Devolutions

REPORT

State of Cybersecurity in SMBs in 2020

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Global cybercrime revenues have reached $1.5 trillion per year, and the **average price tag of a data breach is now $3.9 million per incident.** Yet despite these staggering costs, there remains a common belief among many small and mid-sized businesses (SMBs) **that the greatest vulnerabilities exist in large organizations.** However, there is mounting evidence that **SMBs are becoming more vulnerable than enterprises**, and complacency regarding this reality can have disastrous consequences.

To help SMBs grasp the scope and dynamic of the current cyber threat landscape — and ultimately make decisions that reduce the likelihood and severity of cyberattacks — **Devolutions surveyed decision-makers in SMBs worldwide**[1] on a variety of relevant topics, including privileged access management (PAM), password management practices, and cybersecurity trends.

Here are some of the most notable takeaways from the survey:

[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.

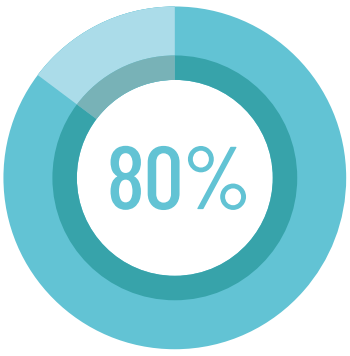
88%

of SMBs are more concerned about the privacy and security of their online data now than they were five years ago. *Click to Tweet*

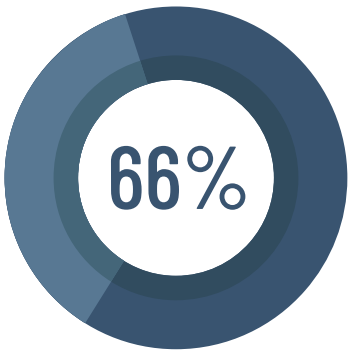
This anxiety is fully justified, given that SMBs have become "ground zero" for cyber crime. **For example:**

One out of every **323 emails** received by SMBs **is malicious.**

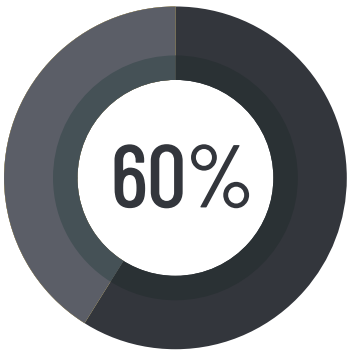
SMBs typically experience at least **eight hours** of system downtime during a cyberattack.



80% of SMBs acknowledge that **malware has evaded their anti-virus software.**



66% of SMBs have experienced **at least one cyberattack** within the **last 12 months.**



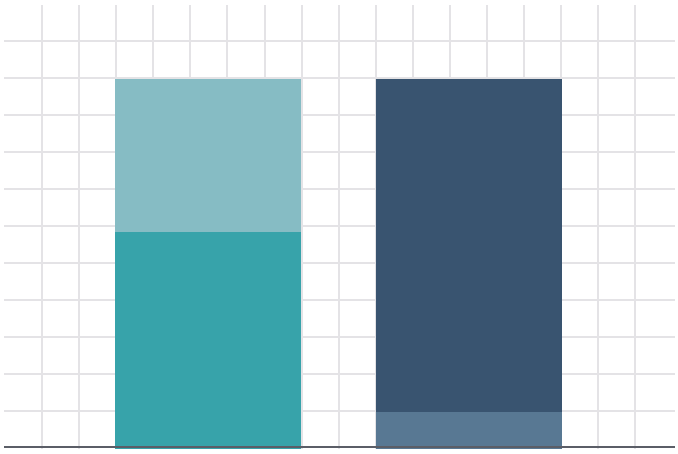
60% of SMBs **go out of business within six months** of a cyberattack.

While **78%** of SMBs consider a PAM solution to be at least somewhat important to their organization's cybersecurity program,

76% of SMBs do not have a fully deployed PAM solution in place. *Click to Tweet*

Hackers are aggressively **targeting high privilege accounts,** and **74% of data breaches** are **triggered by privileged credential abuse.** The account types that all SMBs should be actively monitoring and auditing include:

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



62% 14%

62% of SMBs do not conduct a security audit at least once a year, and 14% of SMBs never perform a conduct audit at all. *Click to Tweet*

Experts recommend **that SMBs conduct at least two routine security audits a year**, although more frequent auditing is encouraged. Security audits focus on **identifying patterns or abnormalities that may indicate vulnerabilities.** A special security audit should also take place **after any significant event**, such as:

- **Security breach**
- **System upgrade**
- **Changes to compliance laws**
- **Digital transformation**
- **Expansion** (or period of significant new employee onboarding)
- **Merger**

57%

of SMBs say they have experienced a phishing attack in the last three years.
Click to Tweet

Research has found that **56% of IT decision-makers** believe that **preventing phishing attacks is their organization's number one cybersecurity priority.** A whopping **90% of cybersecurity breaches include a phishing element, and 94% of malware is delivered by email.**

What's more, given that **hackers launch attacks** on average **every 39 seconds**, it's virtually certain that all SMBs have been attacked many times but are unaware of the extent or damage. Here is what Devolutions' CSO Martin Lemay says about this:

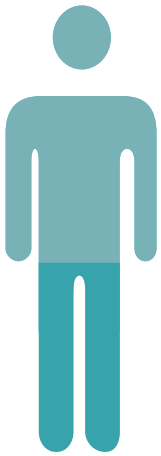
> *Here at Devolutions, within the last 30 days of preparing this Report, 21% of our inbound email traffic consisted of spam and other malicious content, our malware alarms were regularly triggered due to suspicious attachments that reached endpoints, and we detected active phishing campaigns using our domains in the From field.*
>
> *We are able to thwart these attacks because we have a robust Domain-based Message Authentication, Reporting and Conformance (DMARC) policy in place, which is supported by a comprehensive information security infrastructure that provides us with penetrating visibility to detect, respond to, and remediate threats. All SMBs should have the same protection in place because it is not a matter of whether they will get attacked, but how often and how severely.*

97% of SMBs believe that end users bear at least some of the responsibility in the event of a data breach.
Click to Tweet

This level of concern aligns with research that found the number one fear among IT pros is not external hackers, but rather incompetent or negligent end users. In fact, **79% of IT leaders believe that in the last 12 months their own employees have accidentally put company data at risk.**

Even more eye-opening is that **55% of employees who deliberately (but not maliciously) shared data against the rules did so because their company failed to provide them with the necessary tools. Furthermore, 29% of employees did not even feel like they had broken the rules**, because they mistakenly believed they — and not their employers — had ownership of the data they had worked on.

Research has found that **59% of end users rely on the same passwords for all accounts,** and for a very simple (and very human) reason: **they cannot easily remember multiple passwords.** Indeed, the average business **user must keep track of a whopping 191 passwords,** and they are **obligated to input their credentials for various websites and apps 154 times per month.** To close this security gap, SMBs should implement a password manager and force end users to select unique passwords for each account.



47% of SMBs allow end users to re-use passwords across personal and professional accounts.

29% of SMBs rely on human memory for storing passwords. *Click to Tweet*

What makes this practice particularly **dangerous is that it often leads to storing passwords in spreadsheets and other unprotected documents.** It also invariably **leads to password re-use,** which is an enormous risk factor. Even if a password is complex, it nevertheless potentially provides hackers with a key to breach endpoints and networks.

The Takeaway

In light of these glaring statistics and trends, two things are abundantly clear:

1. SMBs must not assume that their relative smaller size will protect them from cyberattacks. On the contrary, hackers, rogue employees, and other bad actors are increasingly targeting SMBs, because they typically have weaker — and in some cases, virtually non-existent — defense systems.

2. SMBs cannot afford to take a reactive "wait-and-see" stance because they may not survive a cyberattack. And even if they do, it could take several years to recover costs, reclaim customers, and repair reputation damage.

ABOUT THIS REPORT

In total, **182 respondents were presented with 24 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 six parts:

Part 1
How SMBs Protect Their Organization Against Hackers — And What They Expect the Cybersecurity Landscape to Look Like in the Future

Part 2
Password Practices and Policies in SMBs

Part 3
Knowledge and Use of Privileged Access Management in SMBs

Part 4
Actions that SMBs are Taking to Increase Cybersecurity Effectiveness

Part 5
Recommendations

Part 6
Profile of Respondents

Part 1

How SMBs Protect Their Organization Against Hackers — And What They Expect the Cybersecurity Landscape to Look Like in the Future

