

2026 SMB Cybersecurity Statistics & Benchmark Report

Insights from 500+ Cyber Assessments of
Small and Medium-Sized Businesses



Table of Contents



Executive Summary	3
A Message from SensCy's CEO	4
Report Background	8
The Data	14
• People	23
• Processes	30
• Technology	42
• NEW! Vulnerability Scanning	50
Conclusion	61
Glossary of Terms	67

Key Theme

The primary risk facing small and midsize organizations is not adoption of advanced technology. It is the absence of disciplined, measurable execution of essential cybersecurity practices. Organizations that treat cyber readiness as a governed, continuously monitored risk function — rather than a periodic IT initiative — materially reduce operational volatility and financial exposure.

A Message from the CEO



Rick Snyder

Chairman and CEO

Cybersecurity is not just a technology issue. It's a business issue. It affects operations, finances, reputation, and trust. And for small and midsize businesses (SMBs) – the backbone of our economy – the stakes are very high.

This is the third year we have published the **SMB Cybersecurity Statistics & Benchmark Report**. We have assessed hundreds of organizations using our NIST-based framework and proprietary SensCy Score®. Our goal is simple: measure where organizations stand so they can take practical steps to improve.

What we continue to see is clear. Most organizations want to do the right things, but many lack the structure and leadership focus needed to build a strong cybersecurity foundation. Tools alone are not enough. Resilience requires engagement, accountability, and a culture that treats cyber risk as a core business responsibility.

The encouraging news is that improvement is achievable. Cyber resilience does not require perfection. It requires commitment and consistency.

I hope this report serves as both a benchmark and a catalyst. When leaders prioritize cyberhealth, they strengthen not only their own organizations, but the broader economy.



Incremental Progress, Persistent Vulnerability

Minor gains hide a larger truth: most SMBs remain unprepared, with weak governance and preventable security gaps — though disciplined action drives rapid improvement. Here are the report's top 5 findings.

1. Cyber Readiness Has Stalled at a Structurally Low Level

While average cyberhealth improved 1.4% over 2025 levels, 93% of SMBs still fail to meet baseline cybersecurity practices.

2. Cyber Risk Lacks Executive Oversight

Only 28% of leadership teams receive regular cybersecurity briefings, and 75% lack formalized cybersecurity policies and training.

3. Avoidable Weaknesses Drive Exposure

55% of SMBs do not conduct cybersecurity awareness training and 55% never perform vulnerability scans. Execution gaps remain the primary driver of risk.

4. Foundational Internet Security Controls are Widely Misconfigured (New 2026 Insight)

78% of organizations have email authentication misconfigurations and 74% have website security weaknesses. The dominant exposure is incomplete implementation of fundamental controls.

5. Meaningful Improvement is Achievable — But Requires Structured Action

Organizations that implement best practices improve cyberhealth by 107% in the first year. Cyber resilience is attainable, but requires disciplined structure and prioritization from leadership.





Executive Summary

Market Context and Report Alignment

Only 34%

of organizations have a mature cybersecurity strategy.

1

26% of SMBs

conduct regular security assessments.

2

\$120k - \$1.2M

the cost of an SMB data breach, depending on the severity of the incident.

3

43% of organizations

reported losing customers after an incident, with 47% reported greater difficulty attracting new customers due to reputational damage.

4

3x less likely

Organizations adopting continuous exposure management are 3x less likely to experience a breach.

5

Sources:

Accenture State of Cybersecurity Resilience Report (1)

Guardz 2025 SMB Cybersecurity Report (2)

Verizon Data Breach Investigations Report (3)

Hiscox 2024 Cyber Readiness Report (4)

Gartner (5)





Background



SMBs Are at Risk



<20%

have dedicated cybersecurity resources ₁

47%

have no cybersecurity budget ₂

54%

believe they are too small for an attack ₃

43%

of cyberattacks are targeted at SMBs ₄

Sources:
Huntress The State of Cybersecurity for Mid-Sized Businesses in 2023 (1)
StrongDM 35 Alarming Small Business Cybersecurity Stats for 2025 (2,3)
Fortinet State of Cybersecurity for Mid-Sized Businesses in 2023 (4)

Background

Six Pillars of a Sound Cybersecurity Strategy (NIST)

Identify

Understand the organization's cybersecurity risk and assets that support critical functions.

Detect

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Protect

Implement the appropriate safeguards to ensure the delivery of critical infrastructure services.

Respond

Develop and implement the appropriate activities to take action regarding a detected cybersecurity incident.

Recover

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Govern

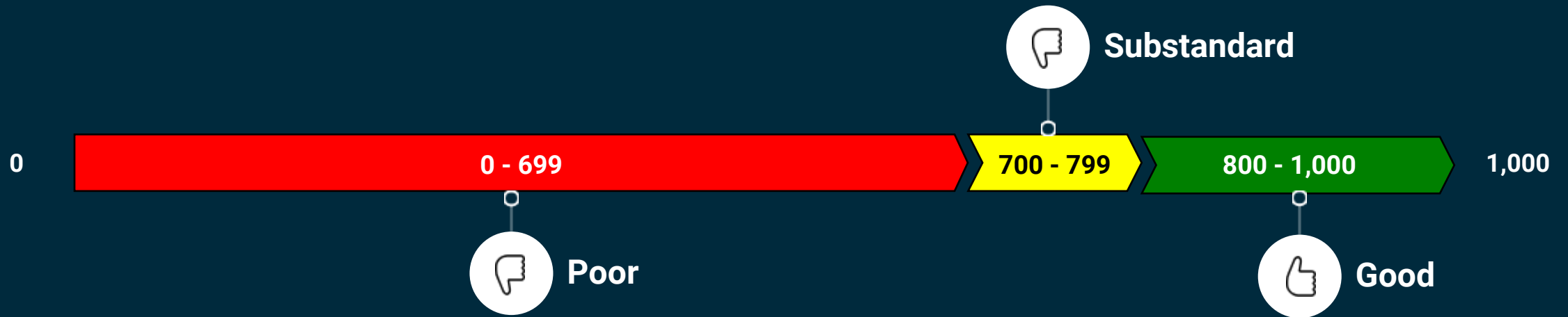
Establish and manage the policies, procedures, and processes to implement and monitor the framework.



Background

The SensCy Score®

A guided cyberhealth assessment everyone can understand, using 39 questions and collecting 100+ data points.



The SensCy Score is a proprietary algorithm that generates a numeric representation of cyberhealth from the SensCy cybersecurity assessment. **The SensCy Score is like a credit score for a company's cyberhealth.** Like a credit score, companies should strive for an 800+ score.

The Cybersecurity Assessments



500+

cybersecurity
assessments conducted
with SMBs across the
United States

39

Industries / Sectors
Scored

SMBs

1,000 or fewer employees

**Assessment
Parameters**

Conducted with a
representative of the SMB and
a cyber professional from
SensCy



The Data

What the Cybersecurity Assessments Reveal



93%

of assessed companies do not follow baseline cybersecurity practices, making them prone to phishing and ransomware attacks.

504

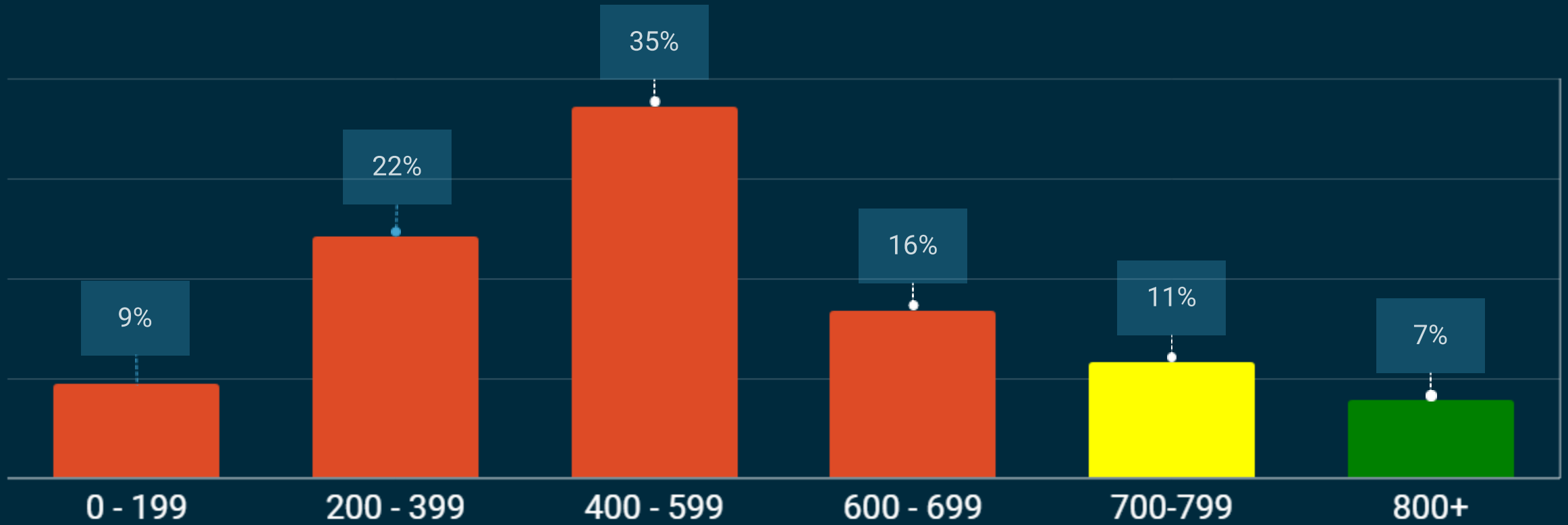
The average initial SensCy Score of SMBs across all sectors since 2022.

107%

Companies that adopted best practices were able to improve their score by an average of 107% in the first year.

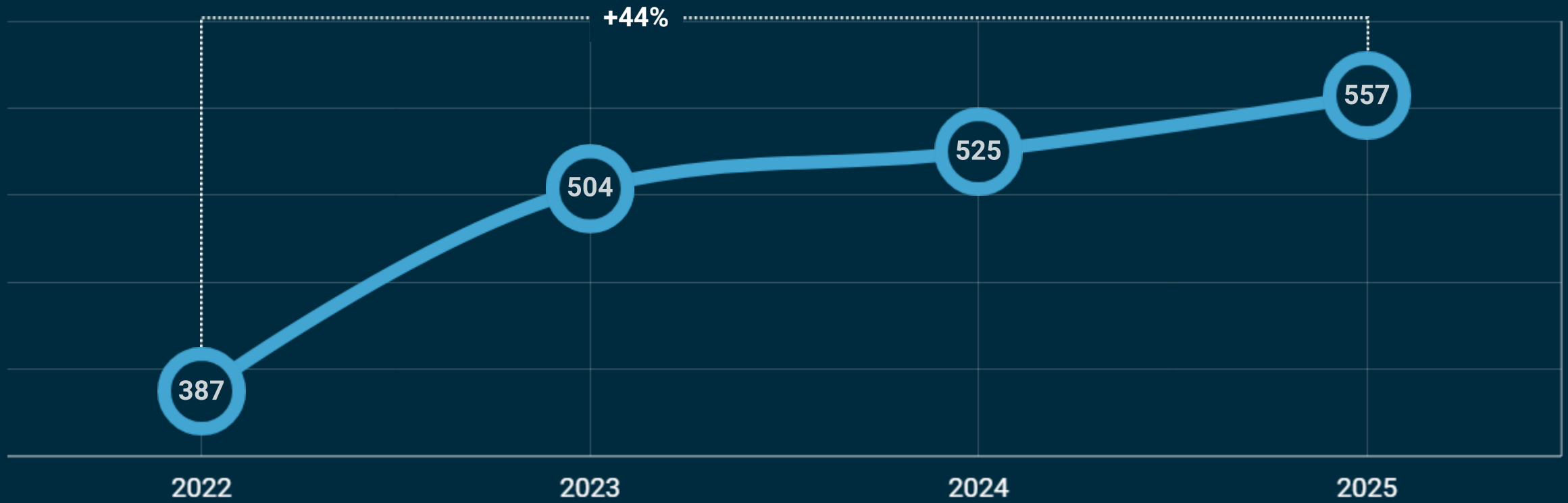
Initial SensCy Score Distribution

The below shows the distribution of all SensCy Scores taken by SMBs for the first time. The average score across all companies measured is 504. While this average is a 1.4% increase over our 2025 findings, the distribution of scores remains alarmingly low.



Average Initial SensCy Score by Year

While we have seen a 44% improvement in SMBs' initial scores since 2022, scores are still remarkably low. **Remember to think of this data as a credit score for a SMBs cyberhealth, with 800+ being considered good.**



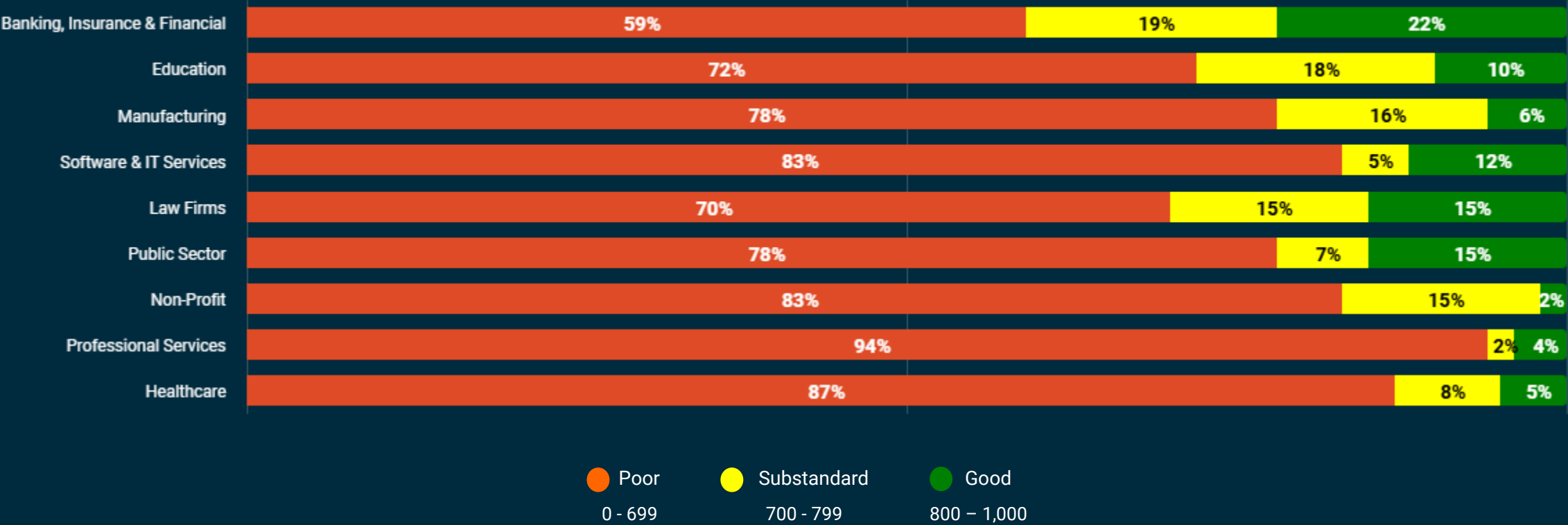
Average SensCy Scores by Industry

Scores suggest a concerning lack of preparedness across all industries. **KEY TAKEAWAY:** the financial and education sectors are leading in cybersecurity practices, while their peers in healthcare and professional services are far behind.



