Devolutions

STATE OF CYBERSECURITY IN SMBs in 2021-2022

TABLE OF CONTENTS

EXECUTIVE SUMMARY

While the pandemic forced many SMBs to scale back their operations, hackers shifted into a higher gear. Cyberattacks against SMBs — especially against their remote workers — have increased throughout 2020 and 2021.

What's more, the consequences of a breach have never been more severe. Global cybercrime collectively costs victims $16.4 billion USD each day, and in 2021 the average cost of a data breach in SMBs climbed to $2.98 million per incident. This is a staggering price tag that many companies simply cannot afford, which is why 60% of SMBs go out of business within six months of getting hacked.

To help SMBs grasp the scope and dynamics of the current cyberthreat landscape — and ultimately make decisions that reduce the likelihood and severity of cyberattacks — **Devolutions surveyed decision-makers in SMBs worldwide**[1] across five core topics:

- **Cyberattacks and Threats in SMBs**
- **Password Management in SMBs**
- **Use of Privileged Access Management in SMBs**
- **Cybersecurity Training & Management in SMBs**
- **Cybersecurity Investment in SMBs**

[1] Organizations that participated in the survey are those that self-identified as SMBs. This approach reflects the fact that the definition of SMB varies depending on the industry and sector.

Here are some of the most notable takeaways from the State of Cybersecurity in SMBs in 2021-2022 survey:

72%

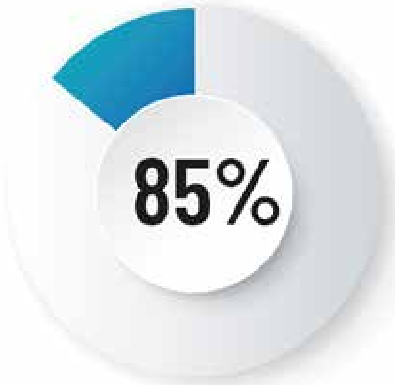
of SMBs are more concerned about cybersecurity now compared to a year ago.

This elevated level of anxiety among SMBs is justified.
The last year has seen a dramatic increase in the frequency, size, and severity of cyberattacks — including the ultra-sophisticated SolarWinds/Solorigate supply chain breach that targeted extremely high-profile victims.

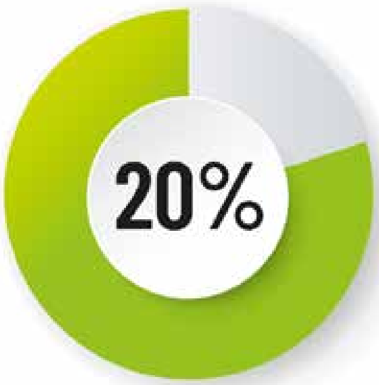
The 3 cyberthreats that SMBs are most concerned about are: **ransomware, phishing, and malware.**

This is a shift from Devolutions' State of Cybersecurity in SMBs in 2020-2021 survey, which found that the top cybersecurity concerns among SMBs were cloud computing vulnerabilities. However, it is not surprising that ransomware has now taken top spot.

Consider these alarming statistics:



of managed service providers (MSPs) see ransomware as a common threat to SMBs.



of ransomware victims are SMBs.

In 2021, an organization falls victim to a ransomware attack once every 11 seconds.

Global ransomware costs are expected to reach $20 billion by the end of 2021.

52% of SMBs **have experienced a cyberattack in** the last year.

10% have **experienced more than 10 cyberattacks.**

Does this mean that 48% of SMBs are "safe and secure"? No, it does not. It is virtually guaranteed that some, most, or possibly all SMBs that did not register a cyberattack in the last year were in fact targeted — and probably multiple times — but are unaware.

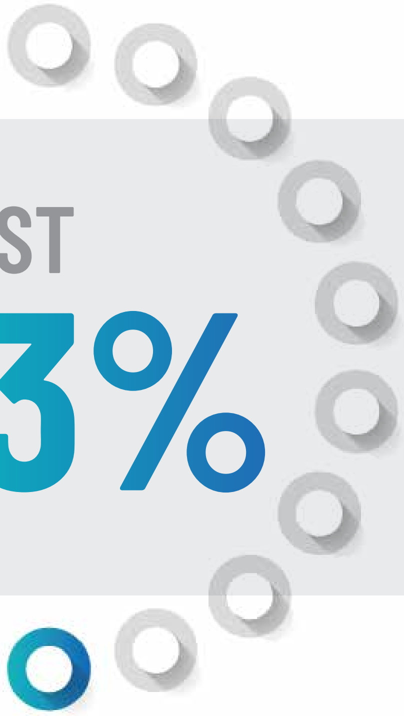
> There are only two types of organizations: those that have been hacked and those that don't know it yet!
>
> — *ITPortal.com*

1/5

SMBs are **using insecure methods to store passwords**, such as spreadsheets, documents, and writing passwords down on paper.

This is likely due to a false sense of security — i.e., "We have not been hacked yet, and so our password management practices must be safe and strong."

Unfortunately, the opposite is true. It only takes a single breach to trigger enormous and potentially catastrophic consequences, including customer loss and lasting reputation damage.



JUST

13%

of SMBs **have a fully deployed PAM solution in place.**

This is down from 24% in the Devolutions' State of Cybersecurity in SMBs in 2020-2021 survey. While there are many reasons that may explain this dip, one likely factor is that some SMBs are turning to password managers as a PAM substitute.

This is a mistake! **While password managers play an important role in the overall security mix**, they are fundamentally not built to manage access to privileged accounts and cannot provide the visibility, control, and governance required to safeguard sensitive data, support compliance requirements, and manage at scale.

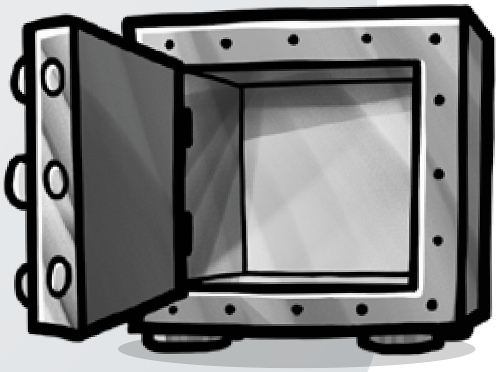
61% of SMBs **are not monitoring the full roster of privileged accounts in their organization.**

This is a massive vulnerability — and one that may have already been exploited several times without detection. For example, hackers routinely target local administrator accounts, because many SMBs give this access level to all employees.

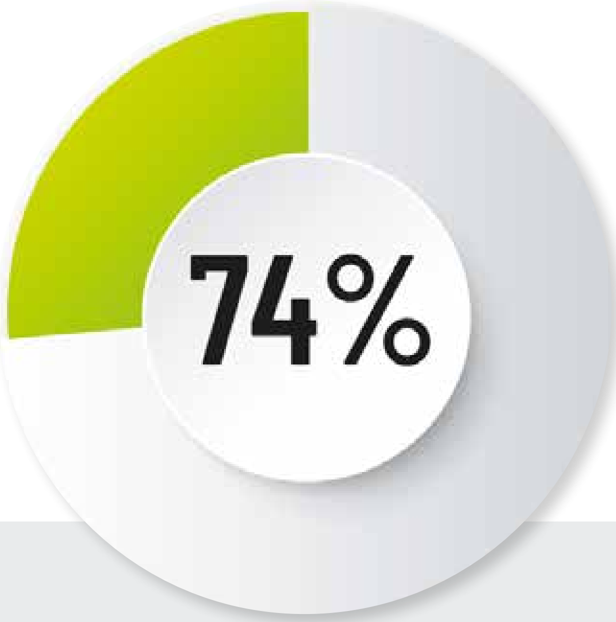
Once inside, hackers hide undetected while they scrutinize an SMB's defenses and carry out successful cyberattacks.

79%

of SMBs **believe that end users bear some responsibility in the event of a data breach.**



Research has found that nearly half of all data breaches are caused by employee negligence or carelessness. This means SMBs that focus 100% of their cybersecurity investments and efforts trying to stop hackers are still vulnerable — because their own people may trigger costly breaches.



of SMBs are **providing their workforce with cybersecurity training.**

This is a 14% drop from the Devolutions' State of Cybersecurity in 2020-2021 survey. What is behind the plunge? The most likely root cause is the pandemic. Dealing with rapid and unprecedented change has forced many SMBs to focus exclusively on core business activities.

However, providing their people with cybersecurity training must be part of this focus! Hackers have increased attacks against SMBs during the pandemic, and are setting their sights on remote workers who are often much more vulnerable outside of the corporate network environment.

40%

of SMBs **do not have** a comprehensive and updated **cybersecurity incident response plan.**

Research has found that organizations with a comprehensive and well-tested cybersecurity incident response plan reduced the cost of a breach by an average of $2 million, compared to organizations without a robust plan and suitable team in place. **We have all heard the saying “time is money” — well in this case, it is a literal truth!**

26%

of SMBs **allocate less than 5% of their IT budget to cybersecurity.**

While it is true that spending money on cybersecurity is not a magic wand that will make SMBs invulnerable, the basic fact remains that all else being equal, an SMB that has a more robust and updated cybersecurity profile is going to be much safer than one with vulnerabilities.

Experts advise that organizations **should allocate between 7-10% of their IT budget** towards cybersecurity technology and training.

RECOMMENDATIONS

In the State of Cybersecurity in SMBs in 2021-2022 report, we have also included **15 targeted recommendations** to help SMBs address the gaps, vulnerabilities, and concerns highlighted by the survey.

All of the recommendations are practical, proven, and affordable for SMBs.

ABOUT THIS REPORT

In total, 440 respondents were presented with 25 questions. The answers to each question (grouped by percentage), along with insights, commentary, and sources of further information, are presented in the remainder of this report, which is organized into seven parts:

PART 1
Cyberattacks and Threats in SMBs

PART 2
Password Management in SMBs

PART 3
Use of Privileged Access Management in SMBs

PART 4
Cybersecurity Training & Management in SMBs

PART 5
Cybersecurity Investment in SMBs

PART 6
Recommendations

PART 7
Profile of Respondents

PART 1

CYBERATTACKS AND THREATS IN SMBs

Hackers have increased their attacks against SMBs during the pandemic. At the same time, the growing migration of services to the cloud and the increase in remote workers has greatly expanded the attack surface, giving hackers more gateways and opportunities to steal sensitive, confidential, and proprietary data.

In part 1 of the survey, we asked SMBs a series of questions regarding their level of concern about the privacy and security of their company's data, as well as their experience with cyberattacks and breaches in the past year.

Question 1

With the difficult year that has passed, and considering the significant data breaches that have recently occurred, rate your level of concern regarding the privacy and security of your company's data:

72%

We are **more concerned** about cybersecurity than last year

25%

We have the **same level** of concern as last year

3%

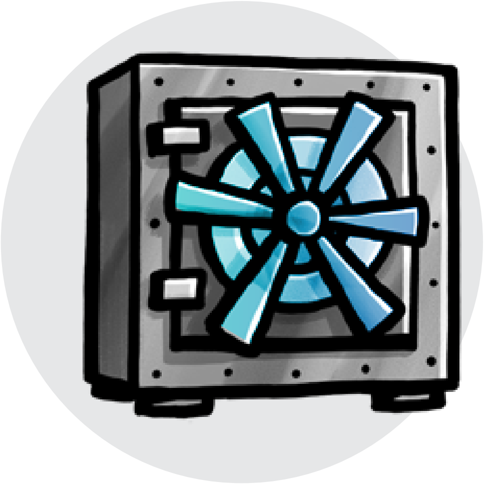
We are **less concerned** about cybersecurity than last year

Commentary

Nearly 3 out of 4 (72%) SMBs said they were more concerned about cybersecurity now than they were a year ago. **This mindset is a continuation of a trend that we discovered in the State of Cybersecurity in 2020-2021 report, in which approximately 9 out of 10 (88%) SMBs acknowledged that they were more concerned about cybersecurity than five years ago.**

This elevated level of anxiety among SMBs is justified. The last year has also seen a dramatic increase in the frequency, size, and severity of cyberattacks — including the ultra-sophisticated SolarWinds/Solorigate breach that targeted extremely high-profile victims, such as The Pentagon, the U.S. Treasury, the U.S. Department of Homeland Security, Microsoft, Cisco, Intel, FireEye, Deloitte, and several others. Unfortunately, since hackers are notorious for using the same playbook over and over again until it stops working, experts predict that there will be many more supply chain attacks in the months and years ahead.

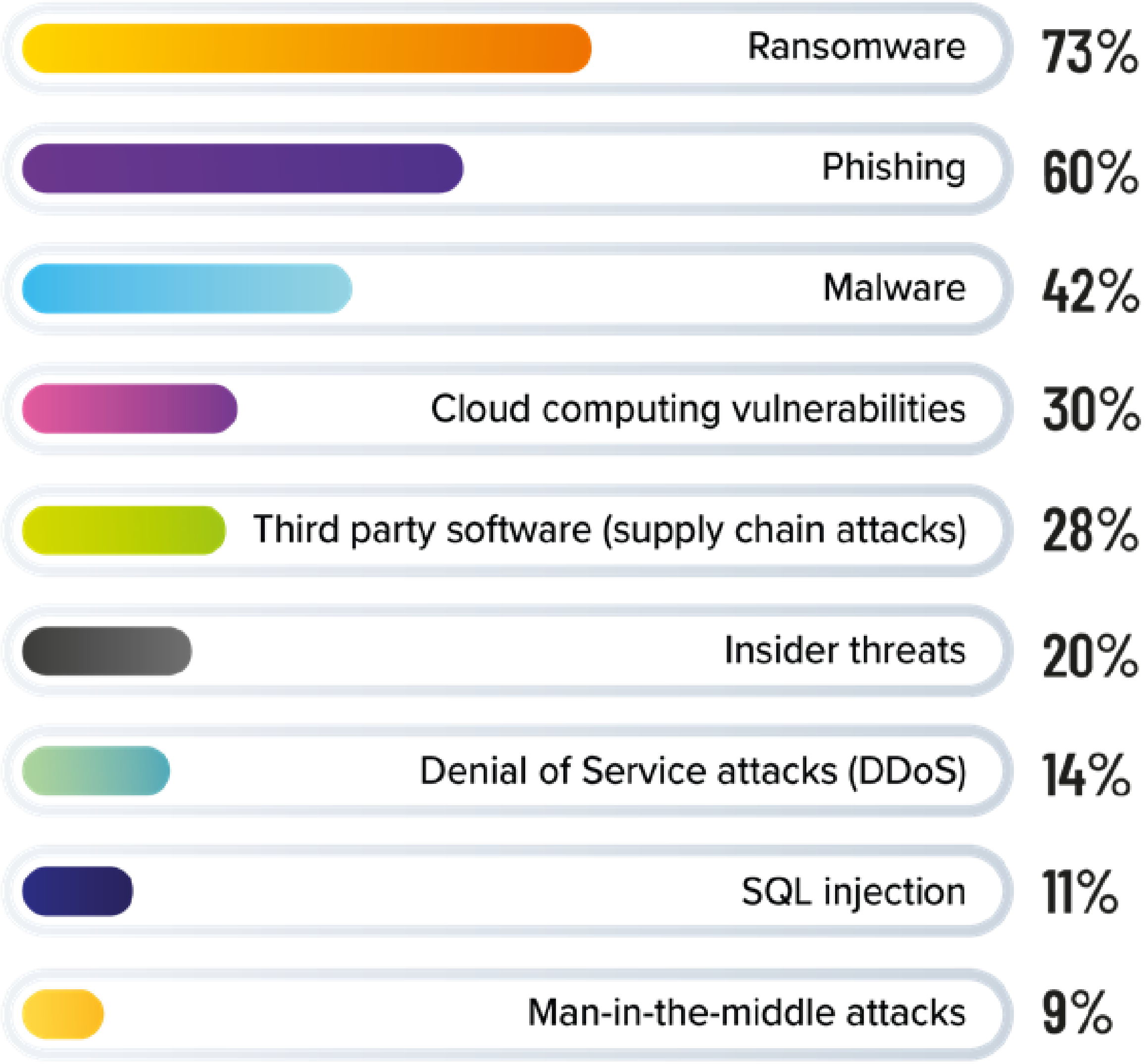
The takeaway for SMBs is unmistakably clear: They should be extremely concerned, and they should take immediate — yet intelligent — action to reduce their risk.



In the recommendations section of this report, we explore multiple cyber security strategies, policies, projects, and tools that SMBs should implement now — not later.