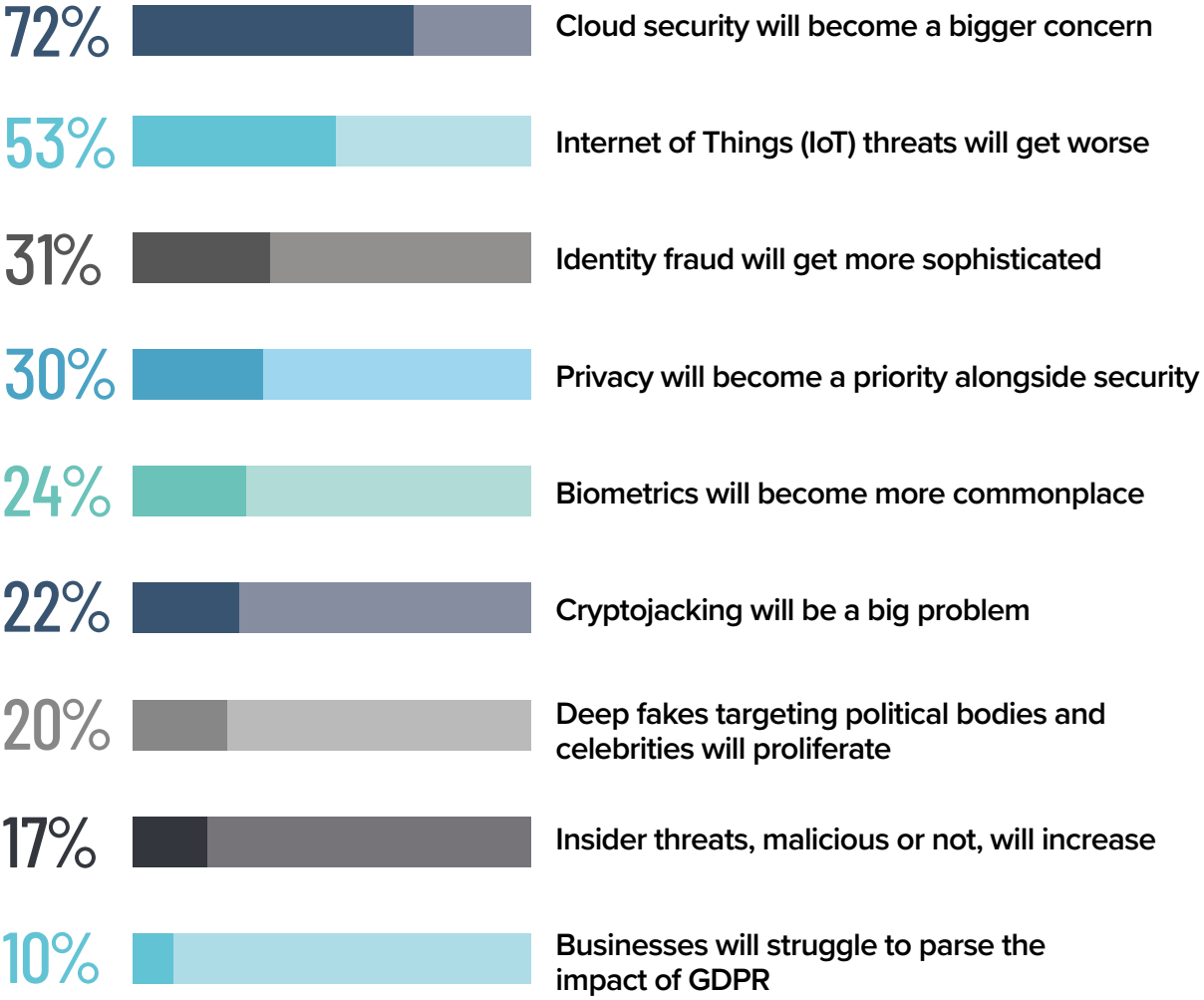
About this Part

In the past, when defending against hackers, it was generally acceptable for SMBs to rely on perimeter-based security tools, such as anti-virus software, secure web gateways, and firewalls. But these days, this approach is not enough. Cyber criminals have dramatically evolved their attack strategies and tools, and SMBs need to do the same — or else they may find themselves victimized by a costly and potentially catastrophic cyberattack.

In the first part of our survey, **we asked SMBs to share how they are responding to this elevated level of risk, and what they expect the cybersecurity landscape to look like in the years to come.**

QUESTION 1

Which top cybersecurity trends do you anticipate happening more in the next three years?
(Please select up to three)



COMMENTARY

It is interesting that 72% of SMBs believe that cloud security will become a bigger concern in the next three years. There are many significant advantages to moving data to the cloud, but for several years improving security was not among them. However, this is no longer the case. **Today, the cloud is considered just as safe — and in some cases safer — than legacy on-premises data centers.** For example, cloud service providers:

- Carefully monitor security at all times.
- Conduct ongoing penetration and vulnerability testing.
- Store data in multiple locations, which protects information from hardware failure and corruption.

This is a level of continuous scrutiny that most SMBs cannot provide. Indeed, recovery times are four times faster for SMBs that use cloud services compared to those that do not.

It is also notable that **53% of SMBs believe that IoT threats will get worse in the coming years.** Some of the major risks include:

- The proliferation of vulnerable access points (e.g. printers)
- Sabotage
- Botnets

With respect to the latter, a notorious attack in 2016 saw hackers seize control of 100,000 poorly secured IoT devices and launch a massive botnet attack that took down Internet service for millions of customers.

Somewhat surprisingly, **only 17% of SMBs think that the rise of insider threats — both malicious and those caused by human error — will be a major concern in the next three years.** What makes this perception so worrisome is that **72% of IT professionals believe their organization is vulnerable to insider threats.**

QUESTION 2

Are you more concerned about the privacy and security of your online data now than you were five years ago?

YES

88%

NO

12%

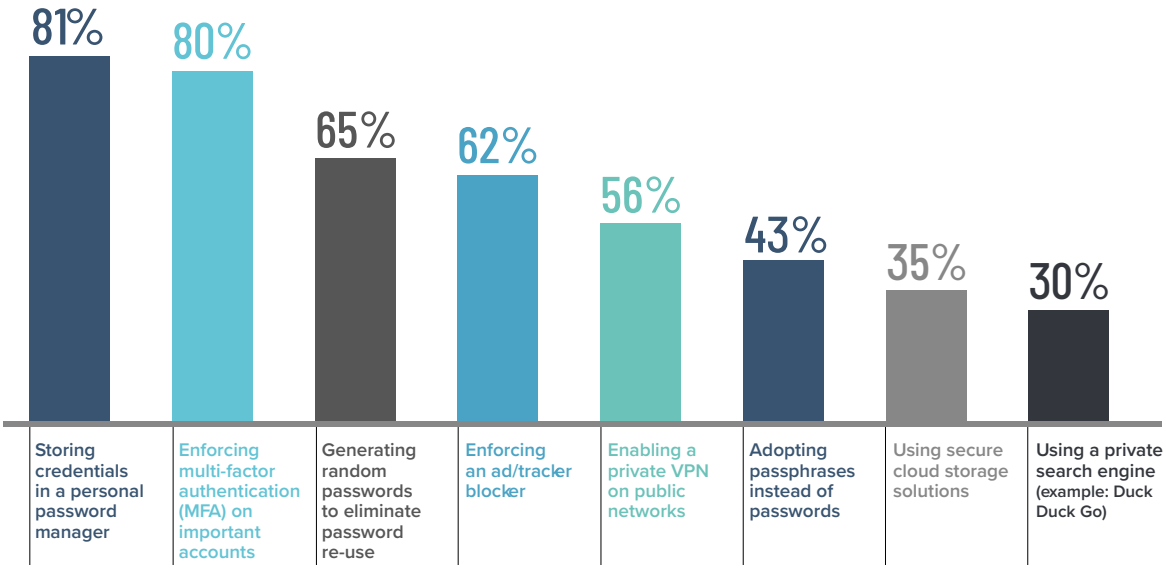
COMMENTARY

The surging popularity of social media across the business landscape is not entirely positive because it has led to a massive rise in cyber crime. Research has revealed that **22% of social media users have been hacked at least once, and 14% have been hacked multiple times.** Furthermore, the **data of more than 1.3 billion social media users has been compromised within the past five years,** and up to **40% of social media sites have some form of turn-key hacking tools or services available for purchase on the dark web.**

Overall, data security and transparency will continue to be huge concerns going forward, especially in the aftermath of recent data privacy scandals. The bad news is that we will see more online security scandals and incidents in the years ahead, not less. But the good news is that the data security field is expected to grow immensely.

QUESTION 3

Which precautions are you currently taking to protect your personal data?
(Please select all that apply)



COMMENTARY

The growing popularity of personal password managers is a positive trend, particularly because leaving password management to end users is unwise. **Research has found that end users typically choose weak passwords, re-use the same passwords, store passwords unsafely, and share passwords insecurely.**

It is also encouraging to see that more SMBs have adopted two-factor authentication (2FA), which is related to the concept of Zero Trust. While strong passwords or passphrases are important, **they are not enough.** Account security needs to be augmented by something physical that end users have access to, like a keychain token, USB token, smartcard, SMS, etc. Of course, 2FA is not a "bulletproof" security feature, but it is a step in the right direction, and a small price to pay for added protection and peace of mind.

Part 2

Password Practices and Policies in SMBs

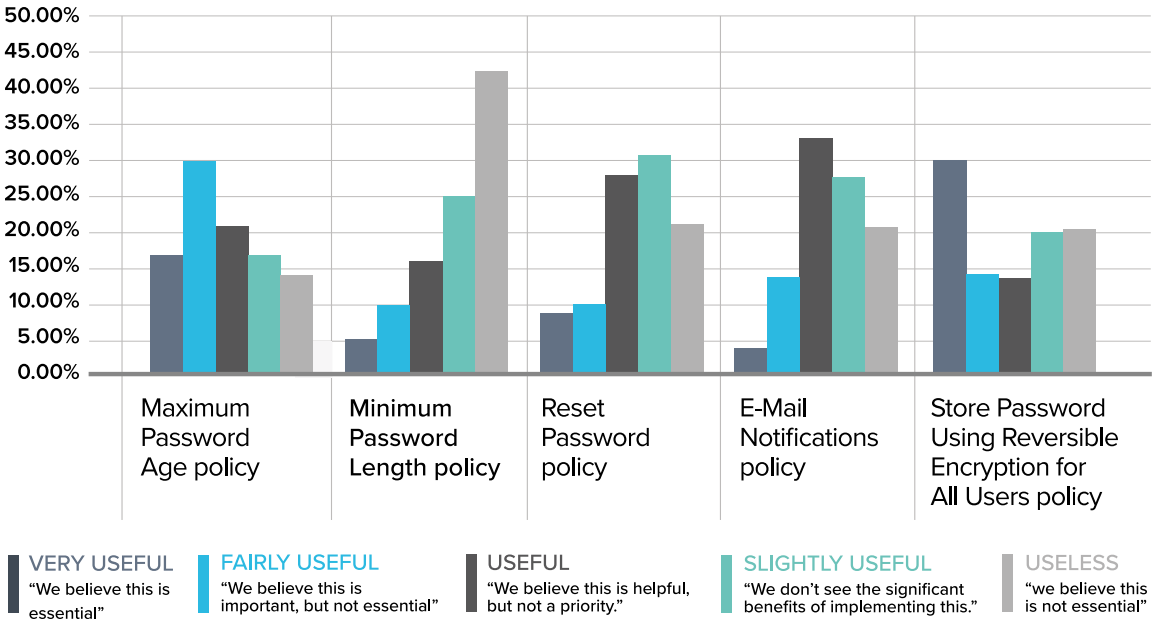
About this Part

On the information security landscape, passwords are viewed as “the keys to the kingdom.” Unfortunately, hackers are finding it surprisingly easy to steal these keys — especially from SMBs that overlook this critical threat vector — and launch attacks against endpoints and networks. Research has shown that **81% of data breaches are caused by compromised, weak, and re-used passwords, while 29% of all breaches (regardless of attack type) involve the use of stolen credentials.**

In the second part of our survey, we asked SMBs to identify the password practices and policies they are relying upon to keep their data and reputations safe.

