Devolutions

THE STATE OF IT SECURITY

IN SMBS IN 2023-2024

WHERE IT MEETS SECURITY

We are excited here at Devolutions to unveil the fourth edition of our annual report on the current landscape of IT security among small and medium-sized businesses (SMBs) globally. This year, we're shifting our focus to spotlight the most striking and significant statistics, diving into why they matter. While we've observed steady progress among SMBs in bolstering their cyber defenses, glaring oversights continue to persist. These lapses not only threaten financial stability but also jeopardize reputational integrity.

Despite advancements in security measures, SMBs remain firmly in the crosshairs of cybercriminals. In 2023 alone, nearly 43% of all cyberattacks were directed at SMBs. Alarming spikes in incidents such as ransomware payments and Internet of Things (IoT) malware attacks indicate that this year has been particularly challenging. The stakes are higher than ever as technology — especially artificial intelligence — serves as both a tool and a potential threat, underscoring the imperative to commit more resources to cybersecurity.

The report identifies a heightened level of concern among SMBs regarding cyber threats — and rightfully so. Our survey data shows a 9% increase in cyberattacks against the participating companies, consistent with the report that 71% of businesses fell victim to ransomware attacks in 2023.

While the majority of our survey respondents believe they have adequate protection against cyber risks, this report poses a critical question:

Is that confidence well-placed?

Table of contents

Methodology

This online survey was conducted from March 2023 to May 2023 by Devolutions, among 217 IT executives and decision-makers from worldwide-based small and medium-sized businesses operating in the IT field and other domains.