Question 2

Select the 3 cyber threats you are most concerned about:



Commentary

Ransomware has the dubious distinction of being the cyber threat that SMBs are most concerned about. This is a shift from the State of Cybersecurity in 2020-2021 report, which found that cloud computing vulnerabilities were the top cybersecurity concern among SMBs. Nevertheless, it is not surprising that ransomware has taken top spot. Consider these chilling statistics:

- **2021, an organization falls victim to a ransomware attack once every 11 seconds.**
- **Global ransomware costs are expected to reach $20 billion by the end of 2021.**
- **20% of ransomware victims are SMBs.**
- **85% of managed service providers (MSPs) see ransomware as a common threat to SMBs.**

Understandably, SMBs are also worried about phishing (60%), and the numbers bear this out:

- **94% of malware is delivered by email.**
- **90% of incidents and breaches include a phishing element.**
- **28% of phishing attacks are targeted.**
- **21% of ransomware involve social actions, such as phishing.**

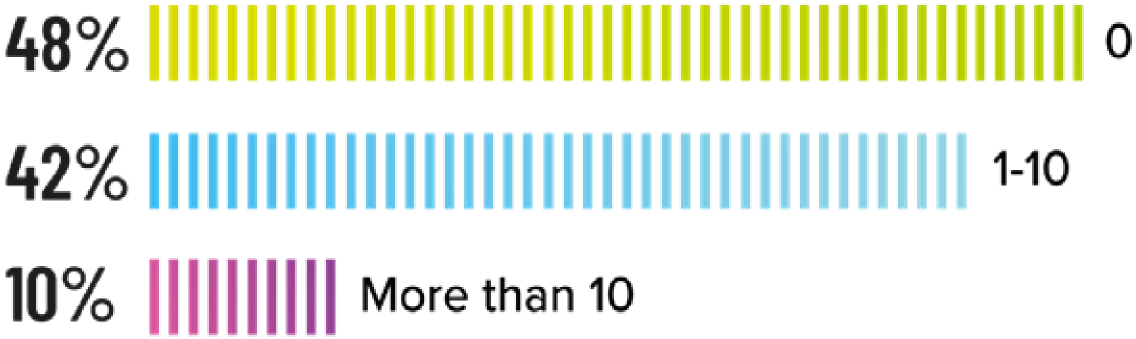
Concerns about malware round out the top three most nerve-racking threats.

It is also notable that only 28% of SMBs are concerned about supply chain attacks. As highlighted earlier in this report, supply chain attacks are on the rise. While third party vendors are certainly part of the solution, SMBs also need to be proactive.

In the recommendations section of this report, we highlight tips to help SMBs protect themselves against ransomware, phishing, and supply chain attacks.

Question 3

How many times has your company experienced a cyberattack or data breach in the last year?



Commentary

At first glance, this may seem like a "good news, bad news" story. The good news is that about half of SMBs (48%) are seemingly safe and out of harm's way, because they were not targeted by hackers in the past year. The bad news is the majority of SMBs (52%) have been attacked at least once — and 10% more than 10 times.

Unfortunately, the reality is that this is more likely a "bad news, worse news" story — because it is virtually guaranteed that some, most, or possibly all of the 48% of SMBs that did not register a cyberattack in the last year were in fact targeted — and probably multiple times. As pointed out by ITPortal.com: "There are only two types of organizations: those that have been hacked and those that don't know it yet!"

In the recommendations section of this report, we look at the core elements of a comprehensive and effective response plan, which is crucial for responding to and recovering from attacks.

Question 4

Do you believe that your company is likely to be targeted by hackers now or in the near future?

YES

81%

NO

19%

Commentary

The fact that approximately 1 in 5 SMBs do not believe they will be targeted by hackers now or in the near future points to an enduring — and potentially catastrophic — myth that many owners and executives believe: that they are too small to be attacked. In reality, the opposite is true.

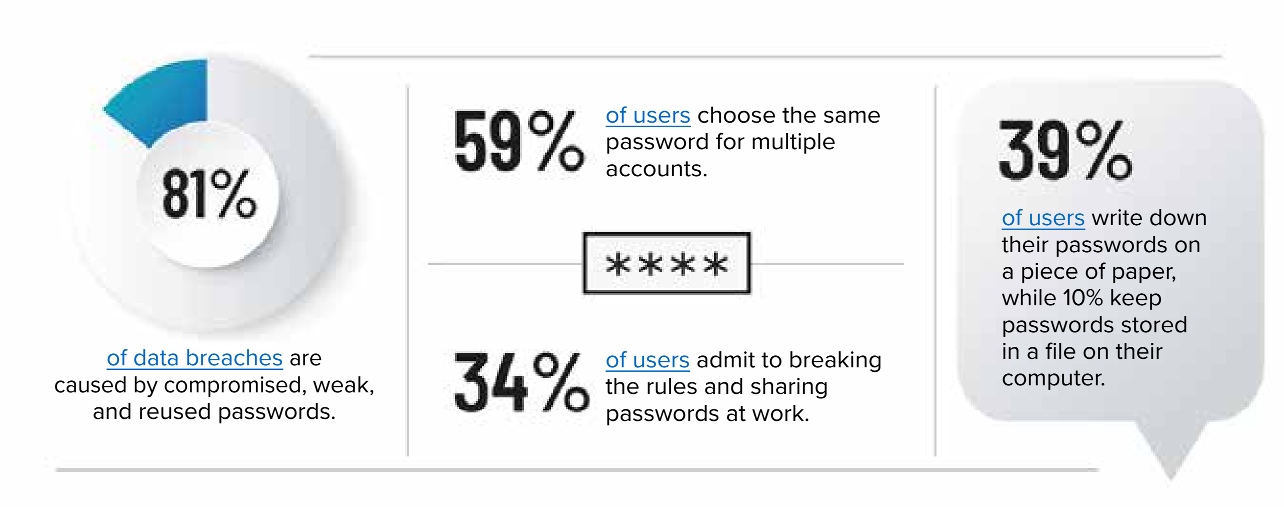
Not only are hackers targeting SMBs, but they are increasing their attacks for a very practical reason. Compared to most large organizations and enterprises, SMBs have weaker — and in some cases, virtually non-existent — defenses.

As such, when it comes to cybersecurity threat exposure, the first and most important thing SMBs must accept is that their relatively small size is not an advantage. It is actually a liability, because hackers will assume they are vulnerable. It is up to SMBs to demonstrate otherwise, or else it is not a question of if an attack will occur, but when and how severe it will be. Indeed, IBM's 2021 Cost of a Data Breach Report revealed that the average cost of a data breach in SMBs has climbed to USD 2.98 million per incident — which is the highest total in the 17-year history of the report.

PART 2

PASSWORD MANAGEMENT IN SMBs

Employees who can “manage themselves” are highly valued. However, there is one area where it is vital for SMBs to take the initiative and enforce standards and practices: password management. Consider the following:



81%

of data breaches are caused by compromised, weak, and reused passwords.

59% of users choose the same password for multiple accounts.

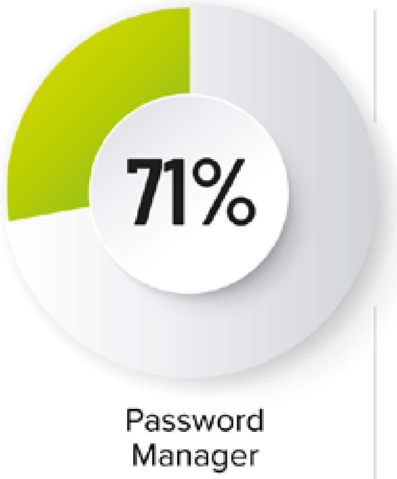
34% of users admit to breaking the rules and sharing passwords at work.

39% of users write down their passwords on a piece of paper, while 10% keep passwords stored in a file on their computer.

In Part 2 of the survey, we asked SMBs to share their password management perspectives, practices, and policies in 2021.

Question 5

How does your company store passwords?



9%	We write them down and store them offline
7%	Other method (please list)
6%	Documents (e.g., Word Doc, Google Doc, etc.)
5%	Spreadsheets
2%	Web Browsers

Commentary

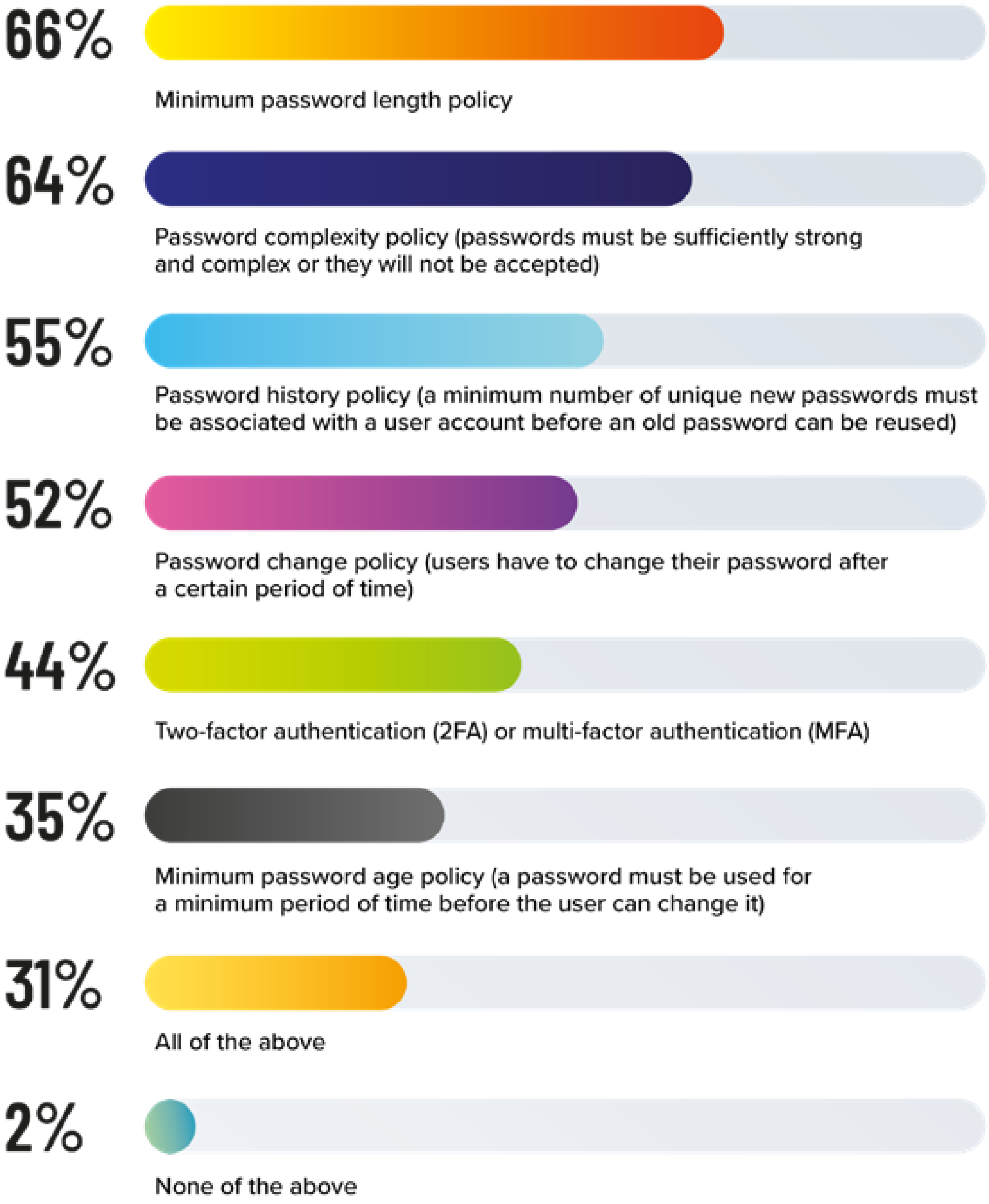
In the State of Cybersecurity in SMBs in 2020-2021 survey, 81% of SMBs relied on a password manager to store passwords. While there are many factors that could be responsible for the 10% year-over-year drop, among the most likely is a mistaken belief among SMBs that they are not as vulnerable as large enterprises and government organizations.

Related to this concern is the fact that 20% of SMBs surveyed are using insecure methods to store passwords (e.g., spreadsheets, documents, and writing passwords down on paper). Again, this is likely due to a false sense of safety. Unfortunately, it only takes a single breach to trigger enormous, and potentially catastrophic, consequences.

In the recommendations section of this report, we look at why password managers are such an effective cybersecurity tool, and what features and functions SMBs should look for when choosing a solution.

Question 6

Which of the following password policies and practices do you use in your company? Select all that apply.



Commentary

Despite the fact that the cybersecurity landscape is getting worse and worse, only about 3 in 10 SMBs (31%) have a password management policy that covers all of the essentials:

- **Minimum password length**
- **Sufficient password complexity**
- **Minimum password history**
- **Minimum password age**
- **MFA/2FA**

Why is “password change policy” not included as part of a robust password management approach? The view of this practice has changed over time. In the past, it was advisable to require users to change their passwords every few months, or at least once a year. However, the U.S. National Institute of Standards and Technology (NIST) has reversed course on this, and now only advises changing passwords in the event of a known or suspected data breach. This is because research has found that when users are obligated to change their passwords, they tend to choose credentials that are simpler to remember — and therefore easier to hack than what they had been using before the switch.

We also see in the response to this question that only 44% of SMBs are enforcing MFA/2FA. Frankly, this number should be 100%. What explains the gap? It likely has to do with the fact that when MFA first arrived on the scene many years ago, it was a difficult product for many SMBs to implement because tools were expensive and complex to configure. On top of this, users were either reluctant to adopt it because it was an extra login step they did not like, or they did not have a personally-owned or company-supplied smartphone (these days smartphones are cheap and everywhere, but that has not always been the case!).

Now, however, there is no reason — or excuse — for SMBs not to implement MFA, which Microsoft considers “the most effective tool against cyberthreats within an organization.” Fortunately, the worldwide password management solution marketplace is booming, and is estimated to be worth a whopping $2.05 billion by 2025. This means businesses of all sizes — including SMBs that have historically been ignored by many service providers — have an increasing number of products to choose from.

In the recommendations section of this report, we list the core elements of a robust password policy —which of course includes using MFA — that all SMBs should adopt now, not later.

Question 7

Does your company advise or require employees to use a personal password manager to protect their personal accounts?

YES
47%

NO
53%

Commentary

SMBs that do not require employees to use a personal password manager are potentially putting their people and company in harm's way. This is because hackers are increasingly targeting personal accounts in order to steal data that can be used to breach corporate endpoints and networks. Indeed, though cybersecurity experts warn against doing so, in reality many employees use their personal accounts — email, social media, chat apps, and so on — for work purposes. While this is convenient and expedient, it is also a significant risk. For example, research has found that around 15% of emails sent to personal accounts contain corporate sensitive information.

The other reason why SMBs should make it mandatory for employees to use a personal password manager, is that doing so promotes good security hygiene habits — such as always choosing strong, unique passwords — that carry over to the work environment. Essentially, being cybersecurity aware should be an ongoing commitment, and not something that employees only think about and focus on during the workday. Hackers operate 24/7, and employees need to be vigilant at all times.

Question 8

Does your company have a process in place to revoke account access for ex-employees?

YES

92%

NO

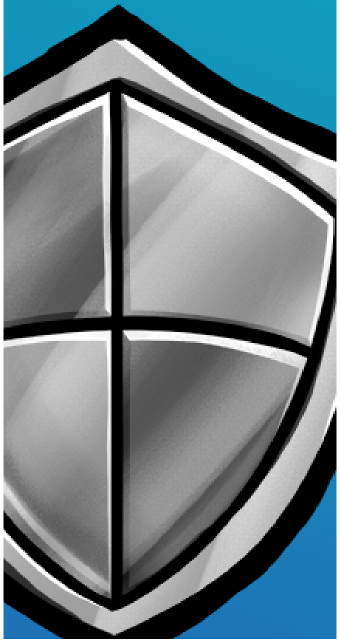
8%

Commentary

The 92% of SMBs that have a process in place to revoke account access for ex-employees are on the right track. However, the 8% that do not are heading in the wrong direction — a direction that could lead to a data breach.

In a survey, 25% of workers said they could still access accounts from past jobs — including former IT staff and managers who had the proverbial "keys to the kingdom" (i.e., access to privileged accounts). Granted, most of these workers do not intend to steal data, wreak havoc, or carry out any other illicit activities. But what if they are attacked by hackers who, in the course of their snooping, discover these old accounts and their associated credentials? Then the consequences could be severe, if not catastrophic.

In the recommendations section of this report, we look at the three steps that all SMBs should include in their access deprovisioning process.