QUESTION 4

Please rank each password policy factor on a scale from useful to useless

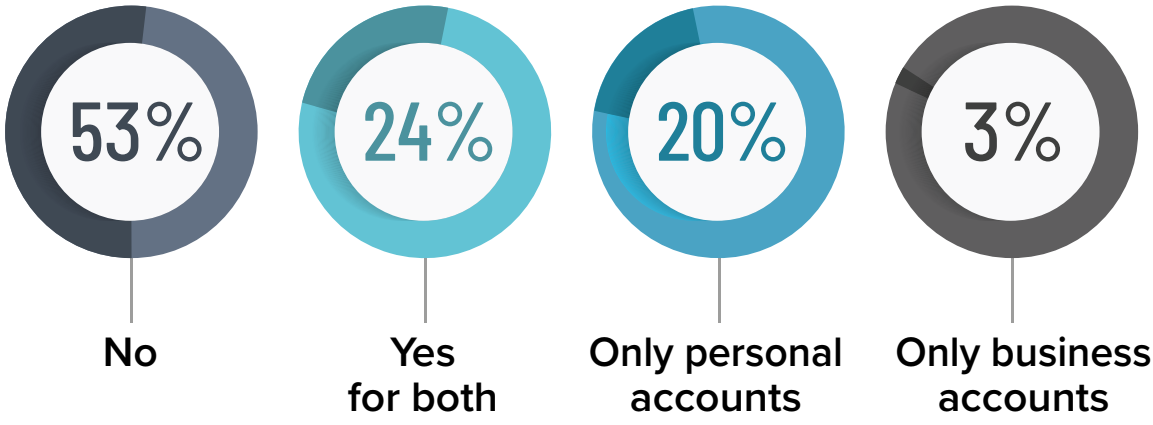


COMMENTARY

It is not a good sign that **70% of SMBs think that storing passwords using reversible encryption is at least slightly useful (and of those 21% believe it is very useful)**. This method has been **strongly criticized** in the information security community. Basically, storing passwords using reversible encryption is the same as storing clear-text versions. By default, this policy should never be implemented. The rare exception is when application requirements significantly outweigh the need to protect password information. It is also troubling to note that **only 43% of SMBs believe that enforcing a minimum password length policy is very useful.** Frankly, all SMBs should view this policy as essential and mandatory. That being said, many end users struggle to choose and/or remember long, complex passwords. To remedy this, a good password manager is advised.

QUESTION 5

Do you re-use passwords across any accounts (business and/or personal) ?

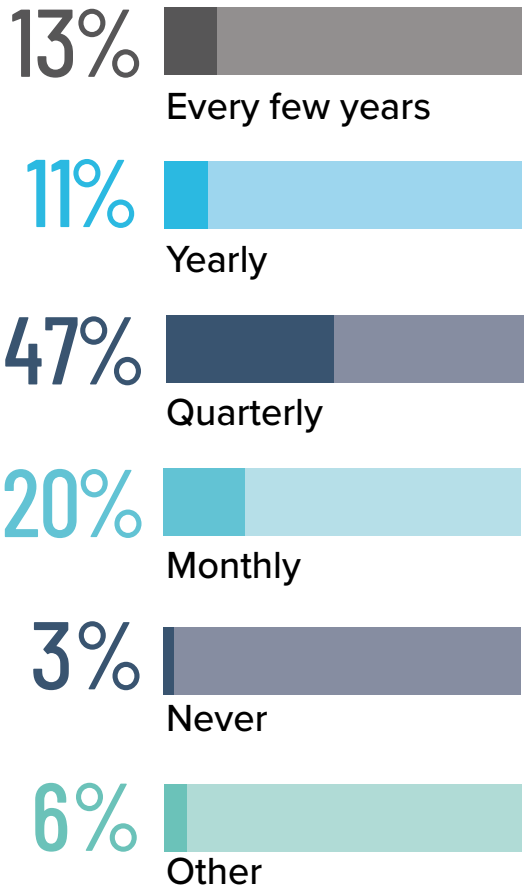


COMMENTARY

Research has found that **59% of end users rely on the same passwords for all accounts,** and for a very simple (and very human) reason: **they cannot easily remember multiple passwords.** Indeed, the average business user must keep track of a whopping 191 passwords, and is obligated to input their credentials for various websites and apps 154 times per month. To close this security gap, SMBs should implement a password manager and force end users to select unique passwords for each account.

QUESTION 6

How often do you change passwords for your business accounts?



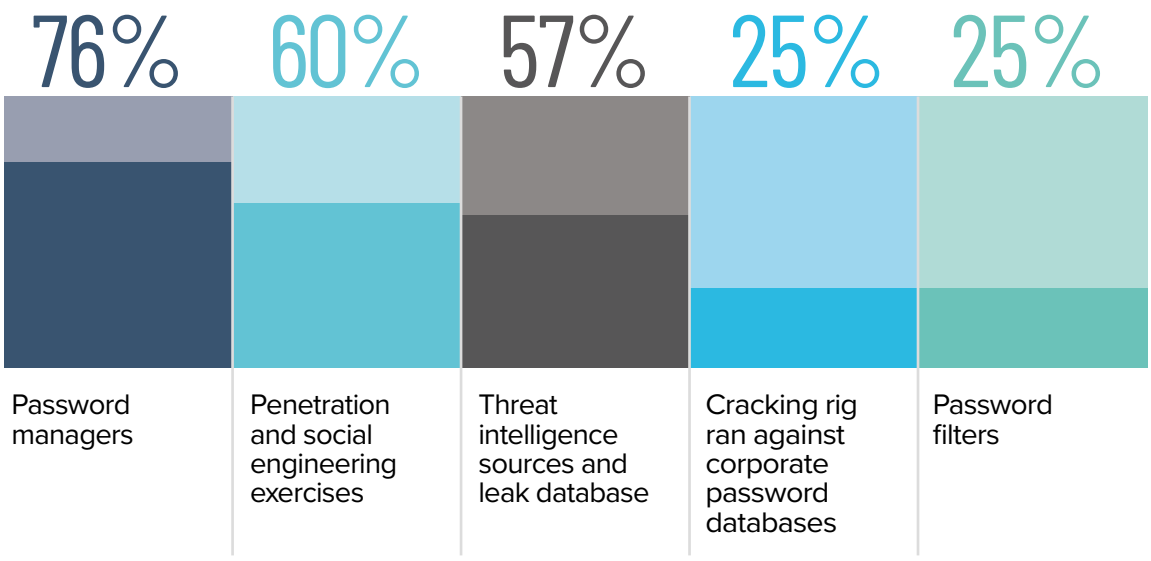
COMMENTARY

In the past, the National Institute of Standards and Technology (NIST) urged businesses to force end users to change their passwords on a regular basis (e.g. monthly, every three months, etc.). However, **NIST has now reversed its position and is advising password changes only when there is evidence of a compromise.**

The reason for this is both understandable and unfortunate: **when creating new passwords, end users typically choose weaker, easier-to-crack credentials.** The root cause of this problem — and the bane of existence for many IT professionals — is a condition dubbed "security fatigue." This sets in when end users are overwhelmed and exhausted by the need to remember multiple passwords, practices, and rules related to information security.

QUESTION 7

In your opinion, which technologies or control measures are best suited to validate and monitor good password practices? (Please select up to three)



COMMENTARY

The trend towards greater adoption of password managers is positive. However, it is important for SMBs to note that (so-called) free **password management tools typically impose several limitations**, including:

- No phone support, and long delays in responding to emails
- Difficult to configure and deploy
- Various restrictions, such as limited encrypted file storage size and no online backup

It is also encouraging to discover that **60% of SMBs are using penetration and social engineering exercises**, which can help detect data breaches launched by insiders.

Part 3

Knowledge and Use of Privileged Access Management in SMBs

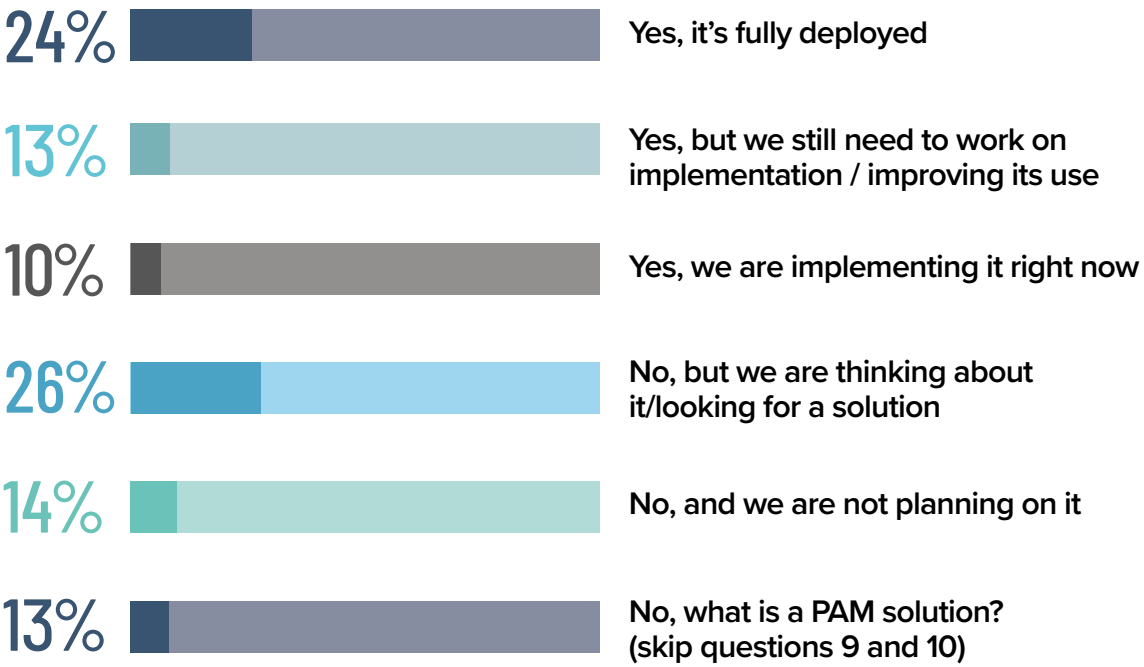
About this Part

Privileged Access Management (PAM) solutions enable SMBs to establish secure access to critical assets, as well as monitor, record, and audit high privileged accounts to ensure compliance. Yet despite this importance, **88% of organizations with more than one million folders lack appropriate access limitations, and 58% of organizations have more than 100,000 folders accessible to all employees.** In addition**, 55% of organizations do not know how many privileged accounts they have** or where they are located; more than **50% of organizations have privileged accounts that never expire or get deprovisioned; and 72% of organizations do not store all of their privileged accounts in a secure privileged access management vault or password manager.**

In the third part of our survey, we asked SMBs about the current state of their overall PAM knowledge and usage.

QUESTION 8

Does your organization have a PAM solution in place?



COMMENTARY

There are a few reasons some SMBs are slow, reluctant, or uninterested in adopting a PAM solution. These include the **high cost of some PAM solutions**, which are typically targeted to and priced for larger organizations; **a lack of internal expertise** to implement and manage a PAM solution; and **confusion regarding what to focus on when evaluating various products.** With respect to this latter obstacle, SMBs are advised to focus on six must-have features of a PAM solution : ease of deployment and management, secure password vault, logging and reporting, built-in two-factor authentication, account brokering and role-based access to credentials.

QUESTION 9

How much of a priority is PAM in your organization's cybersecurity program?