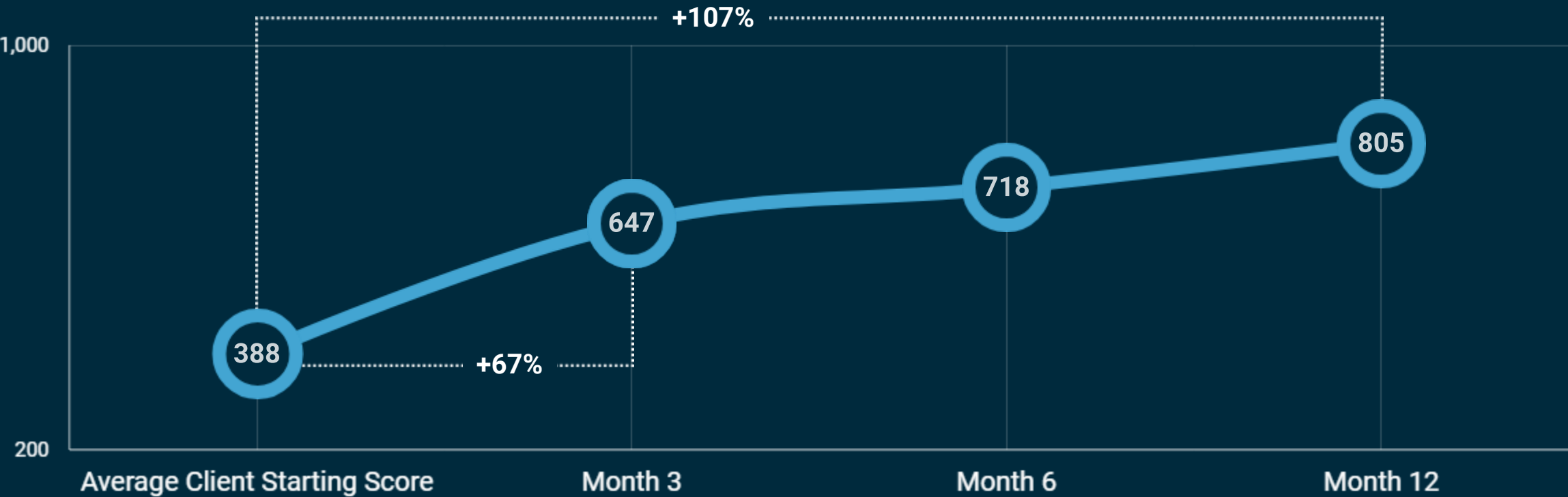
SensCy Score Distribution by Industry

While cybersecurity maturity varies by industry, one thing is clear: far too many organizations still fall into the substandard and poor categories.



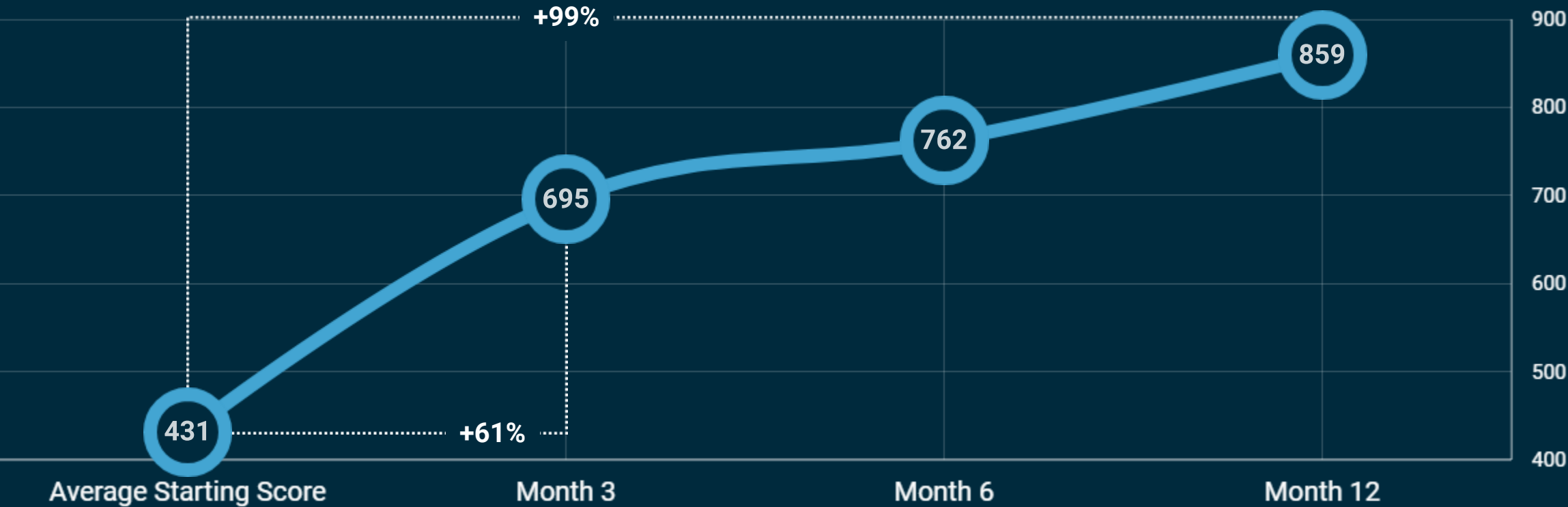
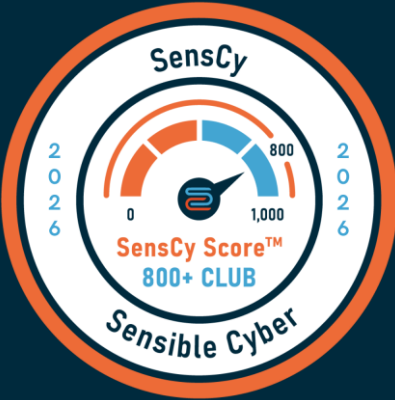
Average Score Improvement within SensCy Clients

While initial SMB scores are low across the board, SensCy clients saw significant improvement by implementing cyber hygiene best practices. The chart below shows the average scores of clients that have been with SensCy for one year. On average, **their scores improved by 107%, with a 67% improvement in the first three months.**



Score Improvement — 800+ Clients

The chart below shows the average scores of all SensCy clients who achieved an 800+ score within one year of becoming a client. The **average score improvement was 99%**, with a **61% improvement achieved in the first 3 months**.





Measuring Cyber Risk & Resilience

In measuring cyber risk and resilience, the SensCy Score examines people, processes, and technology, which are all components of a strong cybersecurity program, culture, and risk mitigation strategy.

PEOPLE

PROCESS

TECHNOLOGY





People

PEOPLE

PROCESS

TECHNOLOGY

88% of cyberattacks can be avoided as they are caused by human error.

A strong cybersecurity program requires a strong cybersecurity culture.

Leadership

Must stay informed through executive risk briefings. The goal is to build a security-minded culture through governance, policy, training, and technology.

Employees

Invest in employees. Train them to be the first line of defense.

IT Personnel

Know that IT $\neq$ cybersecurity. Know which tools and why. Focus on proper configuration, deployment, and management. Get assistance from professionals.

The following section will look at how SMBs responded to some of the people-related questions in the assessment.



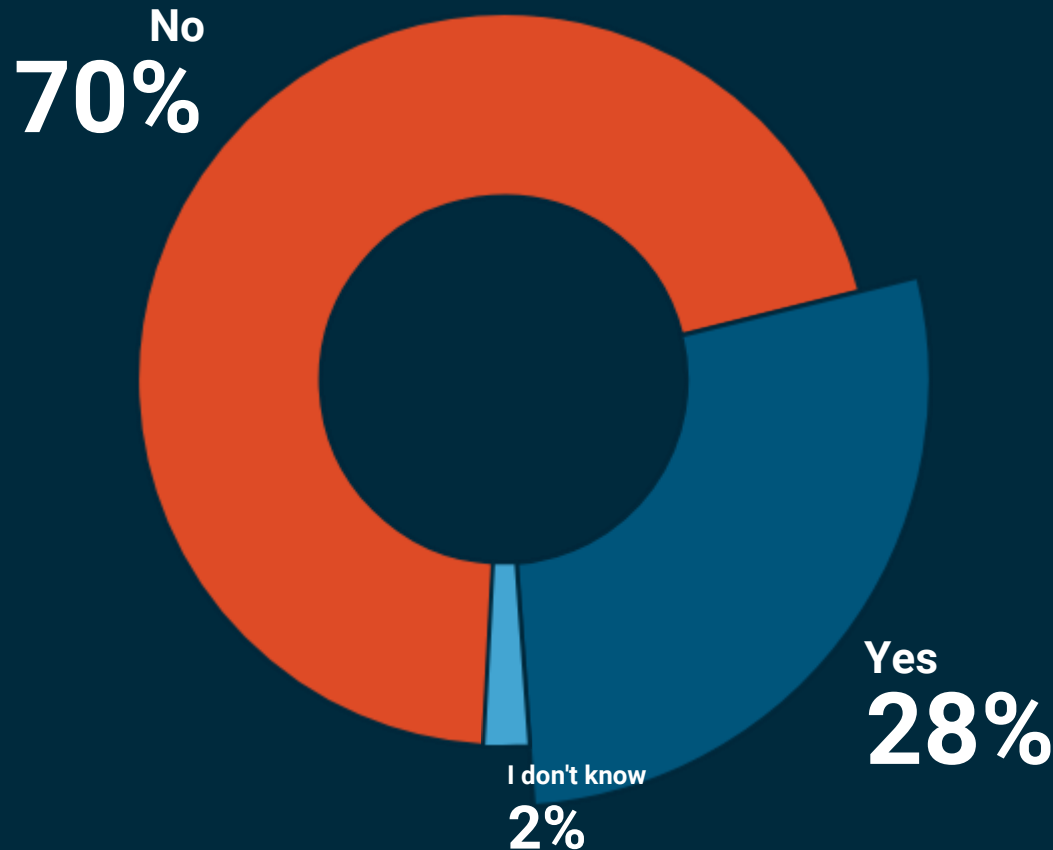
Executive Cybersecurity Briefings

PEOPLE

PROCESS

TECHNOLOGY

Question: Do the owners, executives, or board of directors receive regular cybersecurity status briefings?



Key Takeaways

- Best Practice Answer: Yes (28%).
- SensCy has observed that if briefings are occurring, they are often done ad-hoc and not part of a regular leadership agenda.
- Cybersecurity is a business risk. Briefings must occur at the highest levels of organizations to help leadership understand current posture, risk profile, preparedness, and potential outcomes.



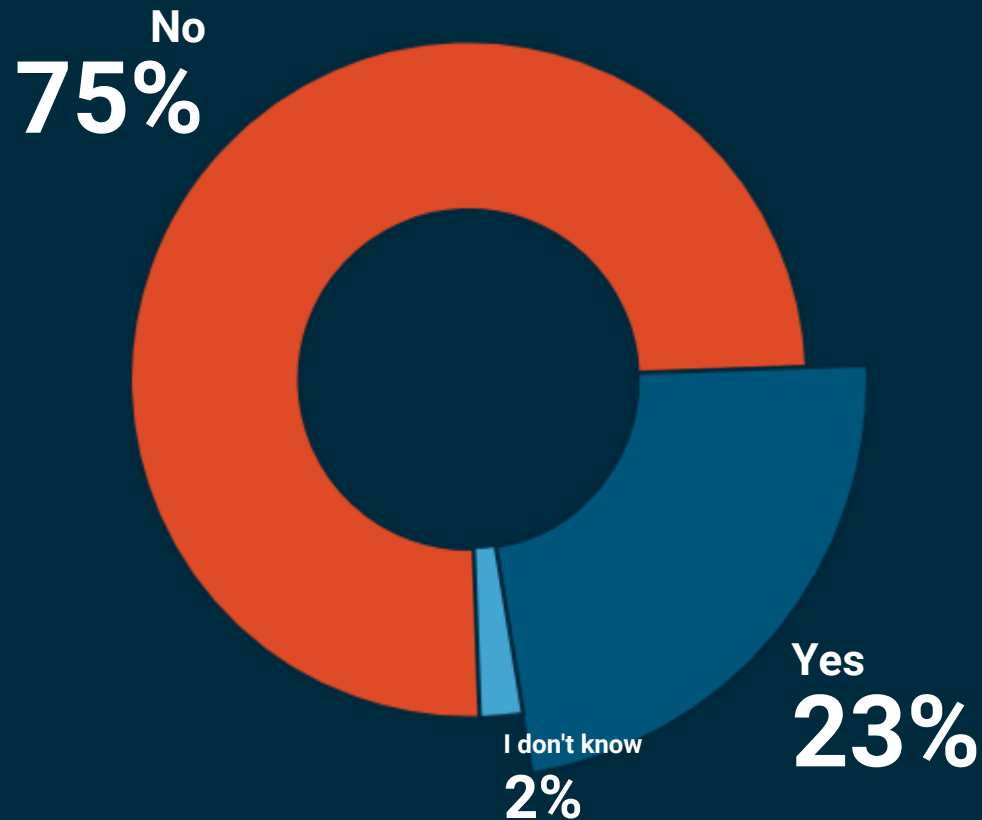
Written Cybersecurity Policies

PEOPLE

PROCESS

TECHNOLOGY

Question: Does your company have written cybersecurity policies and a formal process to train employees on your cybersecurity policies?