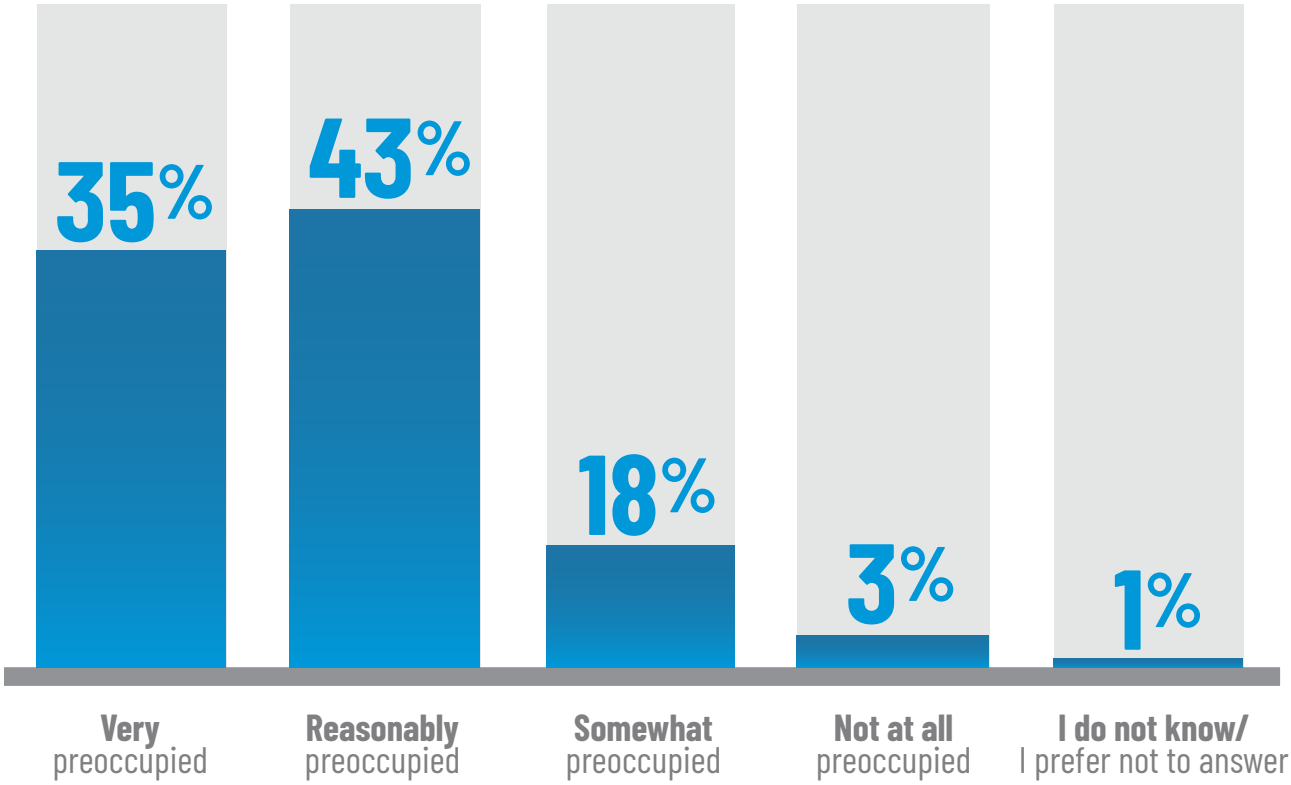
Section 1

RISING CONCERN BUT PERSISTENT THREATS

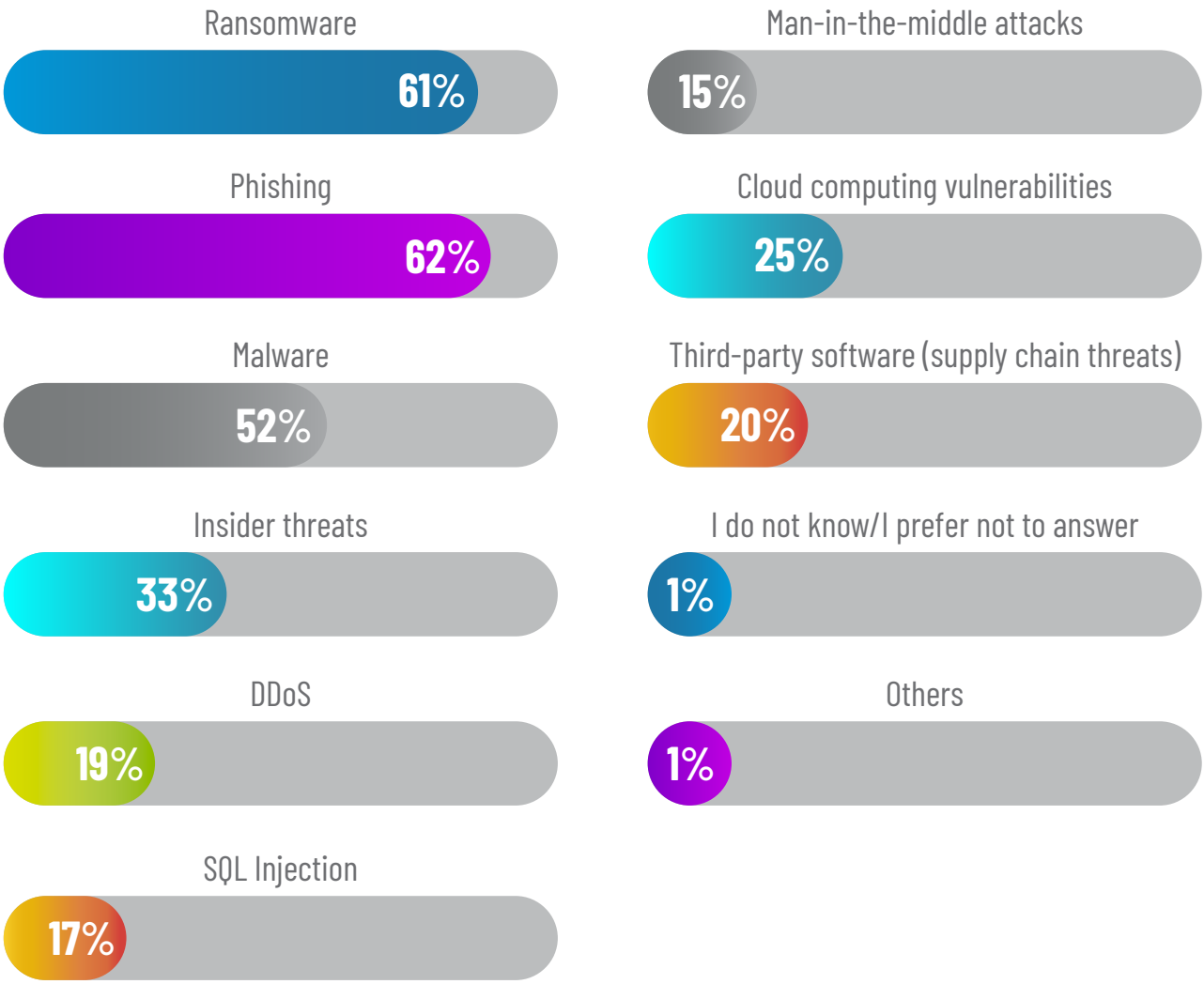
The fact that 78% of respondents are more concerned about cybersecurity is a double-edged sword.

Heightened awareness is good: it can lead to proactive measures. But the same top threats — Ransomware (61%), Phishing (62%), and Malware (52%) — have not changed since last year, indicating that concern has not yet translated into effective countermeasures for these specific threats. Password security and phishing are the most popular training topics, aligning with the types of threats organizations are most concerned about. But is the training effective, given that these are also the most prevalent attack types?

LEVEL OF CONCERN OF COMPANIES IN RELATION TO THE CONFIDENTIALITY AND SECURITY OF THEIR DATA

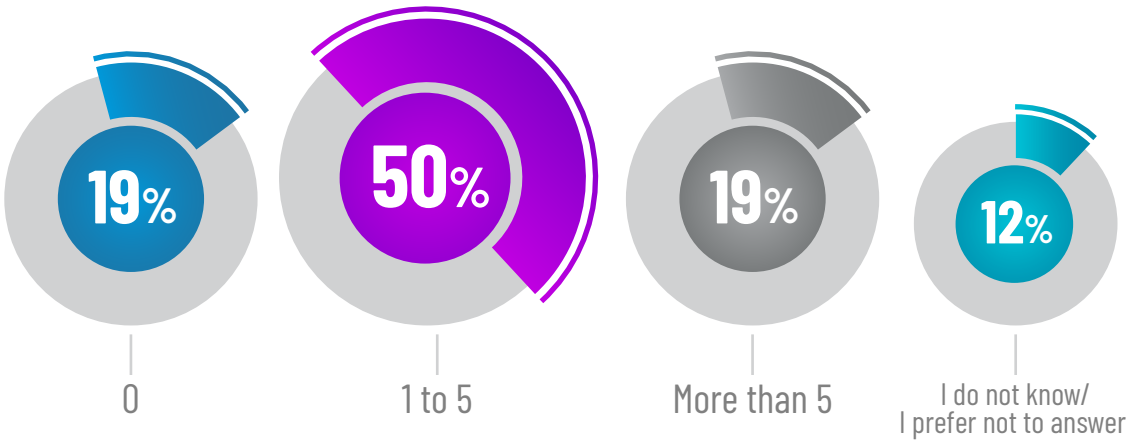


TOP THREE CYBERSECURITY THREATS
OF GREATEST CONCERN



And that fear is totally understandable. The 9% year-over-year increase in cyberattacks, with 69% of respondents falling victim, shows that SMBs are still very much a target.

