

2025

IT Trends

for Small and Medium Businesses

Top IT Priorities and Challenges

Table of Contents

Introduction.....	3
Executive Summary.....	4
How SMBs Manage Their IT	8
Cybersecurity.....	16
Cloud Services and AI.....	28
Top IT Investments for the Year.....	34





Over the last 30+ years, we have helped build thriving communities of happy, productive, and supported businesses. As of 2025, we serve more than 550 small and medium-size businesses (SMBs), helping them anticipate and mitigate risk, simplify their IT footprint, and optimize their IT spend.

Our passion for SMBs is based on the huge effect they have on the world¹:

- Small businesses created over 70 percent of net new jobs since 2019.¹
- SMBs keep the local communities thriving by creating local jobs and sourcing local supplies (which in turn creates jobs with those vendors).²
- Companies with fewer than 250 employees account for 44% of all private employment jobs in the country.¹

But there are also some real risks for SMBs:

- 23.2% of private sector businesses in the U.S. fail within the first year. After five years, 48.0% have faltered. After 10 years, 65.3% of businesses have closed.³
- Inflation is a key reason for businesses to fail.⁴
- Any kind of cyberattack has the potential to shut a small business down.⁵

Our annual IT survey will reveal industry trends and give you an idea of what other business owners are thinking about—along with how IT can be used to support growth. Our quarterly reports will provide detailed insights into key topics like cybersecurity, productivity enhancers, scalability and reliability for cloud solutions, and the relevance and application of AI. This information is designed to help SMBs plan for business growth without feeling unprepared for unforeseen events like the pandemic.

The beginning of a new year is a fitting time to reflect on what makes your business move forward—and what introduces risk. This reflection can help you set the right priorities for the year ahead.



Naveen Rajkumar
CEO & President, ISOutsourcing

¹U.S. Department of Treasury, "Small Business and Entrepreneurship in the Post-COVID Expansion," September 2024.

²GovPilot.com, "Why Supporting Local Businesses In Your Community Is Vital."

³Vena Solutions, "What Percentage of Businesses Fail? Averages by Time, Industry and Locale," September 2024.

⁴CashFlowFrog.com, "10 Reasons Why Small Businesses Fail," October 2024.

⁵Cybercrime Magazine, "60 Percent of Small Companies Close Within 6 Months of Being Hacked," January 2019.



Executive Summary

This report presents the findings from a 2024 survey on the state of IT in small and medium businesses. Survey findings, which are detailed throughout this report, include:

CHALLENGES IN REMOTE AND HYBRID WORK:

Key challenges include managing devices (23%), connectivity issues (23%), and ensuring secure collaboration (22%).

SMBs leverage solutions like endpoint management and unified communication tools to address these concerns.

STRATEGIC IT INVESTMENTS:

52% of businesses focused on optimizing IT spending, while 41% prioritized recruiting skilled IT talent.

Top investment priorities include aligning IT with business goals, addressing security risks, and maximizing ROI.

IT MANAGEMENT MODELS:

IT gaps include project management (44%) and data security (39%), key areas where IT can better support business needs.

CYBERSECURITY AS A TOP PRIORITY:

48% of SMBs reported experiencing security threats in the past year, emphasizing the critical need for robust cybersecurity measures.

16% of respondents lack a disaster recovery plan, while 18% lack cybersecurity insurance.

Top cybersecurity concerns include data breaches (35%), phishing attacks (29%), and ransomware (10%).

ADOPTION OF CLOUD AND AI:

94% of SMBs have integrated cloud services, citing flexibility (23%), scalability (22%), and cost savings (21%) as primary motivators.

AI and automation are gaining traction, with applications in marketing (25%), customer service (23%), and operations (22%).

Our Respondents

We conducted a survey targeting 50,000 small and medium-sized businesses across the United States. We received responses from 221 SMBs¹ representing a diverse range of industries, including technology, business services, architecture, engineering, and construction (AEC), healthcare, consumer services, financial services, manufacturing, legal, artificial intelligence (AI), public sector, professional services, and tourism and hospitality.

Companies' annual revenue



¹Gartner: Small businesses make less than \$50 million annually, and mid-size businesses make less than \$1 billion annually.
www.gartner.com/en/information-technology/glossary/smbs-small-and-midsize-businesses

Q: What are your company's annual revenues?