PART 3

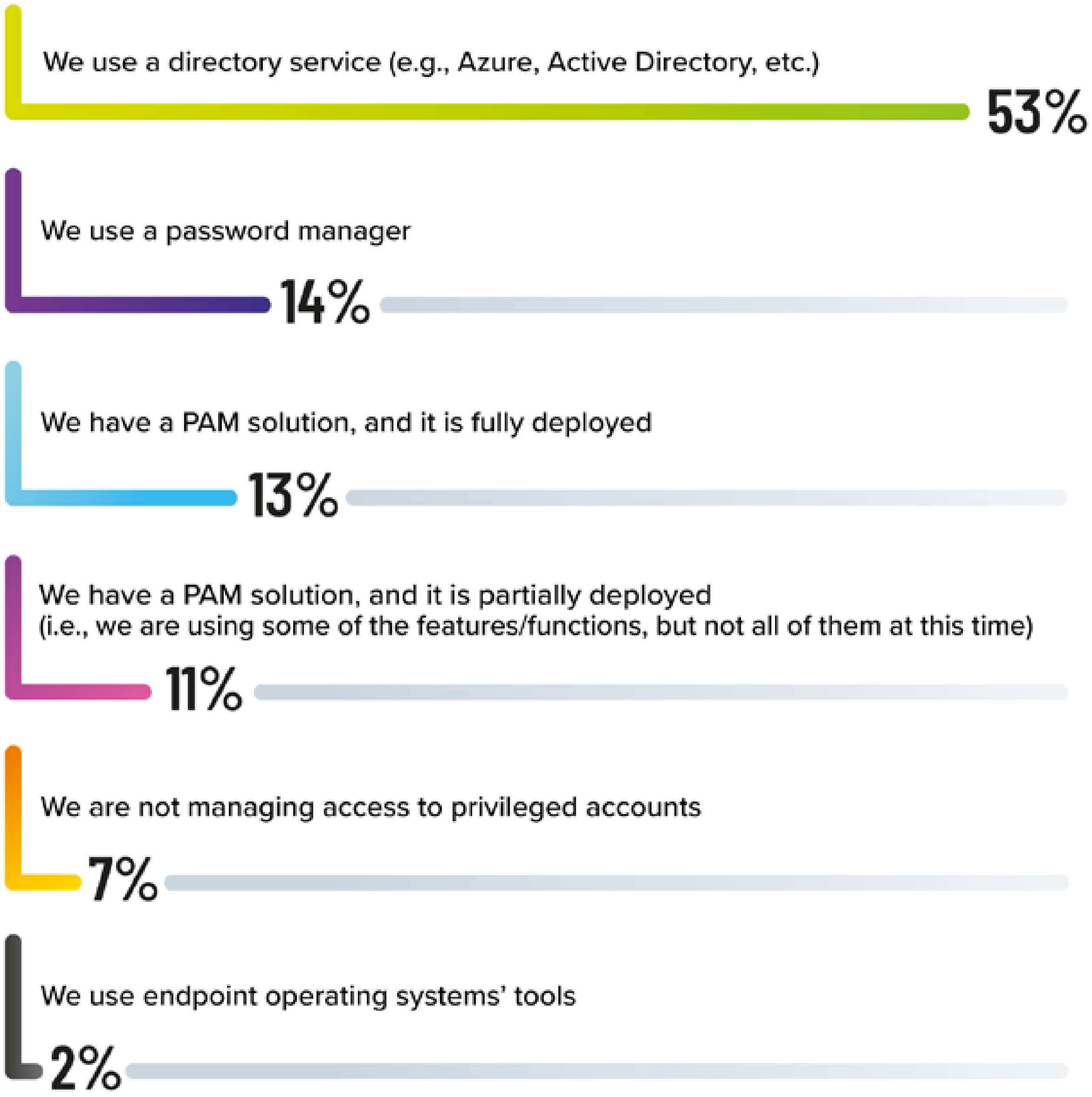
USE OF PRIVILEGED ACCESS MANAGEMENT IN SMBs

In the past, Privileged Access Management (PAM) was viewed primarily as a means to optimize administrative efficiency by managing passwords. However, in recent years, PAM has evolved into an essential technology for preventing security breaches and credential thefts, including those carried out by rogue insiders.

In the third section of our survey, we focused on the use of Privileged Access Management in SMBs:

Question 9

How do you manage access to privileged accounts in your company?



Commentary

Just over half (53%) of SMBs are using a directory service such as Azure or Active Directory (AD) to manage access to privileged accounts. While this may be expedient, it is not robust. Most security threats in a directory service environment trace back to unauthorized access. A PAM solution establishes a secure environment where only trusted users can access specific files, folders, and groups.

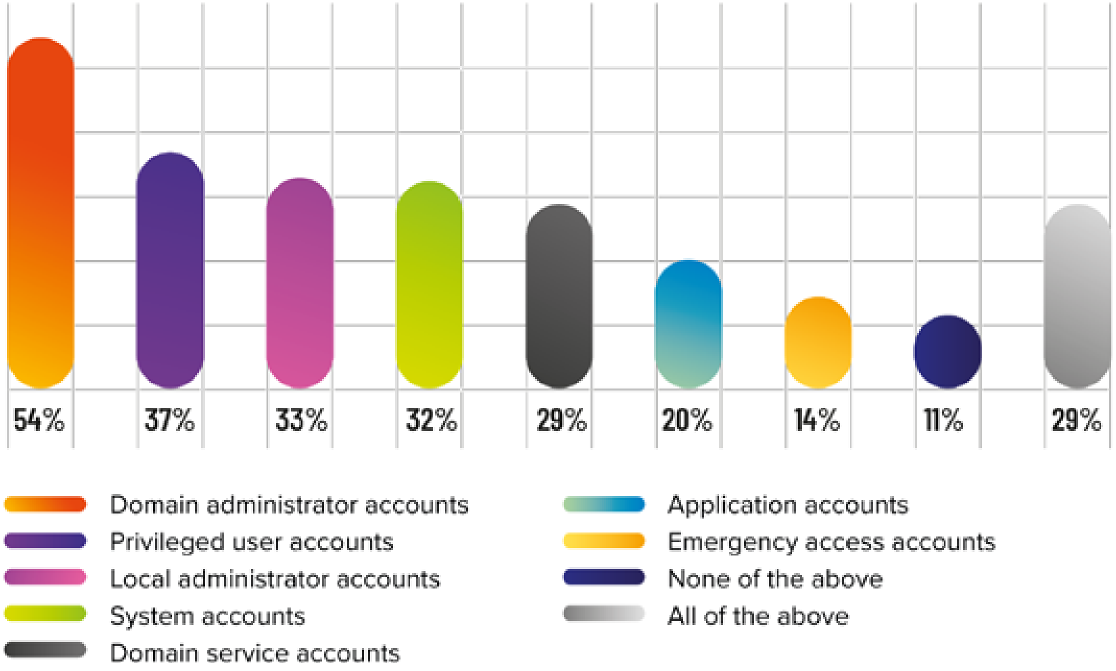
It is also notable that 13% of SMBs have a fully-deployed PAM solution in place — which is down from 24% in the State of Cybersecurity in SMBs in 2020-2021 survey. While there are many reasons that may explain this dip, one likely explanation is that some SMBs (14% in this year's survey) are turning to password managers as a PAM substitute. However, this is not viable. While password managers play an important role in the overall security mix — such as reducing cybersecurity fatigue among users — they are fundamentally not built to manage access to privileged accounts, as they do not provide the visibility, control, and governance required to safeguard sensitive data, support compliance requirements, and manage at scale.

As for the 7% of SMBs that are not managing access to privileged accounts, the message is clear: make this the number one priority right now! It is not just their company's success that is on the line. Considering that 60% of SMBs go out of business within six months of a cyberattack, their very survival could be at stake.

In the recommendations section of this report, we take a closer look at how SMBs can use a PAM solution to bridge the gap between authentication and authorization. We also highlight what SMBs should look for when evaluating potential PAM solutions.

Question 10

Which privileged accounts do you monitor in your organization? Select all that apply:



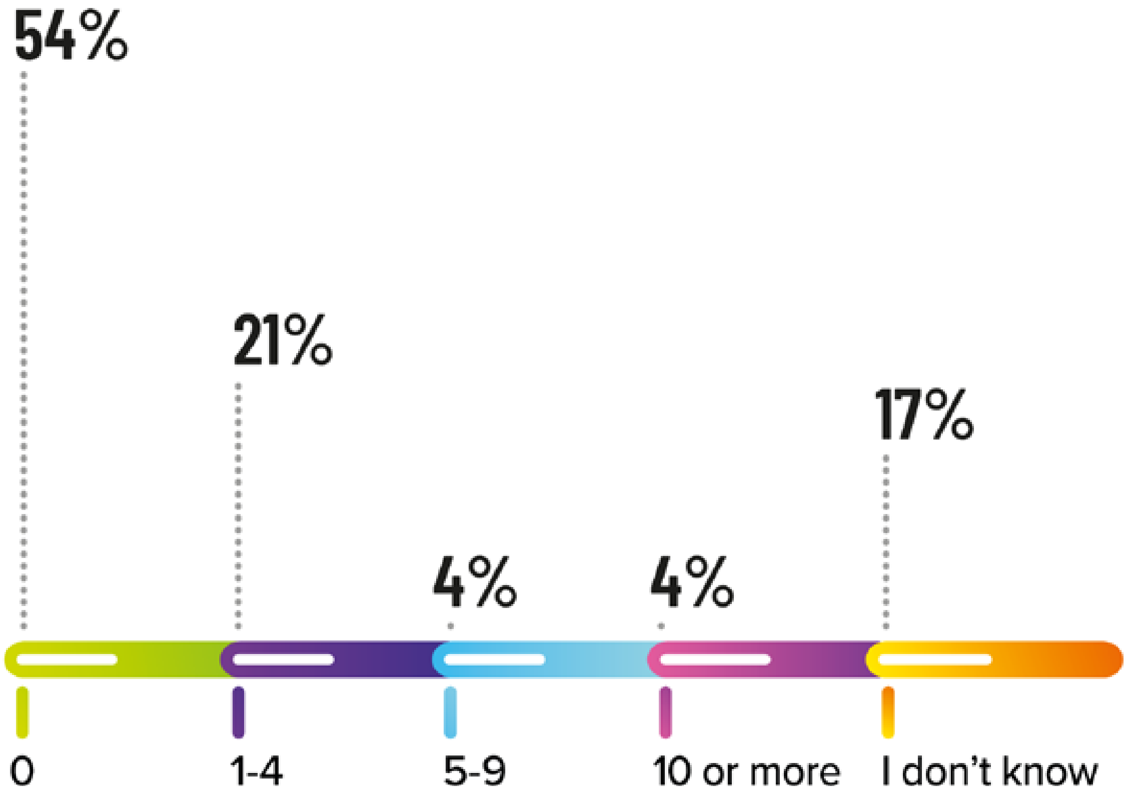
Commentary

61% of SMBs are not monitoring the full roster of privileged accounts in their organization, which means that hackers could exploit them — or may have already done so several times. For example, hackers routinely target local administrator accounts, because many SMBs give this access level to all employees. However, once breached, hackers hide undetected while they scrutinize an organization's defenses and plan what is almost certainly going to be a successful attack that could last for days, weeks, months — or even years.

In the recommendations section of this report, we provide more information on different types of privileged accounts. We also highlight signs of privileged account abuse, and share best practices for stopping it.

Question 11

In the last year, how many privileged access account violations have you had in your organization?



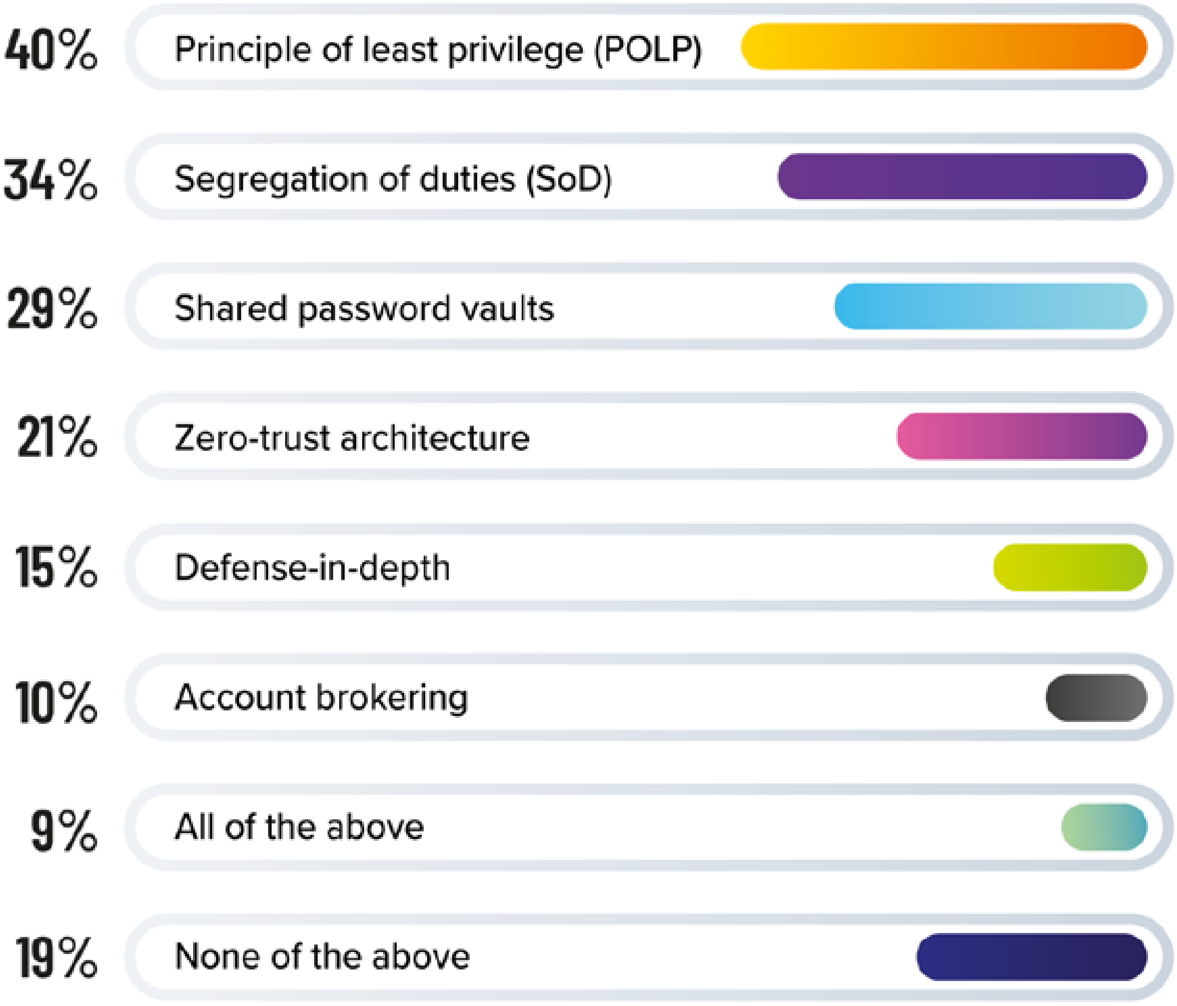
Commentary

32% of SMBs have experienced privileged access violations in the past year, with 4% of SMBs surpassing 10 incidents. What's more, given how prevalent this threat vector has become, it is highly likely that most of the SMBs that are unaware of privileged access violations in the last 12 months have been victimized at least once, if not multiple times.

Indeed, SMBs need to keep hackers from invading their endpoints and networks. But at the same time, they must prevent internal users — both those who have "gone rogue" and those who make honest mistakes — from improperly accessing privileged accounts, and acquiring or releasing sensitive information.

Question 12

What policies, practices, and/or tools do you have in place to support your company's management of privileged accounts? Select all that apply.



Commentary

Why are only 9% of SMBs checking all of these boxes when it comes to managing privileged accounts? It is because many SMBs believe they are too small to be attacked. Yet the facts state otherwise.

As was revealed in the responses to question 3 (in part 1 of this survey), 52% of SMBs experienced between 1 and 10 cyberattacks in the last year — and 10% experienced 11 or more. Clearly, there is a gap between what some SMBs perceive is happening, and what is actually happening. Unfortunately, hackers are exploiting this gap with a growing arsenal of advanced cyberthreats including next-generation ransomware, supply chain attacks, phishing, spyware, and the list goes on.

In the recommendations section of this report, we look at best practices for implementing several essential cybersecurity policies and technologies, including: POLP, SoD, shared password vaults, zero-trust architecture, defense-in-depth, and account brokering.

PART 4

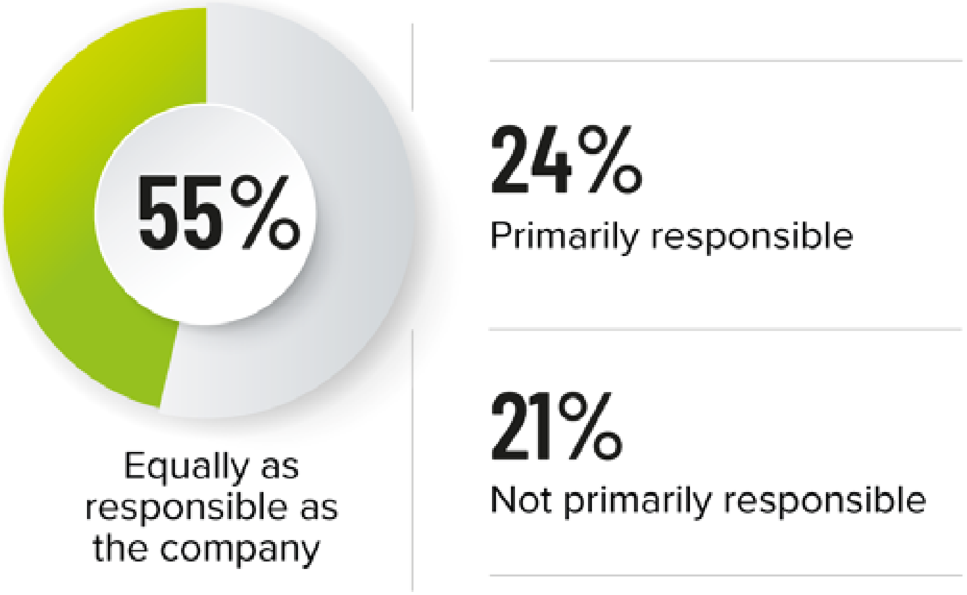
CYBERSECURITY TRAINING & MANAGEMENT IN SMBs

While it is vital for SMBs to implement robust and up-to-date tools that thwart hackers, to protect themselves from rogue and negligent users, they also need to focus on their internal policies, practices and protocols — or what InfoSec experts call “the human firewall.”

In part 4 of the survey, we focused on cybersecurity-related training and management in SMBs:

Question 13

Generally, how responsible do you think end users are in the event of a data breach?



Commentary

The majority (79%) of SMBs believe that end users bear some responsibility in the event of a data breach. However, nearly a quarter (24%) believe that end users are primary responsible — which is concerning. Research has found that nearly half of all data breaches are caused by employee negligence or carelessness. This means SMBs that focus 100% of their cybersecurity investments and efforts trying to stop external hackers and internal rogue users are still vulnerable — because some of their own people may unwittingly and unintentionally trigger costly breaches.