NUMBER OF CYBERATTACKS BUSINESSES FELL VICTIM TO IN THE LAST YEAR



The actual figures could well be higher than reported, considering that not every cyberattack is officially recorded — this includes those that are currently underway. These statistics serve as a stark reminder that SMBs simply cannot afford to neglect IT security or cybersecurity. The average financial impact of a data breach has escalated to a record-breaking $4.54 million USD per incident across organizations of all sizes. Specifically for SMBs, the monetary repercussions can vary significantly, ranging from $120,000 to $1.24 million USD per episode, influenced by multiple factors such as the volume of compromised records.

Amidst the evolving digital landscape, it becomes clear: vigilance and action must supersede concern. For SMBs, the cost of inaction isn't just financial — it's the very survival of the business.

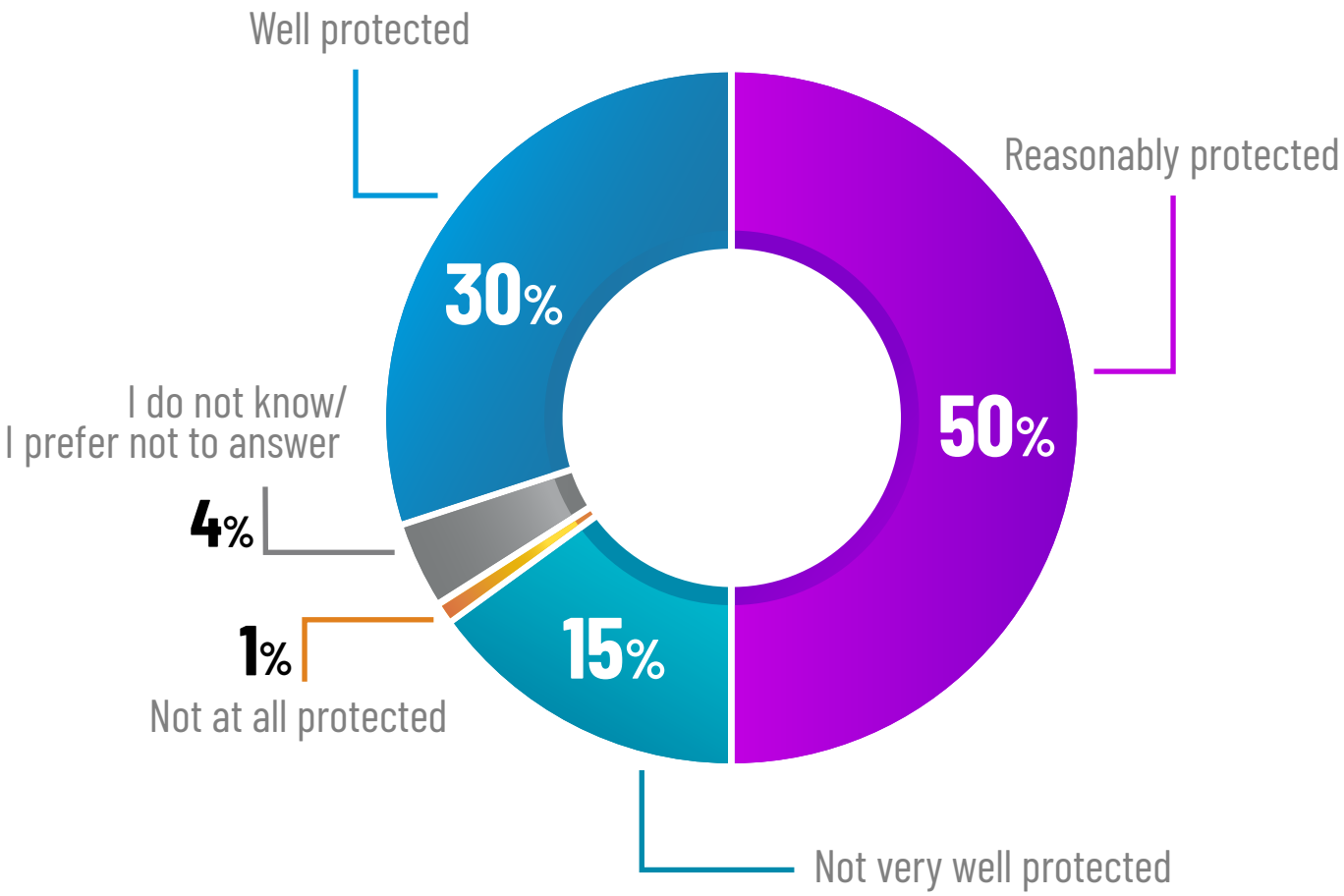
David Hervieux,
CEO of Devolutions

Section 2

COMPLACENCY RISK

While 80% of respondents consider themselves well protected, less than 60% employ essential security measures like password managers, two-factor authentication, or cybersecurity training. This disconnect between perception and reality can be a dangerous blind spot.

