
2026
Small Business Cybersecurity Awareness & Practices Survey
NATIONAL CYBERSECURITY ALLIANCE

2026 Small Business
Cybersecurity
Awareness & Practices
Survey

# Executive Summary

Small and medium-sized businesses are the backbone of the American economy — and an increasingly attractive target for cyber threats. Yet for many, the gap between awareness and action remains wide. This report presents findings from a comprehensive survey of 1,000 SMB leaders, offering an unvarnished look at where businesses stand today: what protections they have in place, where critical gaps persist, and what it will take to build a more resilient small business community.

The results reveal a landscape defined by four interconnected tensions: a confidence that outpaces readiness, security tools that are adopted but not fully operationalized, AI that is embraced faster than it is governed, and a workforce that is eager to learn but often left without a clear roadmap. These are not failures of intent — they are failures of infrastructure, guidance, and prioritization. Addressing them is both urgent and achievable.

## SURVEY AT A GLANCE

**1,000**
**SMB leaders surveyed**
Across the U.S.

**2–1,000**
**Employee range**
Micro-SME to mid-market

**10**
**Industries represented**
Including tech, healthcare, financial services, and retail

C-suite to manager — all respondents hold decision-making authority

# Key Findings

### THE VISIBILITY GAP IS REAL.

A combined 56.1% of SMBs cannot confirm a clean security record over the past 12 months — 50.5% reported a confirmed or suspected incident, while an additional 5.6% were unsure whether a breach had even occurred. For many organizations, the danger isn't just the attack itself; it's not knowing when one has happened.

### RISK IS GROWING, BUT CONFIDENCE REMAINS HIGH.

Nearly three-quarters of SMB leaders (72.3%) report that their cyber risk has either increased or stayed the same over the past year. Yet 86.3% maintain medium-to-very-high confidence in their ability to manage that risk. This confidence gap — between how secure leaders feel and how prepared they actually are — is one of the most consequential findings in this report.

### TOOLS ARE IN PLACE. BEST PRACTICES ARE NOT.

Most SMBs have adopted foundational security controls, but adoption alone is not protection. While 86.8% have implemented multi-factor authentication, only 51.1% require it across all key business accounts. While 88.4% have data backups, only 61.4% have actually tested them. Having a tool and using it correctly are two different things — and the gap between them is where attacks succeed.

### AI ADOPTION HAS OUTPACED AI GOVERNANCE.

AI use among SMBs has reached 87.3%, driven primarily by the desire to save time and automate routine work. Yet only 45.6% of organizations have implemented formal guidelines for AI use, leaving the majority of the workforce navigating sensitive data privacy and security decisions without a clear policy framework.

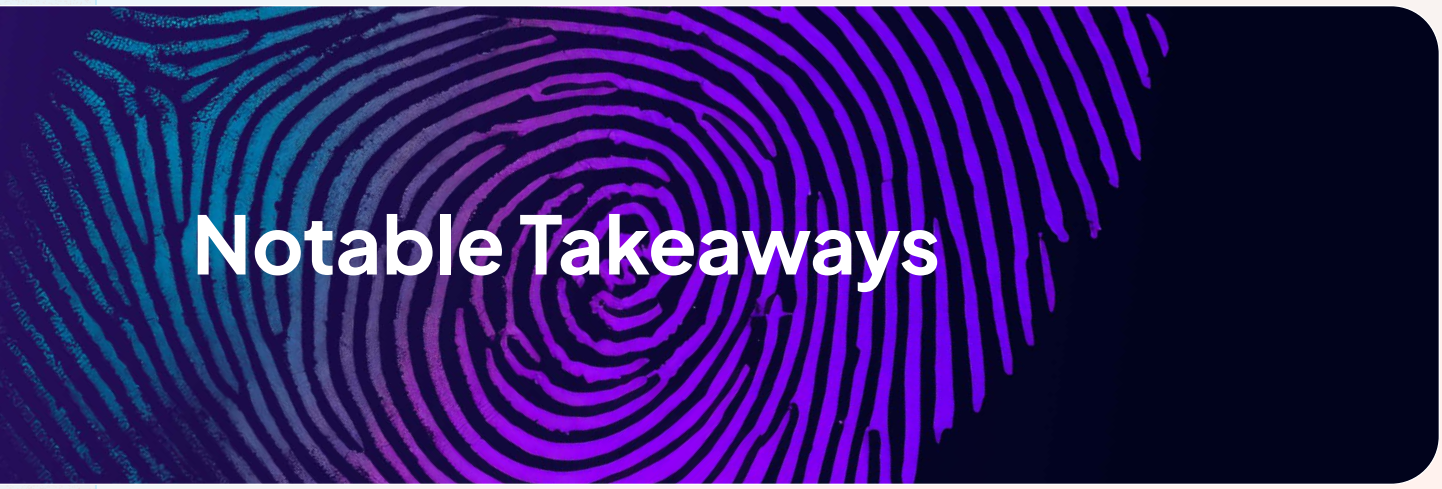
### SMB LEADERS WANT TO ACT — AND ARE ASKING FOR GUIDANCE.