In the recommendations section of this report, we look at ways that SMBs can improve their workforce's cybersecurity wareness.

Question 14

Does your company provide ongoing cybersecurity training on aspects like reporting incidents, social media risks, password security, phishing, securing passwords, etc.?

YES

74%

NO

26%

Commentary

This is yet another good news, bad news scenario. The good news is that 74% of SMBs are providing their workforce with cybersecurity training. But the bad news is that in the State of Cybersecurity in 2020-2021 survey, the proportion of SMBs that provided ongoing cybersecurity training was 88%. What is behind this 14% plunge?

Not surprisingly, the most likely root cause is the pandemic. Dealing with rapid and unprecedented change has forced many SMBs to focus exclusively on core business activities. However, providing their people with cybersecurity training IS part of this focus! Hackers have increased the attacks against SMBs during the pandemic, and are setting their sights on remote workers who are often much more vulnerable outside of the corporate network environment.

In the recommendations section of this report, we highlight several practical ways for SMBs to keep their remote workers safe — and their company secure.

Question 15

Does your company have a comprehensive and updated Incident Response Plan?

YES
60%

NO
40%

Commentary

It has been said that “a failure to plan is a plan to fail.” However, when it comes to cybersecurity threats, the failure to have a comprehensive and updated Incident Response Plan could be catastrophic — because the faster a company can respond to a breach, the less likely it is that it will lead to lost revenue, customer loss, and reputation damage. Plus, it is often far easier — and much less expensive — to catch and clean up a breach early.

If a comprehensive and updated Incident Response Plan is so vital, why are 40% of SMBs overlooking this requirement? It is likely because they do not know where to start.

In the recommendations section of this report, we look at the core elements of a comprehensive and effective response plan, which is crucial for responding to and recovering from attacks.

Question 16

Do you perform comprehensive cybersecurity audits in your company at least twice a year?

YES

50%

NO

50%

Commentary

Half of SMBs said they perform at least two comprehensive cybersecurity audits a year, which is a 12% rise from the State of Cybersecurity in SMBs in 2020-2021 report. It is encouraging to see that more SMBs realize the wisdom of detecting vulnerabilities on their own — instead of waiting for hackers or rogue/negligent actors to do it for them.

Still, the proportion of SMBs that are performing at least two cybersecurity audits a year should be 100%, because it only takes a single breach to create massive losses — and trigger "why didn't we prevent this from happening in the first place?" regrets and stress.

To help SMBs avoid this pitfall, **in the recommendations section of this report**, we highlight key activities that should be included in a comprehensive audit process.

PART 5

CYBERSECURITY INVESTMENT IN SMBs

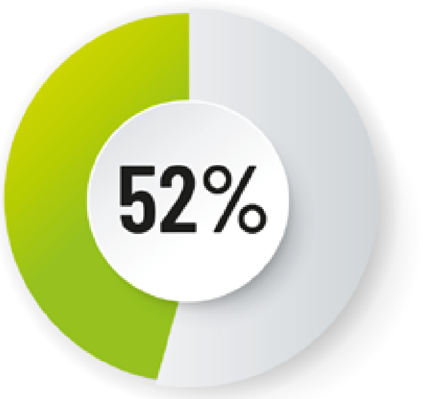
The volatility of the pandemic has compelled all organizations — but especially SMBs — to take a deep and at times difficult look at their priorities and strategies, and ensure that the focus going forward is on “need-to-have” vs. “nice-to-have” resources. Without question, investing in cybersecurity tools and training falls into the former category.

Indeed, we only need to reflect on the massive Solorigate supply chain attack — which some experts have heralded as the most sophisticated breach in history — and the surge in ransomware, phishing, spyware, and other cyberthreats to realize that the ROI of wisely investing in cybersecurity can be more than an issue of profit and loss for SMBs: It can mean the difference between survival and extinction.

In Part 5 of our survey, we explored cybersecurity investments in SMBs:

Question 17

What cybersecurity investments has your company made to date? Select all that apply.



We have implemented a password manager

30%	We have hired a CISO or other security expert
25%	We are working with a managed service provider (MSP)
21%	We have implemented a dedicated PAM solution
19%	None of the above
5%	All of the above

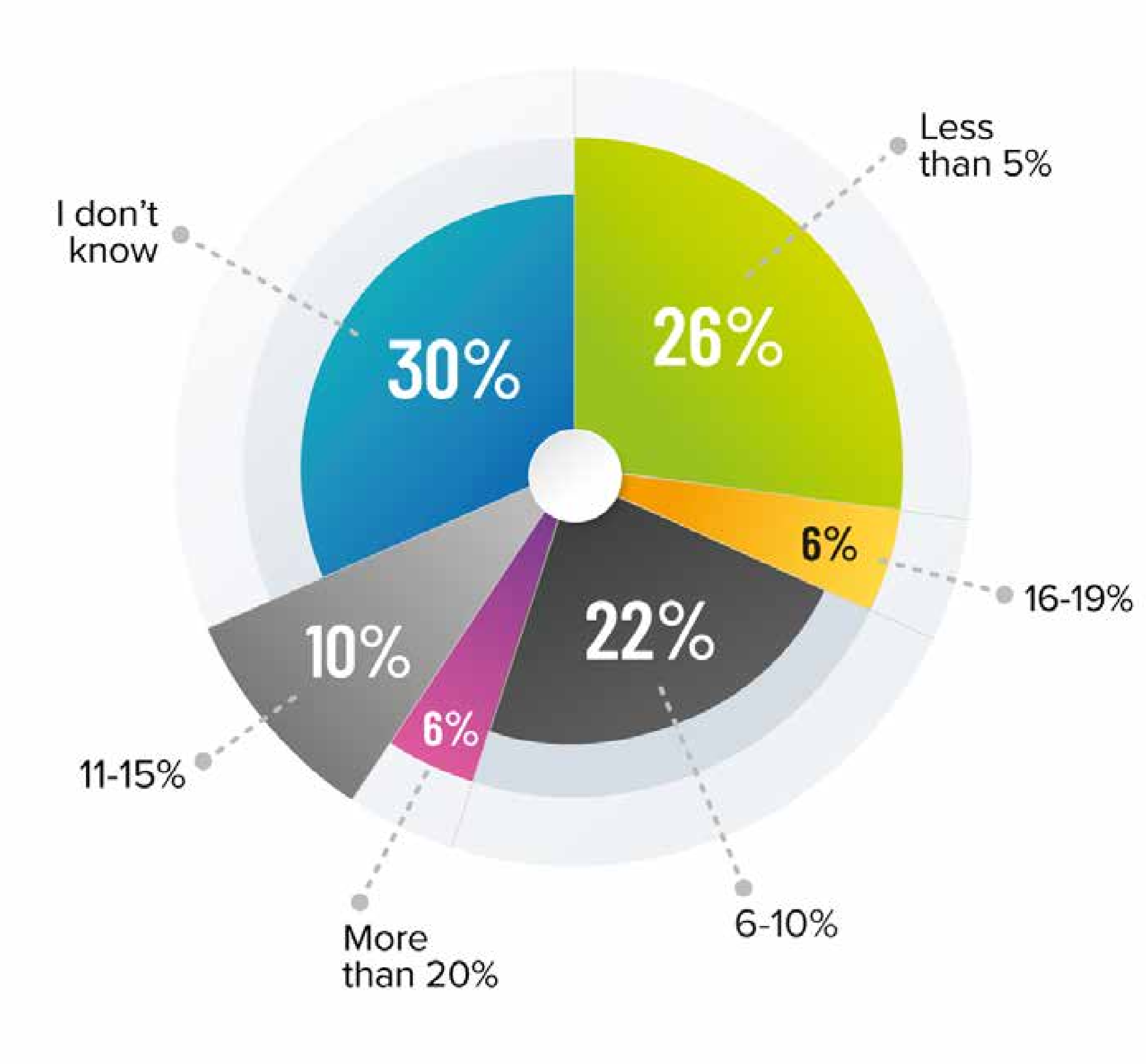
Commentary

It is alarming that only about 1 in 4 SMBs have implemented a dedicated PAM solution. As we explored in Section 4 of this report, PAM solutions are not exclusively meant for large organizations. SMBs must also identify, control, and monitor privileged account access. On a more positive note, 52% of SMBs have implemented a password manager, and 1 in 4 are working with an MSP.

In the recommendations section of this report, we provide tips to help SMBs choose the best MSP for their organization.

Question 18

Of your company's overall IT budget, percentage-wise, how much is allocated for cybersecurity (including technology, training, etc.)?



Commentary

For several years, many experts have advised organizations to allocate between 7% and 10% of their IT budget to cybersecurity technology and training. However, a survey by Gartner has found that, on average, cybersecurity spending accounts for just 5.7% of IT expenditures — and in SMBs, this proportion can be considerably lower.

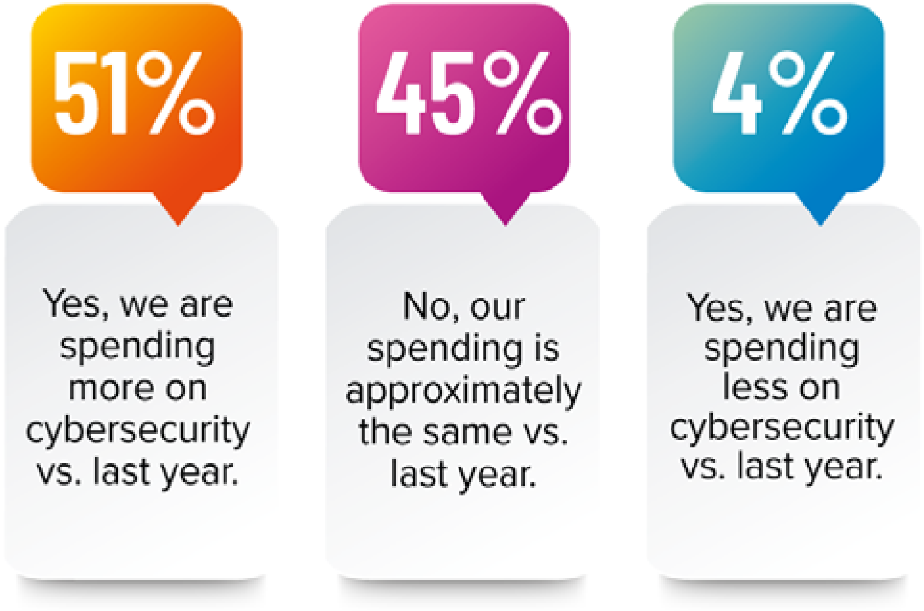
While it is certainly true that merely spending money on cybersecurity is not a magic wand that will make SMBs invulnerable, the basic fact remains that, all else being equal, an SMB with a more robust and updated cybersecurity profile is going to be significantly safer than one that has significant vulnerabilities. Furthermore, the first thing that hackers frequently do after breaching an organization (often through unguarded privileged accounts), is scan the cybersecurity defense landscape to see what they are up against. If they sense that it is going to be a tough battle to remain undetected, they are less likely to move ahead with a full-scale attack. Conversely, if they see that they can easily roam across networks and endpoints without getting caught, they usually prepare for a silent onslaught that can last for months or years.

A common reason why some SMBs neglect to spend a sufficient amount of their IT budget on cybersecurity is that SysAdmins and other InfoSec professionals struggle to convince executives that spending in this area is not an expense, but an investment.

In the recommendations section of this report, we share some valuable tips for helping cybersecurity champions in SMBs to get decision-makers to loosen the proverbial purse strings — and in doing so, make their organizations stronger and safer.

Question 19

In the last year, has your company's total spending on cybersecurity changed?



51% — Yes, we are spending more on cybersecurity vs. last year.

45% — No, our spending is approximately the same vs. last year.

4% — Yes, we are spending less on cybersecurity vs. last year.

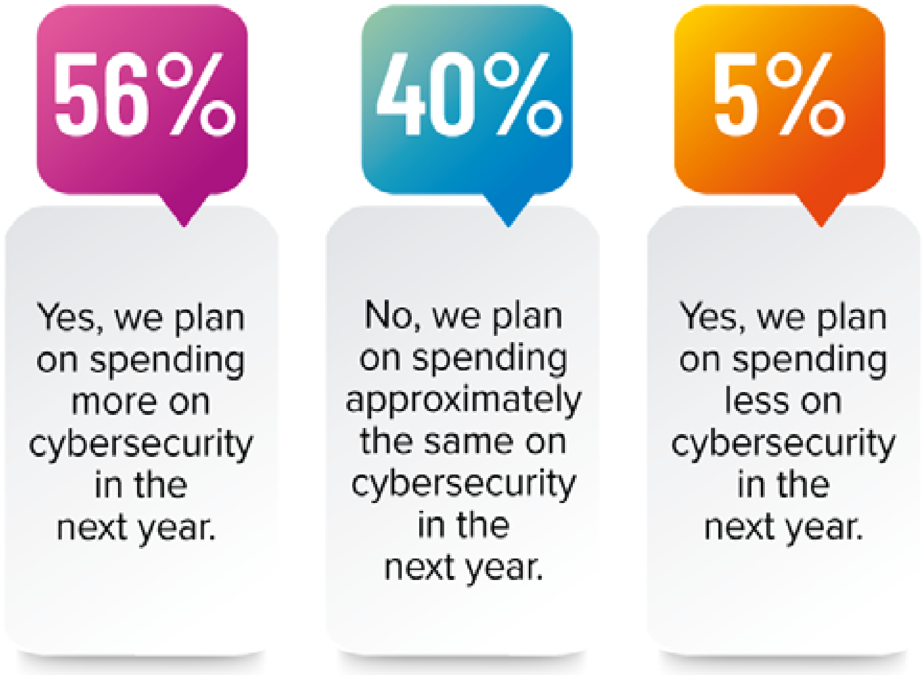
Commentary

The vast majority of SMBs are spending the same or more on cybersecurity vs. last year, which is not surprising. The pandemic forced organizations of all sizes to rapidly implement measures to ensure business continuity, which included protecting remote workers from both old and new cyberthreats — including a nearly 700% surge in phishing attacks.

In addition, the shockwaves of the massive Solorigate supply chain attack continue to reverberate, as organizations around the world realize that they could be a single, seemingly harmless and ordinary SaaS update away from having their confidential data stolen and sold to the highest bidder on the dark web.

Question 20

In the next year, do you anticipate your company's total spending on cybersecurity will change?



Commentary

While it is good news that 96% of SMBs are spending the same or more on cybersecurity now vs. last year, this does not necessarily mean that the most important priorities are being addressed. It is categorically cheaper, simpler, and faster to prevent a cyberattack than it is to investigate and clean up in the aftermath. And in some cases, the reputation damage can linger for years.

In the recommendations section of this report, we highlight critical cybersecurity projects that SMBs should focus on and implement now rather than later.

PART 6

RECOMMENDATIONS

When it comes to cybersecurity strategies and solutions, there are several areas where SMBs can — and in many cases, must — address vulnerabilities now, not later.

We strongly **advise all SMBs to proactively analyze and audit their current cybersecurity profile**, and as necessary **carry out these targeted recommendations:**

1 SMBs need to realize they are not “too small to be attacked”

2 SMBs need to proactively protect themselves from the “big 3” cyberthreats: ransomware, phishing, and supply chain attacks

3 SMBs need to implement a comprehensive and effective incident cyberattack response plan

4 SMBs need to implement a password manager solution with the right features and functions

5 SMBs need to implement a robust password policy

6 SMBs need to implement an effective access deprovisioning process

7 SMBs need to implement a privileged access management (PAM) solution to bridge the gap between authentication & authorization

8 SMBs need to protect, monitor & update all privileged accounts

9 SMBs need to implement 4 essential security principles: principle of least privilege (POLP), segregation of duties (SoD), zero trust, and defense-in-depth

10 SMBs need to improve their workforce’s cybersecurity awareness

11 SMBs need to keep remote workers from becoming “the weakest link” in the cybersecurity defense chain

12 SMBs need a comprehensive cybersecurity audit process

13 SMBs need support from managed service providers (MSPs) to close the cybersecurity defense gap

14 SMBs need to increase the proportion of their IT budget that is allocated to cybersecurity

15 SMBs need to focus on 5 security projects in 2021-2022: secure remote access management, secure digital vault, secure password management, multi-factor authentication (MFA), and automation

1 RECOMMENDATION

SMBs Need to Realize They Are Not "Too Small to Be Attacked"

This recommendation calls for decision-makers in SMBs to change their mindset from the incorrect assumption, "we are too small to be attacked by hackers," to the correct understanding, "hackers will increasingly target us because of our small size."

Indeed, long gone are the days when hackers almost exclusively set their sights on large enterprises and organizations. Today, hackers are exploiting the reality that many SMBs have weak or virtually non-existent cybersecurity defenses — yet they have an abundance of private, confidential, and proprietary data that can be used to commit identity theft and sold on the dark web.

SMBs IN THE CROSSHAIRS:

- 43% of cyberattacks **target small businesses.**
- **In 2021, the average cost of a data breach in SMBs has** climbed to USD $2.98 million per incident**.**
- 81% of data breaches **are caused by compromised passwords, and 30% involve internal rogue users.**

Furthermore, during the pandemic, hackers dialed up their attacks on SMB remote workers — and this adverse trend will not fade when the public health crisis starts to normalize. On the contrary, in the years to come we should expect to see hackers increasingly target remote workers to breach endpoints, networks, and servers.