Key Takeaways

- Best Practice Answer: Yes (23%).
- SensCy has observed that if an SMB had cybersecurity policies, employee exposure is often limited to the onboarding process.
- Every company has HR policies. Why? Because they mitigate business risk. Cybersecurity is a business risk, and companies must have policies in place to address this risk. Since employee mistakes are our largest risk area, we must find ways to help our employees understand these policies.



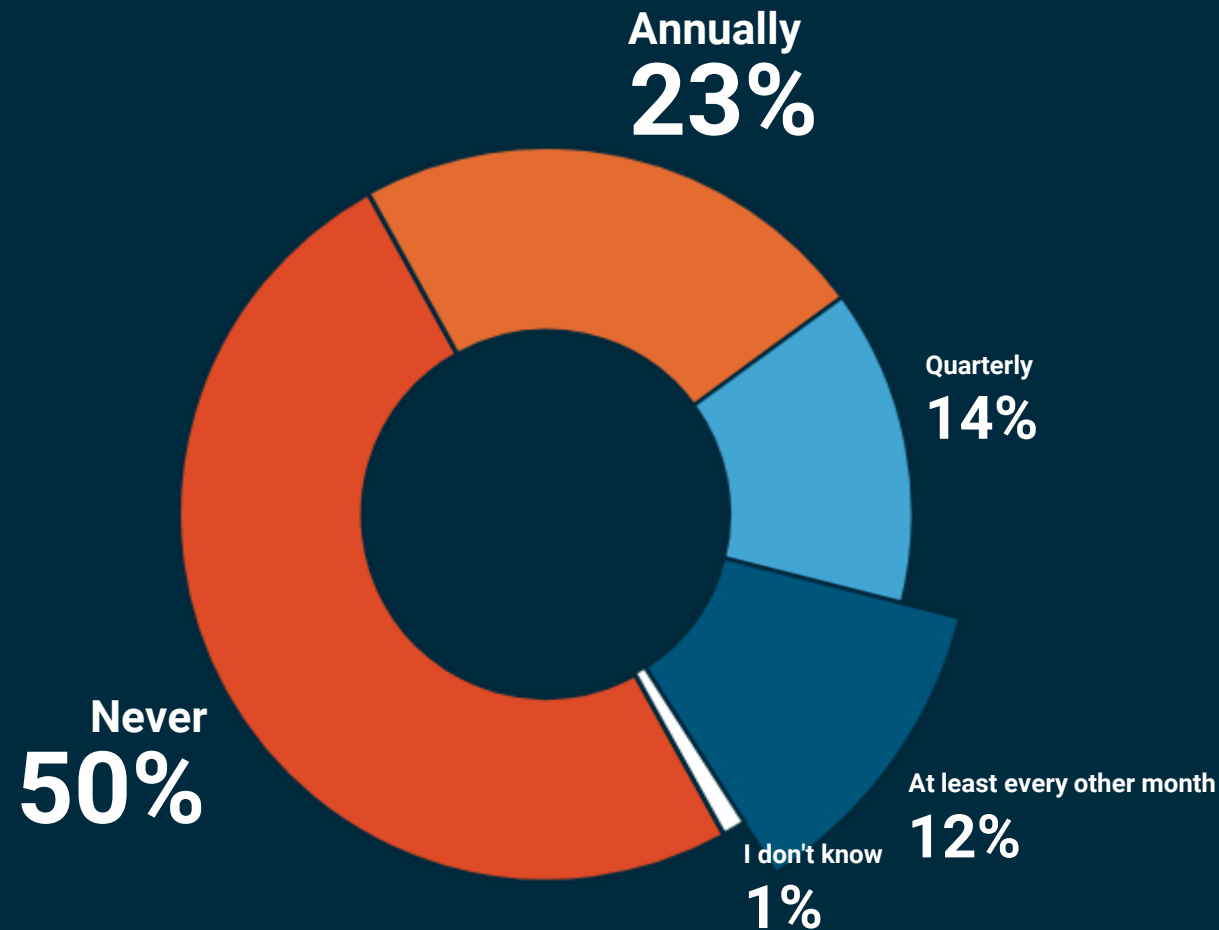
Cybersecurity Awareness Training

PEOPLE

PROCESS

TECHNOLOGY

Question: How often is cybersecurity awareness training conducted?



Key Takeaways

- Best Practice Answer: At least every other month (12%).
- SensCy has observed that if an SMB offers training to employees, it is not done consistently enough to change behavior.
- 88% of successful cyberattacks are still caused by human error; therefore, employees are the largest risk. Focus on converting them to first line of defense. Investing in a cybersecurity awareness training program is a critical step toward resilience.



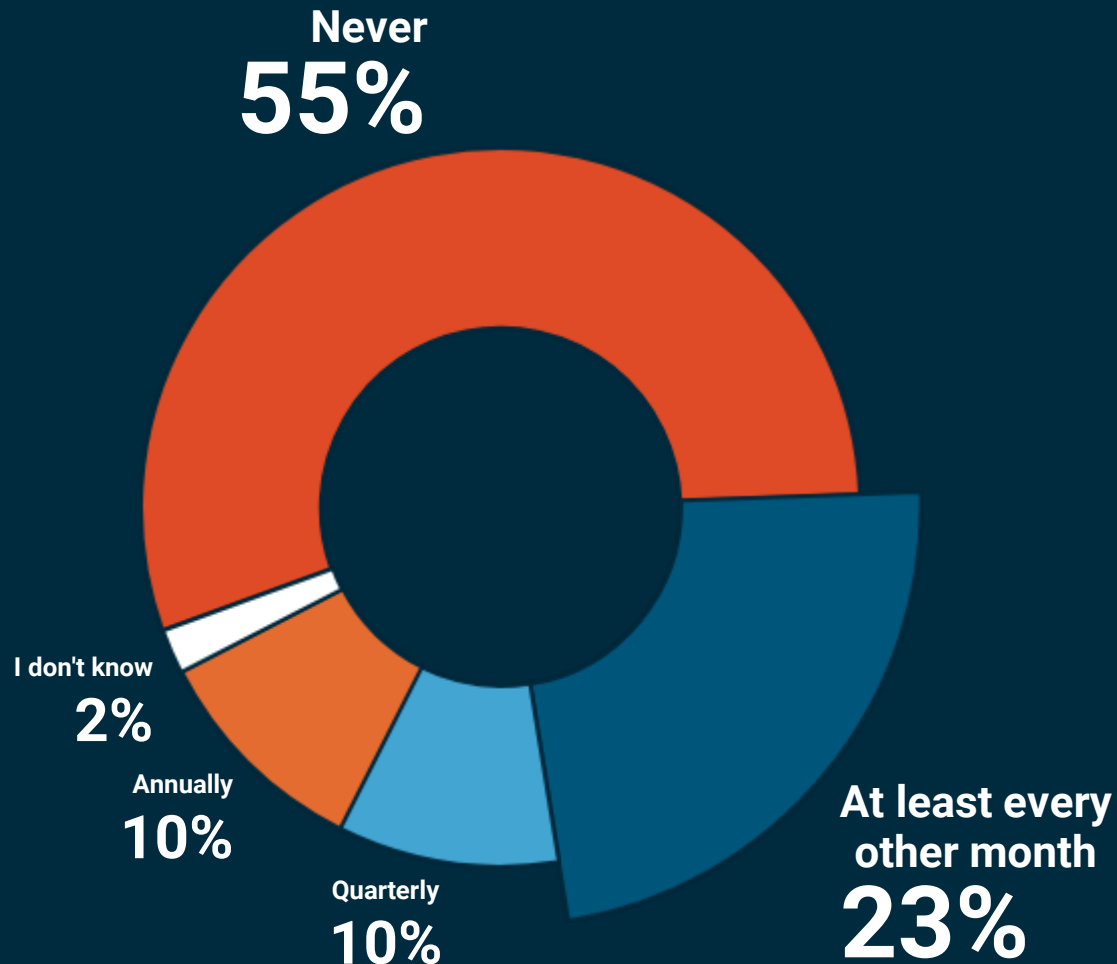
Phishing Simulations

PEOPLE

PROCESS

TECHNOLOGY

Question: How often are phishing simulations conducted?



Key Takeaways

- Best Practice Answer: At least every other month (23%).
- Phishing simulations are designed to safely test how employees respond to real-world attack tactics, helping organizations identify human vulnerabilities before attackers do.
- SensCy has observed that if an SMB provides phishing simulations to employees, it is not done consistently enough to change behavior.



Phishing Simulations - Impact

PEOPLE

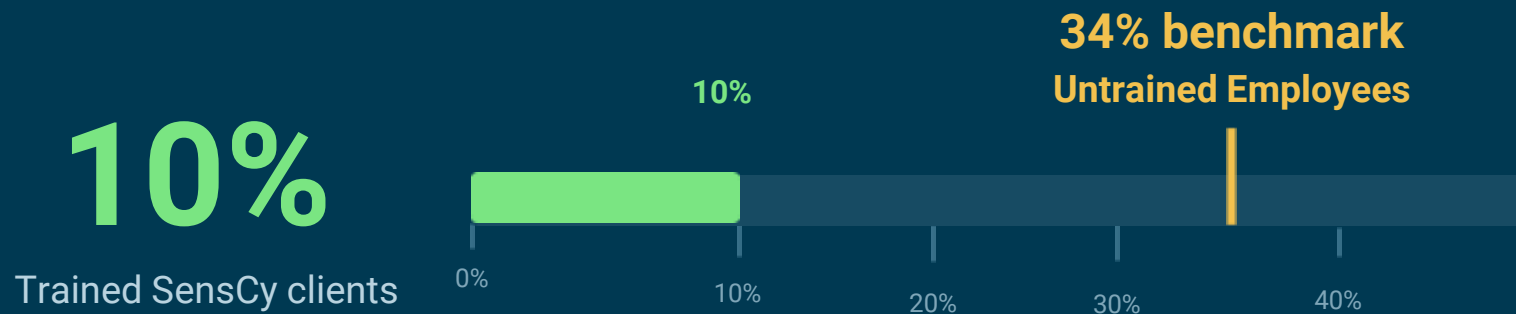
PROCESS

TECHNOLOGY

Studies show that 34% of untrained employees click on phishing links, download malicious attachments, or provide credentials when socially engineered through email. Additionally, 45% of ransomware is delivered through phishing. This is an area of high risk.

Meaningful improvement can be achieved through a combination of consistent cybersecurity awareness training and phishing simulations. The below shows trained employee click rates (with training and/or phishing simulations occurring every month) vs. untrained employee click rates.

Click Rate - *Lower is better*



Trained SensCy clients

34% benchmark
Untrained Employees

Click rate = % of employees who failed a phishing simulation

Impact vs benchmark

-24 pts

≈71% lower than 34% average

EXECUTIVE TAKEAWAY:

Meaningfully fewer clicks
= meaningfully less risk



A stylized illustration of a modern office environment. Several people are seated at desks, working on computers. The desks are equipped with multiple monitors, keyboards, and office chairs. The office has a clean, organized appearance with a tiled floor and some potted plants. The overall color palette is dominated by blues, oranges, and greys.

Summary

People

PEOPLE

PROCESS

TECHNOLOGY

The key to resilience lies in turning your biggest risk—your people—into your first line of defense.

However, the data reveals significant gaps that many organizations still face. **Only 28% of leadership teams receive regular cybersecurity briefings, and half of SMBs do not conduct awareness training.** These shortcomings leave employees and leadership unprepared to recognize and respond to threats, highlighting the critical need for a people-first approach to cybersecurity.

By fostering a culture of vigilance through consistent training, clear communication, and active leadership involvement, organizations can empower their teams to detect and address threats effectively. This focus on teamwork and shared responsibility builds stronger defenses and helps ensure the organization is prepared to face evolving cyber challenges.





Processes

Accountability is key to a strong cybersecurity program. Repeatable processes are how organizations build resilience over time.

NIST Pillars

Ensure your strategy covers each of the NIST pillars: Identify, Detect, Protect, Respond, Recover, and Govern.

Vulnerability Identification

Proactive and persistent notifications of vulnerabilities are key.

Accountability

Address vulnerabilities as they are identified. Develop a plan to respond should and incident occur.

PEOPLE

PROCESS

TECHNOLOGY

The following section will look at how SMBs responded to some of the process-related questions in the SensCy cybersecurity assessment.