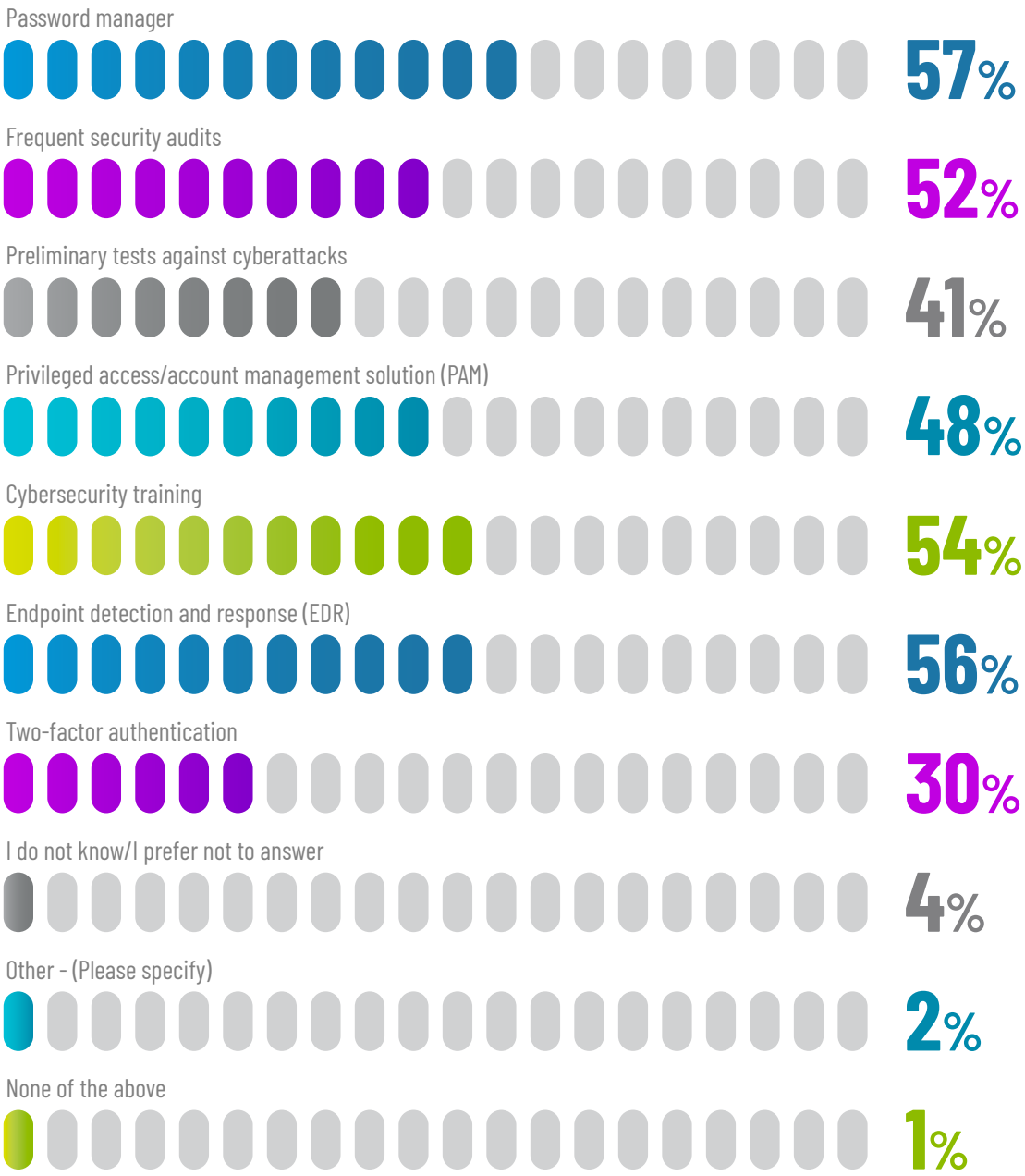
EVALUATION OF ORGANIZATIONAL CYBERATTACK PROTECTION LEVELS



Various factors could contribute to this disconnect.

Financial constraints, often attributed to the smaller scale of the organization, could limit the budget allocated to cybersecurity measures. Additionally, there's a tendency to underestimate the evolving complexity of cyberattacks, which are becoming increasingly sophisticated. Moreover, employee behavior and a lack of adequate cybersecurity training can further weaken the defense infrastructure, as end users are commonly viewed as the most vulnerable element in the cybersecurity equation.

SECURITY MEASURES IMPLEMENTED IN BUSINESSES




In the realm of cybersecurity, perception is not always synonymous with protection. A genuine sense of security lies not in belief, but in the continuous adaptation to, and implementation of, the changing digital defenses.
Martin Lemay,
CISO at Devolutions