As such, when it comes to cyberthreat exposure, the first and most important thing SMBs must accept is that their relatively small size is not an advantage. It is actually a liability, because hackers will assume they are vulnerable. It is up to SMBs to demonstrate otherwise, or else it is not a question of if a cyberattack will occur, but when it will occur and how severe it will be.

2 RECOMMENDATION

SMBs Need to Proactively Protect Themselves from the "Big 3" Cyberthreats: Ransomware, Phishing, and Supply Chain Attacks

While SMBs should be concerned about a wide range of cyberthreats, such as spyware and cloud security challenges, the survey revealed that three in particular are triggering the most anxiety: ransomware, phishing, and supply chain attacks. Below, we provide strategies to help SMBs protect themselves against these common, costly and potentially ruinous hazards.

RANSOMWARE BY THE NUMBERS:

- 20% of ransomware **victims are SMBs.**
- 85% of MSPs **see ransomware as a common threat to SMBs.**
- **In 2021-2022, an organization falls victim to a ransomware attack once** every 11 seconds**.**

Strategies to Protect SMBs Against Ransomware:

- Develop a comprehensive incident response plan that clearly identifies what to do — and who should do it — in the event of a ransomware attack.

- Implement a backup system that supports multiple iterations or archived data in case one copy of the backup has infected or encrypted files. Backups should also be regularly tested for data integrity and to ensure operational readiness.

- Deploy anti-virus and anti-spam software — and add a warning banner/signature on all emails that reminds users about the dangers of clicking links and opening attachments.

- If practical, disable script macros and force users to view rather than open files that are transmitted through email; embedding malware inside Word/Excel macros is a common vector for ransomware attacks.

- Keep all devices, software, hardware, and applications (including cloud locations) fully updated and patched, preferably through a centralized patch management system.

- Use application whitelisting and software restriction policies to block the execution of programs in common ransomware locations (e.g., temporary folders).

- Use a proxy server for Internet access.

- Use an ad blocking software.

- Restrict access to common ransomware vectors, such as social networking sites and personal email accounts.

- Assess and monitor third parties who have access to the network, and ensure that they diligently follow cybersecurity best practices.

- Participate in cybersecurity information sharing programs and organizations (e.g., MS-ISAC and InfraGard).

- Provide end users with ongoing cybersecurity training on topics such as social engineering and phishing. We look closer at this in Recommendation #10.

- Implement a reporting plan that tells end users how and when to report unusual or suspicious activity.

Strategies to Protect SMBs Against Phishing:

- Train employees on how to detect malicious emails. One way to support this goal is by running simulated phishing campaigns — which can yield some surprising (in the disturbing sense) results. For example, in 2020 14% of insurance workers failed a global phishing test.

- Require all employees to choose strong, unique passwords for accounts. Using a reputable password manager is highly recommended.

- Enforce multi-factor authentication (MFA) to reduce the risk of account takeover.

- Implement a secure email gateway that automates anti-spam, anti-malware, and policy-based filtering.

- To increase the capacity to identify and block spam, implement SPF (Sender Policy Framework), DMARC (Domain-Based Message Authentication, Reporting & Conformance), and DKIM (Domain Keys Identified Mail).

- Implement anomaly detection at the network level for inbound and outbound e-mails.

PHISHING BY THE NUMBERS:

- **In the first half of 2021 there was a** 22% surge **in the volume of phishing attacks compared to the first half of 2020.**

- **Nearly** 1.5 million new phishing sites **are created each month.**

- 1 in every 99 emails **is a phishing attack.**

Strategies to Protect SMBs Against Supply Chain Attacks:

- Perform an in-depth vendor evaluation and ensure that all third parties comply with the following: regularly test the strength of their cybersecurity resilience; provide evidence of the latest source code scan and/or application penetration; deploy application firewalls or network segmentation that restricts access to application programs or object source code; comply with relevant policies and/or regulations (e.g., SOC 2, GDPR, CCPA, NIST, ISO-27001/2, CIS, CSA CCM, etc.); operate an employee security awareness program.

- Use a privileged access management (PAM) solution to block hackers who attempt to follow a common attack trajectory — known as the "privileged pathway" — which starts with perimeter penetration, then compromises privileged devices and endpoints, and culminates in a data breach. We look at the elements of a PAM solution in Recommendation #7.

- Use honeytokens, in which a dormant privileged account is created and monitored. If hackers attempt to breach the account, an alert is triggered that indicates the environment has been breached.

SUPPLY CHAIN ATTACKS BY THE NUMBERS:

- **In the first quarter of 2021,** 42% more organizations **were hit by a supply chain attack compared to the last quarter of 2020.**

- **Supply chain attacks in 2021 are expected to** increase 400% **vs. 2020.**

- **An analysis of high profile supply chain attacks between January** 2020 and July 2021 **found that 20% targeted data, 12% targeted suppliers' internal processes, 16% targeted people, and 8% targeted financial assets.**

To guard against these three and other cyberthreats, the Devolutions Security Team advises SMBs to implement the following principles:

Principle of least privilege (POLP), which means that users only get the access they need to carry out their day-to-day activities. If elevated privileges are necessary for a specific project or activity, these should be temporarily granted, and then removed immediately once they are no longer required.

Zero trust, which means that nobody is automatically trusted, and all network activity is assumed by default to be malicious.

Segregation of duties (SoD), which is rooted in the view that when multiple people are involved in a sensitive workflow, there is a lower risk that an individual will manipulate or misuse organizational resources.

Defense-in-depth, which uses multiple layers of protection to slow hackers down, as they attempt to snake their way to the perimeter through to mission-critical assets.

We dive deeper into these policies and explore best practices in Recommendation #9.

3 RECOMMENDATION

SMBs Need to Implement a Comprehensive and Effective Cyberattack Response Plan

A comprehensive and effective cyberattack incident response plan covers all six of the following elements: preparation, identification, containment, eradication, recovery, and lessons learned.

Preparation Tasks Include:

- Reviewing security policy, updating security policy, documenting security policy, and standardizing security policy.
- Establish secure communication channels for incident handling and response with internal and external sources.
- Performing risk assessment.
- Identifying sensitive, private, confidential, and proprietary assets.
- Defining and prioritizing critical security incidents that must be focused on.
- Creating an Incident Response Team (see callout box on next page).

Identification Tasks Include:

- Monitoring IT systems to identify deviations from normal operations, and confirm if they represent actual security incidents and not false positives.
- Upon verification of actual security incidents, collecting evidence, and establishing type and severity.
- Fully documenting all observations and findings.

As a best practice, the Incident Response Team should include the following roles :

Team Leader: drives and coordinates team activity, and helps the team stay focused on mitigating damage and accelerating recovery.

Lead Investigator: collects and analyzes evidence, identifies root cause, directs security analysts, and implements rapid system and service recovery.

Communications Lead: spearheads messaging and communications inside and outside of the company.

Documentation & Timeline Lead: Documents all team activities — with a focus on investigation, discovery and recovery activities — and develops realistic timelines for each stage of the incident.

HR/Legal Representation: provides strategic and operational advice, since an incident may or may not develop into criminal charges.

SMBs that do not have the in-house specialists to supply all of these roles should partner with an outside consulting firm or managed service provider (MSP). **We provide additional insights of what SMBs should look for in an MSP in Recommendation #13.**

Containment Tasks Include:

- Executing short-term containment tactics (e.g., isolating the breached network segment).
- Focusing on long-term containment strategies.
- Implementing temporary fixes to support day-to-day operations.

Lessons Learned Tasks Include:

- Perform a retrospective of the incident within two weeks of the incident.
- Completely documenting the incident, including actions taken to contain it.
- Identifying any aspects of the incident response process or plan that could be improved.

For further guidance, we highly recommend that SMBs download the Incident Handler's Handbook prepared by the SANS Institute. The elements discussed in this section are based on this valuable and practical reference.

Eradication Tasks Include:

- Removing viruses, malware, and all other threats from affected systems.
- Identifying and permanently block the root cause of an attack.
- Taking action to prevent duplicate or similar attacks in the future.

Recovery Tasks Include:

- Methodologically and carefully bringing affected production systems back online.
- Testing and verifying affected production systems to ensure they are back to normal activity.

4 RECOMMENDATION

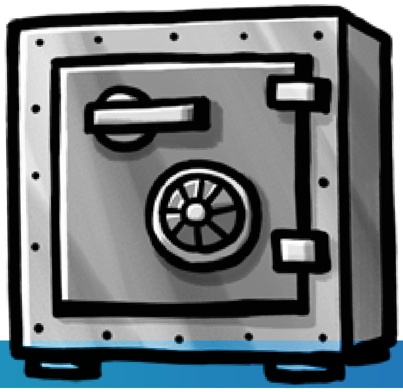
SMBs Need to Implement a Password Manager Solution With the Right Features and Functions

With a password manager solution, users only need to remember two sets of login credentials instead of dozens, allowing them to become virtually passwordless. The first set of credentials is for their own system, and the second is to access the solution.

In addition, if the password manager solution supports Microsoft's Single Sign-On (SSO), then users only need to create and remember one set of login credentials. SMBs that use SSO can even take things a step further and implement passwordless authentication with solutions that use hardware or biometrics.

Key features and functions that SMBs should look for when choosing a password manager solution include:

- **End-to-end strong encryption**
- **Multi-factor authentication (MFA)**
- **Secure password vaulting (i.e., sharing)**
- **Strong password generator**
- **Role-based permissions**



Password Manager Solutions: Cloud-Based or On-Premises?

Neither cloud nor on-premises password manager solutions are inherently superior. There are pros and cons of each model:

Deployment

- Cloud: Contrary to what some non-IT folks believe, cloud password management solutions are not hosted somewhere "in the air". Rather, they are hosted by a service provider. Customers, however, can access those resources as often as they want, and from any internet-enabled device.

- On-premises: On-premises password management solutions are deployed in-house, and within a business's infrastructure. Unlike a cloud model, the business rather than the service provider is responsible for maintaining the solution and all associated processes.

Control

- Cloud: With cloud password management solutions, the service provider maintains control — not because they are trying to wrestle it away from customers, but because (as discussed above) they are responsible for hosting and maintaining the solution. As such, they require control in order to keep things operational and secure.

- On-premises: With on-premises password management solutions, businesses keep all resources in-house and are in total control. While this is an advantage for some businesses, it can be a drawback for others — especially SMBs — that lack the infrastructure and specialized employees to continuously optimize and secure the solution.

Security

- Cloud: In the past, concern regarding security was the number one reason businesses hesitated to adopt cloud apps, resources, and solutions (including but not limited to cloud password management solutions). However, in recent years cloud security has dramatically improved. For example, cloud password management service providers monitor security 24/7, implement multiple types of security, and conduct ongoing penetration testing. This is a level of deep, ongoing protection that many SMBs cannot achieve due to limited budgets and lack of cybersecurity specialists.

• On-premises: Since on-premises password management solutions are hosted, maintained, and controlled within a business's IT infrastructure, they are inherently more secure than cloud solutions. Note that this does not mean that cloud solutions are insecure. Rather, it simply means that on-premises solutions provide an enhanced layer of security. For some businesses, this enhanced layer is important or may be essential for compliance reasons (more on this in the next section). For other businesses, this enhanced layer is not required, and as such choosing a cloud solution may be more practical and affordable.

Compliance

• Cloud: When it comes to compliance, businesses need to ensure that the cloud password management solution service provider they choose adheres to relevant compliance standards such as SOC 2 Type II and ISO 27001:2013. In addition, service providers should use cryptographic design in their solution.

• On-premises: Some businesses in certain industries, such as healthcare, may be required to maintain full in-house control of their data (i.e. their data cannot be stored outside their environment with a third-party service provider). In this case, choosing an on-premises password management solution is necessary.

Cost

• Cloud: With a cloud password management solution, businesses do not need to purchase software or hardware. Instead, they purchase a license or a subscription and access the solution over-the-web. The type of access they are entitled to depends on what kind of license/subscription they have. For example, some solutions provide access to specific machines, while others provide access to specific users. This latter model is much more business-friendly, because it enables end users to access the solution from wherever they are, and through any device.

• On-premises: On-premises password management solutions are typically more costly than cloud solutions. This is because it is necessary for businesses to implement the required IT infrastructure and processes, while also covering ongoing operating and maintenance costs. Many SMBs lack the budget and the personnel to meet these requirements, and therefore focus on cloud solutions instead.

Implementation

- Cloud: Cloud password management solutions "should" be easy to implement. We emphasize "should" because unfortunately this is not always the case. Some cloud solutions are straightforward and deploy rapidly, while others are highly (and needlessly) complex, and they require significant configuration and testing. SMBs that opt for a cloud solution need to ensure that implementation is smooth rather than stressful. Examining credible reviews and taking advantage of a free trial are good ways to verify this.

- On-premises: On-premises password management solutions are inherently more complex to implement than cloud solutions because they are hosted and maintained in-house. As such, they must be configured and integrated with the environment. SMBs that choose an on-premises option should ensure that the service provider has resources and programs to make the implementation experience as fast and trouble-free as possible.

Devolutions' Security Team Offers the Following Advice to SMB Decision-Makers:

The never-ending debate between cloud and on-premises solutions strikes again when it comes to password manager solutions. However, in our opinion, the discussion should revolve around what the specific password management needs are for the organization. These needs may vary according to multiple factors, such as (but not limited to):

- User location and roles
- Availability requirements
- IT environment size and complexity
- Value of data to protect
- Compliance and security requirements

In some cases, hybrid deployments that combine elements of both cloud and on-premises solutions could solve distinct needs, instead of selecting only one more restrictive product. Furthermore, one solution could be deployed multiple times to address problems such as segregation of duties. Regardless of what they choose — on-premises, cloud, free, or paid — SMBs should that they clearly define all needs before shopping for technology, and while it is obviously necessary to address today's need, it is just as vital to anticipate future requirements as well.

5 RECOMMENDATION

SMBs Need to Implement a Robust Password Management Policy

We encourage all SMBs to develop and enforce a robust password management policy that includes all of the following elements:

Implement Multi-Factor Authentication (MFA)

Even the most diligent and careful user can make a costly password-related mistake. For example, in a hurry they could accidentally put their password in the wrong field. Or, they could have no idea their computer has been compromised by a keylogger (a.k.a. keystroke logger). In most cases, MFA will stop hackers from accessing accounts, even if they have the correct login credentials.

Implement a Password Manager

With a password manager, users only need to remember two sets of login credentials instead of dozens, allowing them to become virtually passwordless. For a deeper look at what features and functions SMBs should look for when choosing a password manager solution, along with an analysis of the pros/cons of cloud vs. on-premises deployment, see Recommendation #4.

Use Passphrases

When users are obligated to remember passwords (i.e., when implementing passwordless authentication is not feasible), then length needs to be favored over complexity. However, the vast majority of users cannot remember a 16+ character password without resorting to patterns and tricks such as “Leetspeak”, which involves changing letters for similar characters (e.g., “p@55w0rd” instead of “password”). Unfortunately, these techniques are widely known and easily exploited by hackers.

Passphrases are much longer than a typical password — which makes it less vulnerable to brute force attacks — and contain letters, symbols, spaces and numbers. For example: “My Purple Dog, Paul, Loves When I Play Frisbee With Him”. It is wiser to choose a passphrase that doesn’t make logical sense and is not associated with the user. For even stronger security, users can mix languages.

Change Passwords After Evidence of a Compromise

In the past, organizations were advised to have end users regularly change passwords. These days, however, the guidance from the U.S. National Institute of Standards and Technology (NIST) is very different: users are better off not regularly changing passwords, because research has shown that they typically choose weaker, easier-to-crack credentials. Some of the most common passwords in 2021 include: 123456, qwerty, and iloveyou. Instead, users should only change passwords when there is evidence of a compromise.

Compare Passwords Against a List of Known Weak and Compromised Passwords

Before a new password is selected, it should be compared against a list of known weak or compromised passwords. It is important for this list to include words related to a user's personal or work environment, such as the company name and the username. This is a good protection against a dictionary attack, which will try a list of known passwords. Common dictionary passwords include things like "qwerty1!" and "1122334455667788", and the most known password list would be rockyou.txt.

To check for evidence, SMBs can use the online Have I Been Pwned? repository, which finds all email addresses associated with a particular domain that have been caught up in known data breaches. It is also possible to receive email notifications if email addresses appear in future breaches. This helps prevent hackers from bypassing 2FA with social engineering, as the SMB will know when to change passwords and on which services.

In addition to vetting all potential passwords for business accounts, SMBs should strongly advise users to vet passwords to their personal accounts too. This is because hackers often breach personal accounts into order to steal data that is used to carry out spear phishing attacks. For example:

- A user adds in a personal email to a friend who is also a supplier "by the way, remember to send in your invoice to Sheila in Accounts Payable on Monday morning".

- A snooping hacker pretends to be the supplier, and sends an email to Sheila asking her to update the bank account number on file.

- Since the email appears to be legitimate and ordinary, Sheila complies with the request.

- The actual supplier sends in an invoice, which is paid — but to the (fraudulently) updated bank account.

By the time the theft is discovered — which could be days, weeks, or even months down the road — hackers have drained the account. And to make matters worse, the SMB is still responsible for paying the legitimate vendor, and this amount may include interest!

Enforce Just-in-Time Access for Privileged Accounts

Hashes are often stored on a system when users or administrators connect on a machine. This can lead to a pass-the-hash attack, in which hackers steal hashed credentials and reuse them to trick an authenticated system into creating a new authenticated session on the same network. Importantly, it is not necessary to crack the password — just to capture it, which means that it does not matter how long or complex the password/passphrase is. To reduce this risk, SMBs should implement just-in-time access for privileged accounts by using a robust Privileged Account Management (PAM) solution. We look at the elements of a PAM solution in Recommendation #7.

