffing, or operational focus.**

Let's look at how this training gap plays out across sectors. While IT Services leads with 45% offering continuous training and just 7% reporting none, Education tells a different story: 29% continuous training, 20% with none at all. Manufacturing and Healthcare show similarly troubling gaps. Even in highly regulated or data-sensitive environments, a consistent training culture is far from guaranteed.

Why This Matters

Cybersecurity isn't a product you install — it's a culture you maintain.

And culture only sticks when it's relevant, ongoing, and role-specific.

Tools can't stop what users don't understand.

When training is infrequent or poorly reinforced:

- **Phishing susceptibility increases**
- **MFA fatigue and password reuse become normalized**
- **Reporting behaviors break down**

Compared to 2023, the story around training has actually gotten worse. Last year, 41% of SMBs reported offering ongoing training — this year, that number dropped to 39%. Meanwhile, the share of organizations offering no training at all jumped from about 10% to 17%.

The message is clear: while threats are evolving, training practices are slipping backward. Despite better tools and greater awareness, many SMBs are failing to invest in their most critical line of defense — their people.

SMBs that take training seriously will empower their teams, reduce their risk, and build a security culture that lasts.

The rest?
They'll keep reacting to the same mistakes — one click at a time.

> Training isn't optional.
>
> It's your frontline — and if it's not continuous, it's not effective.
>
> *Simon Chalifoux, CIO, Devolutions*

Conclusion

Conclusion: Progress Is Real — But Exposure Remains High

The six key insights in this report reveal a consistent pattern: SMBs are thinking more seriously about cybersecurity — but they're still struggling to operationalize that awareness. From PAM and AI to insider threats and training, the gap between knowing and doing remains wide.

But the story doesn't stop there.

The broader survey data reveals a landscape where risk remains persistent and progress is uneven:

- **43% of SMBs faced at least one cyberattack in the past year**
- **Only 31% were able to detect the incident within minutes**
- **48% are concerned about the cybersecurity impact of geopolitical instability**
- **Despite 88% adopting MFA, 29% still struggle with weak or reused passwords**
- **Just 35% of SMBs have full cyber insurance coverage**

These stats tell us that technology adoption isn't the same as security maturity. Many SMBs are doing the right things — but not deeply enough, or not consistently enough, to keep pace with today's threats.

There's no denying the momentum: budgets are rising, awareness is growing, and leadership is more engaged than ever. But the report overall message is clear:

Perception is ahead of execution. Strategy is forming — but behavior is lagging.

The good news? SMBs have never had more access to affordable tools, smarter training, and partner support than they do today. But to truly close the gap, it's not enough to deploy new tools — **security must be embedded into every layer of your organization.**

Cybersecurity isn't about fear — it's about readiness.
And readiness means more than tools.
It means awareness, alignment, and action.

At Devolutions, we believe that SMBs deserve solutions designed for their scale, their speed, and their reality. You don't have to do everything — but you have to start. Because in cybersecurity, doing nothing is the biggest risk of all.

David Hervieux, CEO, Devolutions

Future Outlook

Future Outlook: What to Expect in 2025 and Beyond

If 2024 was the year of awareness, 2025 must be the year of alignment. SMBs are no longer in denial about cybersecurity — but many remain in a transitional phase. The good news? That transition is finally accelerating.

The future isn't about outrunning every threat — it's about building the reflexes to respond with clarity, confidence, and control. SMBs that focus on resilience, not perfection, will win.

1. PAM Will Go Mainstream — and Get Simpler
With more SMBs demanding lightweight, low-friction PAM solutions, vendors are responding. Expect **easier integrations, modular pricing**, and **cloud-native features** that fit the pace of small teams — not just enterprise IT.

2. AI Will Shift From "Exciting" to "Expected"
As costs drop and capabilities mature, AI tools are becoming standard. But **trust, transparency, and strong governance will be key** — especially with **66% of orgs predicting AI will have the biggest impact on cybersecurity by 2025.**

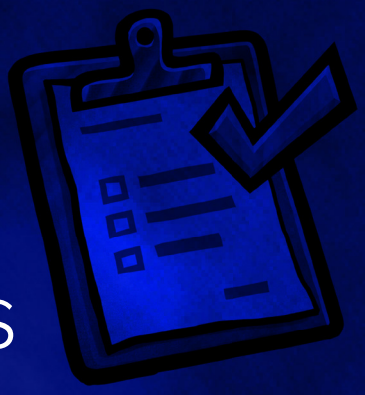
3. Training Will Move From "Required" to "Cultural"
Regulators and insurers are pushing for **continuous, measurable user training.** Expect to see **gamified learning, real-time microcoaching**, and **role-based modules** become the norm — not the exception.

4. Strategy Will Overtake Reaction
SMBs are shifting from **compliance-driven defense** to **long-term resilience**. The smartest teams won't just defend against threats — they'll build strategies that reduce stress, improve retention, and drive IT maturity.

5. Global Events Will Keep Reshaping Risk
From nation-state threats to supply chain attacks, the external risk landscape is shifting fast. SMBs that stay agile — **with flexible tools and clear playbooks** — will be better prepared for the next unknown.