Executive Summary

In today's interconnected world, small and medium-sized businesses (SMBs) operate in an increasingly complex digital environment, where technology adoption, cybersecurity, and workforce optimization are critical to their success.

The 2025 SMB IT Trends Report sheds light on the priorities, pain points, and opportunities shaping the IT strategies of SMBs across diverse industries, including technology, healthcare, financial services, manufacturing, and more.

Regardless of industry, SMBs handle sensitive data—from payment details and proprietary business information to customer and employee personal records—that malicious actors can exploit. Threats include data ransom, spear phishing attacks, and the illicit sale of information on the dark web, making SMBs a prime target for cybercriminals.

Proactive cybersecurity measures are no longer optional—they are a critical component of business resilience. Investing in robust security solutions, conducting regular security assessments, and establishing comprehensive disaster recovery plans are essential to mitigating the growing risk of cyberattacks. These actions safeguard valuable assets, protect a company's reputation, and ensure business continuity in an evolving threat landscape.

The challenges facing SMBs extend beyond cybersecurity. The IT skills shortage remains a pressing issue, with 90% of organizations expected to experience severe impacts, resulting in up to \$6.5 trillion in losses by 2025. SMB IT leaders often operate under significant time and budget constraints, slowing progress in acquiring talent and implementing necessary technological initiatives. This resource gap amplifies the urgency for SMBs to optimize their IT strategies and build resilient infrastructures.

The stakes are high: Customer trust hinges on adequate data protection. Consumers, who are increasingly aware of data breaches, will not hesitate to shift their business elsewhere if they perceive a lack of security. Even the slightest lapse in preparedness—whether due to a natural disaster or a cyberattack—can lead to catastrophic business disruptions, from halted operations to significant financial losses. Downtime for a single day can harm a company's continuity and erode customer loyalty.

This report's findings emphasize the need for SMBs to take proactive measures to strengthen their IT infrastructure, safeguard against cyber threats, and build resilient systems that support business continuity. As SMBs strive to do more with fewer resources, effectively leveraging technology will be the key to overcoming challenges and unlocking growth opportunities.

Top IT Pain Points: Addressing Business Challenges



SECURITY



BUDGET



TALENT



AI

Top IT Concerns for SMBs based on the survey results.

- **Security & Ransom Attacks.** Cybersecurity threats, data breaches, and vulnerability management. The increasing frequency of ransomware attacks poses a significant threat, leading to data corruption, downtime, and potential financial penalties.
- **Budget constraints.** Limited IT budgets hinder investment in critical technologies and infrastructure.
- **Talent acquisition & development.** The increasing demand for skilled IT professionals makes it challenging to recruit, train, and retain talent, impacting efficiency and innovation.
- **AI Application Management.** The complexities of deploying, monitoring, and maintaining AI systems.

HOW SMBs MANAGE THEIR IT





Insights and Industry Breakdown


The data shows that businesses are taking diverse and innovative approaches to manage their IT, with no single dominant model. The choice between in-house, outsourced, or hybrid depends on a variety of factors, including company size, industry, budget, and specific IT requirements. This diversity demonstrates the adaptability and flexibility of businesses in meeting their unique IT needs.

(54%) of SMBs in the technology sector favor having an in-house IT department. This is due to the need for specialized skills and control over their technology stacks. Since these companies are immersed in technology, they may feel more comfortable hiring and working with internal IT staff.

Business Services prefers a hybrid approach (63%), to balance cost efficiency with specialized IT expertise. Their familiarity with offering and consuming professional services could be a factor also.

Other industries demonstrate a more balanced mix of in-house, outsourced, and hybrid models, suggesting diverse needs and priorities.

Q: Do you have an in-house, outsourced, or hybrid IT team?



“By outsourcing some of our IT operations to ISOutsource, we have greatly improved our cybersecurity, successfully defended against multiple cyberattacks, and protected our critical data and business.”

— Manager, Technology Company

45%

In-House

45% of SMBs rely on an in-house IT team to manage their technology needs. To work well, this option requires attracting and retaining skilled IT talent. SMBs who have in-house IT teams also occasionally use external managed services providers (MSPs) with specific skillsets to perform vulnerability assessments, implement Cybersecurity Maturity Model Certification (CMMC), and/or apply their knowledge of regulatory compliance (HIPAA, etc.) to certain projects.