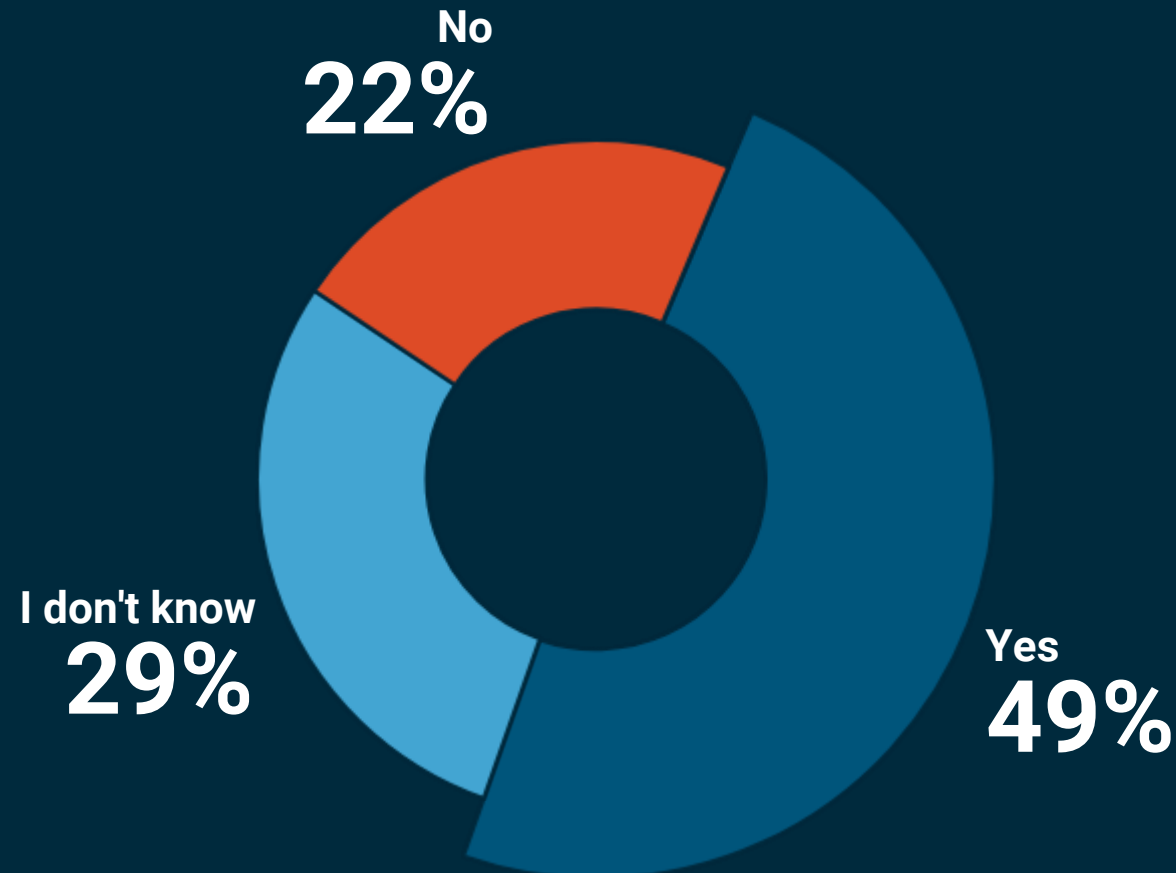
Asset Inventory

PEOPLE

PROCESS

TECHNOLOGY

Question: Does your company maintain an up-to-date inventory of all the software that your employees have access to, and all of your company hardware?



Key Takeaways

- Best Practice Answer: Yes (49%).
- *"We cannot protect it if we don't know we have it."* Sound familiar?
- With each addition, new risks are introduced into the technology stack. Confidence an environment is truly secure requires an up-to-date inventory.



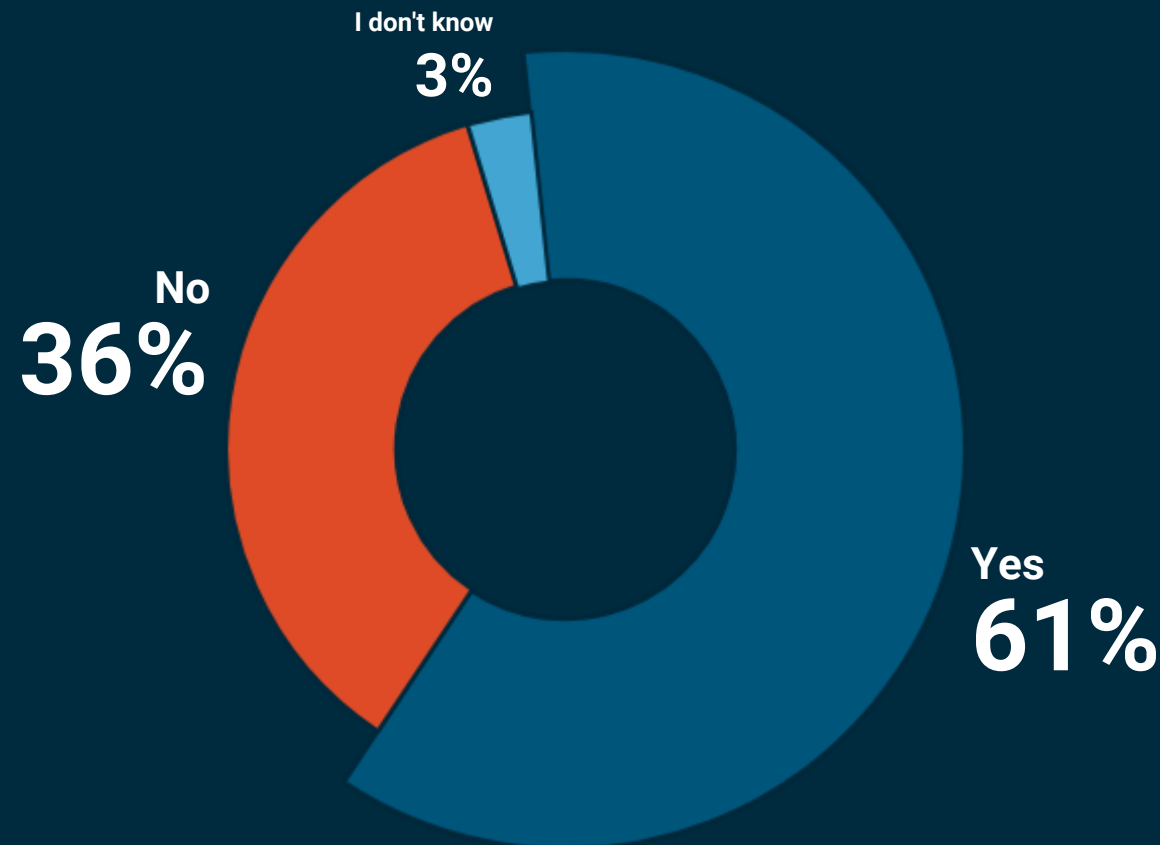
Notification of Critical Security Patches

PEOPLE

PROCESS

TECHNOLOGY

Question: Is your company notified when critical security patches are released for all your software and hardware?



Key Takeaways

- Best Practice Answer: Yes (61%).
- Unpatched systems allow for threat actors to deploy ransomware and other malicious malware that can disrupt your business or lead to stolen data. Fast notification of these vulnerabilities is critical to mitigating them.
- SensCy has observed significant gaps in the configuration, monitoring, and follow-through of notifications.



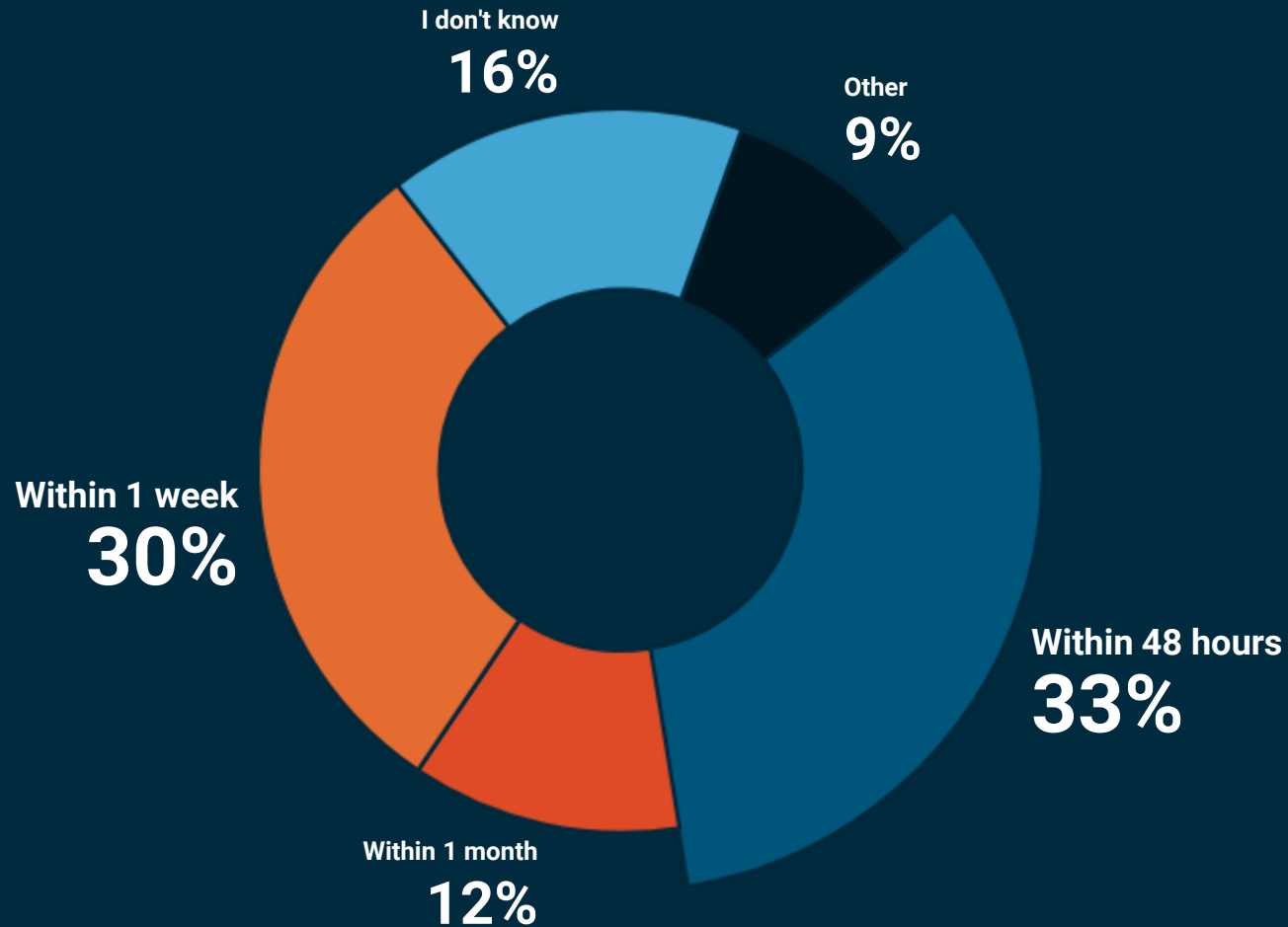
Installation of Critical Security Patches

PEOPLE

PROCESS

TECHNOLOGY

Question: How soon does your company install critical security patches after they are released?



Key Takeaways

- Best Practice Answer: Within 48 hours (33%).
- While 61% of SMBs report receiving notifications of critical security patches, only 33% are installing them within 48 hours.
- Unpatched systems create an open window for threat actors to disrupt operations or steal sensitive data — and the longer organizations wait to install critical patches, the wider that window becomes.



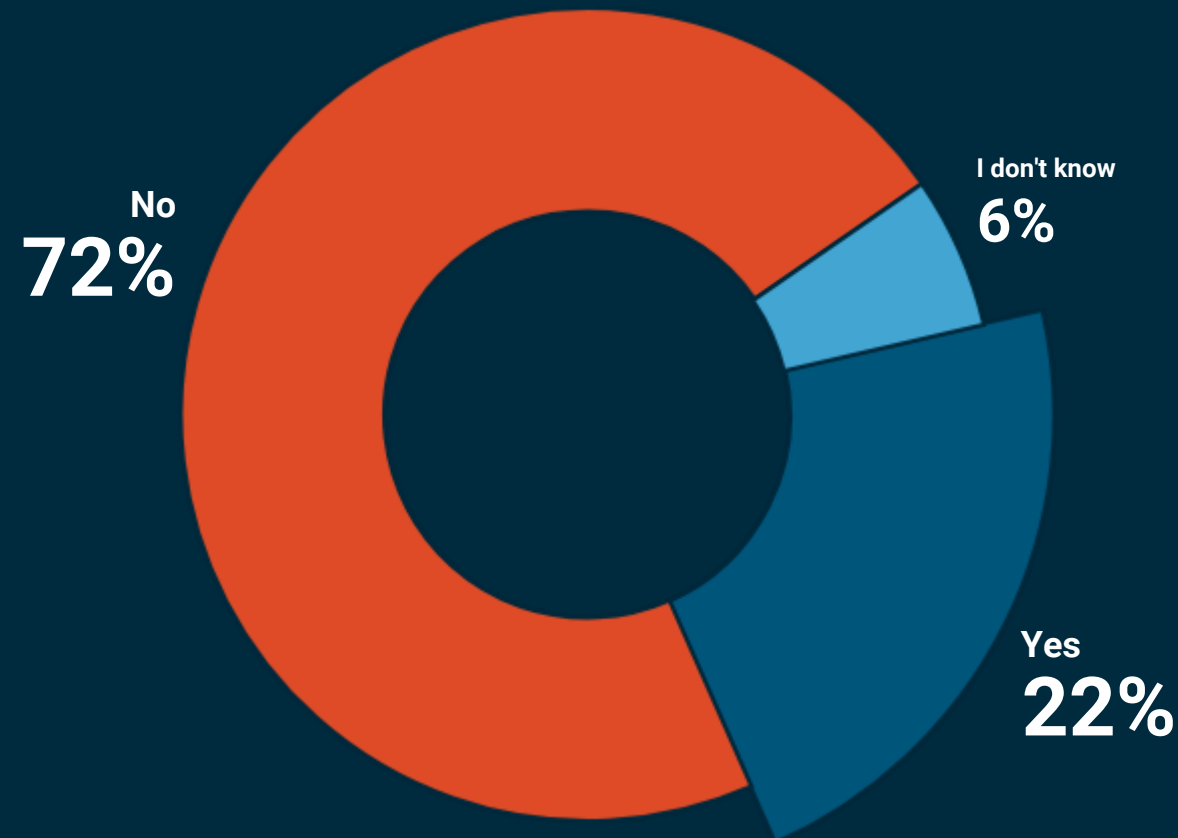
Penetration Testing

PEOPLE

PROCESS

TECHNOLOGY

Question: Does your company perform penetration testing at least annually?