Enforce a Password History Policy

SMBs should enforce a password history policy to ensure that end users do not select old passwords. The Center for Internet Security (CIS) recommends setting this value to 24 or more. In addition, the policy should also enforce a minimum password age. Otherwise, users could change their password multiple times within a few minutes, in order to re-use the preferred password they started with.

Eliminate Password Re-Use

A surprisingly common practice is for users — and even some administrators — to re-use passwords across multiple accounts. While this is convenient, it is also very risky and ill-advised. However, there are also scenarios where password re-use is not intentional. For example, when a generic OS image is used to quickly setup systems, it will contain the same default local administrative account (a.k.a. backdoor accounts for administrators). Unfortunately, this means that compromising one machine unlocks all of them.

An excellent and practical solution to this problem for SMBs is to implement Local Administrator Password Server (LAPS) for Windows domains, or rely on a third-party solution. This allows for different passwords to be used by all computers and servers, and it helps mitigate the risk and severity of large scales attacks.

Enable Copy/Paste Passwords

In theory, users should not be allowed to copy/paste passwords. But in reality, it is advised — because otherwise, users are likely to choose a password that is both easy to remember and simple to type. As advised by NIST: "Verifiers SHOULD permit claimants to use 'paste' functionality when entering a memorized secret. This facilitates the use of password managers, which are widely used and in many cases increase the likelihood that users will choose stronger memorized secrets".

Enroll End Users in a Cybersecurity Training Platform

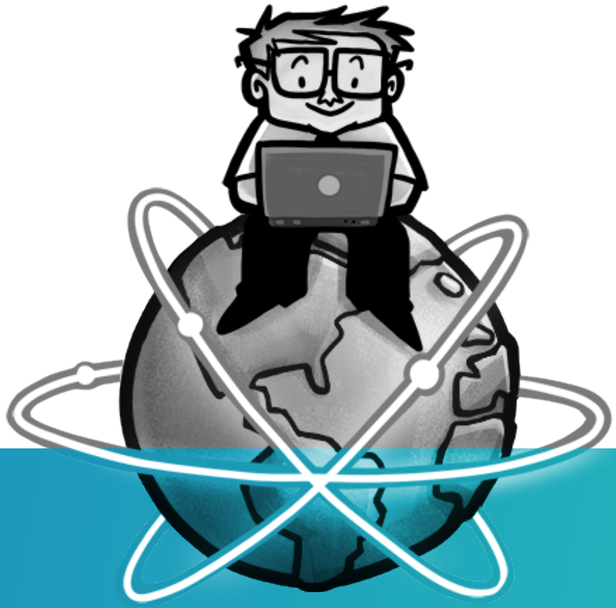
SMBs are urged to enroll their end users in a cybersecurity training platform that covers topics such as social engineering, email security, mobile device security, safe web browsing, safe social networking, protection of health information, etc. Managers can also track user progress to identify knowledge gaps and training needs. **We explore this further in Recommendation #10.**

6 RECOMMENDATION

SMBs Need to Implement an Effective Access Deprovisioning Process

In many SMBs, when an employee leaves (voluntarily or involuntarily), the focus is on retrieving assets. For example, an employee is told to return their corporate-supplied laptop, smartphone, client files, building access card, and so on. Obviously, asset retrieval is a core part of the termination process — but it is not the full picture.

As part of a comprehensive strategy for dealing with employee departures, it is also extremely important for SMBs to deprovision access. Indeed, a recent survey found that 25 percent of workers said they could still access accounts from past jobs — including former IT staff and managers who had the proverbial "keys to the kingdom" (i.e., access to privileged accounts). And separate research has found that over 50% privileged account passwords never get deprovisioned at all!



To close this gap, SMBs should implement an effective access deprovisioning process that includes the following steps:

Immediately Change the Employee's Password

The first and most important step is to change the employee's password, so that they — or someone on their behalf, operating with their permission or otherwise — cannot access their old account(s).

Disable Access to All Accounts

There are two options for removing employee access: deleting accounts and locking accounts. Deleting accounts is preferred, since this eliminates the possibility of future access. However, there may be situations where it is necessary to preserve accounts if they contain valuable data, such as important files, correspondence, etc. In that case, SMBs should lock accounts until the data can be safely and properly archived elsewhere (after which the accounts can be deleted).

Change Passwords on Shared Privileged Accounts

SMBs should change the credentials for any privileged accounts that were shared with the employee. These accounts include any that provide elevated user rights, as well as:

- Domain Administrator Accounts
- Local Administrator Accounts
- Emergency Access Accounts
- Application Accounts
- System Accounts
- Domain Service Accounts

We take a deeper look at these types of privileged accounts in Recommendation #8.

7 RECOMMENDATION

SMBs Need to Implement a Privileged Access Management (PAM) Solution to Bridge the Gap Between Authentication and Authorization

Users with privileged account access are given “the keys to the kingdom” so they can be more productive and efficient, while carrying out their day-to-day tasks. Unfortunately, privileged users are also prime tagets for hackers who want to breach devices and networks, and ultimately steal data. **In fact, 74% of data breaches are triggered by privileged account abuse.**

What’s more, 72% of organizations do not store all of their privileged accounts in a secure access vault, 58% of organizations have more than 100,000 folders accessible to all employees, and in over 50% of organizations, privileged accounts never expire or get deprovisioned.

Many InfoSec experts believe that privileged user accounts represent the riskiest and most dangerous type of privileged access, because of how common they are, how much access to sensitive data they grant, and how easily hackers can compromise them.

All of this begs the question: Why don't SMBs simply shut down all privileged accounts? The answer is because identity is not always associated with a specific user. Rather, it is associated with a role, team, or group. Examples of accounts where shared access is typically a requirement include:

- Domain Administrator Account
- Local Administrator Accounts
- Emergency Access Accounts
- Application Accounts
- System Accounts
- Domain Service Accounts

We look closer at these types of accounts in Recommendation #8.

GOOD TO KNOW

SMBs are advised to create dual accounts for higher privilege users. The first account has relatively limited access and is for day-to-day tasks. The second account has more access and is for administrative duties. The second account is managed by the PAM system and configured with enhanced security, such as account brokering and password rotation after use.

Fortunately, there is a practical way for SMBs to bridge the gap between identity management (authentication) and access management (authorization): implement a PAM solution.

A PAM solution uses role-based access control (RBAC) to function as a gatekeeper for shared accounts, adding a critical layer of privileged account monitoring and auditing. Key features that SMBs should focus on when choosing a PAM solution include:

- A secure vault that safely and properly stores credentials and other sensitive data that must be shared across multiple users (e.g., software license keys, etc.).

• Account checkout request functionality, which allows Admins to approve or reject requests on a case-by-case basis (and in the case of approvals, set a time limit for access to avoid privileged accounts being left unattended).

• Automated password reset upon check-in.

• Built-in multi-factor authentication (MFA).

• Account brokering, which enables users to access privileged accounts without ever seeing login credentials. Account brokering also prevents users from accessing resources outside of a workflow provided by the PAM solution, reducing the potential for credential abuse.

• Account discovery, which automatically scans and discovers privileged accounts from an Active Directory provider. For SMBs this is far more practical and effective than when using standalone identification providers — such as identity access management (IAM) systems, databases, network equipment, and servers — which must be manually queried to discover accounts.

• Ease-of-deployment and management.

In addition, more sophisticated PAM solutions support Privileged Session Management (PSM). This utilizes a specialized server that brokers authentication behind-the-scenes, and can even record the activity of remote sessions. PSM is especially important for organizations that have contractors and “boomerang” employees (i.e., employees who leave the organization and then return). These users typically need more scrutiny and limited access.

8 RECOMMENDATION

SMBs Need to Protect, Monitor, and Update All Privileged Accounts

Despite the critical importance of safeguarding privileged accounts, research has found that 55% of organizations do not know how many privileged accounts they have, or where they are located.

One of the key reasons for this oversight is that many SMBs are unaware of what types of privileged accounts they must protect, monitor, and update. They include:

- **Domain Administrator Accounts**
  These hold the keys to the "crown jewels," because they grant control of the entire AD domain (all controllers, workstations, and member servers). Access to Domain Administrator Accounts should only be given on an as-needed basis.

- **Privileged User Accounts**
  These grant more privileges — and hence more risk — than ordinary user accounts across one or more systems. For example, users may be able to modify or remove software, change application configurations, etc.

- **Local Administrator Accounts**
  These grant administrator-level access to local machines, and are typically used by IT teams to set up new workstations and carry out maintenance tasks. Hackers often target vulnerable Local Administrator Accounts to establish a foothold inside a network. From there, they evaluate their victims' cybersecurity defense tools and systems before launching an attack.

- **Emergency Access Accounts**
  Sometimes called break-the-glass accounts or firecall accounts, these are usually disabled by default until a critical incident happens — such as a cyberattack — in which case they can be accessed by specific users to restore secure systems and retrieve usage logs.

Application Accounts

These are used by applications to access various functional resources, such as databases and networks. They are also used to carry out automated tasks like software updates. Usually, Application Account passwords are stored in unencrypted text files on the network, so they can be quickly and easily retrieved by users across the organization. Unfortunately, hackers target known and unpatched vulnerabilities to steal these passwords, so they can establish remote access, change system binaries, and even elevate standard accounts to privileged accounts in order to spread throughout the network.

GOOD TO KNOW

In many cases, Privileged User Accounts are not assigned to a specific user, but they are instead shared across administrators. Basically, the rule that SMBs should adopt is this: Any account that grants users anything more than a standard account qualifies as a privileged account, and it must be managed and monitored accordingly.

System Accounts

These are used by services and applications (instead of human users) to launch processes and carry out scheduled tasks. The good news is that System Accounts typically do not have the ability to log onto systems. The bad news is that they often have passwords that never change, because SMBs either completely forget about them, or they have never known about their existence in the first place. As a result, System Accounts are frequently targeted by hackers, who launch binaries at elevated privileges in order to carry out remote access attacks.

Domain Service Accounts

These enable various applications and systems to communicate and access required resources, in order to call APIs, run reports, etc. They are typically used for updating security patches, backups, and deploying software. Many SMBs rarely — if ever — change the password, which is what hackers are counting on.

All SMBs need to be concerned with privileged account abuse carried out by rogue insiders, as well as by hackers who have seized user accounts (often without victimized users being aware that anything has happened). Some of the signs to watch for include:

- A user deviates from their normal baseline activity. This may include unusually short or long session duration, accessing/reading/changing files outside of a normal work routine, or atypical keystroke patterns (which can be detected through biometrics analytics that use machine learning to study a specific user over time).

- A user transfers files to a personal workstation, when they are only authorized to transfer files to corporate systems.

- A user account is accessed by multiple endpoints at the same time.

- Multiple users are logged in from the same endpoint.

- Dormant accounts come back to life.

- Unusual window titles.

SMBs should also keep in mind that hackers will often run small tests to see if their presence is detected. They will also create accounts and add them to high-privileged groups, and then wait weeks or months before accessing them.

To close this gap, SMBs need to fully deploy a comprehensive — yet easy to use and manage — privileged access management (PAM) solution to secure and monitor all of their privileged accounts, because failure to do so can lead to expensive data breaches, lingering reputation damage, and in some cases outright closure. In **Recommendation #7 we dive deeper into the purpose of a PAM solution, and highlight factors that SMBs should look for when choosing a solution.**

9 RECOMMENDATION

SMBs Need to Implement 4 Essential Security Principles: Principle of Least Privilege, Segregation of Duties, Zero Trust, and Defense-in-Depth

About Principle of Least Privilege (POLP)

POLP is a policy in which end users are given only the amount of access they need to carry out their jobs — nothing more and nothing less. In addition to minimizing the size of the attack surface, **POLP offers additional security benefits, including:**

Stronger security: Before implementing POLP, SMBs must first analyze current access levels for each user. This process often reveals that many — and in some cases, most — users have too much access in the first place, and it can be reduced accordingly.

Thwarting malware: POLP can help contain malware to a single device or to a limited number of devices, which can give SMBs the time they need to investigate, contain, and remediate a threat.

Greater stability: POLP prevents end users with relatively low-level accounts from executing changes that would affect the entire system.

Data classification: POLP helps SMBs identify what data they have in their ecosystem, where it lives, and who has access to it.

Audit readiness: POLP significantly simplifies and streamlines the auditing process.

Depending on the operating system, POLP can be implemented across one or multiple factors, such as:

- **Role** (e.g., project managers, resource managers, etc.)
- **Seniority** (e.g., supervisors, managers, executives, etc.)
- **Business Unit** (e.g., development, marketing, HR, etc.)
- **Location** (e.g., head office, field offices, etc.)
- **Time** (e.g., office hours, after office hours, etc.)
- **Typically, administrators will customize a POLP profile that fits their SMB's specific needs and seeks to balance the need for strong security with the fact that end users require sufficient access to be productive and efficient.**

POLP Best Practices Include:

Evaluate access levels: In consultation with users, SMBs should evaluate each role to determine the appropriate access level. The default access should be set to "least privilege", and greater access should be granted only as needed.

Communicate effectively: SMBs should communicate the purpose of POLP to all users, so they understand that the approach is not intended to stifle their productivity, but rather to protect the organization.

Deploy one-time-use credentials: When temporary privileged access is required, SMBs should deploy one-time-use credentials that are granted at the last possible moment, and then revoked immediately after use. This approach, which is known as privilege bracketing, can be used for individual users as well as processes or systems.

Enforce account separation: SMBs should separate administrator accounts from standard accounts, and separate higher-level system functions from lower-level system functions (see next section on Segregation of Duties).

Continuously monitor and regularly audit: It is very important for SMBs to have full visibility in order to see exactly what end users do and when they do it. In addition, SMBs should regularly audit end user privileges to ensure that access is appropriate. This includes removing access for all employees who have left the company and having a method to automatically revoke privileged access in the event of an emergency.

About Segregation of Duties (SoD)

The same factors that make SMBs especially vulnerable to hackers also make them susceptible to attacks from users/ex-users, vendors, contractors, and other rogue insiders. Of course, sometimes breaches are not the result of some illicit activity, but due to negligence, incompetence, or human error. This is where SoD enters the picture.

SoD is a policy that forbids a single individual from being responsible for carrying out conflicting duties. The goal, as highlighted in the ISO/IEC 27001 framework, is to reduce opportunities for either the unauthorized or unintentional manipulation or misuse of organizational assets. Basically, when multiple people are involved in a sensitive workflow, there is a smaller chance that anyone will try and break the rules, or that mistakes will go undetected. SoD has been used for many decades in accounting, risk management, and financial administration.

SoD Best Practices include:

Define and assign roles that minimizes risk: Prevent conflicts of interest (real or apparent), wrongful acts, fraud, and abuse when assigning one or multiple roles to an employee.

Align tasks with roles: SMBs should set up permissions and access rights to align with task and role segregation, which should be based on the Principle of Least Privilege (as discussed above).

Analyze access levels for escalation: SMBs should ensure that no single individual has an opportunity to combine multiple accesses to promote himself to a higher (and unauthorized) access level on a given system or domain at any given time.

Integrate with HR policies: SMBs should implement human resource management policies that support a comprehensive SoD program. This includes training supervisors and managers to recognize when a subordinate or any other colleague has conflictual, risky or unnecessary wide set of tasks that could be transferred to another and more appropriate role.

In addition, some SoD assurance can be obtained when performing the following:

Audit regularly
SMBs should perform ongoing cybersecurity audits and pay particular attention to potentially fraudulent activities. We look at elements of a cybersecurity audit in Recommendation #12.

Rely on third-party expertise for monitoring
SMBs that lack in-house expertise in this area are advised to work with a managed service provider (MSP), since malicious activity is almost always covert and difficult to detect. It will also grant the benefit of applying SoD between internal auditing versus operational roles. We highlight factors that SMBs should focus on when choosing an MSP in Recommendation # 13.

About Zero Trust

Zero trust is based on the idea that nobody should be automatically trusted — even if they are behind the perimeter or using a trusted network. Instead, prior to accessing parts of the network, users, machines and apps should be authenticated through technologies such as MFA, IAM, encryption, analytics, etc. A key element of zero trust is POLP, which is discussed above.

It is important to clarify that a zero-trust approach does not involve eliminating the perimeter. Rather, it leverages network micro-segmentation to move the perimeter in as close as possible to privileged apps and protected surface areas. In other words, instead of putting a security guard in the lobby of a building, zero trust puts a security guard in front of the elevators, stairwells, each office, etc.

The zero-trust concept aligns with what many Admins and other InfoSec professionals have been saying for years: assume that everyone — including those inside the SMB — represents a potential cybersecurity threat until it is proven otherwise. The extension of this vision is that the "castle-and-moat" approach to perimeter security is out, and micro-segmenting and granular perimeter enforcement is in.

Zero Trust Best Practices:

• 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 using MFA in real-time.

• Extend identity controls to the endpoint to recognize and validate all devices. Just verifying users is not enough.

• Organize users by group/role to support device policies. For more insight on implementing Privileged Identity Management (PIM), read our article here.

• Leverage automatic de-provisioning, along with the capacity to wipe, lock, and un-enroll stolen or lost devices.