25%

Outsource

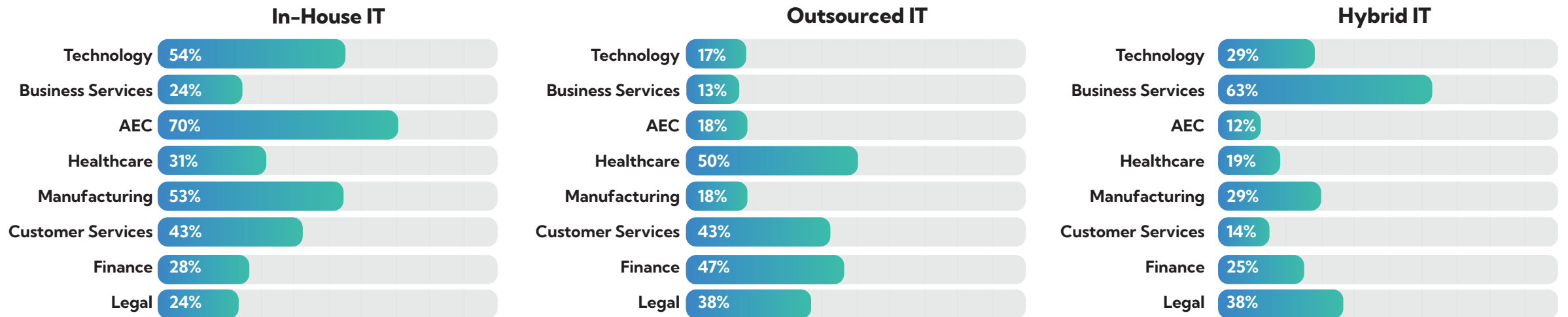
25% of SMBs fully outsource their IT services. This option can provide access to specialized skills and cost savings, particularly for smaller businesses that may not have the resources to maintain a full in-house IT department. The size of the business is a factor also, as smaller businesses might not have the budget or even enough work for a full-time IT resource.

30%

Hybrid

30% of SMBs use a hybrid approach, combining in-house expertise with outsourced services. This strategy allows companies to retain control over critical IT functions while using external providers for specific needs or projects. These businesses can quickly call on their IT partners' expertise thanks to their existing relationship.

How Different Industries Approach IT: In-House, Outsourced, or Hybrid?



Navigating the Challenges of a Remote/Hybrid Workforce

Businesses are embracing flexibility and overcoming IT challenges to offer remote and hybrid work options.

90% of businesses have at least **26%** or more of their workforce operating remotely or in a hybrid model.

Top IT challenges faced in supporting remote/hybrid work



Managing Devices (41%): Ensuring security, compatibility, and proper maintenance of devices used outside the traditional office environment.



Connectivity Issues (41%): Providing reliable and secure internet access for remote employees.



Security Concerns (40%): Protecting sensitive data and systems accessed from various locations and networks.



Collaboration Challenges (39%): Facilitating effective communication and teamwork among dispersed employees.

Top IT Challenges Supporting Remote/Hybrid Workforce

41% Managing Devices

41% Connectivity Issues

40% Security Concerns

39% Collaboration Challenges

Q: What are the biggest IT challenges you have faced in supporting a remote or hybrid workforce? (Select all that apply)

Opportunities

For **device management**, SMBs can start by ensuring most devices get regular software updates. They should consider investing in comprehensive endpoint management solutions. These tools will provide centralized control over all devices, enabling IT teams to monitor, manage, and secure endpoints effectively. Efficient device provisioning can also simplify the set-up and deployment of new devices.

If an SMBs' Internet Service Provider (ISP) is not reliable, it might be time to consider a new provider to solve **connectivity issues**. There are virtual private network (VPN) and software-defined wide area network (SD-WAN) options as well, along with bandwidth management tools.

MFA can add an extra, yet critical, layer of security to users' logins. There are many good endpoint security solutions, including antivirus, anti-malware, and firewall toolsolutions, which are essential for protecting devices from various cyber threats. Developing, testing, and regularly updating an incident response plan is crucial for minimizing the impact of security breach incidents. An SMB's plan should outline steps for detecting, responding to, and recovering from incidents.