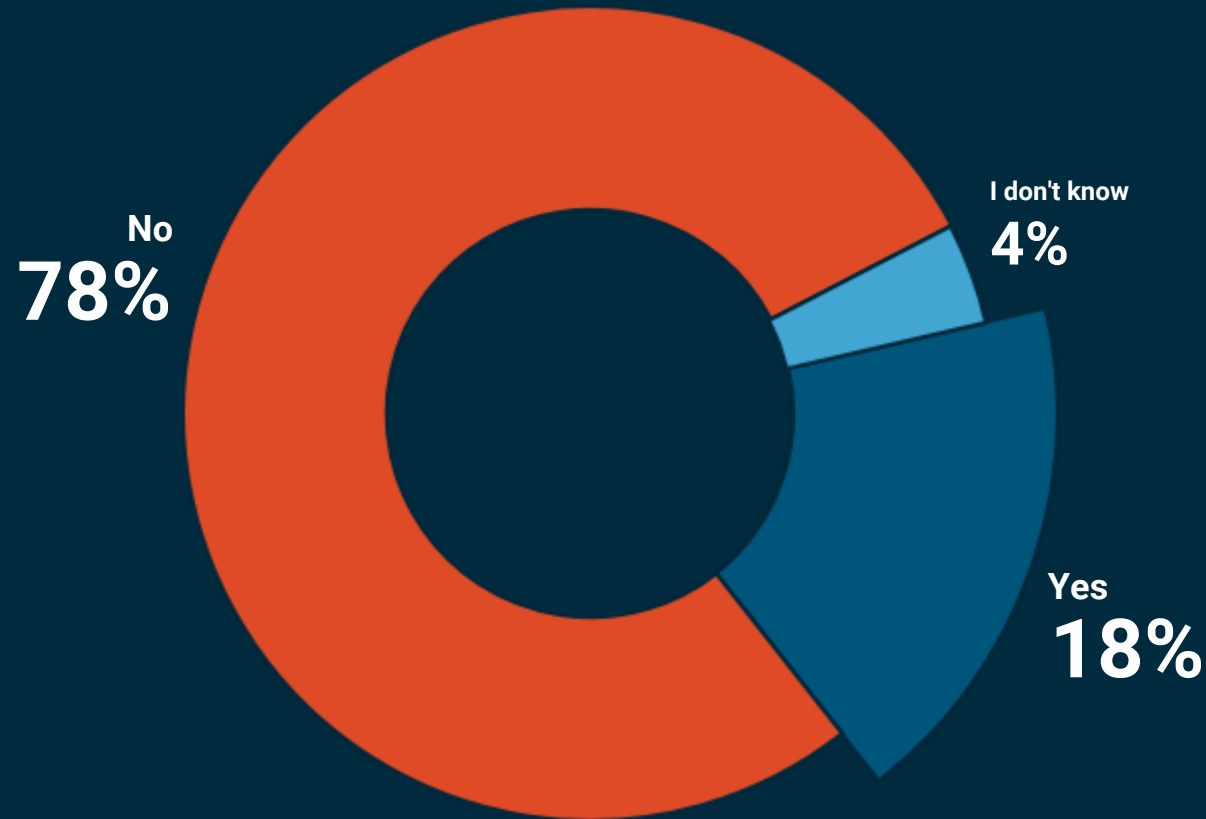
Key Takeaways

- Best Practice Answer: Yes (22%).
- A penetration test helps identify and exploit vulnerabilities in your systems before threat actors can.
- Conducting penetration tests enhances security posture, ensures compliance with regulations, protects sensitive data, and minimizes the risk of costly breaches.



Dark Web Scanning

Question: Does your company actively search the dark web for exploited company information?



PEOPLE

PROCESS

TECHNOLOGY

Key Takeaways

- Best Practice Answer: Yes (18%).
- The dark web is a marketplace where threat actors buy, sell, and share stolen data, including information taken from business systems and third-party breaches.
- Dark web monitoring helps identify whether organizational data — such as usernames and login credentials — has been exposed, so action can be taken before it leads to account compromise or a larger cyber incident.



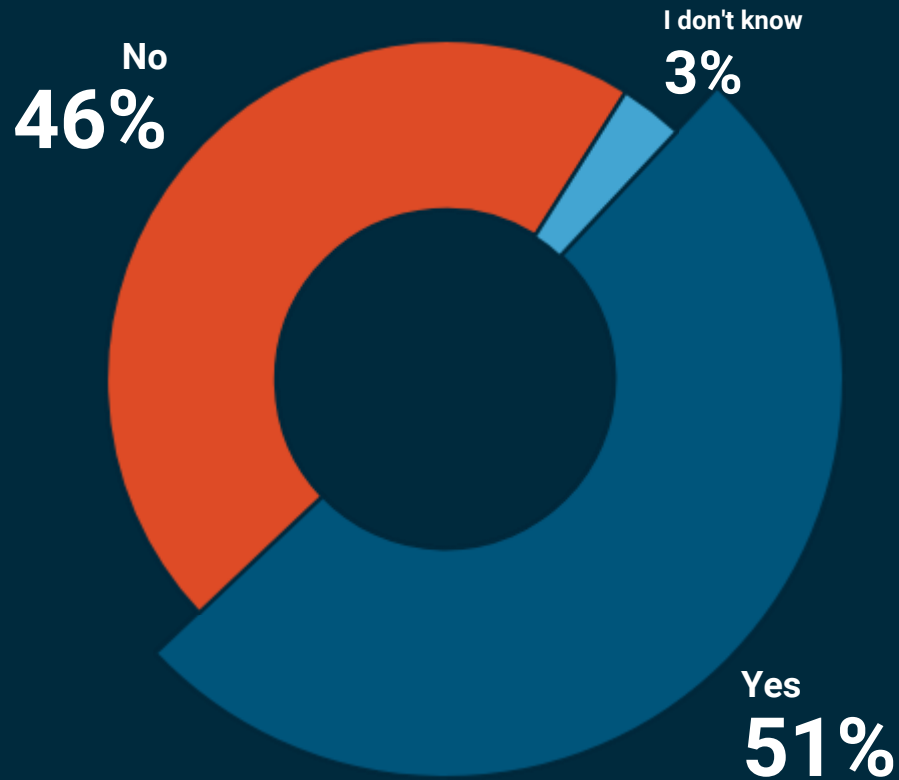
Desktop Admin Rights

PEOPLE

PROCESS

TECHNOLOGY

Question: Does your company prohibit employees from having admin rights on their desktops and/or laptops?



Key Takeaways

- Best Practice Answer: Yes (51%).
- If admin rights are not disabled on desktops and laptops, users can install any program — including malicious ones — and can accidentally (or purposefully) create a cybersecurity incident.
- Users with admin rights can change critical security settings, too. Restricting admin rights creates a more secure environment.



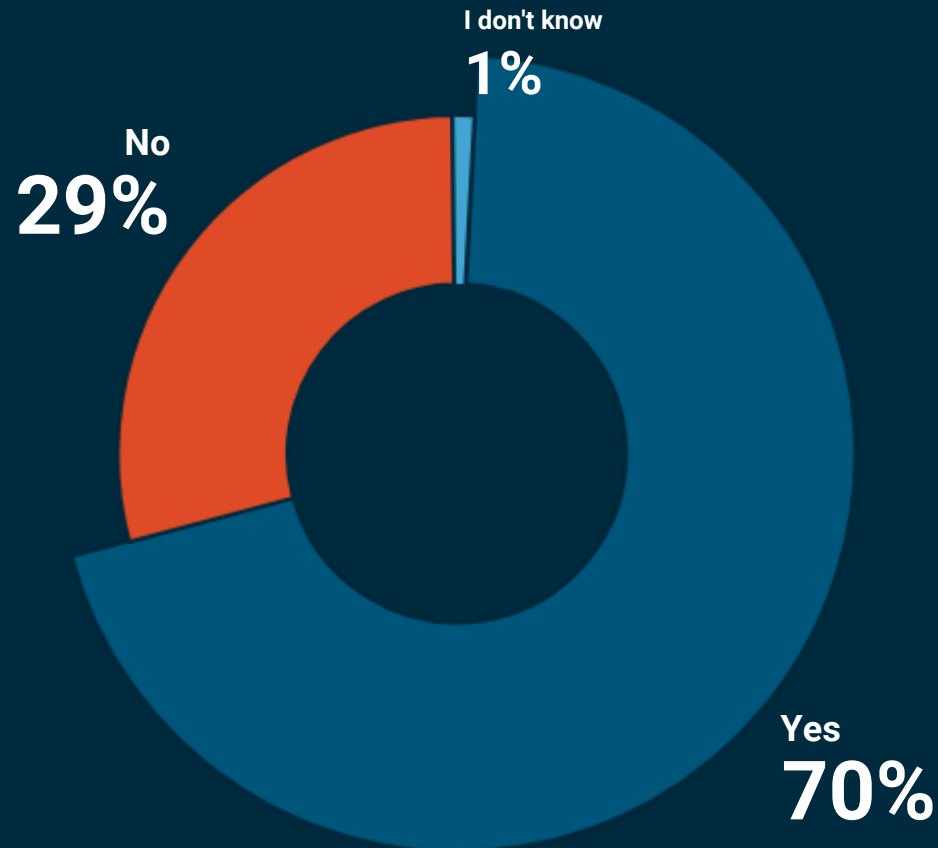
Complex Passwords

PEOPLE

PROCESS

TECHNOLOGY

Question: Does your company have a password policy that enforces the use of complex passwords with a minimum of 8 characters?



Key Takeaways

- Best Practice Answer: Yes (70%).
- A strong password policy is a foundational defense against unauthorized access.
- The most significant breaches happen when threat actors have access to company systems via username and password. Long passwords that include special characters are difficult for threat actors to crack.



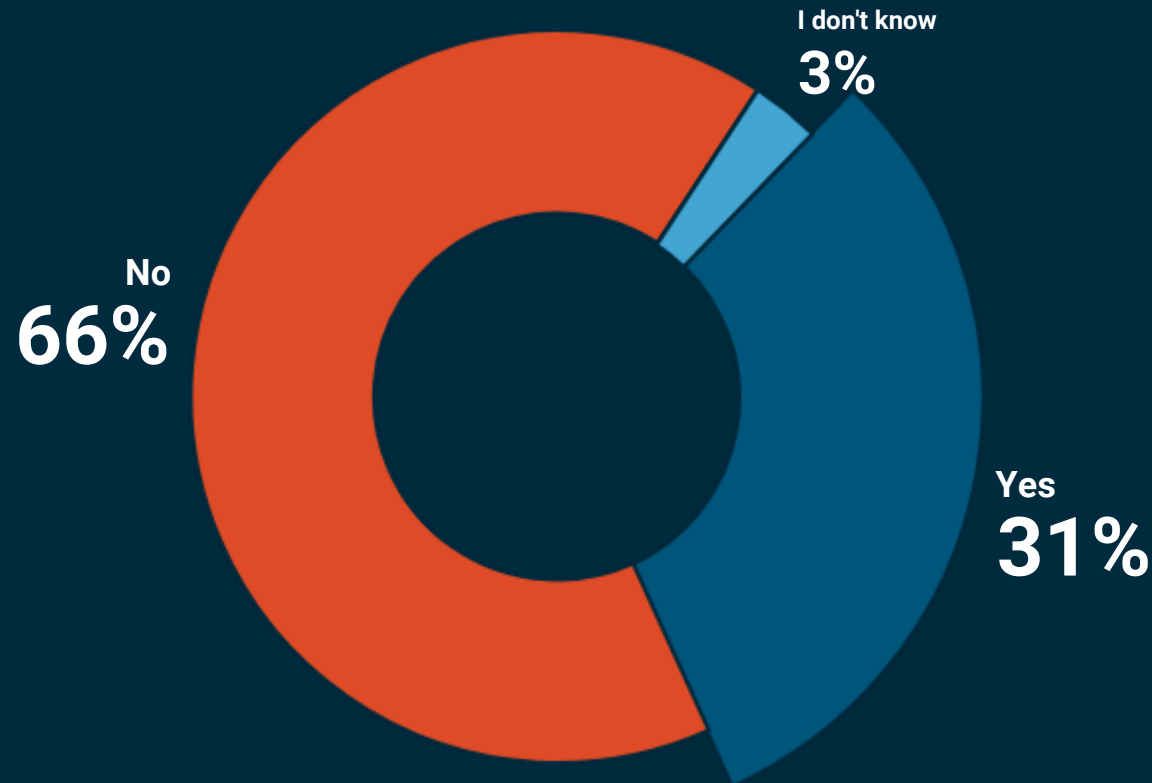
Incident Response Plan

PEOPLE

PROCESS

TECHNOLOGY

Question: Does your company have a cybersecurity incident response plan?



Key Takeaways

- Best Practice Answer: Yes (31%).
- A step-by-step incident response plan significantly reduces the downtime and financial impact resulting from a cybersecurity incident.
- A well-designed plan will direct all parts of the organization during this unique crisis and guide leadership on what questions to ask at each stage of the incident, and how to communicate the incident to employees and other stakeholders.