The appetite for education is strong: 55.7% of leaders say they are likely or very likely to participate in a free or low-cost cybersecurity training program within the next six months. The top requested resources — employee training, leadership guidance on risk management, and incident response templates — point to a workforce ready to engage when given the right tools and direction.

---

NATIONAL CYBERSECURITY ALLIANCE

This report was developed in partnership between the National Cybersecurity Agency and CISA.



# Notable Takeaways

## VISIBILITY GAP

A combined 56.1% of SMBs are unable to confirm a clean security record over the past 12 months. While 50.5% reported a confirmed or suspected incident, an additional 5.6% admitted they were “not sure” if a breach had occurred. This suggests that for many organizations, the primary risk isn’t just the attack itself, but a lack of internal telemetry and logging to identify when an intrusion has actually happened.

When parsing by industry, technology/software/telecommunications employees had the highest incidence rate, with 76.4% reporting a confirmed or suspected incident/not sure. Financial services/insurance (67.1%), manufacturing/engineering/industrial (58.1%), and healthcare (58.2%) were all also above the overall rate.

**56.1%**

**are unable to confirm a clean security record**

## THE “STATUS QUO” RISK

Nearly three-quarters of SMB leaders (72.3%) report that their cyber risk has either increased or remained stagnant over the last 12 months. With only 17.9% seeing a reduction in risk, it is clear that for the vast majority of organizations, security efforts are, at best, only keeping pace with the threat landscape.

**72.3%**

**report increased or remained stagnant cyber risk**

## THE SMB CONFIDENCE PARADOX

Despite 72.3% of leaders reporting that their cyber risk is either increasing or holding steady, there is a high sense of personal and organizational efficacy. 86.3% of respondents maintain “Medium” to “Very High” confidence in their ability to manage risk, and 58.8% are highly confident they could recover quickly from being taken offline for a day or more. This suggests a potential gap between perceived readiness and the reality of an intensifying threat landscape.

72.3%

**86.3%**

**maintain “Medium” to “Very High” confidence**

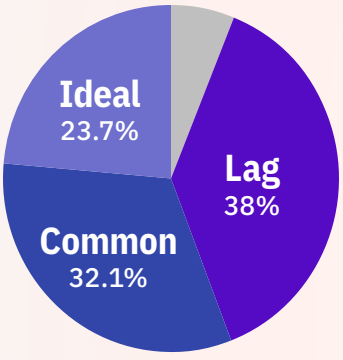
## MATURITY GAP

There appears to be a maturity Gap between adopting a security tool and operationalizing it to its full potential.

While a majority (86.8%) of organizations have implemented Multi-Factor Authentication (MFA), only 51.1% meet the best practice of requiring it for all key business accounts. Over one-third of businesses (35.7%) only require MFA for “some” accounts, creating a significant security “blind spot” that attackers can exploit to gain lateral access.

There appears to be a disconnect between having a backup and ensuring it actually works. While 88.4% of businesses have backups, only 61.4% follow the best practice of regularly testing those backups indicating over a quarter of the market (27%) is relying on “untested” backups. In a real-world ransomware scenario, these businesses are at high risk of discovering their data is unrecoverable only after it’s too late.

Leadership awareness is high, but the frequency of review suggests that for many, cybersecurity is treated as a periodic event rather than a continuous business risk.




**The Ideal:** Only 23.7% of organizations meet the best practice of evaluating cybersecurity as a business risk on a monthly basis.