6. Remote Access Will Demand Smarter Security
VPNs and portals helped SMBs go remote — but they weren't built for today's risks. **74% still rely on VPNs**, and **41% cite unauthorized access as a top concern.** In 2025, securing remote access will mean **moving beyond perimeter defenses** to **identity-driven, monitored models** — like Just-in-Time Access and Zero Trust.

Recommendations



Recommendations: What SMBs Should Do Next

Cybersecurity doesn't need to be perfect — it needs to be practical, consistent, and aligned with your actual risks.

Based on this year's data, here are five priorities every SMB should consider moving forward:

1.

Move Away from Manual PAM

52% of SMBs still use spreadsheets to manage privileged access.

Start with a lightweight PAM solution that integrates with your stack and supports just-in-time access, session logging, and policy enforcement — without a full-time admin. Devolutions Server offers exactly that, purpose-built for SMBs without the enterprise overhead.

The Devolutions solution:

Workforce password management

Devolutions Workspace / Devolutions Hub / Devolutions Server

https://devolutions.net/solutions/

2.

Make Training Continuous, Not Occasional

Training isn't a checkbox. It's culture.

Go beyond annual webinars. Build role-based, ongoing programs. Simulate phishing. Reward engagement. Make training stick — not just exist. Our Devolutions Academy platform offers on-demand security education for users, admins, and MSPs — making it easy to reinforce the habits you need to protect your team.

The Devolutions solution:

Devolutions Academy

We offer a free continuing education platform designed for the realities of small teams.

https://academy.devolutions.net/

3.

Bridge the Confidence –Posture Gap

Most leaders feel confident. Most teams don't. Run quarterly posture reviews with IT, security, and execs. Compare assumptions to audits. Ask: Are we actually prepared — or do we just think we are?

If you're using Devolutions solutions like Devolutions Server or Devolutions Hub Business, leverage built-in audit trails, access reports, and credential usage logs to surface the truth — and spark better security conversations across your organization.

The Devolutions solution:

Remote access management

Devolutions Gateway / Devolutions Launcher
Devolutions Workspace / Devolutions Hub / Devolutions Server

https://devolutions.net/solutions/

4.

Get Proactive About Insider Threats

Insider risk is real — and under-addressed.

Create a documented strategy: policy + monitoring + onboarding/offboarding. Bake it into your PAM and training flows. Don't treat insider threats like edge cases — treat them like inevitabilities. With Devolutions Hub Business, you can centralize account access and enforce least privilege — while still empowering your team to work fast.

The Devolutions solution:

Privileged access management

Devolutions PAM / Remote Desktop Manager / Devolutions Gateway / Devolutions Launcher / Devolutions Workspace / Devolutions Hub / Devolutions Server

https://devolutions.net/solutions/

5.

Match Budget to Exposure — Not History

60% increased their budget. But many still underinvest.
Instead of just spending more, spend smarter — align your cybersecurity investment with the real size of your risk surface. Focus on tools that offer scalability without complexity, and value that grows with your business. Devolutions solutions are priced for SMBs — and built to scale as your needs evolve,

No lock-in. No complexity. Just the features you need, when you need them.

The Devolutions solution:

Remote connection & IT management

Remote Desktop Manager / Devolutions Gateway / Devolutions Launcher / Devolutions Workspace / Devolutions Hub / Devolutions Server

https://devolutions.net/solutions/

You don't need to fix everything at once. But you do need to start fixing something — with clarity, consistency, and leadership.

Final Word from Our CEO

David Hervieux, CEO, Devolutions

"We talk to SMBs every day. And the truth is, most of them know what they're up against — they just don't know where to start, or whether they're doing enough.

This report confirms what we've been hearing for years: it's not about awareness anymore. It's about action. You can't just feel secure — you have to build systems, habits, and cultures that back that up.

That doesn't mean doing everything. It means doing the right things, at the right time, for your organization. That's the approach we've always taken at Devolutions — practical, flexible, and built for teams who need real protection without extra complexity.

If this report helps you take one step forward — review your training, formalize your access policy, or just have a better conversation with your team — then it's already done its job.

Start small. Stay consistent. You'll get there."

Devolutions

How Devolutions Can Help

Built for SMBs: Tools that Work Like You Do

At Devolutions, we believe SMBs shouldn't have to choose between simplicity and security. That's why we've developed a suite of Privileged Access Management, Password Management, and Remote Access tools — built specifically for small IT teams.

What makes our approach different?

Designed for SMBs
lightweight, cost-effective, and fast to deploy

Secure by default
enterprise-grade encryption, audit trails, and granular access controls

Flexible and scalable
deploy on-prem or in the cloud, with no compromise

Accessible anywhere
mobile-ready and remote-first workflows

Backed by experts
world-class onboarding and in-house support

Devolutions

Whether you're just starting with PAM or looking to formalize remote access, Devolutions gives you the tools to move forward — with confidence and control.

Several resources are available to you:

Devolutions Academy
https://academy.devolutions.net/

Devolutions documentation
https://docs.devolutions.net/

Devolutions forum
https://forum.devolutions.net/

Devolutions blog
https://blog.devolutions.net/

Contact Us

Email: sales@devolutions.net
Website: www.devolutions.net
Live Chat: Available on our website
Phone: +1 844 463-0419