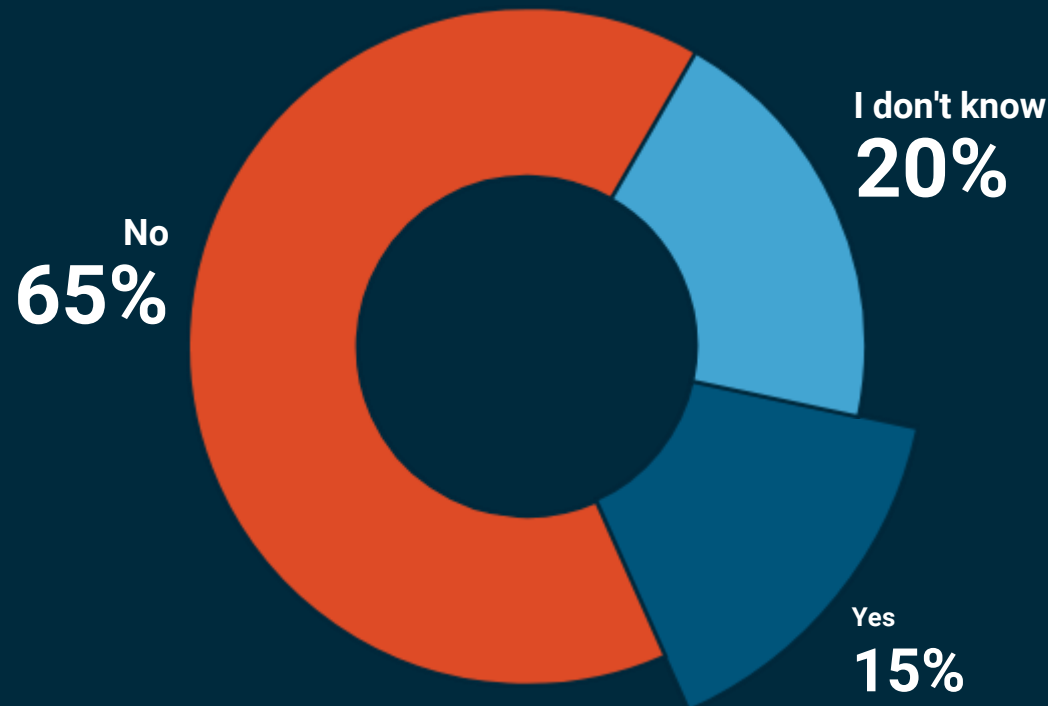
Incident Response Plan Annual Updates

PEOPLE

PROCESS

TECHNOLOGY

Question: Does your company have a formal process to ensure your cybersecurity incident response plan is updated at least annually?



Key Takeaways

- Best Practice Answer: Yes (15%).
- Many parts of the organization will have a role in the response to a cybersecurity incident. Each person should know their role before an incident occurs.
- It's important to take employee turnover and operational changes into consideration and review your plan at least annually.





Back-ups

PEOPLE

PROCESS

TECHNOLOGY

Backing up data properly is critical to recovering from ransomware. While SMBs are doing a great job in ensuring data is backed up properly, they are lacking in testing successful restoration and encryption.

85%

of SMBs have their back-ups on a separate network or in a cloud service specifically designed for backing up data.

78%

of SMBs are backing up their data at least daily.

57%

of SMBs have encrypted their back-ups.

42%

of SMBs have tested a successful restoration from back-up in the last six months.





Summary

Processes

PEOPLE

PROCESS

TECHNOLOGY

Building a stronger cybersecurity posture starts with clear processes and accountability.

Yet the data reveals critical gaps in how SMBs manage these foundational practices.

Only 31% of SMBs have a formal cybersecurity incident response plan, leaving many organizations without a structured approach to mitigate and recover from attacks. Additionally, just 15% update response plans annually, failing to account for operational changes and emerging threats. This lack of preparedness can lead to prolonged downtime and increased financial impact in the event of a cyber incident.

Establishing accountability through well-defined policies and response plans ensures issues are addressed quickly and effectively. This disciplined approach not only reduces risk but fosters a culture of proactive cybersecurity management across the organization.





Tools & Technology

Having the right tools and technology in place is key to both protection and recovery.

Conduct cybersecurity assessments to continuously know where you stand.

Prioritize

Build a cyberhealth plan that prioritizes issues based on severity.

Execute

Implementation of the cyberhealth plan begins with the risk mitigation process.

PEOPLE

PROCESS

TECHNOLOGY

The following section looks at how SMBs responded to some of the technology-related questions in the SensCy cybersecurity assessment.



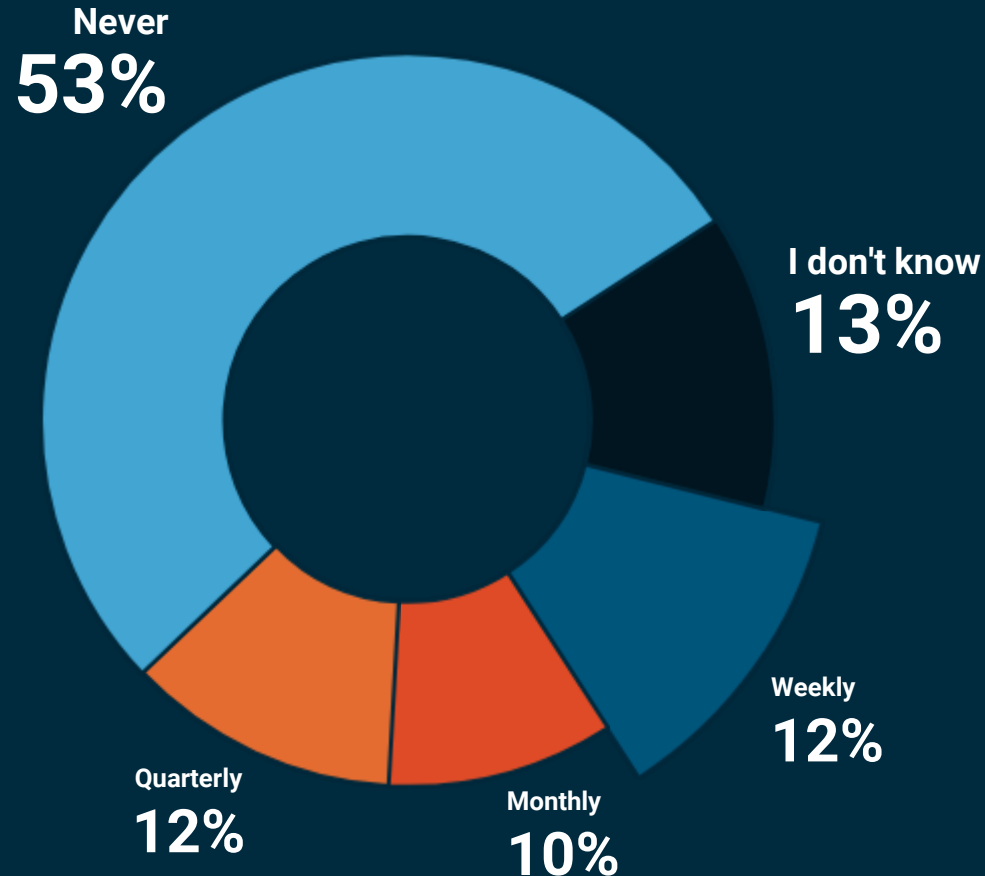
Internal Vulnerability Scanning

PEOPLE

PROCESS

TECHNOLOGY

Question: How often does your company perform internal vulnerability scans?



Key Takeaways

- Best Practice Answer: Weekly (12%).
- Internal vulnerability scans are security scans conducted within an organization's network to identify vulnerabilities in systems, applications, and computing devices that could be exploited by threat actors.
- Internal scans focus on threats that originate within the organization, such as misconfigurations, outdated software, or unauthorized access by employees or contractors.



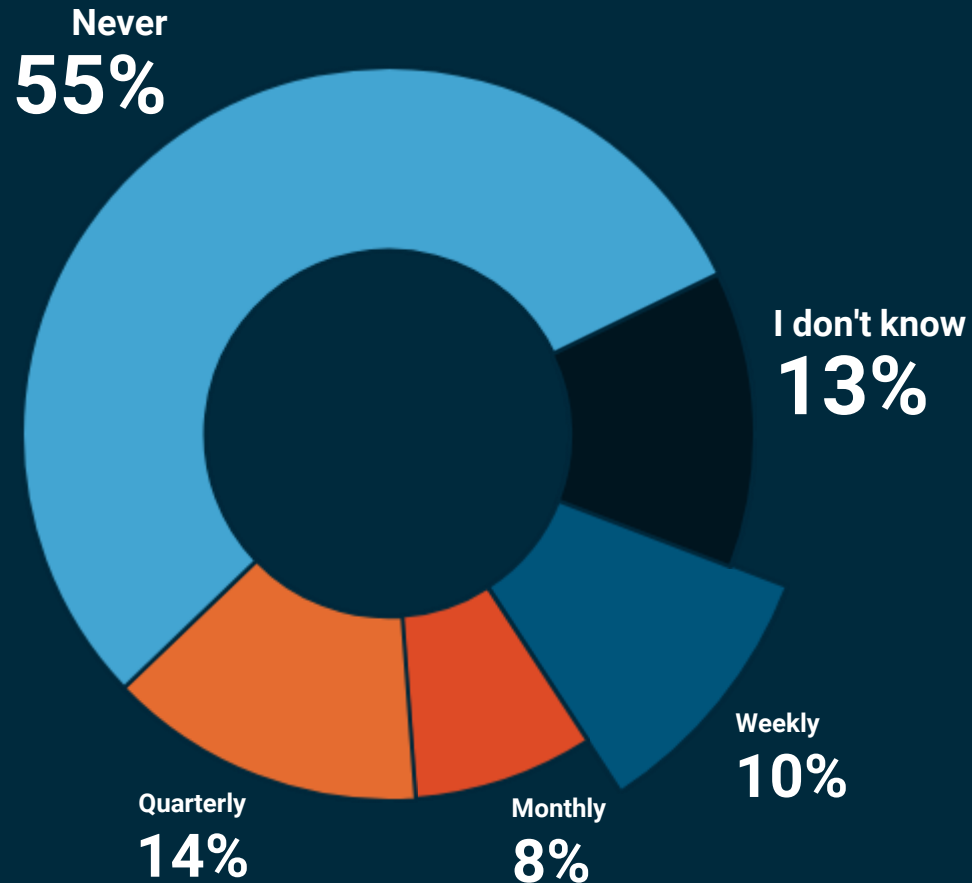
External Vulnerability Scanning

PEOPLE

PROCESS

TECHNOLOGY

Question: How often does your company perform external vulnerability scans?



Key Takeaways

- Best Practice Answer: Weekly (10%).
- External vulnerability scans are performed on an organization's internet-facing assets to identify vulnerabilities that attackers could exploit from outside the network, such as web servers, email servers, and cloud environments.
- External scans identify security misconfigurations, outdated software, botnets, and other compliance issues.



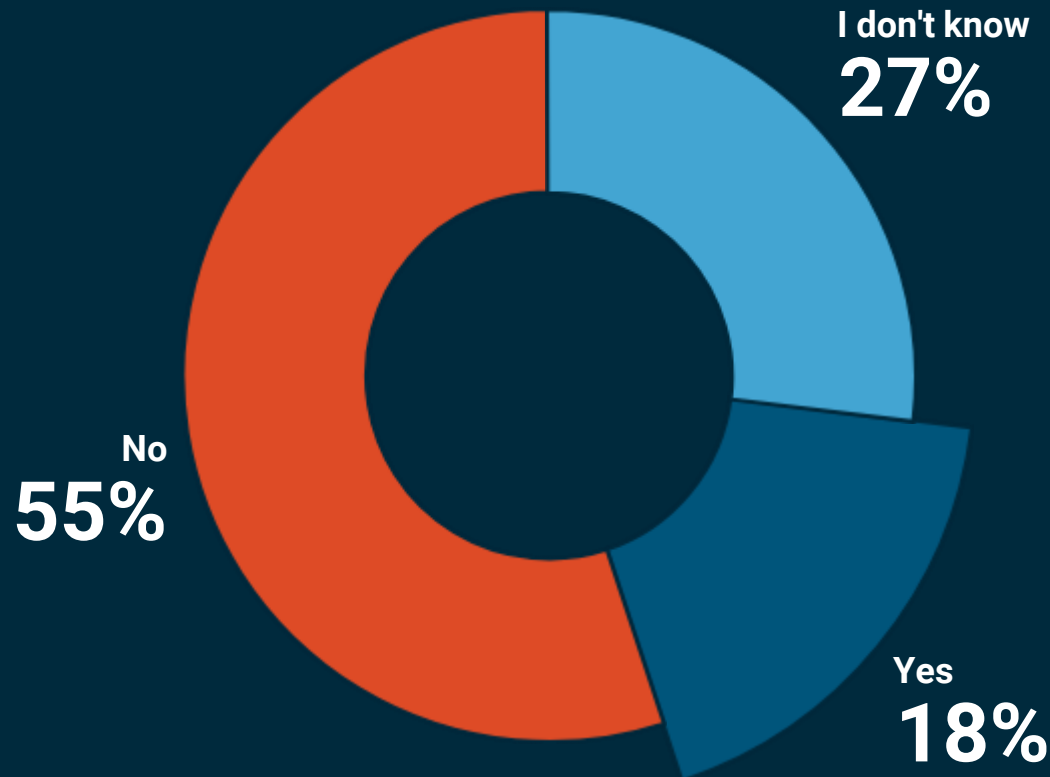
Password Keeper

PEOPLE

PROCESS

TECHNOLOGY

Question: Does your company provide a password manager to employees?