**The Common Practice:** Most leadership teams (32.1%) default to a quarterly review. While quarterly is better than nothing, it may not be frequent enough to respond to the rapid 12-month risk increase noted in your earlier data.

**The Lag:** Nearly 38% of leaders evaluate security only “sometimes,” “rarely,” or “never,” indicating that for a large portion of the market, security remains a reactive rather than proactive priority.

## AI GOVERNANCE LAG

While AI adoption has reached 87.3% among SMBs, policy development is struggling to keep pace. Only 45.6% of organizations surveyed have implemented formal guidelines, leaving a significant portion of the workforce to navigate complex data privacy and security risks without a clear roadmap. The most common reason cited for AI adoption was “to save time or automate routine tasks,” with nearly half of respondents (49.1%) citing this use case.



**45.6%**

**have implemented formal guidelines**

## RELIANCE ON “HUMAN-FIRST” DEFENSES

When asked what tools or support would be most helpful, the data shows a heavy reliance on educational and training-based defenses over technical infrastructure. 42.4% of respondents prioritize “short training for employees,” and 44% are looking for “guidance or training for business leaders on how to manage risk.”

There is a strong appetite for low-cost resilience; 55.7% of leaders indicated they are “likely” or “very likely” to participate in free or low-cost non-technical training programs in the next six months.

This focus on training exists even though leaders identify social engineering/email scams (49.1%) and vulnerable websites (27.2%) as their top areas of vulnerability. While training addresses the human element, it leaves the technical vulnerabilities (like unpatched websites or lack of MFA) secondary to behavioral change.



**44%**

**are looking for guidance or training**



**55.7%**

**are likely to participate in free or low-cost training**

# Segmented Findings

## BREACHED VS. NOT BREACHED

### Breach victims have better readiness

Companies that have experienced a breach consistently report stronger cybersecurity preparedness behaviors than those that have not, suggesting that many organizations may only operationalize security best practices after experiencing an incident.

Incident response planning shows the largest gap. Nearly three-quarters of breached organizations (74.9%) report having a documented and followed response plan, compared with 51.5% among companies that have not experienced a breach. Conversely, organizations without a breach are five times more likely to report having no response plan at all (30.3% vs. 5.9%), indicating that many businesses remain unprepared until a real-world event forces process changes.

Security controls follow a similar pattern. Businesses that have experienced a breach are significantly more likely to enforce multi-factor authentication (MFA) across most or all key accounts (58.4% vs. 44.8%), while companies without a breach are more than twice as likely to report not using MFA at all (13.8% vs. 5.9%). Backup readiness also differs: 70.3% of breached organizations report having tested backups, compared with 53.8% of those without a breach, suggesting that organizations that experience incidents place greater emphasis on recovery preparedness.

Leadership oversight also appears stronger among organizations that have experienced incidents. Nearly one-third of breached organizations review cybersecurity risk monthly (31.5%), compared with 19.8% of organizations without a breach, while companies without an incident are more likely to review cybersecurity only rarely or never (17% vs. 4.8%). Taken together, the data suggests a clear pattern: organizations that have experienced a breach tend to develop stronger governance, controls, and recovery practices – often as a direct response to the incident itself – while those without that experience are more likely to lag in proactive preparedness.

## AI ADOPTION AND USE × BUSINESS SIZE

### AI Adoption and Use × Business Size

While efficiency is the primary driver of AI adoption across businesses of all sizes, the specific motivations evolve as organizations grow. Across every company size segment, the most common reason for adopting AI is to save time or automate routine tasks, cited by roughly 44–50% of companies with fewer than 250 employees and rising to 63.6% among organizations with 501–1000 employees. Smaller businesses appear to be adopting AI more cautiously overall, with 20% of companies with fewer than 50 employees reporting they have not adopted AI tools, compared with just 2.3% among the largest companies surveyed.

As companies scale, AI use cases begin to expand beyond efficiency into customer experience and strategic experimentation. The share of businesses using AI to improve customer service or responsiveness increases steadily with company size, rising from 21% among the smallest businesses to 47.6% among companies with 250–500 employees. Larger SMBs are also more likely to adopt AI to explore new capabilities, suggesting that while smaller organizations focus primarily on operational productivity, larger businesses increasingly view AI as a tool for innovation and competitive advantage.