Collaboration issues can often be addressed with updated tools, including Microsoft 365 and Google Workspace. A unified communication solution can integrate various communication channels (e.g., email, chat, video conferencing) into a single platform, enhancing collaboration and productivity.



How SMBs Allocate and Optimize Tech Investments

Majority of businesses (90%) dedicate 5% of their overall budget to IT, indicating a significant investment in technology. Only 10% allocate less than 5% of the budget to IT.

Top priorities when making IT investment decisions:

- **Aligning with business goals (48%)** to ensure IT investments support overall strategic objectives and drive business growth.
- **Addressing security risks (45%)** to prioritize investments in cybersecurity and protect critical assets and data.
- **Maximizing ROI (37%)** to focus on IT solutions that deliver a strong return on investment and contribute to business value.
- **Supporting growth initiatives (41%)**. SMBs are investing in IT solutions that streamline workflows, automation tasks, and optimize processes to enhance overall productivity and reduce operational costs.

Top IT Investment Priorities

48% Aligning with Business Goals

45% Addressing Security Risk

37% Maximizing ROI

41% Supporting Growth Initiatives

Q: Do you prioritize IT investments in your business? (Select all that apply)

Insights

Small and medium businesses are balancing their immediate IT needs and long-term goals. Especially for smaller businesses, immediate operational needs might take precedence over long-term IT investments. This explains the lower budget allocation in some cases. However, even these businesses recognize the importance of strategic IT investments to address pressing issues like security and operational efficiencies.

For other companies, aligning IT investments with long-term strategic goals ensures sustained growth and competitiveness. By focusing on cybersecurity, return on investment (ROI), and growth support, businesses can build a resilient and adaptable IT infrastructure that meets both current and future needs.



Cybersecurity:

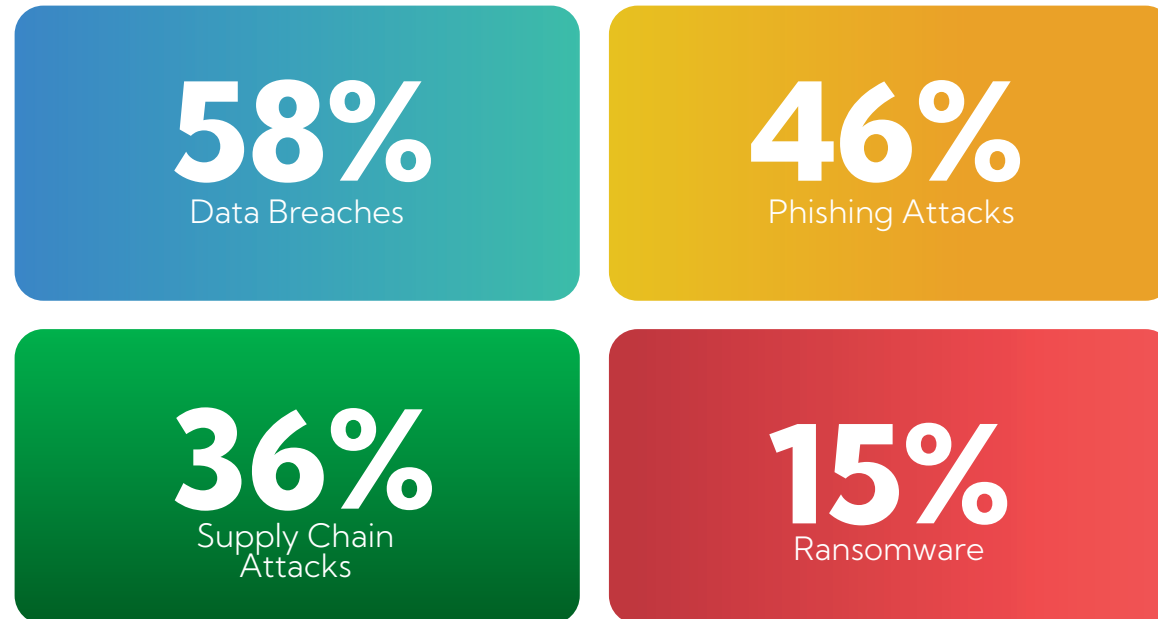
A Looming Threat for SMBs

In today's interconnected world, where businesses rely heavily on technology, cybersecurity is no longer an extra but a critical necessity. Cyberattacks can have devastating consequences, from financial losses and reputational damage to disruption of operations and loss of sensitive data. This report reveals the top cybersecurity concerns for SMBs and highlights the urgent need for proactive measures to mitigate these risks.