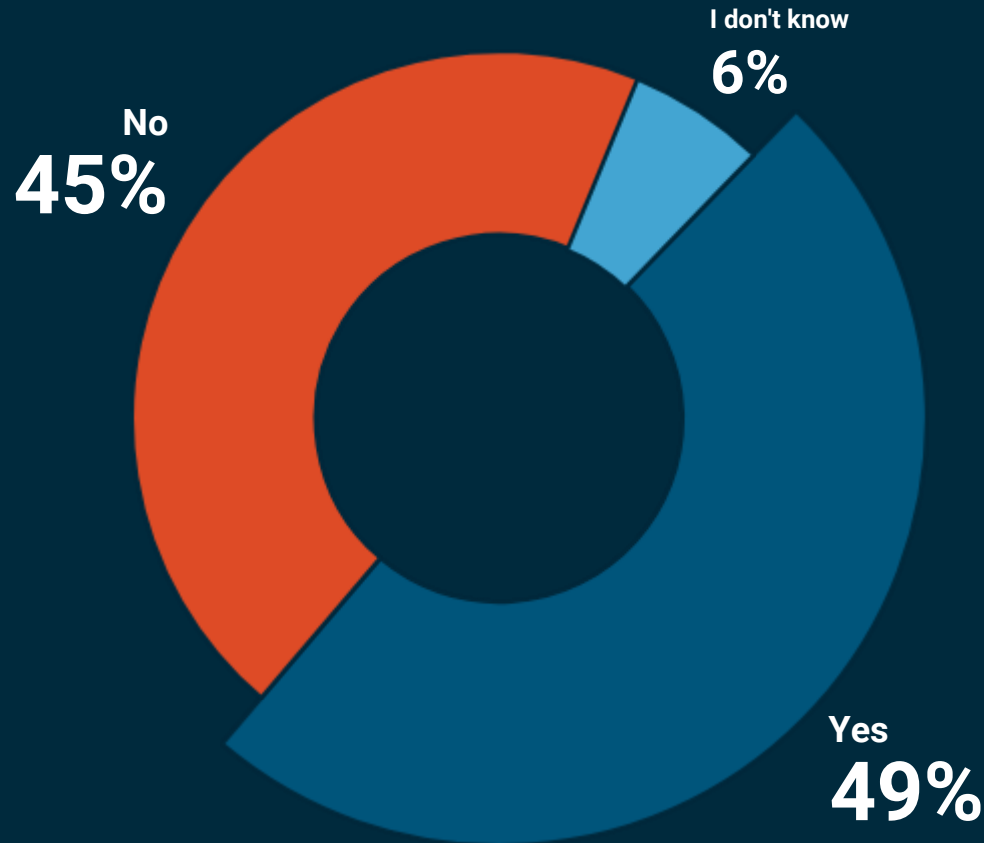
Key Takeaways

- Best Practice Answer: Yes (18%).
- A password manager, or password keeper, is a tool that securely stores and manages employees' login credentials for various accounts, ensuring that passwords remain strong, unique, and protected.
- Password managers prevent employees from high-risk activities such as reusing passwords and entering credentials on malicious sites.



Virtual Private Network (VPN)

Question: Does your company require a virtual private network to access systems when not in the office?



PEOPLE

PROCESS

TECHNOLOGY

Key Takeaways

- Best Practice Answer: Yes (49%).
- A VPN is a security tool that encrypts and routes internet traffic through a secure server, masking a user's IP address and location.
- VPNs create a private, secure communication tunnel between a device and the internet, protecting data from hackers, ensuring secure communications for remote employees accessing company systems.



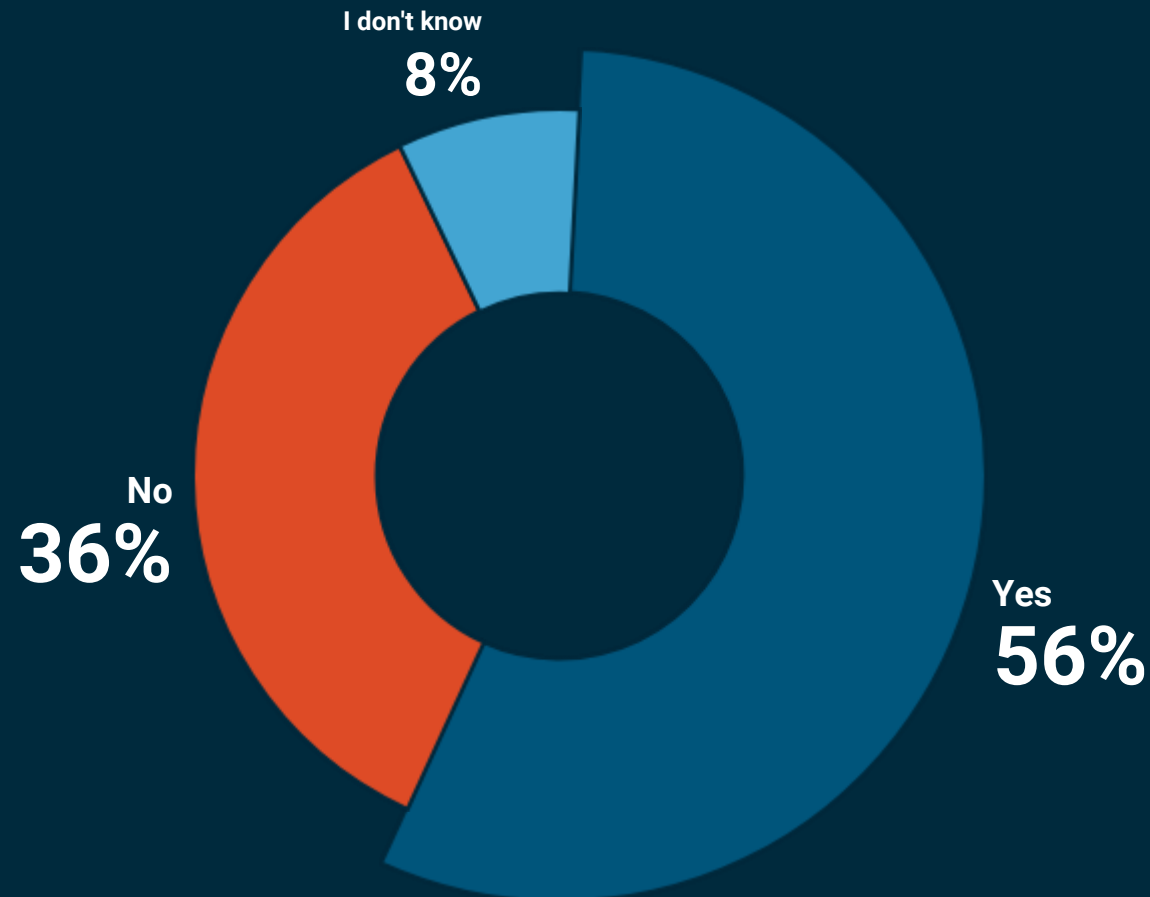
Endpoint Protection Platform

PEOPLE

PROCESS

TECHNOLOGY

Question: Does your company have an endpoint protection platform (EPP)?



Key Takeaways

- Best Practice Answer: Yes (56%).
- An EPP is a security solution designed to detect, prevent, and respond to cyber threats targeting endpoint devices such as laptops, desktops, and mobile devices.
- EPP solutions block ransomware, spyware, and other malicious software to protect endpoints from cyberattacks and prevent users from downloading malicious software.





Two-Factor Authentication

PEOPLE

PROCESS

TECHNOLOGY

Two-Factor Authentication (2FA), or Multi-Factor Authentication (MFA), protects organizations from compromised employee credentials by requiring something employees *know*—like a username and password, and something employees *own*—like a mobile device with a code to access systems.

61%

of SMBs require 2FA for email, including when access is through a web app or a personal device.

66%

of SMBs require 2FA for privileged users (admin accounts).

48%

of SMBs require 2FA for all employees & contractors on all systems.





Summary

Tools & Technology

PEOPLE

PROCESS

TECHNOLOGY

The foundation of a resilient cybersecurity strategy lies not just in having tools, but ensuring the right ones are in place and effectively used.

However, the report reveals that many SMBs lag in critical areas. **More than half of SMBs never perform internal or external vulnerability scans**, and only 18% provide password management tools to their employees. Additionally, while 61% require 2FA for email access, far fewer extend this protection to all employees and systems, leaving gaps that threat actors can exploit.

To build a stronger defense, organizations must prioritize tools that address unique risks while ensuring proper implementation and use. Regular vulnerability scans, widespread adoption of 2FA, and accessible solutions like password managers are essential to closing these gaps. When paired with clear processes and a proactive mindset, the right technology empowers organizations to stay ahead of evolving threats.





Vulnerability Scanning Insights

PEOPLE

PROCESS

TECHNOLOGY

SensCy analyzed external vulnerability scanning results to identify the most common security weaknesses.

At a high level, most organizations are not falling victim to sophisticated cyber threats — they are struggling with foundational security controls. The most common issues involve email protection, website security settings, and encryption configuration. While these are not advanced threats, they create serious exposure if left unaddressed.

What follows is a breakdown of the most common categories of risk, what they mean in everyday terms, and how widespread they are amongst organizations.





78%

of companies
scanned had at
least one email
security
vulnerability

Email Security Issues

PEOPLE

PROCESS

TECHNOLOGY

Email security controls prevent attackers from impersonating companies or sending fake emails that appear legitimate. When these controls are missing or misconfigured, organizations are vulnerable to phishing, business email compromise (BEC), and domain spoofing.

Most common issues found:

- **73% Misconfigured Domain-based Message Authentication, Reporting and Conformance (DMARC)**

What it is: A policy that tells email providers how to handle fraudulent emails pretending to come from your domain.

Risk: Without it, attackers can spoof your company and trick customers or employees.

- **53% Misconfigured DomainKeys Identified Mail (DKIM)**

What it is: A digital signature that verifies an email actually came from your domain.

Risk: Without it, email authenticity cannot be verified.

- **19% Misconfigured Sender Policy Framework (SPF)**

What it is: A record that specifies which mail servers are allowed to send email on your behalf.

Risk: Without it, threat actors can send unauthorized email appearing to come from you.





Domain Security Issues

PEOPLE

PROCESS

TECHNOLOGY

Domain Name System (DNS) is the system that translates your website name into an IP address. DNS security prevents attackers from redirecting traffic to malicious servers.

Most common issue found:

- **77% - Misconfigured Domain Name System Security Extensions (DNSSEC)**

What it is: A security extension that prevents DNS tampering.

Risk: Without DNSSEC, threat actors can redirect website visitors or intercept traffic.





Website Security Issues

PEOPLE

PROCESS

TECHNOLOGY

These vulnerabilities relate to how websites and web applications are built and configured.

Most common issue found:

- **Various website security issues were found, from insecure web headers to outdated plugins and mismanaged web forms**

What this means: Weaknesses in how websites handle input, sessions, or security controls.

Risk: Threat actors may exploit flaws to access data, inject malicious scripts, or compromise systems.





47%

of companies
scanned had at
least one
encryption
configuration
issue

Encryption Security Issues

PEOPLE

PROCESS

TECHNOLOGY

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protect data in transit between users and websites.

Most common issues found:

- **42% - improper SSL configuration**

What this means: Outdated encryption protocols or weak settings.

Risk: Threat actors can intercept sensitive data like passwords, credit card numbers, or personal information.

- **22% - Expired or no SSL certificate**

What this means: The bridge of trust and encryption between your server and your users is broken.

Risk: Threat actors can intercept sensitive data like passwords, credit card numbers, or personal information.





Software & Endpoint Exposures

PEOPLE

PROCESS

TECHNOLOGY

These findings relate to publicly exposed systems running vulnerable software.

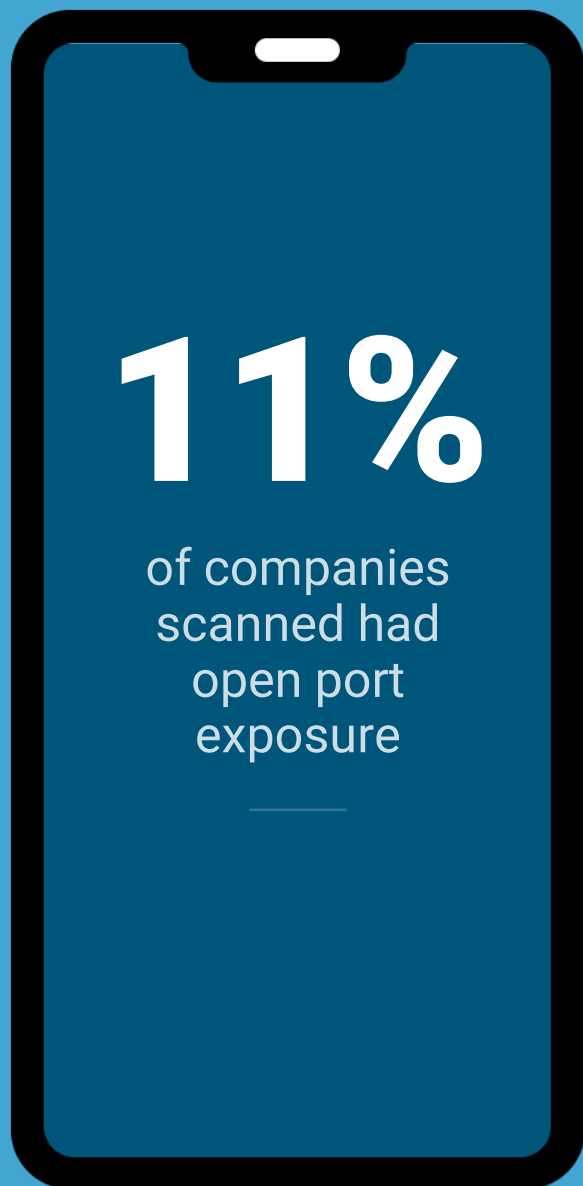
Most common issue found:

- **Various security issues were found on publicly facing desktop, mobile, and server software.**

What this means: Outdated or vulnerable software identified as fully accessible from the internet.

Risk: Known exploits can be used to gain unauthorized access.





Open Port Exposure

PEOPLE

PROCESS

TECHNOLOGY

Computers and servers use numbered *ports* to communicate. An open port exposure means a *door* to your network is open to the internet. Some ports need to be open to function properly. But if ports are left open unnecessarily, it's like leaving a door unlocked that leads to the outside of your building — even if you don't realize it's there.

Most common issue found:

- **11% - had open port exposure**

What it is: Network doors left open to the internet.

Risk: Threat actors can scan them, try to connect, and potentially exploit weaknesses in the services running behind them.





Summary

External Vulnerability Scans

PEOPLE

PROCESS

TECHNOLOGY

Across hundreds of organizations, the common thread isn't sophisticated cyberattacks – it's the incomplete implementation of foundational security controls.