• Educate users to be part of the solution in the new zero-trust environment. For example, users should be encouraged to immediately report phishing attempts or any other suspicious behavior. As highlighted by Deloitte: “The zero-trust mindset shift brings with it a set of design principles that guide security architecture development and build on existing security investments and processes. To enforce access control, companies must have situational awareness of their data and assets; companies that lag on basic cyber hygiene principles and practices may be challenged to realize the full benefits of zero trust.” We explore ways that SMBs can improve cyber hygiene principles and awareness in Recommendation #10.

• Regularly update end user rights based on changes to roles/jobs, as well as changes to prevailing security policies and compliance requirements.

GOOD TO KNOW

It is important to realize that moving to zero trust is a process that will take time — and there will be obstacles along the way that will put leadership, IT, and end-user patience to the test. However, it is well worth the effort given that in network security terms, trust is something that must be earned rather than assumed. Zero Trust is not a one-time project — it is a long-term strategic commitment and objective that must be applied in all areas of the SMB.

About Defense-in-Depth

Defense-in-depth involves implementing multiple diverse controls in an environment to create layers of security, and ultimately slow down hackers as much as possible.

A common analogy used to describe this approach is the "Swiss cheese model." Imagine a ray of light shining from one end of a table to another. Now, start putting slices of Swiss cheese in a line to block the ray of light. While each slice has holes, these are not in the exact same area. This leads to more light getting blocked with each added slice.

The light in this analogy is a cyberattack. The slices of Swiss cheese are various defense tools — technologies, strategies, policies, and processes. The goal is not to completely stop 100% of cyberattacks — because that is not realistic. Rather, the purpose is to make it significantly easier and more effective for SMBs to detect hackers as they try to circumvent controls to reach sensitive assets.

Defense-in-Depth Best Practices:

Assume breach
Hackers have all the time they want to grasp an opportunity to perform a successful attack on a target. With this in mind, control layers should be designed as if a breach has already happened (i.e., answering the “what if?” question), and SMBs should implement proper defenses to prevent or contain hackers’ next moves.

Combine security principles and strategies
When combined, these produce a synergetic effect by limiting and preventing their respective weaknesses, and boosting their overall efficiency. For example, SoD and POLP will contain threats to a subset of the whole business environment, which creates a great opportunity to implement control layers between them. In addition, the four-eyes principle could also be added for privileged access usage using an approval workflow to prevent, or at least detect, unauthorized access attempts. The four-eyes principle requires that any activity by an employee that involves material risk must be reviewed and confirmed by a second employee who is independent and competent.

Technological control diversity
Implement cybersecurity solutions that function differently and represent dissimilar controls. For example, while an anti-malware network filter, a whitelisting app, and an email attachment scanner are all anti-malware tools, they do different things — and can therefore cover a wider area of the attack surface.

Active monitoring of unusual behavior
Once hackers circumvent a control layer, they need to discover how to achieve their overall objective. This involves gathering information, and in some cases testing assumptions. Active monitoring of such behavior is the key component to detect intrusions between control layers. Neglecting this practice will allow plenty of time for hackers to exploit an opportunity without being detected.

Conduct penetration tests on a regular basis
This is ideal for spotting weaknesses in the control layers design, by carrying out simulated attacks on a specific control layer or a combination of control layers. Sometimes, hackers are creative enough to choose an attack path that was not previously identified and secured by the SMB.

10 RECOMMENDATION

SMBs Need to Improve Their Workforce's Cybersecurity Awareness

SMBs that believe, "since we have not yet been attacked, then our people must be aware of cyberthreats," are putting their data, their customers, and their reputation in harm's way — and in extreme cases, they may not survive to correct this: 60% of SMBs go out of business within six months of a cyberattack.

While there are several ways for SMBs to increase their workforce's cybersecurity awareness, among the most practical, effective and affordable is with an online cybersecurity platform. This is a portal that provides employees with self-paced, hands-on, skills-based threat detection and mitigation training in a live and dynamic simulated environment.

A wide range of threats are covered, including the "Big 3" that SMBs are most concerned about according to our survey: ransomware, phishing, and supply chain attacks. We take a deeper look at these threats and how to defend against them in Recommendation #2.

One of the key advantages of online training is that employees get immediate feedback on their decision-making, and move forward through the training based on their performance. Supervisors and managers also access a dashboard and monitor progress, in order identify strengths and weaknesses. For example, an employee may be competent when it comes to steering clear of phishing attempts, but may need additional training in mobile device security.

11 RECOMMENDATION

SMBs Need to Keep Remote Workers from Becoming “the Weakest Link” in the Cybersecurity Defense Chain

Many SMBs worldwide have been in a mad scramble to find a safe and secure solution to deploy and maintain remote access. Even as some SMBs return to a physical office building, a substantial portion of the workforce is expected to remain remote on a full or part-time basis. This means there are hundreds of new entry points that need to be safeguarded against potential hackers. It’s a daunting challenge — especially since most SMBs do not have large IT teams in place.

To address this priority, SMBs should implement and enforce a remote worker cybersecurity policy that includes the following elements:

Mobile Data Hotspots and/or VPNs

Remote workers love public Wi-Fi access, because it is available virtually everywhere these days —doctors’ offices, airports, restaurants, and the list goes on. Unfortunately, hackers love public Wi-Fi as well, because they can snoop, phish, and spoof with remarkable ease. One option to address this risk is to provide remote workers with mobile data hotspots. If this is not cost-effective, then at least remote workers should use a good virtual private network (VPN).

Segmented Home Networks

Many remote workers mistakenly believe their home network is secure, when in fact it can be just as vulnerable as a public Wi-Fi network. As noted above, while using a VPN helps reduce the risk, remote workers with high-risk access should go a step further and segment their home network and isolate it behind a business-grade firewall. It is also the responsibility of SMBs to provide resources and support for this requirement if it is an enforced policy.

Multi-Factor Authentication (MFA)

MFA is an extra layer of security that requires remote workers to verify their identity by providing their login credential, along with another piece of information that could be:

- Something they know, such as the answer to a secret question, a PIN, or a password.
- Something they have, such as a smartphone or a token.
- Something they are, such as their fingerprint, voice recognition, or an eye scan.

The basic idea is that even if a remote worker's login credentials are stolen, it is less likely (albeit not impossible) that hackers will be able to supply the additional information and access a device, application, network, or system.

A Password Manager

To strengthen security, remote workers (along with in-house workers) should use a password manager that offers features such as password rotation, a strong password generator, automatic checks against passwords that have been exposed during hacks, and real-time email alerts in the event of unauthorized access attempts. We look closer at these features in Recommendation #4.

Endpoint Security

Endpoint security is a critical line of defense to keep hackers from launching attacks against devices, and ultimately shifting their attack to networks and integral systems. Key endpoint security tools include:

- Network firewalls (both on endpoints and home networks)
- Anti-virus software
- Software updaters (more below)

In addition, while it may be fine for some SMBs to let their remote-working IT staff decide when to update their software, for general non-technical users the best practice is to put remote devices on a standard image and activate automatic updates for all apps and programs — especially security software.

A USB Data Blocker

If remote workers need to charge their device and the only option is a public USB charging station, they should always use a USB data blocker. This allows the power leads to connect (and the charge to occur), but it does not expose data pins inside the device, thereby preventing data exchange and protecting against malware.

A Secure Remote Access Solution

In remote work, IT professionals must always have secure access to critical assets. Whether they need to update machines in the computer network or to assist users remotely, the ideal is to use a complete remote access solution that is quick and easy to deploy. We focus more on this in Recommendation #15.

Provide Ongoing Cybersecurity Training

All employees need ongoing cybersecurity training — but especially remote workers who can sometimes let their guard down since they are not constantly being reminded to follow best practices.

In addition, remote workers should be cautioned against over-sharing on social media — such as checking in to apps when they arrive at hotels, airports, and so on — since such activity can draw the attention of hackers, who can use the information to hunt down victims. Remote workers should also keep their devices with them, and never leave them unattended for even a few seconds. When leaving home, devices should always be securely locked away vs. left out in the open. We provide more advice on increasing cybersecurity awareness across the workforce in Recommendation #10.

Switch to Cloud-Based Storage

Storing data in the cloud is not just more convenient for remote workers, but it also enhances protection from cyberthreats with protections such as enforcing conditional access, DRM, UEBA, DLP, encryption and more. If a device is stolen, then access to cloud-based data can be easily controlled by revoking access instantly. SMBs that need or want to use on-premise instead of cloud-based platforms would have to rely on their VPN solution or another third party suite to offer similar level of protection.

Screen Protectors

Screen protectors are a highly effective way to keep “shoulder surfers” from snooping and stealing data. And although pandemic-related social distancing has reduced this risk in some locations, it has not eliminated it. Considering how relatively inexpensive screen protectors are, every remote worker should have one!

12 RECOMMENDATION

SMBs Need a Comprehensive Cybersecurity Audit Process

The purpose of a cybersecurity audit is to establish an acceptable degree of assurance that the required controls — data, operational, network, system, physical, etc. — are in place and reducing risk as expected. As per the widely accepted "Three Lines Model" by The Institute of Internal Auditors, auditing is the third line of defense behind management controls and internal control measures.

To proactively close the gaps in their defense profile, SMBs should conduct cybersecurity audits that cover the following aspects:

- **Data Security:** Auditing network access control, encryption use, data security at rest, and transmissions.
- **Operational Security:** Auditing security policies, procedures, and controls.
- **Network Security:** Auditing network and security controls, the security operation center (SOC), anti-virus configurations, security monitoring capabilities, etc.
- **System Security:** Auditing hardening processes, patching processes, privileged account management, role-based access, etc.
- **Physical Security:** Auditing disk encryption, biometric data, multifactor authentication (MFA), etc.

In addition to helping SMBs maintain alignment and monitor performance of their cybersecurity investments, audits can enhance trust with customers and business partners. For example, audit reports can be privately or publicly distributed, and leveraged in proposals and presentations.

How Often Should Cybersecurity Audits Be Performed?

Many companies perform a security audit once or twice a year. However, in some cases they should be done more frequently. Advises TechTarget.com:

> *Quarterly or monthly audits may be more than most organizations have the time or resources for. The determining factors in how often an organization chooses to do security audits depends on the complexity of the systems used and the type and importance of the data in that system. If the data in a system is deemed essential, then that system may be audited more often, but complicated systems that take time to audit may be audited less frequently.*

Best Practices for Preparing for, Conducting, and Assessing a Cybersecurity Audit

- Define clearly the scope and objectives of the cybersecurity audit.
- Review and centralize all security policies that cover data security, operational security, network security, system security, and physical security.
- Review applicable regulations and compliance standards.
- Create a top-down view of the network, which helps reveal potential weaknesses and edge locations.
- Create a list of security team members, and detail their responsibilities.
- Identify and document risks and vulnerabilities.
- Prioritize risk response.

In-House vs. External Cybersecurity Audits

Most SMBs do not have the in-house specialists to carry out a comprehensive cybersecurity audit. And many of those that do still choose to work with an external third-party, in order to eliminate bias and conflict of interest. This helps organizations get a true picture of what is really happening — and what needs to change to close gaps and appropriately manage risk.

13 RECOMMENDATION

SMBs Need Support from MSPs to Close the Cybersecurity Defense Gap

Managed services providers (MSPs) help SMBs increase their capacity and skillset, reduce risk, exploit growth opportunities, enhance user/customer experience, and perhaps most importantly these days in the shadow of the pandemic, embrace change and exploit uncertainty.

To choose the right MSP, SMBs should focus on these factors:

Services

Some MSPs offer a comprehensive range of services, while others focus on specific elements such as information security. For SMBs, what matters most is that the MSP they choose has the proven capacity to serve their particular needs and goals. At the same time, one of the most important services that an MSP should offer — if not the single most vital — is reliable, objective and customized advice and consultation. This includes providing assurance towards cybersecurity competence and data handling (a.k.a. vendor security management).

Responsiveness

SMBs should pay very close attention to responsiveness standards. It is critical to know how long it typically takes an MSP to respond, how fast they resolve issues, and what to expect if on-site support is required. And of course, all of these commitments and standards should be locked into the Service Level Agreement (SLA).

Coverage

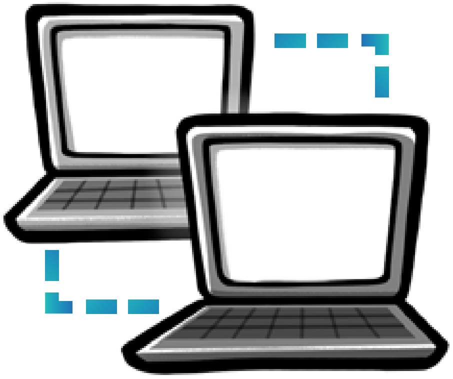
An MSP should monitor the infrastructure 24/7/365, in the event that the network or systems go offline or degrade for any reason.

Business Continuity and Disaster Recovery

SMBs cannot afford to "go off the grid" in the event of a hardware failure, software failure, local power outage, cyberattack, or any other event — because when that happens, employee productivity grinds to a halt, and customers start to head to the competition. To prevent this, SMBs should choose an MSP that has tools and policies to support business continuity and disaster recovery.

Technology and Vendor Neutral

Due to their vast experience, good MSPs have intelligent views on choosing one technology or vendor vs. another. This is perfectly fine, and in fact tapping into this knowledge is one of the benefits of working with an MSP. However, an MSP should not aggressively insist on a specific technology or vendor. Instead, they should adjust and respond to the SMBs preferences and current infrastructure, and have good professional relationships with multiple vendors — since once they are hired, they will be responsible for interacting with them and holding them accountable.



Communication

Most MSPs can have expert-to-expert discussions with members of an in-house IT team. But when it comes to speaking with non-techies, they need to adjust their vocabulary and approach accordingly — especially when it comes to training business users on things like password and access management policies. Any MSP that cannot communicate effectively with diverse audiences is going to be part of the problem, not the solution.

Consistency

On the IT landscape there are good days and there are bad days. Obviously, SMBs cannot expect an MSP to completely protect them 100% from cyberattacks or hardware failures, since this is simply not realistic. But SMBs can and should insist that an MSP is consistent in terms of their approach and professional standards. They should never lose sight of the fact that they work for the SMB — not the other way around!

14 RECOMMENDATION

SMBs Need to Increase the Proportion of Their IT budget That Is Allocated to Cybersecurity

Often, CISOs and other IT professionals who sound the alarm bells about their SMBs' cybersecurity vulnerabilities face tough questions like:

- What is our return on investment?
- Are we spending money that could be allocated elsewhere?
- Are we overreacting and exaggerating the risks?

The following tips can significantly improve the chances of turning skeptics into supporters, and getting buy-in and budget:

- Demonstrate the risks and impact of a cyberattack. For example, a realistic exercise that simulates a ransomware attack can be eye-opening for decision-makers.

- Use plain language and avoid jargon. What is readily known by CISOs *et al* (e.g., multi-factor authentication, zero trust, privileged access management, etc.) may be unfamiliar to CEOs, CFOs, and other stakeholders — or, they may have some awareness and information, but it is incomplete or out-of-date.

- Where possible, quantify risks with numbers (e.g., “This type of breach cost a similarly sized company in our marketplace $1.25 million to investigate and clean-up”) vs. abstract dangers (e.g., “This type of breach involves hackers stealing emails”).

- Be prepared with a proposed plan that includes a strategy for the cybersecurity budget, and a clear list of the technology, training, and/or personnel that needs to be purchased. As advised by ZDNet.com: “There’s no point requesting a budget then just winging it: [decision-makers are] more likely to issue the required funding if there’s a set plan, a strategy they can see and get behind.”

- Identify vendors that offer a no-risk free trial, so that potential tools can be tested in the SMB to confirm security, usability, scalability, flexibility, etc.

Ultimately, the key message that needs to be conveyed — and it can take multiple meetings and discussions — is that investing in cybersecurity is not just about protecting data, but that it adds value to the business by:

- Increasing marketplace loyalty and trust, which translates into greater revenues and higher customer engagement.

- Reducing costs by leveraging automation to replace time-consuming and tedious manual tasks.

- Creating a better decision-making environment, by ensuring that prioritized cybersecurity risks are taken into consideration.

- Establishing that reliable business continuity and disaster recovery tools and workflows are in place.

- Making SMBs more attractive to strategic partners and investors.

15 RECOMMENDATION

SMBs Need to Focus on 5 Security Projects in 2021-2022: Secure Remote Access Management, Secure Digital Vault, Secure Password Management, Multi-Factor Authentication, and Automation

In the distant past, most hackers were “script kiddies” intent on destroying machines and wreaking havoc. Well, that era is over! Today’s sophisticated cyber criminals are driven by dreams of huge payoffs. They are invading SMBs through multiple threat vectors such as data centers, the network edge, and remote offices — essentially anywhere that end users access apps, data, or services over the corporate network or public internet.

To help SMBs survive rather than succumb to a wide range of advanced cyberthreats — including those that bypass conventional anti-virus tools — here are five core solutions that should be implemented now vs. later:

Secure Remote Access Management

The pandemic has massively accelerated the shift to remote working. However, the benefits of a distributed workforce come with major security risks. SMBs need to close these gaps by securely managing employee and contractor access. Affordable, easy-to-deploy IPSec and SSL VPNs are highly recommended for this purpose. In addition, while cloud services are great for mobility and availability, it is important to fully understand the prevailing risk model, and the limits of service provider responsibilities.

Secure Digital Vault

As more business functions are conducted online, organizations must secure employee passwords, vital intellectual property, and private records. This is a challenge for many SMBs, since they tend to focus exclusively on the perimeter, and have little or no visibility into their employees' (often bad) password management practices. A secure digital vault that uses strong encryption and authentication lets employees securely store passwords and digital credentials. At the same time, it gives SMBs the ability to detect vulnerabilities and improve security hygiene on an individual, group, and company-wide basis.