Identify Your Top Cybersecurity Concerns: Emerging Threats That Worry You Most

Cybersecurity is a critical concern for businesses today. Our survey revealed that SMBs are most concerned about these cybersecurity threats:



Q: Which emerging cyber threats are you most concerned about for your business? (Select all that apply)

Data Breaches (58%): Unauthorized access to sensitive information, such as customer data, financial records, personally identifiable information (PII), and intellectual property, poses a significant risk to businesses, potentially resulting in regulatory fines, legal action, and irreparable damage to their reputation.

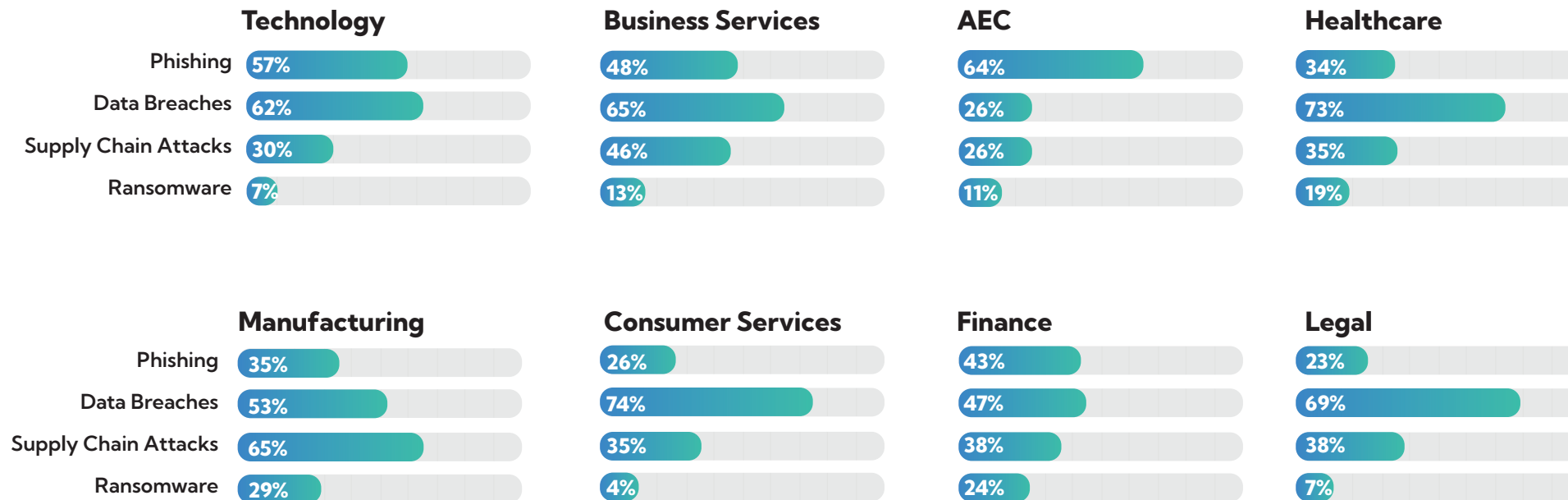
Phishing Attacks (46%): Deceptive attempts to trick individuals into revealing sensitive information, such as login credentials or credit card numbers, remain a prevalent threat. Phishing attacks can lead to account takeovers, financial fraud, and malware infections.

Supply Chain Attacks (36%): Attacks targeting vulnerabilities in a company's supply chain, such as third-party vendors or software providers, are a growing concern. These attacks can compromise multiple organizations through a single point of failure.

Ransomware (15%): Malicious software that encrypts data and demands a ransom for its release continues to disrupt businesses. Ransomware attacks can lead to significant downtime, data loss, and financial losses.

Top Cybersecurity Threats by Industry

According to our data, the Consumer Services, Healthcare, and Legal industries are particularly concerned about data breaches, while Manufacturing and Business Services are more worried about supply chain attacks.