18% ESSENTIAL

20% VERY IMPORTANT

22% IMPORTANT

18% SOMEWHAT IMPORTANT

8% NOT IMPORTANT

14% DON'T KNOW

COMMENTARY

There are several enduring myths that are preventing some SMBs from making PAM a priority in their organization. **These include:**

MYTH
There is no need to worry about PAM if there is an advanced network in place.

TRUTH
A staggering 81% of hacking incidents involve stolen or weak passwords. Once cyber criminals get their hands on passwords — they particularly enjoy grabbing compromised Windows administrator and Unix root credentials — they steal data, commit identity theft, and damage reputations.

MYTH
A PAM solution is unnecessary if passwords are regularly rotated.

TRUTH
In theory, rotating passwords makes sense. However, instead of choosing strong passwords, end users typically head in the other direction and choose weaker passwords.

MYTH
An SMB that does not have a PAM solution and has not been hacked must therefore have enough security and protection in place.

TRUTH
SMBs without a comprehensive PAM solution in place should consider themselves lucky rather than prepared. Sooner or later, this luck will run out and the cost might be enormous — or possibly catastrophic.

MYTH
Implementing a PAM solution also means implementing the Principle of Least Privilege (POLP), Segregation of Duties (SoD), and Zero-Trust architecture — all of which are disruptive to end users and reduces efficiency and productivity.

TRUTH
Admittedly, implementing a PAM solution requires some adjustments to day-to-day workflows. However, it is well worth the effort given what is at stake. The key is to educate end users and hold them accountable so they play an active role in the security solution.

QUESTION 10

In your opinion, what are the most important drivers for PAM adoption?
(Please select up to three)

49%
Segregation of duties and least privilege principle

43%
Multi-factor authentication (MFA) requirements

46%
Audit and compliance

46%
Password management policy enforcement

42%
Secure storage and management of credentials

COMMENTARY

SMBs rely on privileged accounts to increase the efficiency and productivity of their employees. But they must keep in mind that **hackers also rely on vulnerable privileged accounts to breach networks, access critical systems, and steal confidential data**. Given this perfect storm — i.e. SMBs are increasingly relying on privileged accounts, while hackers are increasingly targeting them — it is not surprising that Gartner identified the **implementation of a PAM solution as one of its top** **10 security projects for 2019.**

In addition, PAM helps SMBs prevent insider threats, as well as detect and correct errors. Research has found that **15% of all threats** **are carried out by non-malicious insiders** (i.e. employees who make unintentional but nevertheless serious mistakes) and **13% are carried out by malicious insiders.**

Part 4

Actions that SMBs are Taking to Increase Cybersecurity Effectiveness

About this Part

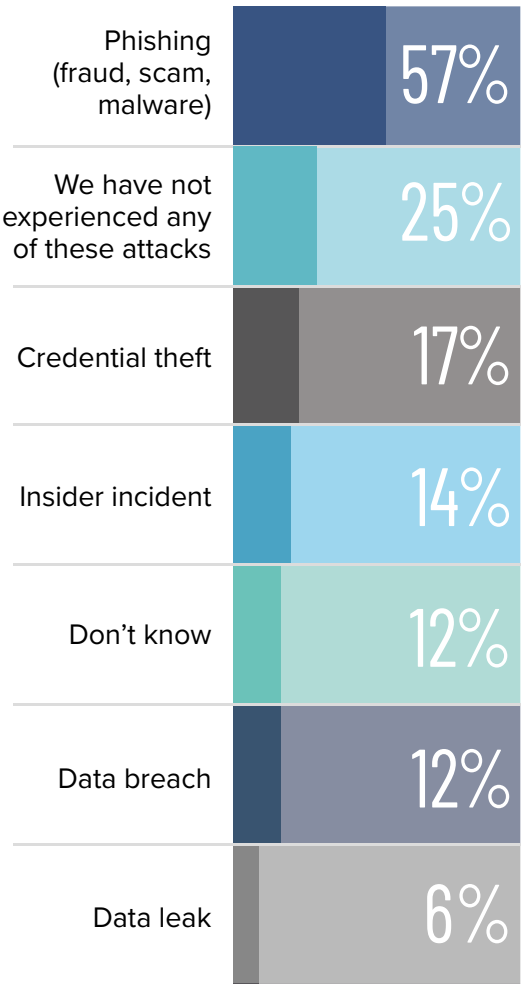
In the past, most hackers wanted to destroy machines and wreak havoc. While this obviously caused financial damage, that was not the main purpose of the attack. However, today's hackers are quite different than their predecessors. **They are financially motivated**, and they focus with laser-like precision on stealing data that they either use to commit identity theft or sell on the dark web.

In addition, there are many costs to a data breach, including: incident investigation, remediation, replacement, customer notification, crisis management, regulatory fines, penalties, and possibly lawsuits. The average cost of a data breach in an SMB is now **$117,000 per incident**. And that is the average — for many SMBs, the cost is significantly higher. And still, the story gets even worse.

The reputation damage caused by a data breach can be more devastating than the financial damage. Ironically, this is one of those situations where bigger is better. For example, while Target and Sony each took a massive reputation hit due to their respective data breaches, neither of them came close to disappearing from the business landscape. However, many SMBs cannot count on bouncing back. If their brand gets associated with a breach, it may be impossible to regain trust in the marketplace. Research has found that within six months of a cyber attack, **60% of small firms** are forced to go out of business. In the fourth part of our survey, we asked SMBs to highlight what actions they are taking to increase cybersecurity effectiveness, and to reduce the risk of being victimized by cyberattacks now and in the future.

QUESTION 11

Has your organization faced any of the following attacks in the last three years?
(Please select all that apply)



COMMENTARY

While phishing has been around for quite a while, it is not going away anytime soon. A whopping **90% of cybersecurity breaches include a phishing element, 94% of malware is delivered by email**, and **56% of IT decision-makers believe that preventing phishing attacks is their organization's number one cybersecurity priority.**

In addition, **14% of SMBs said they have been victimized by an insider threat within the last three years** — although this percentage is likely higher, since **12% of SMBs do not know if they have been attacked during this timeframe**. Research has also revealed that **72% of IT pros admit that their organization is vulnerable to insider threats.**

Their biggest fear is user error (40%), followed by malicious insiders (35%). Furthermore, **74% of IT pros cannot detect an insider threat before data exfiltration,** and **64% of IT pros cannot detect an insider threat in real-time.**

QUESTION 12

If you answered “Yes” to question 11, tell us more about the incident

Below are some of the responses from SMBs:

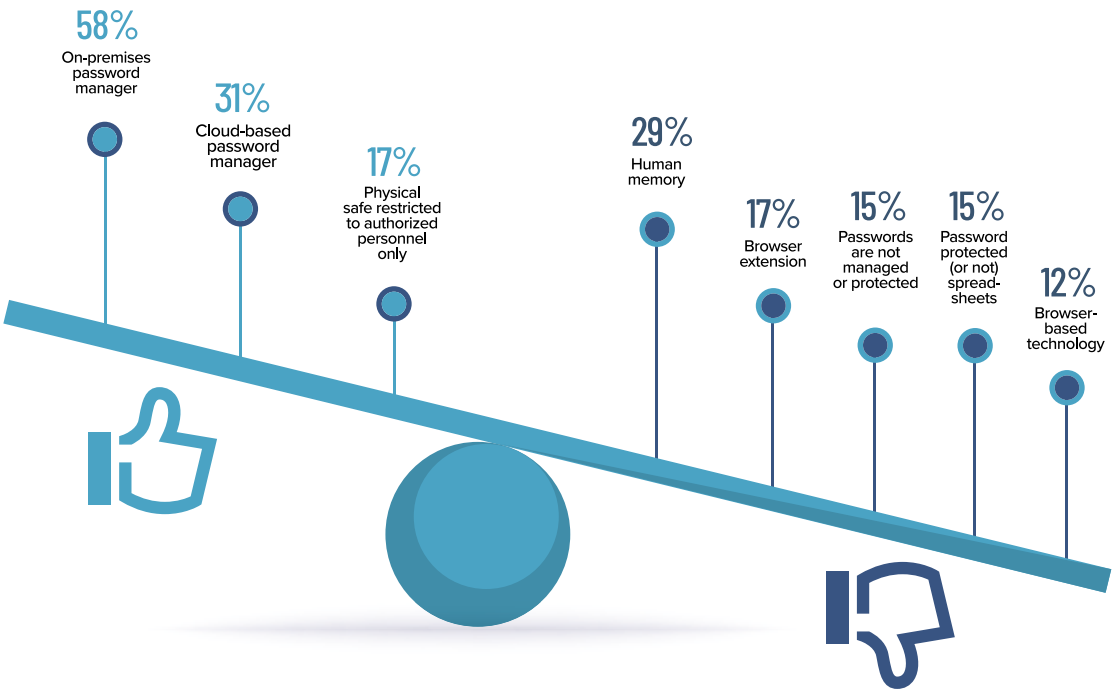
"Phishing tests still show a large number of users clicking the links. For example, a customer was tricked into sending an ACH payment by prodding them about payment. The emails were sent from an external email account with a misspelled domain name.”

"A hacker that got in through a vendor's network embedded themselves into an email conversation between the AP team and the vendor. The hacker then requested a change in banking information for payment. They even confirmed the change via a hacked email thread when the AP team asked for confirmation.”

"A user clicked on a suspicious email. This allowed a hacker to take control of our business email and blast out malicious emails. This caused us to be blacklisted on several email lists.”