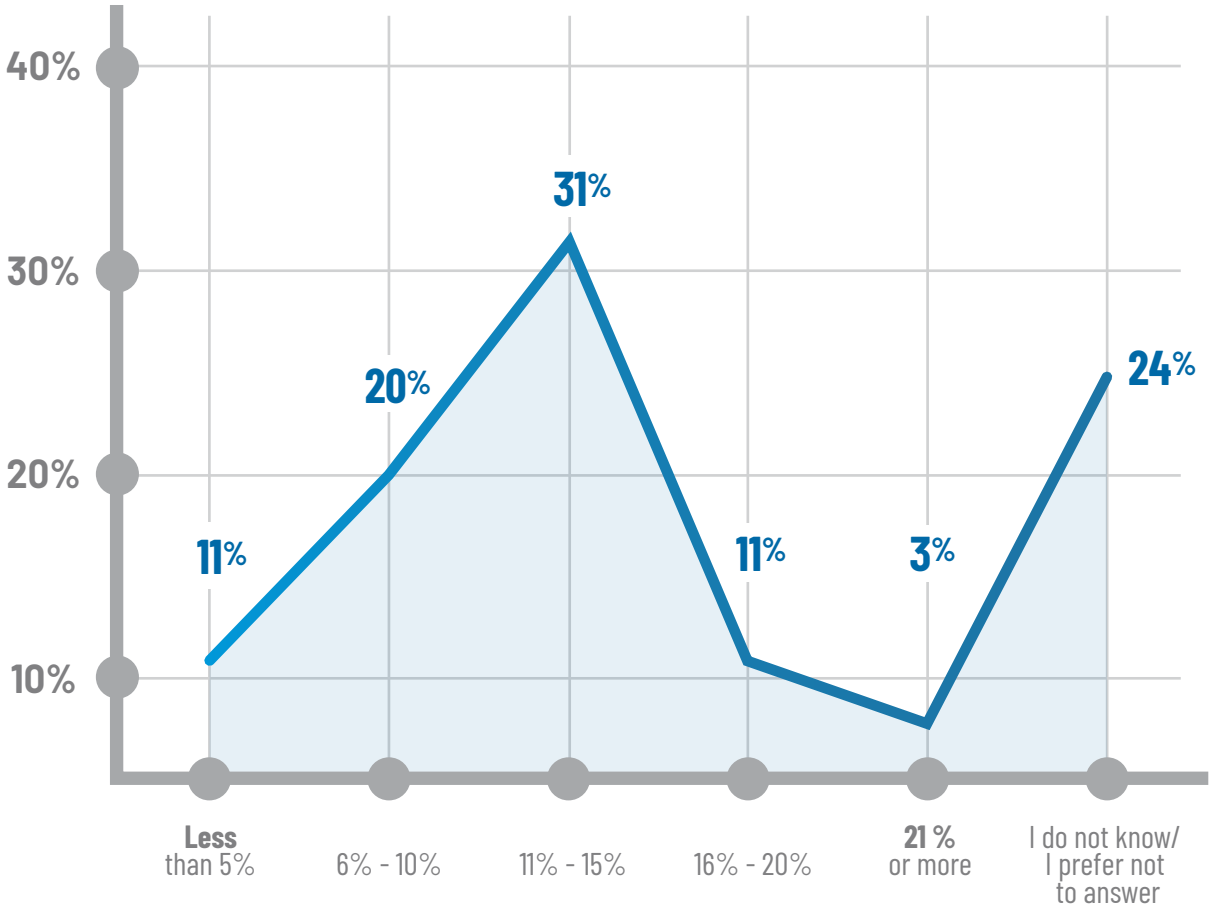
Section 3

EXPERTISE AND BUDGET

Last year, 68% of SMBs were spending the recommended 6–15% budget on IT security. This year, only 51% are meeting the recommended spending.

The drop is significant, but also understandable since SMBs are facing more and more financial pressure. SMBs who can't afford to allocate more money to security should focus their attention on spending the budget they do have more strategically. And speaking of allocating resources strategically: it's encouraging to see that 86% of respondents have invested in cybersecurity expertise either in-house or through external consultants.

BUDGET ALLOCATED TO CYBERSECURITY
AS A PERCENTAGE OF THE TOTAL IT BUDGET



PRESENCE OF A DEDICATED CYBERSECURITY LEAD OR TEAM IN ORGANIZATIONS

Bridging the Gap

51% meeting the recommended budget is a positive sign; however, **it's essential to consider the other 49%.**

What barriers are they facing?

Are they aware of the risks of underinvestment?

This statistic presents an opportunity for awareness campaigns, tailored solutions, or even government incentives.

Cybersecurity Expertise

The fact that 86% of respondents have cybersecurity expertise, either in-house or through external consultants, shows a holistic approach to security.

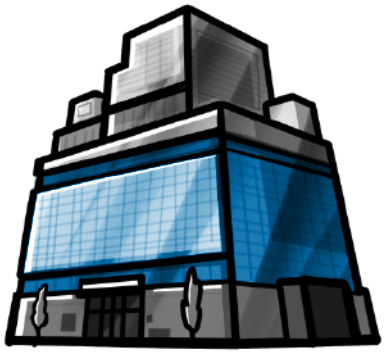
It's not just about tools and software but also about having knowledgeable individuals to implement, manage, and adapt those tools.

In-House OR External Consultants:

In-House Expertise: This suggests that the company values cybersecurity enough to have dedicated personnel. It can lead to quicker response times during incidents and tailored security policies. However, it may also mean a consistent overhead cost.

External Consultants: This indicates flexibility and scalability. SMBs might hire consultants for specific tasks, audits, or implementations. While this might reduce overhead costs, it may also lead to concerns about continuity or the long-term strategy.

Remaining 14%: This is a significant number of businesses without dedicated cybersecurity expertise. It raises concerns about their vulnerability to threats, their ability to respond to incidents, and their overall security posture. Again, this points to a potential area for intervention, education, or support.