Secure Password Management

Primarily due to cost, integration, accessibility, and scalability advantages, many SMBs are going all-in when it comes to adopting digital solutions — everything from software apps to building entrances. However, many of these resources lack robust cybersecurity defense frameworks. Password management, which works in tandem with access management, lets the good guys in and keeps the bad guys out. Key benefits include: applying proper credentials and privileges, enabling automated policy management as employees change roles, and ensuring that employees are verified when accessing digital resources (e.g., apps) and physical locations (e.g., buildings). It is also vital to note that password-protected spreadsheets and other single-user-oriented password management solutions are woefully inadequate. Not only are they tedious to manage, but they are alarmingly insecure.

Multi-Factor Authentication (MFA)

Rumors of the death of passwords have been greatly exaggerated. They are still very much alive — but they are now widely recognized as being a part of the authentication puzzle, rather than the whole picture. SMBs need to augment strong passwords with a second factor: something that employees have (e.g., device), know (e.g., PIN), or are (e.g., biometrics).

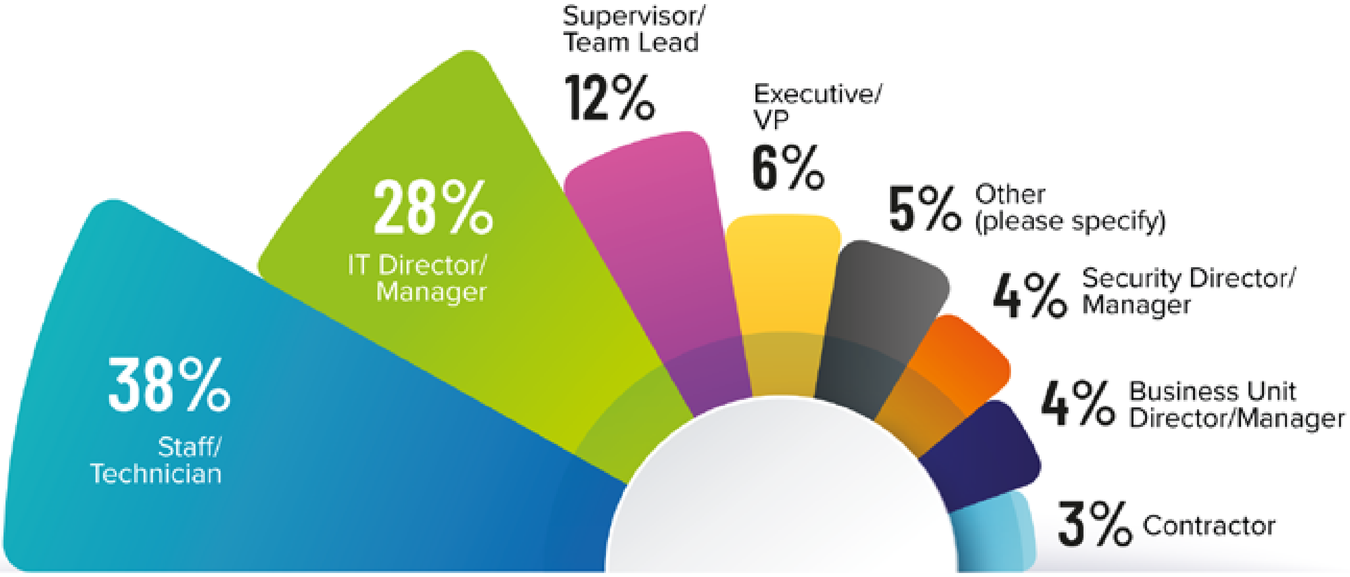
Automation

To avoid getting victimized by hackers, SMBs need to automate, automate, and automate! This is particularly important given the massive shortage of qualified cybersecurity professionals — especially among SMBs, which typically cannot compete in terms of bottom-line compensation with large enterprises. Fortunately, new automation tools are making it easier for SMBs to deal with enterprise-grade security problems — without having to hire an army of security engineers or establish a fully fledged security operations center (SOC). Automation also mitigates security vulnerabilities riggered by human error, speeds up incident response, and enhances overall security operation performance.

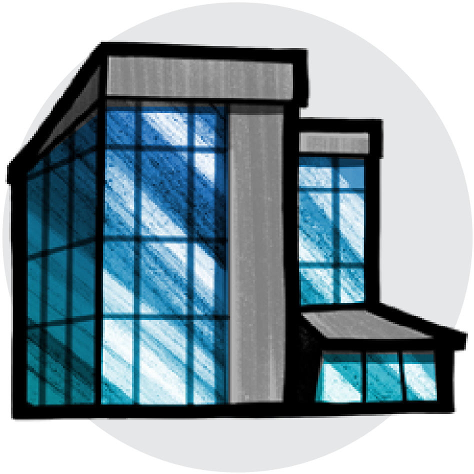
PART 7

PROFILE OF RESPONDENTS

Which title best describes your position within the organization?

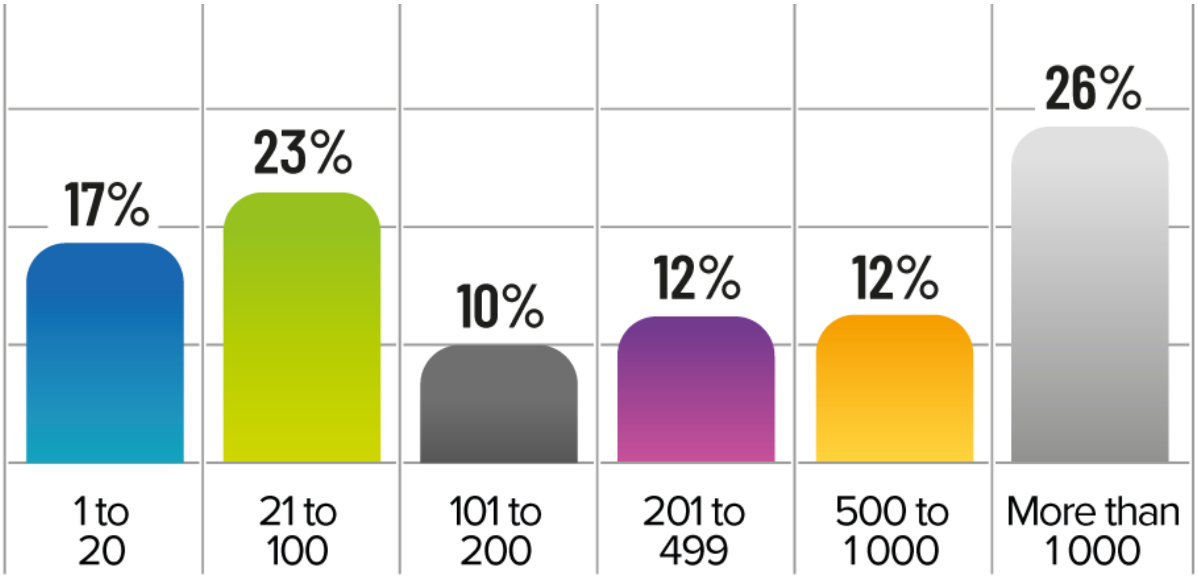


What best describes your organization’s sector?

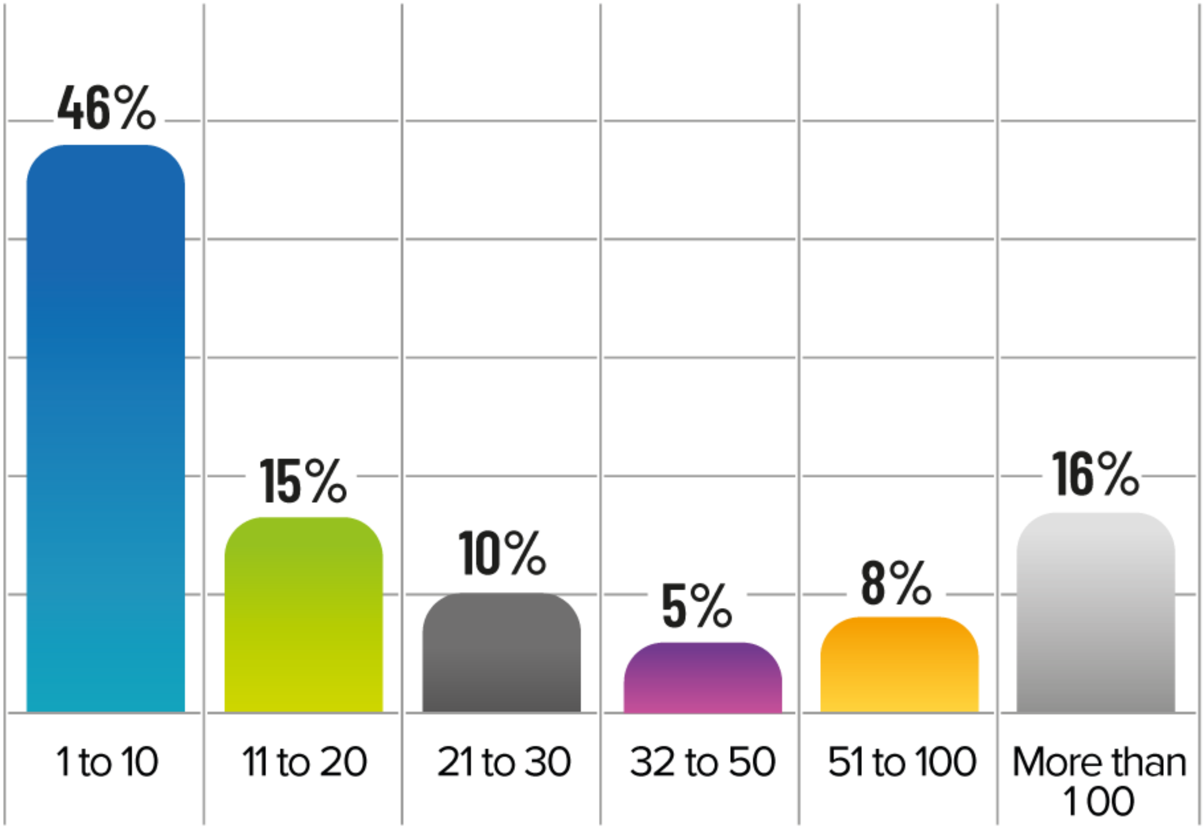


28%	●	IT services
11%	●	Finance and insurance
8%	●	Education
8%	●	Manufacturing
7%	●	Other (please specify)
6%	●	Computer and network security
5%	●	Government
5%	●	Health
3%	●	Construction
3%	●	Retail
3%	●	Technology
2%	●	General services to business
2%	●	Customer service
2%	●	Communications
2%	●	Transportation
1%	●	Entertainment
1%	●	Oil and energy
1%	●	Marketing and advertising
1%	●	Public administration
1%	●	Security, defense technology and infrastructure
1%	●	Utilities

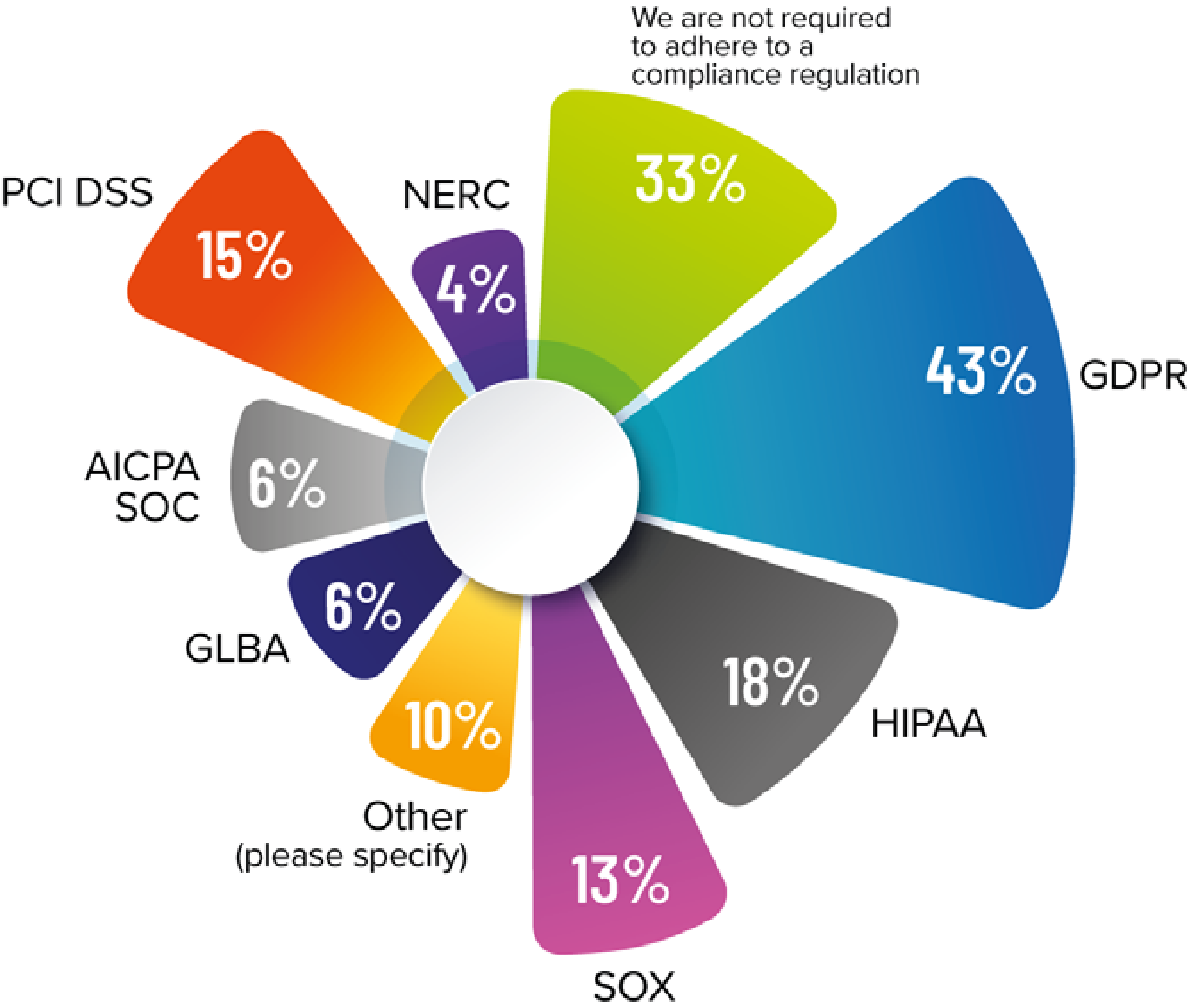
How many people are employed in your organization across all locations worldwide?



How many of your employees work in the IT department?



Please select all of the compliance regulations that your company is required to adhere to:



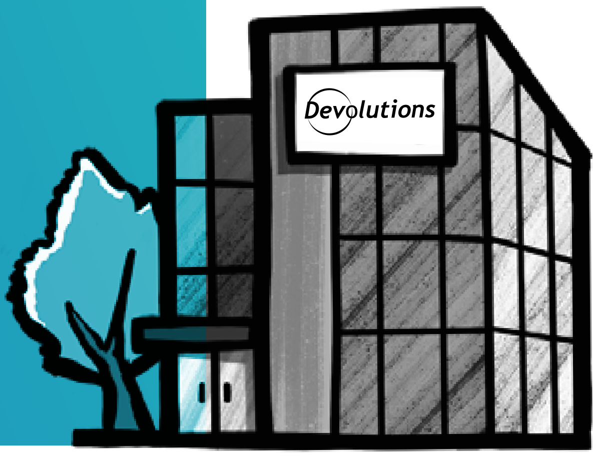
Devolutions

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 and treating them like "second-class citizens" is wrong and unacceptable. That is why we have built a set of Universal Password and Access Management solutions specifically designed to meet the growing needs of SMBs, and 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 **"Universal Password and Access Management for the rest of us!"**

OUR SUITE OF SOLUTIONS

Below is an overview of our suite of solutions.
Free trials are available.

Devolutions Server

Devolutions Server (DVLS) is a full-featured shared account and password management solution with built-in privileged access components to meet the ever-expanding security requirements of SMBs. DVLS also features an integrated PAM component that supports a variety of enhanced functions, including account discovery, account check-out approval, and automatic password rotation.

Learn more here.

Password Hub Business

Password Hub Business (PHB) is a secure and cloud-based password manager for teams. It empowers SMBs to easily and securely vault and manage business-user passwords and other sensitive information through a user-friendly web interface, which can be quickly, easily, and securely accessed via any browser. PHB also features role-based access control, a centralized password vault, a strong password generator and more.

Learn more here.

Password Hub Personal

Password Hub Personal is a safe, easy-to-use and free password manager for individual users who want to store personal passwords in a secure vault, which is only accessible by the user. You can also easily create and access your own Password Hub Personal from your Devolutions Account.

Learn more here.

Remote Desktop Manager

Remote Desktop Manager (RDM) centralizes all remote connections on a single platform that is securely shared between end users and across the entire team. With support for hundreds of integrated technologies — including multiple protocols and VPNs — along with built-in enterprise-grade password management tools, global and granular-level access controls, and robust mobile apps to complement desktop clients for Windows and Mac, RDM is a Swiss Army knife for remote access. RDM also features role-based access control, account brokering, administrative password sharing, session recording, centralized password vaulting, and more.

Learn more here.

Devolutions

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/