QUESTION 13

What does your organization use to manage and protect passwords?
(Please select all that apply)



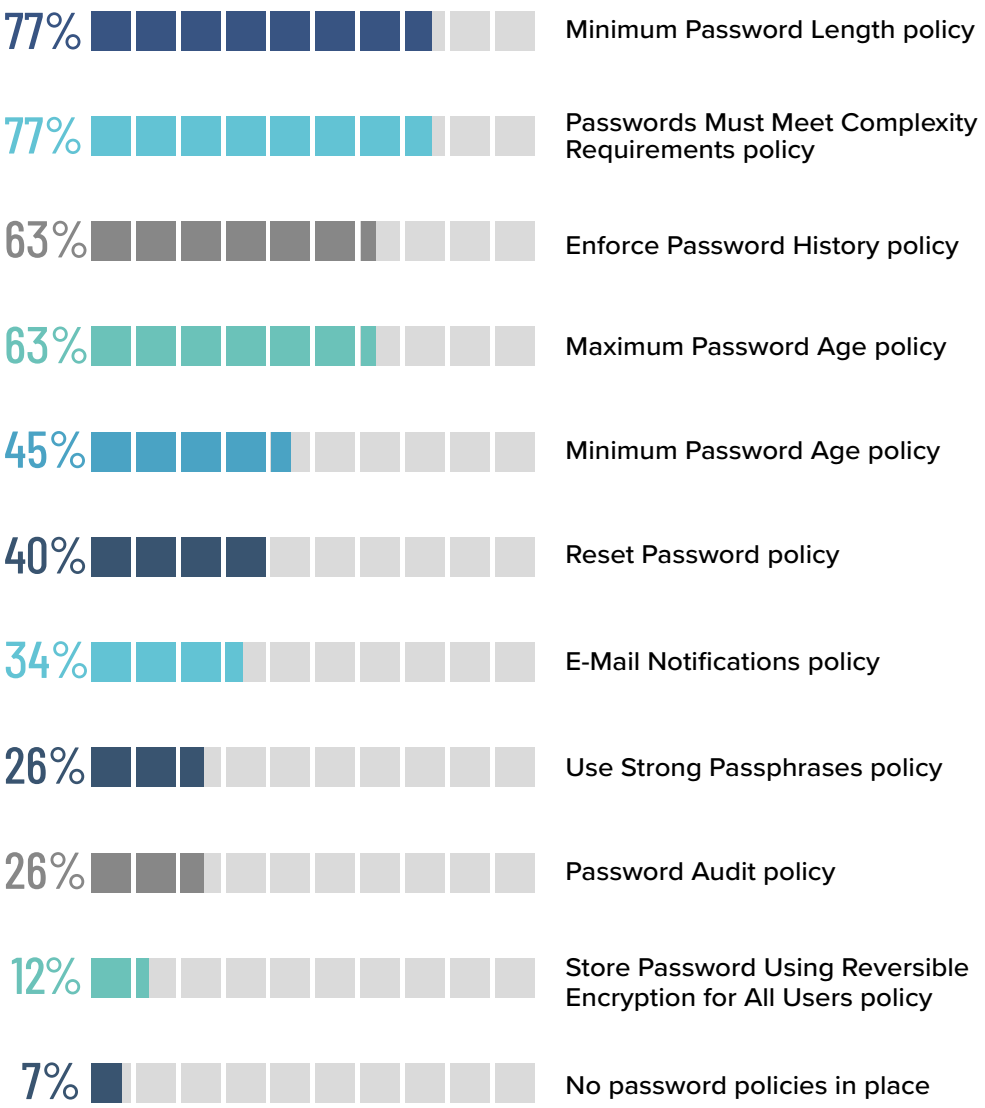
COMMENTARY

It is encouraging that the **majority of SMBs are using a password manager.** With a password manager, end users only need to remember two sets of login credentials instead of dozens (or one set if the password manager integrates with Single-Sign On/SSO). SMBs can even take things a step further and implement password-less authentication that relies on biometrics or hardware.

Less encouraging is the fact that password manager implementation is not comprehensive across SMBs, as **29% are relying on memory for some accounts**, and **15% are using spreadsheets for some accounts.** This approach almost invariably leads to password re-use, which is an enormous risk factor. Even if a password is complex, it potentially provides hackers with a master key.

QUESTION 14

Does your organization have documented and communicated password policies in place?
(Please select all that apply)



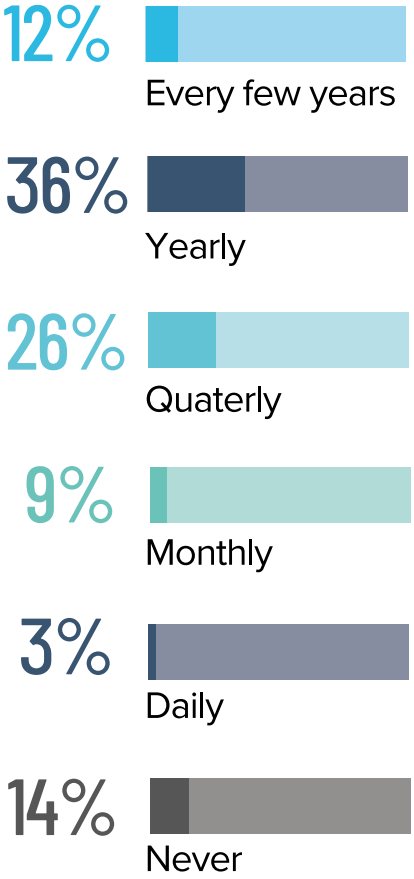
COMMENTARY

In the past, the minimum password length was generally held to be at least eight characters. However, the Center for Internet Security (CIS) recommends setting this value to **24 or more**. In addition, SMBs should enforce a minimum password age policy, in order to prevent end users from changing their password multiple times within a few minutes so they can re-use the preferred password they started with.

Considering that choosing a 24-character password is difficult, SMBs should consider adopting and enforcing **passphrases as a better alternative**. A passphrase is much longer than a typical password, and can contain letters, symbols, and numbers. It does not need to be a proper sentence or grammatically correct.

QUESTION 15

How often do you have a security audit in your organization?



COMMENTARY

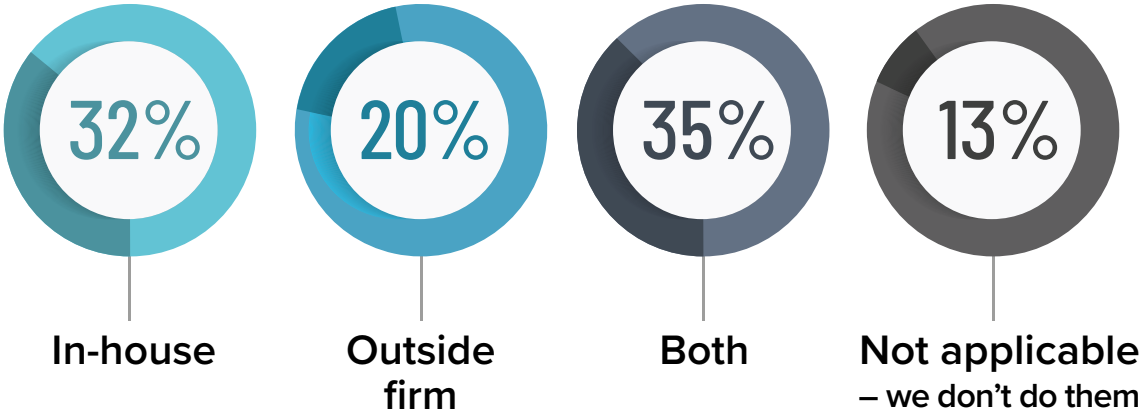
Although experts recommend conducting at least two routine security audits a year, the survey found that **62% of SMBs are falling below this standard** — including **14% of SMBs that never perform audits at all**. Generally, there are two reasons for this oversight.

The first is that SMBs believe they are too small to be targeted by hackers. The second is that SMBs believe that auditing (along with other essential information security procedures) is too expensive.

As discussed throughout this survey, **both of these perceptions are flawed**. SMBs are being targeted by hackers who count on facing vulnerable defense systems, and the cost of a data breach can — and typically does — far exceed the cost of maintaining good data security.

QUESTION 16

Are your security audits handled in-house or by an outside company?



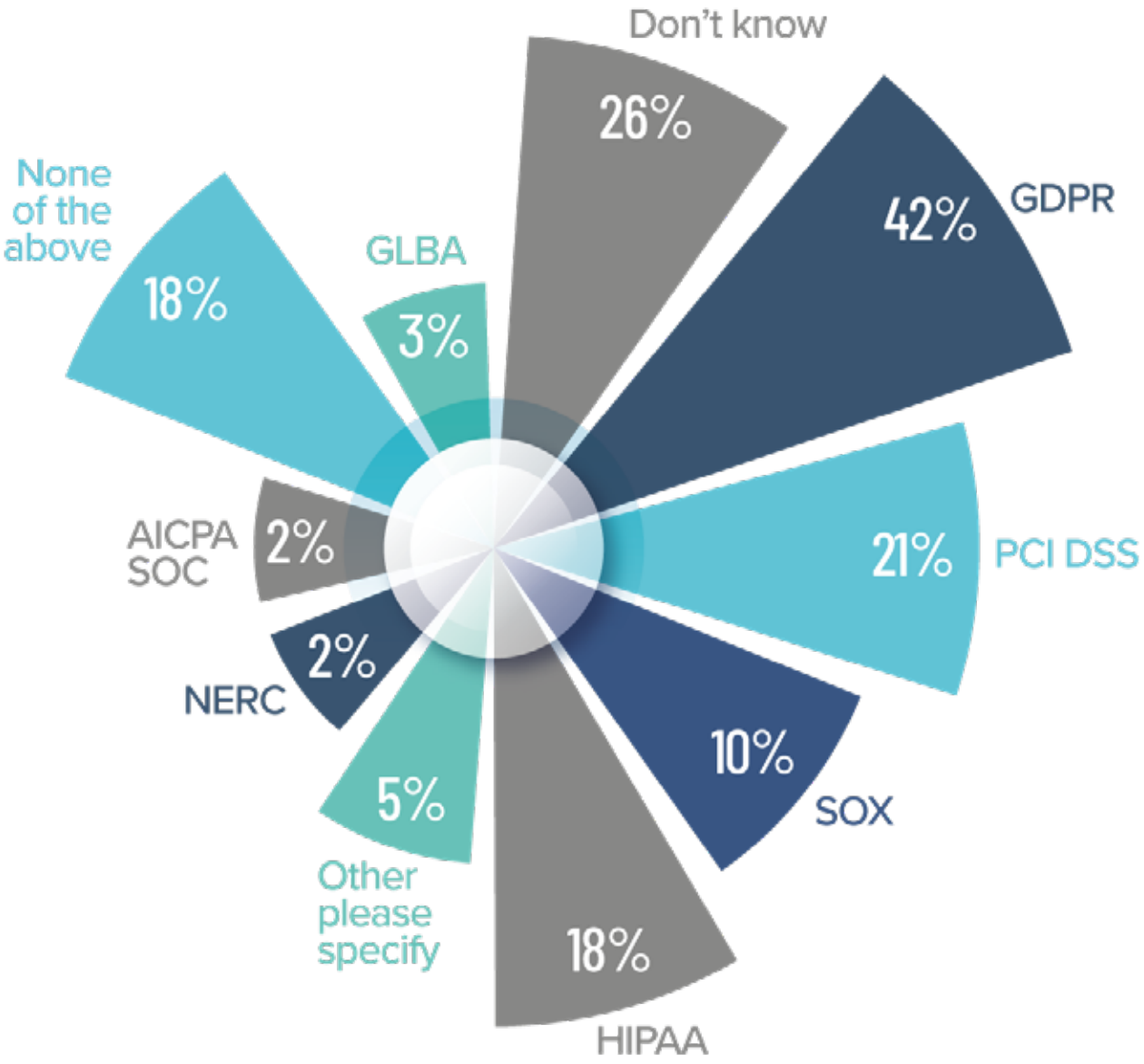
COMMENTARY

Ideally, SMBs would hire external auditors who have advanced skills and tools. In such cases, it is vital for internal IT and security teams to provide all relevant data, establish goals and expectations, and ultimately implement any recommendations that are accepted and endorsed.