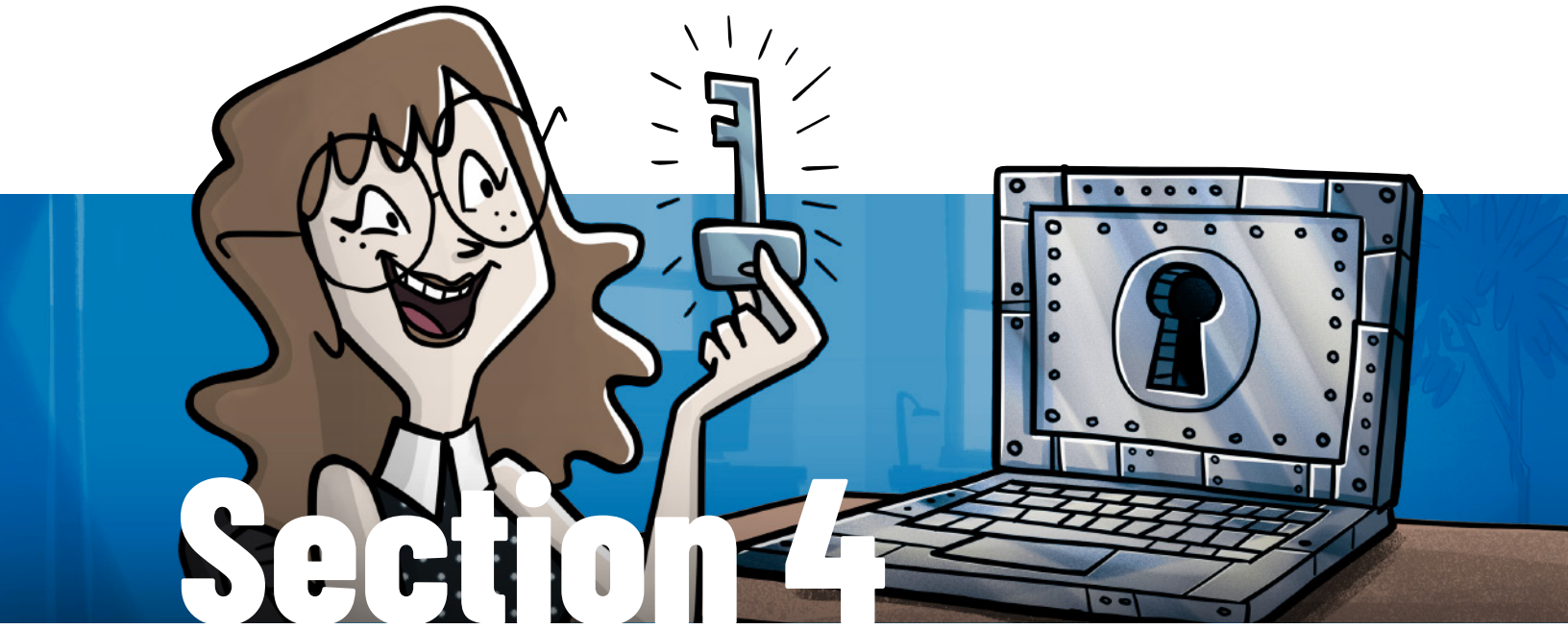


It's not always easy to hire a security team in-house to take care of cybersecurity.

That's why the help of an MSP can become crucial for SMBs. **MSPs help SMBs increase their capacity and skillset, reduce costs and risks, take advantage of growth opportunities, enhance user experience, manage uncertainty, and proactively plan for the future.** To choose the right MSP, SMBs should focus on these seven core factors: services, advice, affordability, fearlessness, responsiveness, business continuity and disaster recovery, and technology and vendor neutrality.

We are in the era of the digital Wild West, where threats are abundant. Organizations absolutely must develop a defense capability to protect their interests and all their stakeholders from often predictable cyberattack opportunities. Whether this capability is developed internally or outsourced, expertise in cybersecurity is crucial to maintain balance.

Martin Lemay,
CISO at Devolutions



Section 4

DEPLOYMENT CHALLENGES

While there's an 8% increase in the deployment of Privileged Access Management (PAM) solutions, 35% report negative experiences, such as delayed or complicated access to resources. This increase in dissatisfaction could signify implementation challenges or a lack of training.

An 8% increase in PAM deployment indicates that more businesses are recognizing the significance of managing privileged accounts. This can be driven by an increased awareness of insider threats, regulatory requirements, or the potential damage that can result from breached privileged accounts.

IMPACT OF PAM CONTROLS ON WORK
VELOCITY AND PRODUCTIVITY IN ORGANIZATIONS

35% **Yes, and the effects have been negative.** It is taking longer and/or it is more complicated to access certain resources.

52% **Yes, and the effects have been positive.** Our approval workflow is better, and productivity has increased.

5% **No,** we have not experienced any effects (positive or negative).

5% **At this time,** we do not have any PAM controls implemented.

3% I do not know/ I prefer not to answer

35% reporting negative experiences is a significant number. While PAM is designed to enhance security, it shouldn't come at the expense of operational efficiency. Delayed or complicated access to resources can impede workflow, reduce productivity, and lead to dissatisfaction.

Even if respondents say that it's sometimes challenging to put a PAM solution in place and use it, 95% think it's important to have one in place.

So is it a lack of training, a lack of resources in place to put the PAM solutions in place from the beginning, or is it that the chosen PAM solutions aren't the best fit for some businesses? **It's a mix of everything.**

Implementing robust security measures is much like fitting a puzzle; while each piece holds importance, it's the alignment and seamless integration that paints the complete picture. It's not enough to recognize the value; the journey to true cybersecurity requires tailored solutions, adequate training, and constant adaptation.

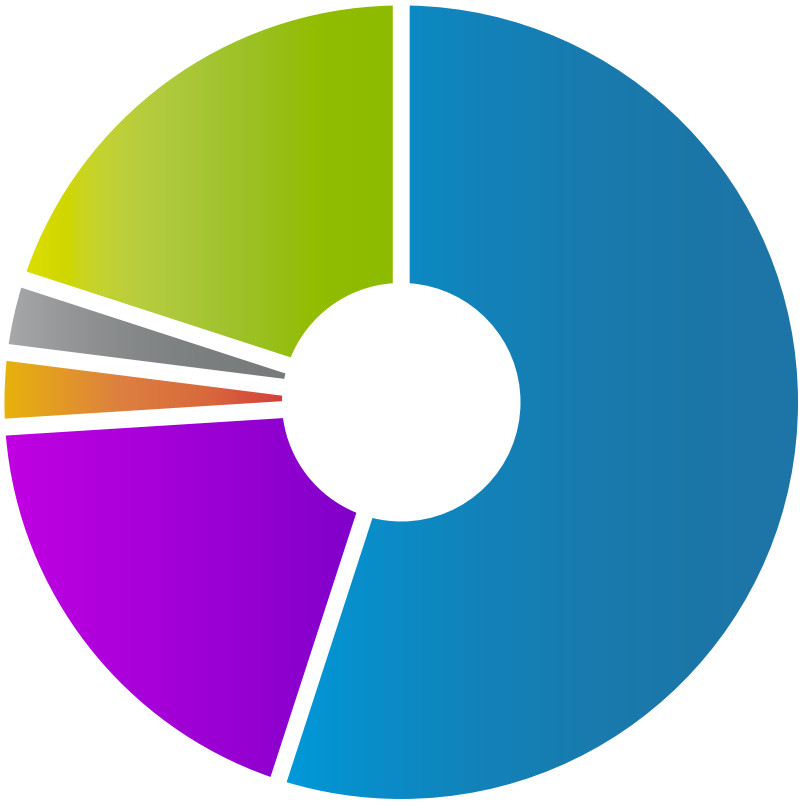
David Hervieux,
CEO of Devolutions

Section 5

CLOUD & AI CONFIDENCE

> Three quarters of the survey participants deem cloud solutions as trustworthy, **with 81% expecting their cloud usage to increase.**