These findings suggest a strong opportunity to standardize baseline security requirements, particularly around:

- Email authentication (DMARC, DKIM, SPF)
- DNS protection (DNSSEC)
- SSL/TLS hardening
- Web application security controls
- Open network ports

Tools &
Technology





Cybersecurity Insurance

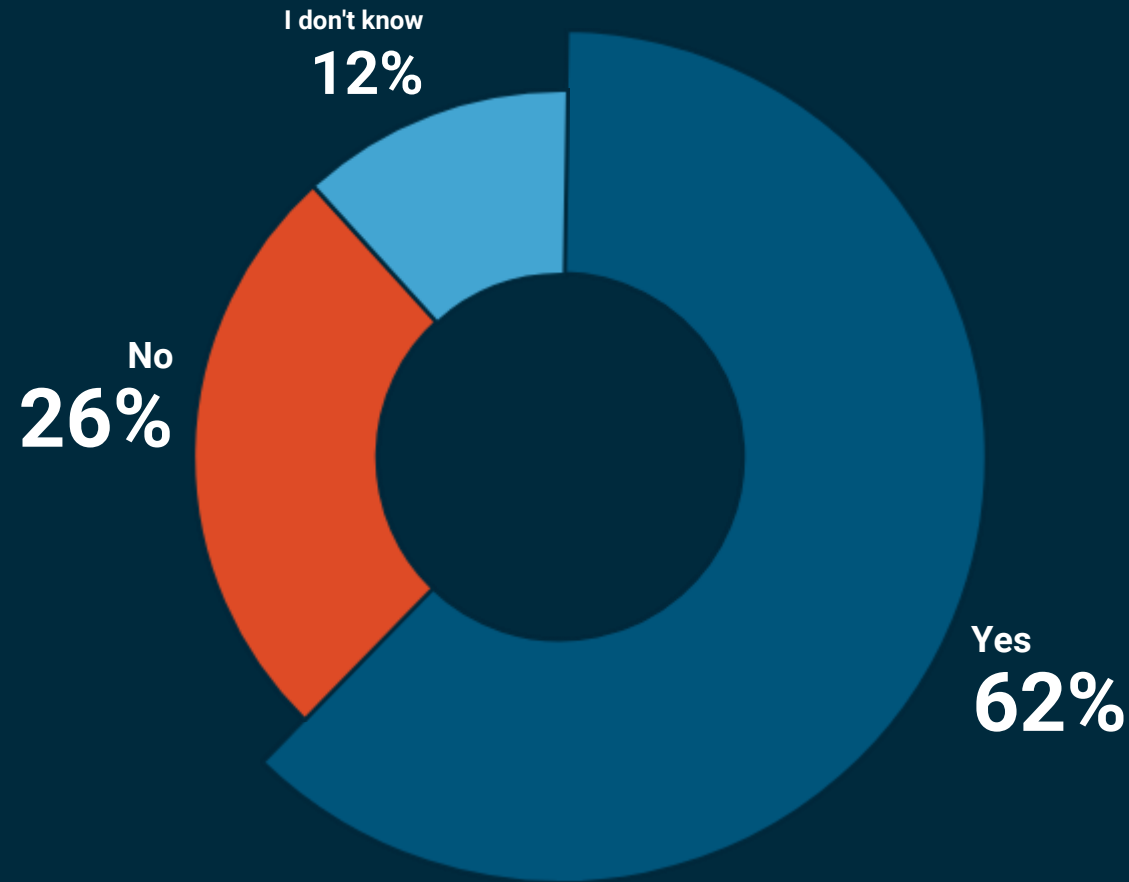
There are many costs associated with a cybersecurity incident, from investigative and recovery costs to legal expenses and regulatory fines. **The total cost can be hundreds of thousands, to millions of dollars** — depending on the severity of the incident.

While insurance cannot cure the reputational damage resulting from a cyber incident, it may prove critical to recovery should an incident occur.

The following section will look at how SMBs responded when asked about cybersecurity insurance.

Cybersecurity Insurance

Question: does your company have cybersecurity insurance?

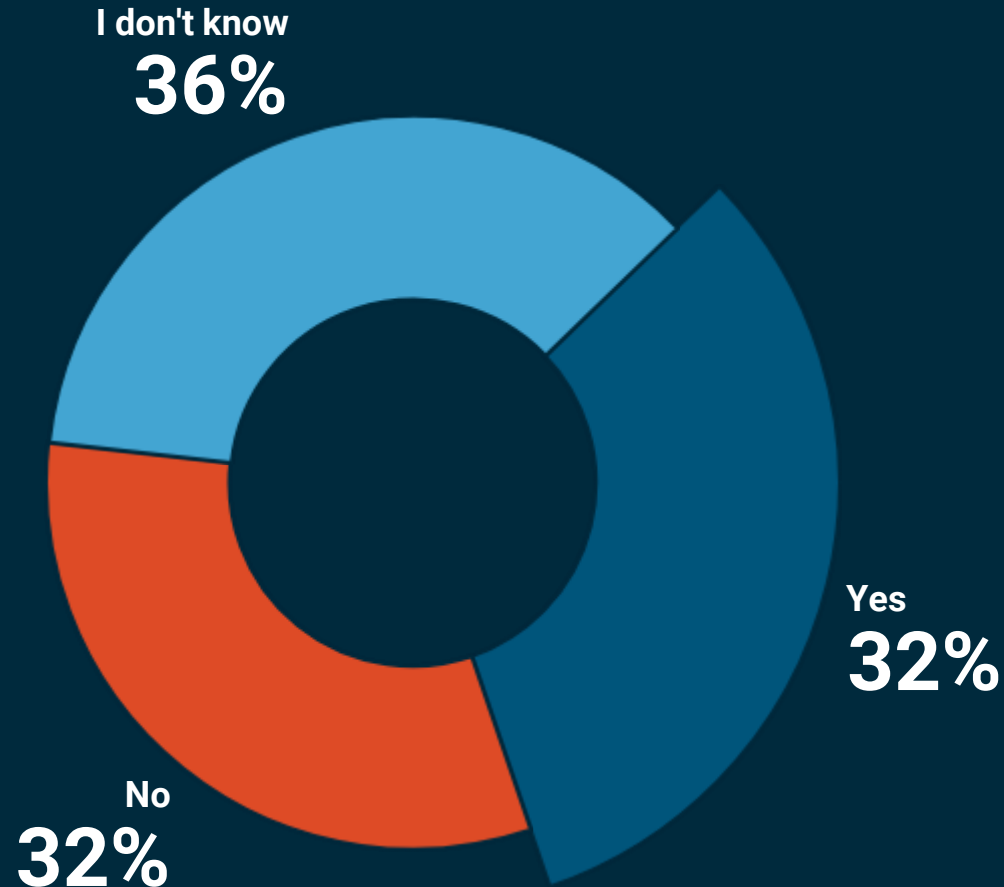


Key Takeaways

- Best Practice Answer: Yes (62%).
- While 62% of SMBs report they do carry cybersecurity insurance, SensCy has found that not all policies are sufficient to fully cover them in the event of an incident.
- SensCy recommends organizations thoroughly review and understand cybersecurity insurance policies to ensure adequate protection.

Ransomware Insurance

Question: does your cybersecurity policy cover ransomware?



Key Takeaways

- Best Practice Answer: Yes (32%).
- Not all cybersecurity insurance policies cover ransomware, often referred to as *extortion* in the insurance world.
- Ransomware is among the most costly of cybersecurity incidents, making it essential to ensure your policy includes ransomware coverage.





Conclusion

Positive Trends for SMBs

What follows are best practice cybersecurity controls adopted by more than 70% of SMBs surveyed.

While this is encouraging, it's important to note that with approximately 36 million SMBs in the United States, the 30% that are not in compliance with these controls could amount to over 10.8 million businesses.





Conclusion

What SMBs are Doing Well

SensCy has observed positive trends in the following areas, with SMB compliance on the rise.

83%

Restrict user rights using the principle of least privilege.

85%

Limit administrative rights to only those whose job it is to update technology.

83%

Pre-install antivirus software on all computers.

74%

Have taken the steps necessary to secure their Wi-Fi.

73%

Have a firewall at the network perimeter and have disallowed inbound connections.



Conclusion

The findings of this report reveal a significant gap in preparedness among SMBs, underscoring the need for accessible and practical cybersecurity solutions across three key areas: People, Processes, and Technology.



People. With human error responsible for 88% of successful cyberattacks, only 28% of leadership teams receive regular cybersecurity briefings, leaving organizations vulnerable to evolving threats.



Processes. While 61% of SMBs receive notifications of critical security patches, just 33% apply them within 48 hours, exposing systems to preventable risks.



Technology. Half of SMBs never conduct vulnerability scans, and only 48% require 2FA for all employees, leaving critical gaps in their defenses.

This report serves as a call to action for business leaders to transition from *reactive* to *proactive* measures. Cyber resilience is not only achievable — it is essential for long-term success.

Take the first step:
Get your SensCy Score®

Be Prepared.
Be Protected.
Act Now.



Scan the code to take the first step in making your organization safer.



About

SensCy

Your **Trusted Guide** to **Sensible Cyber**



At SensCy—short for Sensible Cyber—we believe every SMB deserves access to effective, approachable cybersecurity solutions. Based in Ann Arbor, Michigan, SensCy exists to simplify the complexities of the cyber landscape, empowering SMBs to protect their businesses and build a resilient future.

At the heart of our approach is the trusted NIST Cybersecurity Framework, which provides a clear path for evaluating and strengthening an organization's cyber readiness. Through this framework, we assess cybersecurity posture across six essential pillars: *Identify, Detect, Protect, Respond, Recover and Govern*.

SensCy is more than a platform — we're your partner in creating a foundation that prepares your organization to address challenges, adapt to changes, and safeguard what matters most.



Security Terms

Administrative Rights

Elevated system permissions that allow users to install software, modify settings, manage accounts, and access sensitive data on a computer or a network.

Awareness Training

Teaches employees how to recognize, prevent, and respond to cybersecurity threats — such as phishing, malware, and social engineering — to protect organizational data and systems.

Cloud Services & Access Management (CASB)

Provides visibility, control, and protection for cloud applications by enforcing security policies, preventing data leaks, and blocking unauthorized access to cloud services.

Data Loss Prevention (DLP)

Detects, monitors, and prevents unauthorized access, sharing, or transmission of sensitive data to protect against breaches and ensure compliance.



Security Terms

Dark Web

A hidden part of the internet used by cybercriminals to traffic in stolen data.

Encryption

The process of converting data into a coded format to prevent unauthorized access, ensuring confidentiality and security.

Endpoint

Any device that connects to a network – such as computers, laptops, smartphones, tablets, or servers – which can be targeted by threat actors and require security protection.

Endpoint Detection & Response (EDR)

Monitors, detects, and responds to threats on endpoint devices in real time, using advanced analytics and automation to prevent cyberattacks.



Security Terms

Endpoint Protection Platform (EPP)

Endpoints are devices like laptops and smartphones. EPPs protect these devices from ransomware and other threats.

Firewall

A device or software that monitors and filters incoming and outgoing internet traffic based on predefined security rules, blocking unauthorized access while allowing legitimate communication.

Incident Response Plan

A structured document outlining procedures for responding to, mitigating, and recovering from cybersecurity incidents to minimize damage and reduce downtime.

Malware

Any software designed to harm, exploit, or compromise systems, networks, or devices.



Security Terms

Mobile Device Management (MDM)

Requires something you *know* like a username and password and something you *own* like a mobile device with a code in order to access systems.

Password Manager

A security tool that stores, generates, and auto-fills strong, unique passwords for all accounts, helping users manage credentials and protect against cyber threats.

Penetration Testing

A simulated cyberattack conducted by ethical hackers to identify vulnerabilities in an organizations' systems, networks, or applications.

Phishing

A cyberattack that uses email to impersonate legitimate entities and trick individuals into providing sensitive information, such as passwords or financial data.



Security Terms

Phishing Simulations

Controlled cybersecurity exercises that mimic real phishing attacks to test and educate employees to recognize phishing threats, helping to strengthen an organization's security awareness.

Principle of Least Privilege

Restricts user and system access to only the minimum permissions necessary to perform job duties, reducing the risk of unauthorized access and potential security breaches.

Privileged Access Management (PAM)

Controls, monitors, and secures access to critical systems and sensitive data by restricting elevated permissions to authorized users only, reducing the risk of insider threats and cyberattacks.

Privileged Users

Individuals with administrative control over systems, networks, or data, allowing them to modify configurations, manage user accounts, and access sensitive information.



Security Terms

Ransomware

A type of malware that encrypts a victim's data and demands payment (ransom) to restore access. Involves threat of data deletion or public release if unpaid.

Security Information & Event Management (SIEM)

Collects, analyzes, and correlates log data from multiple sources in real time to detect, respond to, and manage cybersecurity threats and compliance requirements.

Security Patch

A software update that fixes vulnerabilities, bugs, or weaknesses in a system to protect against cyber threats and data breaches.

Tabletop Exercise

A discussion-based drill where key stakeholders test and evaluate an organization's incident response plan by responding to a hypothetical cyber threat in a controlled environment.



Security Terms

Two-Factor Authentication (2FA)

Requires something you *know* like a username and password and something you *own* like a mobile device with a code in order to access systems.

Vulnerability

A flaw or weakness in a system that can be exploited by threat actors to gain unauthorized access or cause harm.

Vulnerability Scan

An automated assessment that identifies security weaknesses and helps organizations detect and mitigate vulnerabilities.

Virtual Private Network (VPN)

A VPN creates a secure communication tunnel, encrypting data between your remote workers and your organization.





Suggested Citation (for Research & Media)

SensCy. (2026). 2026 SMB Cybersecurity Statistics & Benchmark Report (Executive Summary).

Retrieved from: <https://senscy.com/how-prepared-are-small-and-medium-sized-businesses-for-cyber-attacks/>