However, many SMBs conduct in-house audits because they are typically more affordable, faster, and more convenient than relying on external firms or consultants. With this in mind, it is important to ensure that there is no conflict of interest, and that the auditor is not manipulating or withholding any data.

QUESTION 17

Please select all of the compliance regulations that your organization is required to adhere to:
(Please select all that apply)



COMMENTARY

The two most prevalent compliance programs among SMBs are **GDPR** and **PCI DSS**.

GDPR is a regulation that has been implemented across the entire EU and EEA region, and it applies to all organizations that collect, store, and use personal customer data about European citizens —regardless of whether or not the organization itself is located in Europe. GDPR also regulates the transfer of personal customer data outside the EU. GDPR governs a wide range of private customer data, such as:

- Basic information (e.g. name, address, ID number, etc.)
- Web data (e.g. IP address, RFID tags, cookies, etc.)
- Bank details
- Medical information
- Photos
- Updates on social networking sites
- Biometric data
- Racial and ethnic data
- Political opinions
- Sexual orientation

PCI DSS is an acronym for Payment Card Industry Data Security Standard. It is a set of worldwide protection standards developed by major payment card companies, and it is mandatory for businesses that store, process, or transmit payment card data. Guidance is also provided to software, app, and device creators that facilitate payment card transactions. It is intended to protect both consumers and businesses.

Overall, research has found that **72% of customers will boycott a company that appears to disregard the protection of their data, and 50% of customers said they would be more likely to shop at a company that takes data protection seriously.**

SMBs that pursue and achieve compliance establish a common understanding among managers and employees that information security is a strong value that must guide all processes and decisions. This represents a major shift in business culture.

QUESTION 18

Do you educate your end users about cybersecurity?

YES

88%

NO

12%

COMMENTARY

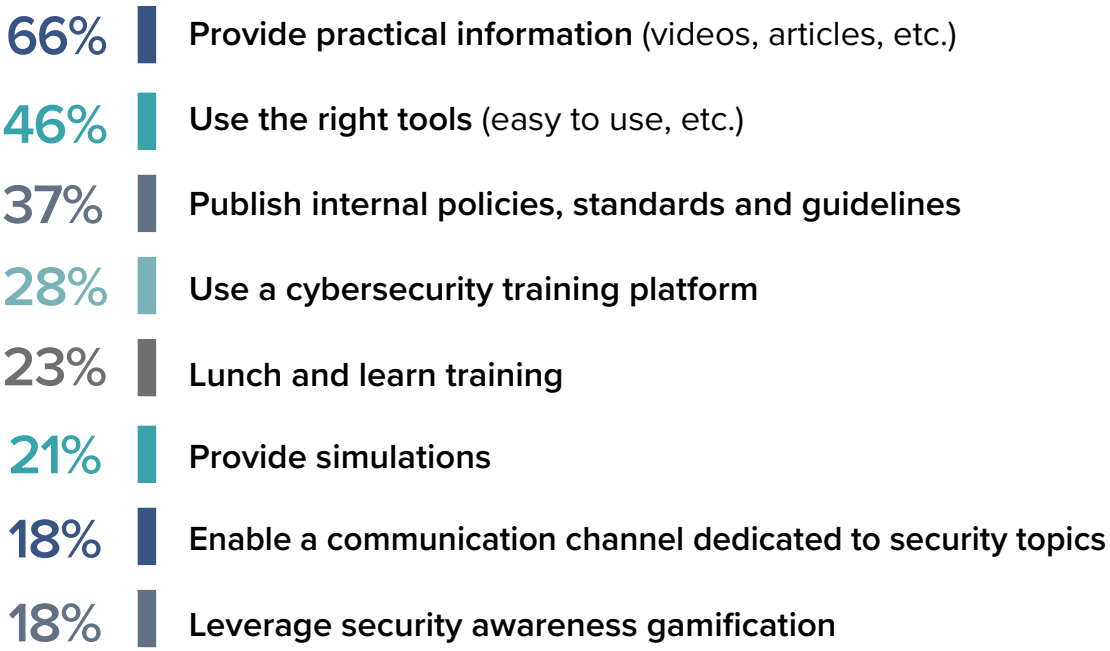
The fact that **88% of SMBs are providing some form of cybersecurity education to their end users is certainly a positive sign.** However, given the risks and potential consequences, the **proportion should be 100%.** In other words, cybersecurity education should be essential rather than optional.

While each SMB needs to develop its own cybersecurity training plan based on specific risk factors and compliance requirements, the approach should generally include the following **mix of non-technical and technical controls:**

- Provide company-wide cybersecurity education with online training platforms
- Identify and analyze all privileged accounts
- Audit and analyze off-boarding practices
- Simplify the message
- Implement Segregation of Duties
- Implement the Principle of Least Privilege

QUESTION 19

What is the best way to teach end users about cybersecurity?
(Please select up to three)

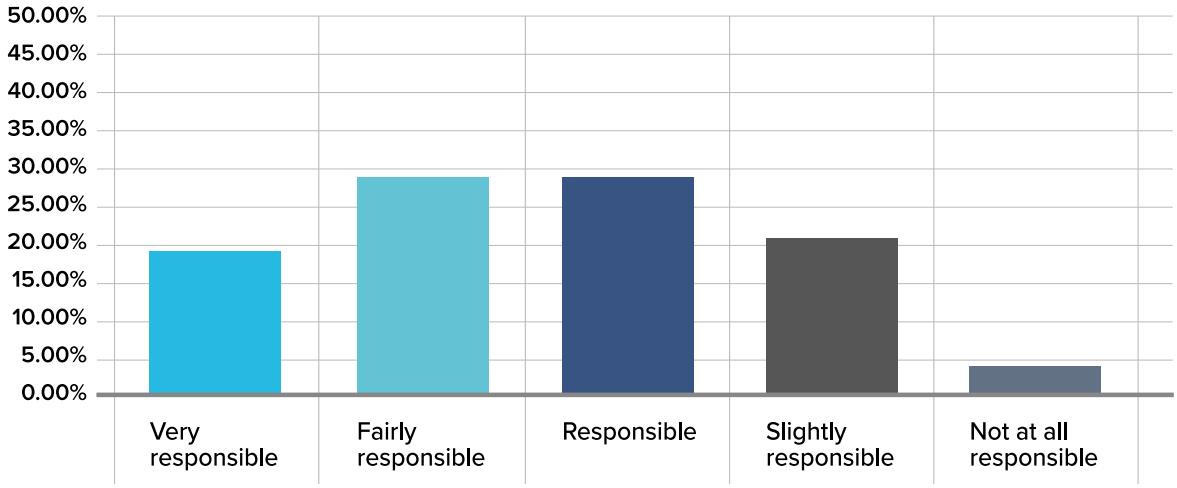


COMMENTARY

As noted earlier in this report, **43% of cyberattacks target SMBs and 60% of SMBs go out of business within six months of a cyberattack.** As such, SMBs should seriously consider investing in an online cybersecurity training platform so that their employees can effectively serve as the last line of defense instead of unwittingly opening the door for hackers. Naturally, there is a fee involved (typically an annual subscription based on the number of employees). However, considering the massive potential costs and consequences of a breach — including lasting reputation damage — it is a prudent investment that can pay dividends for many years to come.

QUESTION 20

How responsible do you think end users are in case of a data breach?



VERY RESPONSIBLE
"End users are primarily responsible for causing data breaches."

FAIRLY RESPONSIBLE
"End users have some responsibility for causing data breaches."

RESPONSIBLE
"End users are significantly responsible for causing data breaches."

SLIGHTLY RESPONSIBLE
"End users have a limited responsibility for causing data breaches."

NOT RESPONSIBLE AT ALL
"End users are blameless for causing data breaches."

COMMENTARY

Virtually all SMBs (97%) believe that end users bear some responsibility in the event of a data breach. However, the degree of culpability varies, with **half saying that end users are fairly or slightly responsible, and nearly half (48%) saying that end users are responsible or very responsible.**

Part 5

RECOMMENDATIONS

When it comes to cybersecurity awareness and protection, SMBs are, overall, trending in the right direction. However, there are still a few worrisome — and in some cases alarming — vulnerabilities that, if exploited by hackers, can lead to costly and potentially catastrophic consequences. In addition, there are the ever-present threats posed by well-meaning but nevertheless negligent end users who accidentally trigger data leaks.

We strongly advise all SMBs to proactively analyze and audit their current cybersecurity profile, and if necessary, **carry out the following core recommendations,** which are further described in the following pages:

1. Implement a Privileged Access Management Solution
2. Enforce Strong Password Management Policies
3. Implement the Principle of Least Privilege
4. Implement Segregation of Duties
5. Provide End Users with Cybersecurity Training

RECOMMENDATION

1 IMPLEMENT A PRIVILEGED ACCESS MANAGEMENT (PAM) SOLUTION

Several years ago, it was fine for SMBs to rely on anti-virus software, secure web gateways, firewalls, and other perimeter-based cybersecurity tools. But these days, it is clearly not enough. External hackers and internal rogue users have upped their game, and SMBs need to do the same by implementing a PAM solution that delivers **seven must-have characteristics and features:**

1- EASE OF DEPLOYMENT AND MANAGEMENT

To avoid costly and complex installation and management problems — and in some cases, nightmares — **SMBs should focus on a PAM solution that:**

- Supports simple wizard-driven deployment.
- Provides an intuitive management console.
- Does not require changes to an existing Active Directory (AD) infrastructure.
- Integrates with Azure AD (if using Office 365).

Furthermore, SMBs should have the option of deploying components across multiple servers to improve performance. And to ensure business continuity, backup and restore functions should be comprehensive, yet straightforward and simple to configure and operate.

2- SECURE PASSWORD VAULT

A staggering **81% of hacking-related breaches** **leverage either stolen or weak passwords.** A centralized secure password vault gives SMBs the confidence that passwords are locked down yet can be retrieved as required by authorized end users to drive productivity and efficiency. It also enables end users to securely share passwords vs. transmitting them through email, spreadsheets, documents, post-it notes, and other staggeringly insecure — and in most cases non-compliant — methods.

3- LOGGING AND REPORTING

Just like large enterprises, SMBs need comprehensive logging and reporting functions to see who, when, how, and why privileged accounts are used across the organization. However, logs and reports are only useful if they deliver accurate on-demand information for all password-related activity, including login attempts and history. With this in mind, **SMBs should focus on a PAM solution that:**

- Offers out-of-the-box reports.
- Provides advanced search capabilities.
- Enables customized reports.
- Supports data export in various formats.