BUSINESSES' LEVEL OF TRUST
IN CLOUD SOLUTIONS



20%
Very confident;
we work continually
with cloud solutions

55%
Reasonably confident

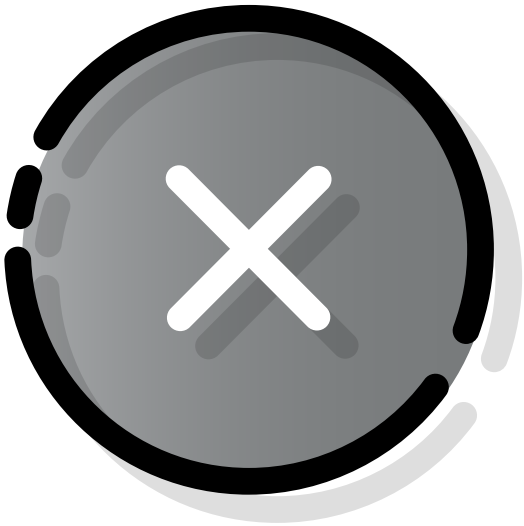
19%
Not very confident;
we have certain doubts about their security

3%
Not at all confident;
we object to using cloud solutions because they are not at all secure

3%
I do not know/
I prefer not to answer

USE OF CLOUD SOLUTIONS
IN THE UPCOMING YEAR

yes
81%



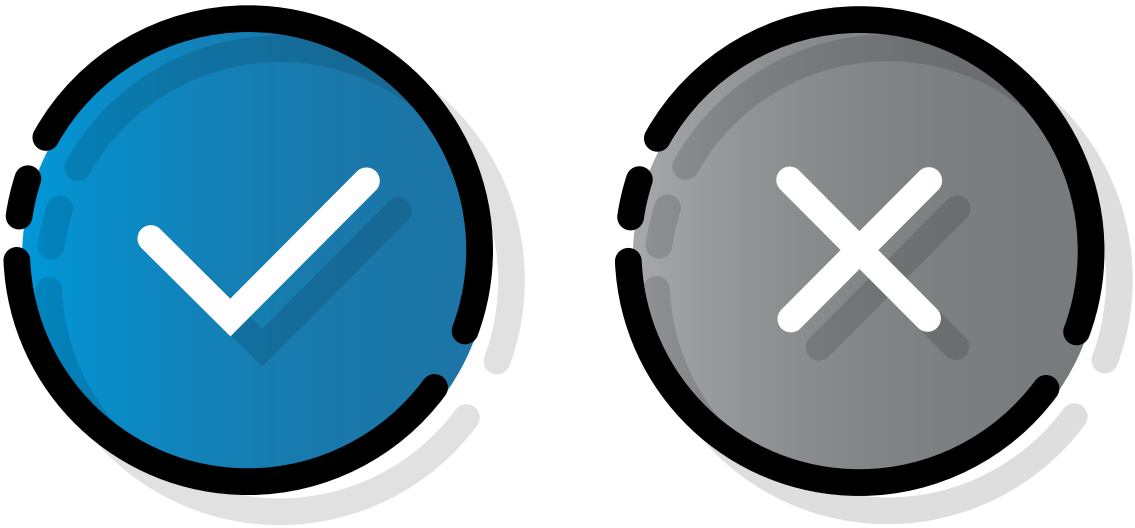
no
10%

(**9%** I do not know/I prefer not to answer)

This optimism extends to AI, with 56% of respondents expressing "confident" trust levels. The increasing reliance on these technologies begs the question: are SMBs prepared for the security challenges they bring?

BUSINESSES' LEVEL OF TRUST IN ARTIFICIAL INTELLIGENCE

USE OF ARTIFICIAL INTELLIGENCE
IN THE UPCOMING YEAR



yes
69%

no
22%

(**9%** I do not know/I prefer not to answer)

While trust and adoption are growing, these technologies are not without risks. Cloud solutions, being internet-facing, can become vectors for cyber-attacks if not correctly configured. AI systems, if improperly designed or integrated, can also introduce vulnerabilities or can be manipulated.

Trusting and adopting a technology is one thing; ensuring it's securely integrated and maintained is another.

The optimism surrounding cloud and AI adoption is a testament to the perceived value of these technologies. **However, the critical question raised is timely and essential: as SMBs ramp up their use of these tools, are they also equipping themselves with the knowledge, strategies, and tools to counteract the associated security challenges?** Given the rapid evolution of technology, a proactive and informed approach to security will be crucial for SMBs to truly benefit from these technologies without falling prey to their potential risks.

Although the statistics indicate that our respondents are receptive to adopting the necessary tools for safeguarding themselves against potential AI-driven cyberthreats, it is concerning to note that a significant portion of respondents, in contrast, are not currently using PAM solutions.

So, yes, the technology is evolving, but are organizations evolving with it?

Section 6

FUTURE INVESTMENTS

Finally, the upward trend in anticipated security spending, particularly in AI, suggests that SMBs are recognizing the need for more advanced tools to fend off cyberthreats. However, will this translate to better security postures, or will it add complexity and new vulnerabilities?