Q: What proactive security measures have you implemented in your business? (Select all that apply)

Opportunities

To assess and improve their cybersecurity levels, SMBs can engage a Managed Service Provider (MSP) to:

Deliver security awareness training. To reduce the risk of human error—such as clicking a malicious link—MSPs can educate employees on how to better identify and avoid potential threats. MSPs' training programs can also raise awareness around industry regulations, to improve workers' compliance habits.

Run a cybersecurity audit. MSPs can assess your IT environment to identify the security gaps you need to address. An audit provides a detailed measurement of your security posture and helps you prioritize IT improvements.

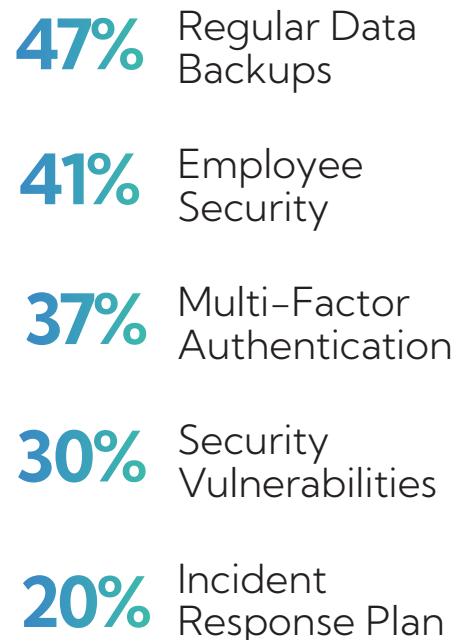
Measure compliance. You can have your MSP manage your compliance along with your security, running regular risk assessments against industry regulations to identify and address areas for improvement. Additionally, your MSP can help build a comprehensive compliance program, including policy development, employee training, and continuous monitoring to ensure ongoing adherence to regulatory requirements.

Insights and Industry Breakdown

According to the 2024 SECUREWORLD “The Alarming Cybersecurity Risks Facing SMBs” news, small and medium-sized businesses (SMBs) face significant cybersecurity threats that are often overlooked. While large enterprises have more resources to invest in cybersecurity, SMBs frequently lack the budget, expertise, and personnel to adequately protect themselves from cyberattacks. 46% of all cyber breaches impact businesses with fewer than 1,000 employees.²

² “The Alarming Cybersecurity Risks Facing SMBs”
secureworld.io/industry-news/smb-alarming-cybersecurity-risks

The Proactive Security Measures That SMBs Are Taking – Or Neglecting



Data backups are a top priority: Regularly backing up data and sending encrypted copies offsite the most common security measure (**47%**), highlighting its importance in protecting against data loss.



Multi-factor authentication is gaining traction: A significant proportion of businesses (**37%**) have implemented multi-factor authentication, enhancing login security.



Incident response planning needs more attention: Only **20%** of businesses have an incident response plan, indicating a potential gap in preparedness for security incidents.

Q: What proactive security measures have you implemented in your business? (Select all that apply)




Opportunities

SMBs can start looking into **multi-factor authentication**. It is worth checking to see if you or your IT partner can enable MFA in your existing solutions, but take a holistic approach. Turning on MFA for just a few applications can leave your remaining tools vulnerable.

SMBs should prioritize developing and regularly testing their **incident response plans** to ensure they are ready to handle security incidents. Just setting a plan once will not cover your IT environment as it evolves—an experienced MSP can help you keep your plan current.

MSPs also provide continuous monitoring, to help **identify and address security vulnerabilities** and threats. This proactive approach often finds issues before they become security incidents.

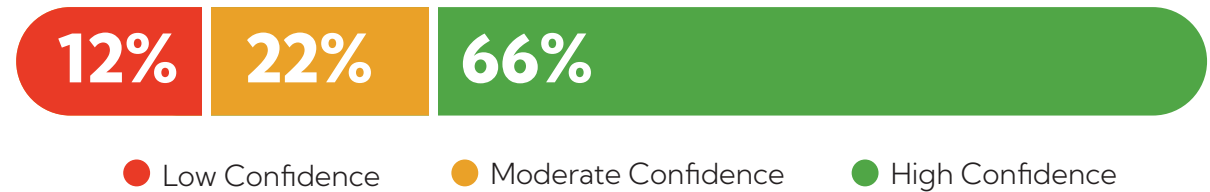


Do you have
an in-house IT
team or do you
outsource IT
services?