4- TWO-FACTOR AUTHENTICATION

SMBs should focus on a PAM solution that offers built-in support for **two-factor authentication (2FA)** and is compatible with a variety of authentication options. 2FA is an extra layer of security that requires end users to enter their login credentials, plus another piece of information. **This extra information can be:**

- Something they know, such as the answer to a secret question or a PIN.
- Something they physically have, such as a smartphone or a token.
- Some physical identifying marker, such as their fingerprint or voice recognition.

5- ACCOUNT BROKERING

Account brokering enables end users to access privileged accounts without needing (and therefore seeing) login credentials. Not only does this **strengthen security, it eliminates the need for constant password rotation** (i.e. automatically generating a new password each time a credential is checked out). At the same time, account brokering blocks end users from accessing resources outside of a defined workflow, which reduces the possibility of credential abuse.

6- ROLE-BASED ACCESS CONTROL

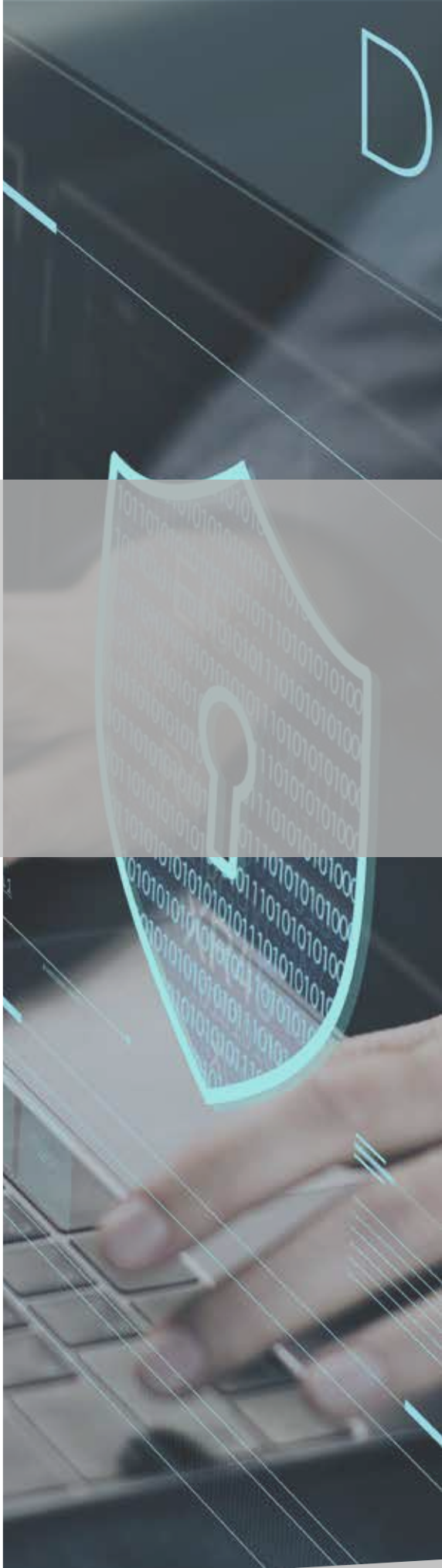
PAM solutions with built-in role-based access control (RBAC) enable SMBs to define various roles and associated access levels, which are then assigned to different types of end users (e.g. IT staff, admin staff, etc.). As a result, end users **can only access the privileged accounts that are associated with their role — no more and no less**. SMBs should also choose a PAM solution that integrates with AD, so they can use existing end users and groups.

7- AFFORDABILITY

Last but certainly not least, SMBs must ensure that a **PAM solution is affordable**. The good news is that various products are now available in the marketplace that fit SMB budgets. This was not the case for many years, when only large organizations and enterprises could purchase excessively expensive licenses and subscriptions.

RECOMMENDATION

2 ENFORCE STRONG PASSWORD MANAGEMENT POLICIES



SMBs are urged to adopt and enforce the following password management policies, which are based on advice from various reputable sources, such as NIST and the Center for Internet Security:

1- USE 2FA

Even the most diligent and careful end user can make a costly password-related mistake. For example, if a user is 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 keystroke logger (keylogger). In most cases, 2FA will stop hackers from accessing accounts, even if they have the correct login credentials.

2- USE A PASSWORD MANAGER

With a password manager, end users only need to remember two sets of login credentials instead of dozens, allowing them to become virtually password-less. The first set of credentials is for their own system, and the second is to access the password manager. The password manager can also make sure end users choose very strong passwords or passphrases (see best practice #3) that are **at least 16 characters in length.**

In addition, if the password manager supports Microsoft's Single-Sign On (SSO), then end 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 password-less authentication with solutions like Microsoft Hello (which uses biometrics) or Yubikey (which uses hardware).

3- USE PASSPHRASES

When end users are obligated to remember passwords (i.e. when implementing password-less authentication is not feasible), **length needs to be favored over complexity.** This is because many end users rely on patterns and tricks to help them remember passwords — such as "Password123!" — or they use the practice of "Leetspeak" — the act of changing letters for similar characters, such as "p@55w0rd" instead of "password". These techniques are widely known and regularly exploited by hackers.

Unfortunately, the vast majority of end users cannot remember a 16+ character password without resorting to these patterns and tricks, which is why a passphrase makes sense. A passphrase is much longer than a typical password (which makes it less vulnerable to a brute force attack), and it contains letters, symbols, spaces, and numbers. For example: "My Big Brown Dog, Paul, Loves When I Play Frisbee With Him." For even greater security, users can mix languages.

4- CHANGE PASSWORDS AFTER EVIDENCE OF A COMPROMISE

In the past, SMBs (along with all other organizations) were advised to have end users regularly change passwords. These days, however, the guidance from NIST is very different: **end users are better off not regularly changing passwords**, because research has shown that they typically choose weaker, easier-to-crack credentials. Instead, users should only change passwords when there is evidence of a compromise.

To check for evidence, SMBs can use services like the Have I Been Pwned? domain search, which finds all email addresses on 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.

5- 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 that are related to an end user's personal or work environment, such as the company name and the username. This is 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 streamline and standardize this process, SMBs should deploy a password manager or remote connection tool that has built-in password checking functionality. For their personal accounts, end users should be encouraged to use a tool like Have I Been Pwned? to see how many times a potential password has been breached.

6- ENFORCE JUST-IN-TIME ACCESS FOR PRIVILEGED ACCOUNTS

Hashes are often stored on a system when end users or administrators connect on a machine. This can lead to a pass-the-hash attack, in which hackers steal hashed credentials and re-use 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 doesn't 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 PAM solution**, which allows administrators to approve or reject access requests. Administrators should also have the option to enforce a mandatory password change after a credential has been used and/or at a scheduled time/date.

7- ENFORCE A PASSWORD HISTORY POLICY

SMBs should enforce a password history policy to ensure that end users do not select old passwords. **Experts recommend** **setting this value to at least 24** (i.e. users cannot choose a password that has been selected among the last 24). In addition, the policy should enforce a minimum password age. Otherwise, end users could change their password multiple times within a few minutes, in order to re-use the preferred password they started with.

8- ELIMINATE PASSWORD RE-USE

A surprisingly common practice is for end users — and even some administrators — to re-use passwords across multiple accounts. While this is convenient, it is also **risky and ill-advised**. However, there are scenarios where password re-use is not intentional. For example, a generic OS image that is used to quickly set up systems contains the same default local administrative account (aka backdoor accounts for administrators). Unfortunately, this means that compromising one machine unlocks all of them. A practical solution to this problem is to implement Local Administrator Password Server (LAPS) for Windows domains, or to 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-scale attacks.

RECOMMENDATION

3 IMPLEMENT THE 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. **There are a number of POLP best practices that SMBs are strongly encouraged to adopt:**

EVALUATE ACCESS LEVELS

In consultation with end users (aka business owners), **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 end users, so they understand that the approach is not intended to stifle their productivity, but rather to protect the organization. Reminding unhappy end users that the majority of SMBs fold within six months of a cyberattack can go a long way to opening minds and changing attitudes.

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 end 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. This is explored further in the next recommendation on implementing Segregation of Duties (SoD).

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.

RECOMMENDATION

4 IMPLEMENT SEGREGATION OF DUTIES (SOD)

The same factors that make SMBs especially vulnerable to external hackers also make them susceptible to attacks from disgruntled or greedy employees/ex-employees, vendors, contractors, and other rogue insiders. And of course sometimes data breaches are the result of negligence, incompetence, or human error. That is where Segregation of Duties (sometimes referred to as Separation of Duties) 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. **However, in recent years the concept has expanded into the cybersecurity space, in order to:**

• Prevent conflicts of interest (real or apparent), wrongful acts, fraud, abuse, and the building of secretive “silos” around activities.

• Detect control failures, such as security breaches, information theft, and circumvention of security controls.

• Prevent errors from taking place due to employees wearing “too many hats.” SMBs are urged to adopt the following SoD best practices:

ANALYZE ACCESS LEVELS

SMBs should ensure that no single individual has unchecked and unmonitored systems access. The exception to this rule in many SMBs will be administrators, who legitimately require access to all applications, databases, etc.

ALIGN TASKS WITH ROLES

SMBs should set up databases to align with task and role segregation, which should be based on the Principle of Least Privilege (as discussed previously).

AUDIT REGULARLY

SMBs should perform ongoing information security audits and pay particular attention to potentially fraudulent activities. SMBs that lack in-house expertise in this area are advised to work with an external firm or consultant, since malicious activity is almost always covert and difficult to detect. In addition, **SMBs should communicate to all end users that audits and checks are being done on a regular basis**, as this helps serve as a deterrent (i.e. would-be rogue users who know that their activities are being monitored are less likely to break the rules).

IMPLEMENT SUITABLE TECHNOLOGY

With respect to technology tools, key features that SMBs should focus on include **role-based access control, support for 2FA, and enhanced PAM functionality.**

INTEGRATE WITH HR POLICIES

SMBs should implement human resource management policies that support a comprehensive SoD program. **These include**:

• Conducting pre-employee screening and continuing ongoing screening past the point-of-hire. The very existence of this policy will discourage employees from carrying out their illicit aims, or even working for the SMB in the first place.

• Training supervisors and managers to recognize, document, and (as required) escalate any change in their subordinates' behaviors and habits, such as an inexplicable rise in secrecy or nervousness when asked normal questions.

• Forcing (if possible) employees to take at least one two-week vacation a year. The irony is that, in rare cases, an employee who seems very hardworking and rarely takes time off may not be motivated by dedication, but instead is terrified of having their illegal acts exposed. Commented Jonathan Middup, a partner at Ernst & Young's Fraud Investigation and Dispute Services Practice: "The profile of a typical fraudster is a long-serving, trusted employee, who works long hours and is reluctant to take their annual leave."