### AI Tool Usage × Business Size

General-purpose AI tools dominate adoption across businesses of all sizes, with ChatGPT emerging as the most widely used platform. Usage ranges from 44.1% among companies with fewer than 50 employees to over 63% among organizations with 250–1000 employees, indicating that conversational AI tools are often the first entry point into AI for SMBs. Other widely adopted platforms follow a similar pattern: Google Gemini usage increases from 35.9% among the smallest firms to 50.8% among the largest, while Microsoft Copilot adoption rises from 30.7% to over 43%, suggesting that AI usage becomes more integrated into daily workflows as organizations grow.

As company size increases, businesses also appear more likely to layer AI into existing software and specialized tools rather than relying solely on standalone applications. The use of AI features built into existing software nearly doubles from 13.8% among the smallest firms to 26.5% among companies with 501–1000 employees, while industry-specific AI tools rise from 12.8% to 18.2%. At the same time, smaller businesses are more likely to report having no AI tools at all, with 13.8% of firms with fewer than 50 employees indicating no AI use compared with just 3% among the largest organizations surveyed. This pattern suggests a progression in adoption maturity: smaller businesses tend to experiment with a limited set of tools, while larger SMBs increasingly integrate AI across multiple platforms and workflows.

# Recommendations

As AI adoption accelerates among small businesses, the survey findings make clear that usage is outpacing governance. With nearly 88% of small business owners already using AI tools, but only a fraction operating under formal policies, many organizations are exposed to avoidable risks — from unintentional data leaks to reliance on inaccurate AI-generated content.

The following recommendations are designed to help small businesses close that gap. Rather than choosing between innovation and security, these practical, low-cost safeguards allow businesses to continue benefiting from AI while protecting sensitive information, maintaining compliance, and building a culture of responsible use across their teams.

# Four Best Practices for AI Adoption

1

### CREATE AN AI ACCEPTABLE USE POLICY (AUP)

Establish written rules defining what information can never be entered into public AI tools (PII, protected health information, financial records, customer data, trade secrets, proprietary code). The policy should also specify which AI tools employees are authorized to use.

2

### KEEP HUMANS IN THE LOOP

Require human review of all AI-generated output before it's used externally or for decision-making — e.g., developers reviewing AI-generated code before deployment, and marketing teams fact-checking AI content before publication. A formal review process should be built into workflows.

3

### CHOOSE BUSINESS-FRIENDLY AI PLATFORMS

Favor business/enterprise-tier AI tools over free consumer versions, since they typically offer stronger contractual data protections, administrative controls, and clearer privacy commitments. Businesses should review each platform's privacy policy, security controls, and data retention practices before adoption.

4

### TRAIN EMPLOYEES ON AI RISKS

Provide regular, short (15–30 minute) training sessions covering safe data handling, recognizing AI-related phishing/deepfake threats, and distinguishing public AI tools from approved enterprise solutions. The survey found 40%+ of small business owners cited brief training as their most-needed resource.

Taken together, these practices show that responsible AI adoption doesn't require sacrificing the efficiency gains AI offers — it requires intention. A written policy, thoughtful platform selection, consistent human oversight, and ongoing employee training form a practical foundation that small businesses can implement at low cost and with minimal complexity. As AI tools continue to evolve and become further embedded in daily operations, businesses that establish these guardrails now will be better positioned to innovate confidently, protect their data and customers, and avoid the costly setbacks that come from unmanaged or ungoverned use.

**NATIONAL CYBERSECURITY ALLIANCE**

A leading non-profit organization, the National Cybersecurity Alliance (NCA) is dedicated to creating a more secure, interconnected world. Advocating for the safe use of all technology, the NCA aims to educate everyone on how best to protect themselves, their families, and their organizations from cybercrime. The organization also creates strong partnerships between governments and corporations to foster a greater "digital" good and amplify the message that only together can we realize a more secure, interconnected world.

staysafeonline.org


cisa.gov

This material is based upon work funded by the Cybersecurity and Infrastructure Security Agency (CISA), part of the U.S. Department of Homeland Security (DHS), under Grant Award Number 23CISCSA00005. The views and conclusions in this document (article/survey/etc.) are those of the authors and do not necessarily reflect the official views of CISA or DHS. CISA does not endorse any commercial products or services; any mention of specific products or services should not be interpreted as an endorsement or recommendation by CISA.