The Cybersecurity Landscape: What Keeps SMBs Up at Night?

These findings suggest a need for businesses to critically evaluate their cybersecurity posture and potentially invest in additional resources or expertise to enhance their defenses.

Confidence in IT Security



While cybersecurity threats are a major concern, businesses express varying levels of confidence in their IT team or provider's ability to mitigate these risks:

66% of respondents expressed high confidence (rating of 4 or 5) in their IT security.

22% indicated moderate confidence (rating of 3).

Worryingly, **12%** expressed low confidence (ratings of 1 or 2).

Closing the Cybersecurity Gap



Businesses expressed interest in their IT team to offer the following cybersecurity services to shore up their defenses:

Managed Security (51%):

Outsourcing security monitoring and management to specialized providers can enhance threat detection and response capabilities.

Security Audit (51%):

Proactive assessments to identify vulnerabilities and weaknesses in your systems, enabling timely remediation and strengthening your security posture.

Incident Response (43%):

Having a well-defined incident response plan can minimize the impact of cyberattacks and ensure a swift and effective recovery.

Security Awareness Training (24%):

Educating employees about cybersecurity best practices and threats can significantly reduce the risk of human error and social engineering attacks.

Q: What cybersecurity services would you like your IT team to offer? (Select all that apply)



"There was a time when our company was subject to frequent cyberattacks and faced serious threats to data security. ISOsource quickly stepped in and established a rigorous network security protection system for us, including firewall upgrades, intrusion detection system installation, etc. Since then, we have not suffered any major cyberattacks, and the company's data security has been effectively guaranteed."

Project Manager, Technology Industry

Insights and Industry Breakdown

The consumer services industry shows a high demand for Incident Response Services, due to its frequent handling of sensitive customer data and the need to quickly address any potential breaches or disruptions to maintain customer trust and minimize financial losses.

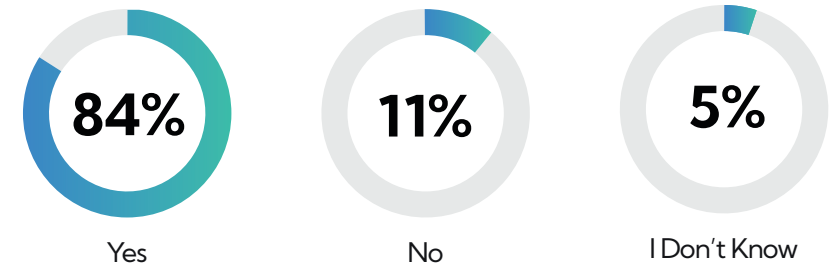
The legal industry prioritizes managed security, due to strict regulatory requirements for data privacy and confidentiality, along with the desire to offload the complexities of security management to specialized providers with expertise in compliance and risk mitigation.

Staying Ahead of the Threat: Addressing Key Cybersecurity Concerns

(82%) have cybersecurity insurance; however, 18% are uninsured, and worryingly, 5% are unsure if they have one. This highlights a critical gap in awareness and preparedness that could leave organizations vulnerable to significant financial and operational risks.

Cybersecurity insurance is not a luxury but a necessity in today's digital landscape. It helps businesses recover from cyber incidents by covering costs related to data breaches, ransomware attacks, and other threats. Having cybersecurity insurance safeguards your assets and maintains customer trust.

Organization Has a Disaster Recovery Plan



Cybersecurity Insurance: Not a Luxury

82% Business have cybersecurity insurance **18%** Business are uninsured

Opportunities

To enhance their cybersecurity, SMBs can work with a virtual (fractional) Chief Information Security Officer (CISO). A virtual CISO from a trusted Managed Service Provider (MSP) develops and implements custom security plans, staying current on threats and compliance requirements. They offer an objective perspective on in-house infrastructure or third-party vendors for security risks.

Additionally, having a disaster recovery plan is essential, but it must be regularly tested and updated. SMBs should consider investing in cybersecurity insurance to help mitigate the financial impact of a disruptive event. An experienced IT partner can help ensure the insurance application is correctly filled out and that the policy provides adequate coverage, reducing the chances of any claims being denied.