TRAIN END USERS

SMBs should provide end users with cybersecurity training, ideally through an online platform. In addition to avoiding common mistakes and reducing errors, training fosters a culture of cybersecurity awareness and vigilance — which is a deterrent. Cybersecurity training is explored further in the next recommendation.

RECOMMENDATION

5 PROVIDE END USERS WITH CYBERSECURITY TRAINING

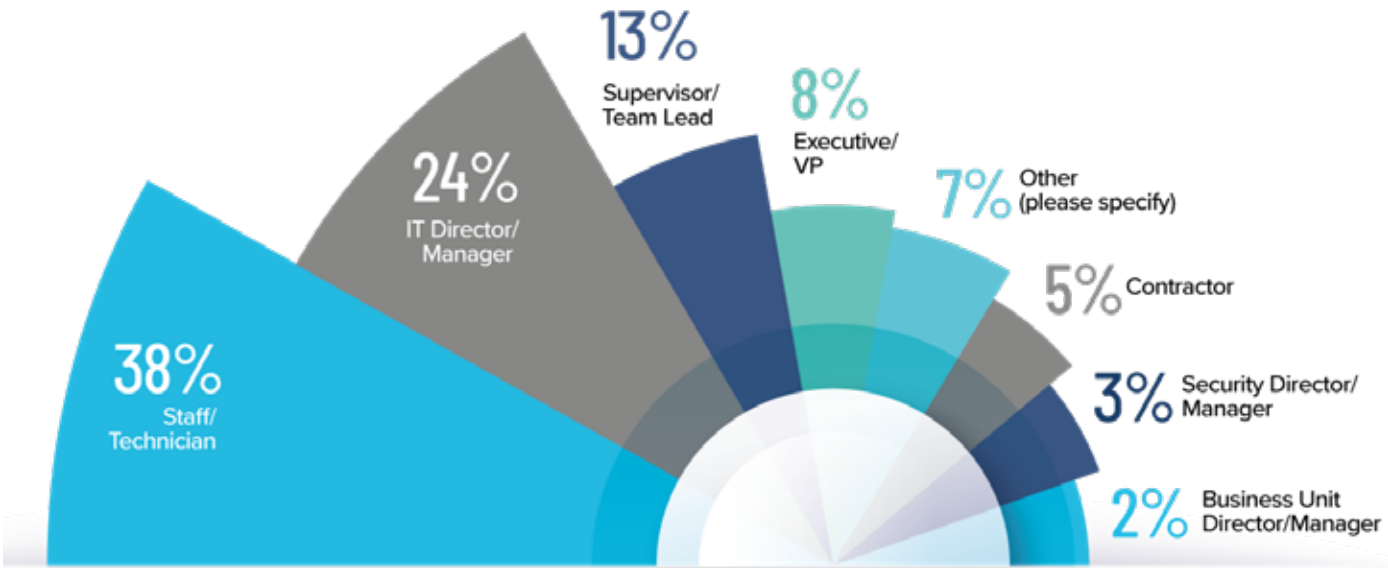
While there are several ways to deliver cybersecurity training, among the most effective and accessible for SMBs is by **enrolling their team in an online cybersecurity platform**. This is a portal that provides end users with self-paced, hands-on, skills-based threat detection and mitigation training in a live and dynamic simulated environment. These threats can include ransomware, phishing, DDoS, and so on, and the training program can be customized to cover specific topics, such as social engineering, email security, mobile device security, safe web browsing, safe social networking, protection of health information, etc.

End users get immediate feedback on their decision-making and move forward through the training based on their performance. Managers can also log into a dashboard and monitor each employee's progress, and then identify an individual's strengths and weaknesses. For example, an employee may be competent in safe web browsing but need additional training in mobile device security.

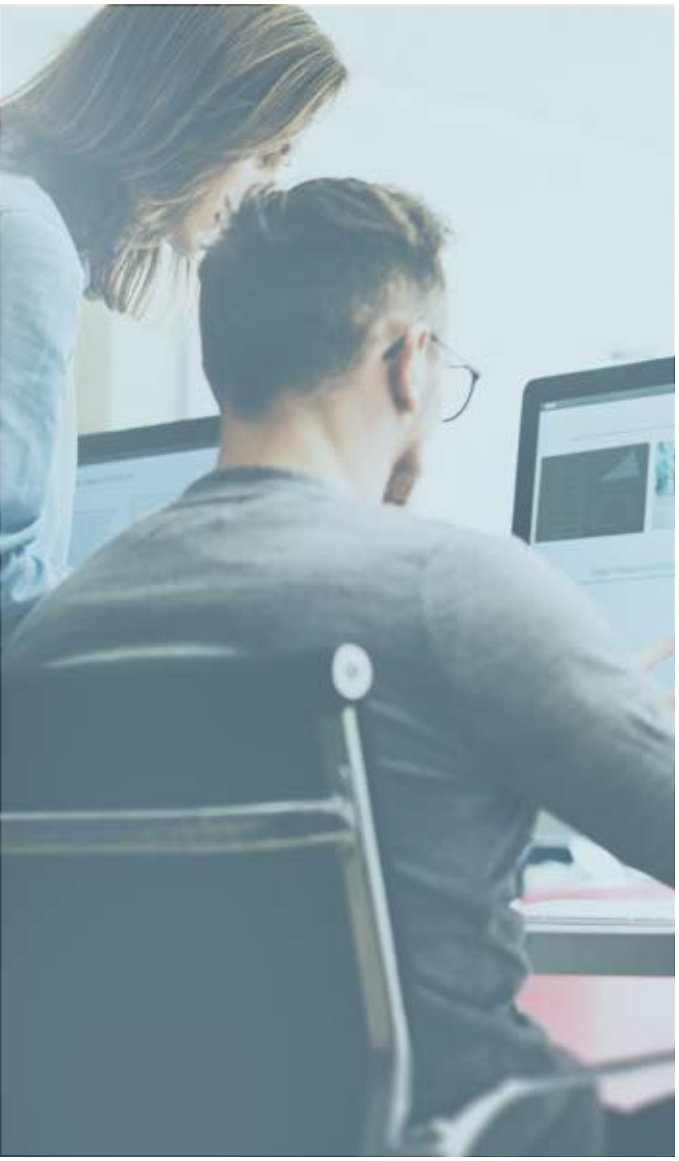
Part 6

Profile of Respondents

Which title best describes your position within the organization?

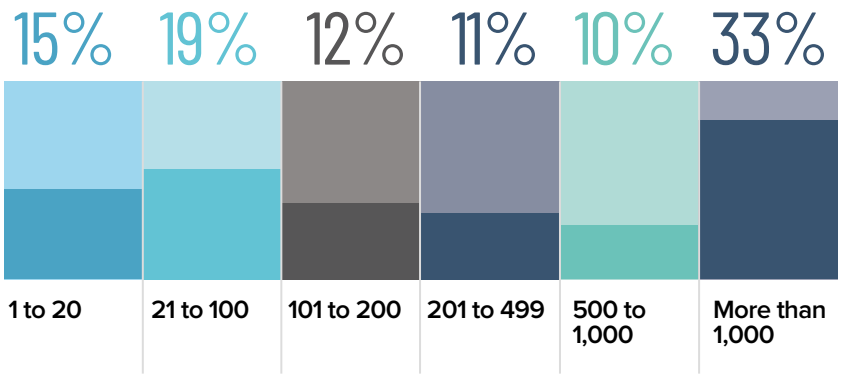


What best describes your organization's sector?

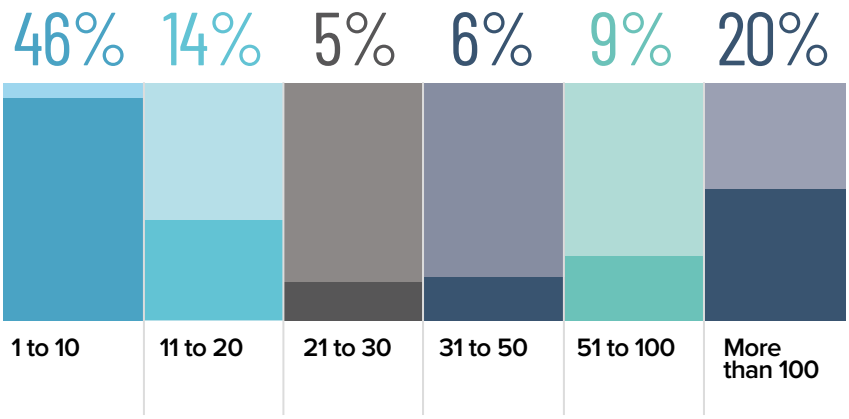


27%	IT services
9%	Health
8%	Education
8%	Technology
8%	Finance and insurance
8%	Manufacturing
4%	Retail
3%	Non-profit
3%	Consumer service
3%	Government
3%	Computer and network security
3%	General services business
2%	Communications
2%	Entertainment
2%	Transportation
2%	Others
1%	Pharmaceuticals
1%	Real estate
1%	Utilities
0.5%	Apparel
0.5%	Law and practice
0.5%	Oil and energy
0.5%	Security, defense technology and infrastructure

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



How many of your employees work in the IT department?



Devolutions :

Helping SMBs Stay Safe and Succeed

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

At Devolutions, we believe that neglecting SMBs and treating them like "second class citizens" on the business landscape 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 in today's business landscape, all companies — not just large organizations and enterprises — need to control 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 (DPS) 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. DPS 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

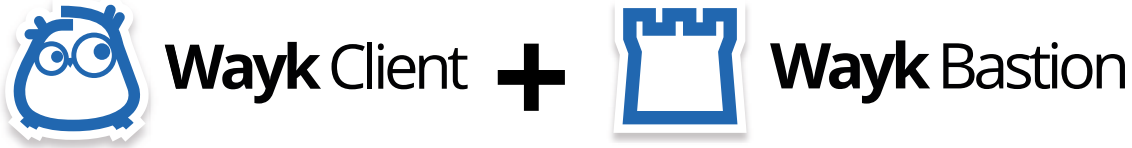
Password Hub Business (PHB), formerly known as Devolutions Password Hub, is a secure and cloud-based password manager for teams. It empowers SMBs to easily and securely vault and manage business-user passwords and other sensitive information through a user-friendly web interface, which can be quickly, 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.

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.



Wayk Client is a flexible, easy-to-use and lightweight remote desktop access solution that reduces setup time and maintains rigorous industry security standards. Wayk Client is the ideal remote desktop access solution for both IT professionals and Managed Service Providers.

Wayk Bastion is a free self-hosted remote access management server for machines running Wayk Agent. All remote desktop connections made by technicians using Wayk Client (license required) are authorized and monitored with corresponding session audit trails.

Learn more here.

CONTACT DEVOLUTIONS

Based in Lavaltrie, Québec, Canada, Devolutions delivers productivity and security solutions to more than 500,000 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/