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.

Martin Lemay,
CISO at Devolutions

Conclusion

As we wrap up this year's edition of our report on the state of IT security in SMBs, we're cautiously optimistic. The trends and data presented paint a picture of an evolving landscape, with SMBs making notable strides in their commitment to cybersecurity.

The awareness and increased concern among these businesses are laudable, and their proactive efforts are evident in the more robust defenses being implemented.

However, with 43% of all cyberattacks in 2023 targeting SMBs and a rise in specialized threats like ransomware and IoT malware, it's clear that there's still significant work ahead. While advancements in technology, including artificial intelligence, provide SMBs with powerful tools to defend themselves, they also introduce new vulnerabilities.

The rise in cyberattacks, especially against businesses that believe they are well-protected, underscores the importance of continuous evaluation and adaptation of security measures.

In essence, while the trajectory is promising, SMBs cannot afford to be complacent. The road to a fully fortified cyber defense is long and winding, and while we can celebrate the progress made, **it's crucial to remember: we are not out of the woods yet.**

RECOMMENDATIONS

Recognizing the growing need to provide tangible solutions and actionable steps for SMBs in the ever-complex world of cybersecurity, we've curated a recommendations section. These tips and strategies are designed to guide you in enhancing your defense mechanisms and ensuring your business is not only prepared but also resilient against the evolving cyberthreat landscape.

1. Instead of adopting a passive stance or believing they're too insignificant to be targeted, SMBs should actively shield themselves from cyber threats. The reality is that hackers are increasingly targeting SMBs, whose security measures are far too often lax.

2. SMBs should adopt a comprehensive set of principles and guidelines that both minimize cybersecurity risks and enhance oversight and control. These principles and policies include: the principle of least privilege, zero trust, segregation of duties, defense-in-depth, and the four-eyes principle.

3. To fortify their IT security posture and reduce the risk of a potentially catastrophic breach, SMBs need to fully implement a privileged access management (PAM) solution that bridges the gap between authentication and authorization.

4. SMBs need a comprehensive plan to ensure that cybersecurity objectives and requirements are communicated in a timely manner to all required stakeholders, and continually monitored and enforced.

5. SMBs should provide users with cybersecurity awareness training that focuses on fundamental issues, risks, and threats.

RECOMMENDATIONS
(continued)

6 SMBs that lack in-house IT security and cloud security expertise, and at this time either do not want to hire additional staff or cannot hire additional staff, should partner with a Managed Service Provider (MSP) to close the skills gap.

7 SMBs should implement a just-in-time gateway solution to eliminate vulnerabilities caused by virtual private networks (VPNs).

8 SMBs need to address security vulnerabilities triggered by remote workers.

9 SMBs must get four core benefits from their remote access tools: improved security, efficiency, governance, and affordability.

10 To get more IT security budget, IT professionals should ensure that any pitch, proposal, or presentation focuses on five elements: trust, compliance, insurance, employees, and ethics.

By following these strategies and maintaining a proactive stance towards cybersecurity, SMBs can fortify their defenses and significantly reduce the risk of falling victim to cyberattacks.

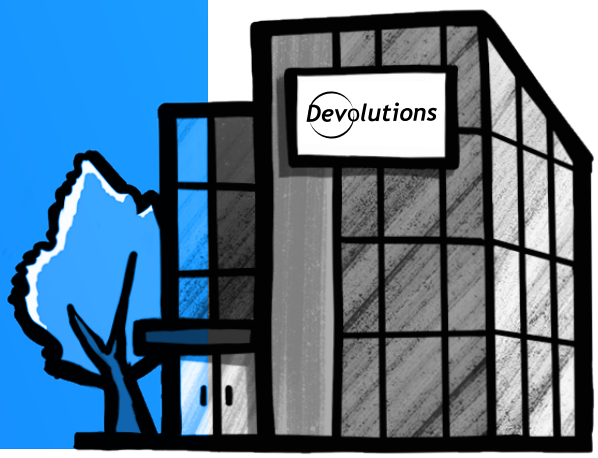
Devolutions

HELPING SMBS STAY SAFE AND SUCCEED

Although 99% of organizations are SMBs, virtually all best-in-class Privileged Access-Management, Password Management, and Remote Connection Management solutions are prohibitively expensive and excessively complex for most SMBs. This leaves SMBs vulnerable to security gaps and compliance breaches, reduces their productivity and competitiveness, and risks sending them backward when they need to move forward on the post-pandemic landscape.

At Devolutions, we believe that neglecting SMBs is unacceptable. That is why we have built a set of Password and Access Management solutions specifically designed to meet the growing needs of SMBs, which are:

- **Available at affordable price positions and multiple licensing models that make long-term sense.**
- **Highly secured and safeguarded by enterprise-grade protection, logging, and monitoring.**
- **Refreshingly simple and fast to deploy either on premises or in the cloud.**
- **Intuitive and easy-to-use for both technical and non-technical business users.**
- **Accessible through smartphone apps to support remote working anytime, anywhere.**
- **Backed by world-class sales engineers and technical support provided by an in-house team of specialists.**



We make best-in-class Privileged Access Management, Password Management, and Remote Connection Management solutions available to SMBs. Because all companies — not just large organizations and enterprises — need to control the IT chaos, strengthen security, increase efficiency, and drive results. We call it **"Password and Access Management for the rest of us!"**

CONTACT DEVOLUTIONS

Based in Lavaltrie, Québec, Canada, Devolutions delivers productivity and security solutions to more than 800,000 IT professionals and business end users in over 140 countries worldwide. Please direct your inquiries and free trial requests to us via the following:

Email: sales@devolutions.net

Phone: +1 844 463.0419

Live Chat via our Website: https://devolutions.net/