Adoption of Cloud Services and AI



Reaping the Benefits of Cloud Adoption

94% surveyed have integrated cloud services into their operations.

Top motivations for cloud adoption include:

Flexibility (42%) which includes adapting to changing business needs and scaling resources as required.

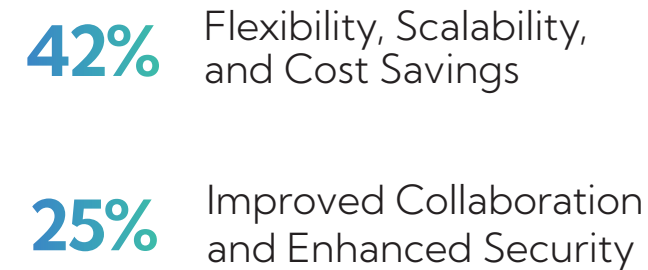
Scalability (42%) the capability to expand or reduce IT infrastructure to accommodate growth or fluctuations in demand.

Cost savings (42%) from the cloud by leveraging shared resources and pay-as-you-go models—reduces SMBs' IT expenditures.

Improved collaboration (25%) facilitating teamwork and communication through cloud-based tools and platforms.

Enhanced security (25%) helps SMBs access advanced security features and expertise offered by cloud providers.

Top Motivations for Cloud Adoption



Q: What are the primary benefits you have realized or expect to realize from cloud adoption? (Select all that apply)

Why the Cloud?

SMBs move to the cloud for many reasons, but **cost savings** tops the list. Cloud services are hosted by the providers, which means SMBs don't need to buy, run, maintain, and retire on-premises software, servers, and other hardware. This adds up to lower capital expenditures. Monthly cloud costs are predictable, and the solutions are **flexible**, scaling up and down as needed.

Today's cloud solutions offer **enhanced data security**; cloud environments and storage are based in professionally run data centers with high security standards. Moving to the cloud also reduces downtime, with most providers offering **high-availability uptime** performance of 99% and higher.

Flexible work and remote access are also benefits, with anywhere access for on-site, hybrid, and remote employees—wherever there is an Internet connection, employees can get their work done.





The Rise of AI and Automation: Transforming Business Operations

We are in an AI and automation revolution, with **90%** of SMBs using intelligent tools.

Top areas where AI and automation are being implemented:

Marketing (42%): Automating campaigns, personalizing content, and analyzing customer data.

Customer Service (41%): Providing 24/7 support through chatbots, automating responses, and personalizing interactions.

Sales (34%): Qualifying leads, automating outreach, and predicting customer behavior.

Operations (13%): Streamlining workflows, optimizing resource allocation, and improving efficiency.

SMBs can or expect to realize these primary benefits from AI and automation:

Improved Productivity (44%): Automating repetitive tasks and freeing up employees for more strategic work.

Cost Savings (44%): Reducing labor costs, optimizing resource utilization, and minimizing errors.

Increased Efficiency (44%): Streamlining workflows, accelerating processes, and improving overall productivity.

Enhance Decision Making (32%): Enhancing decision-making through data-driven insights and improved efficiency.

Improve Customer Experience (25%): Improving customer experience through personalized interactions and faster service.

Q: Which areas have you implemented AI or automation? (Select all that apply)

Q: What are the primary benefits you have realized or expect from AI or automation? (Select all that apply)



"One of our major success stories involves ISOutsource IT solutions. Their expertise significantly streamlined our operations, boosting efficiency and productivity."

– Architecture, Engineering, and Construction Professional

Insights and Industry Breakdown

In looking at how different industries embrace AI, the Business Services, AEC, Healthcare, and Legal industries are leading the way in AI adoption. Surprisingly, the Technology, Manufacturing, and Finance industries are lagging.

Opportunities

AI and automation are hot topics, with **44%** of respondents to the Splunk “State of Security 2024” report ranking generative AI as a top initiative,³ surpassing cloud security.

SMBs are adopting these tools to enhance efficiency, reduce operational costs, and stay competitive.

Automation tools streamline repetitive tasks like data entry, customer service, scheduling, and financial reporting so teams can focus on higher-value work. SMBs are also using these tools to reduce human error in areas like compliance and financial management.

AI helps SMBs make data-driven insights, optimize workflows, and enhance customer service. Smaller companies are also using AI tools to write marketing copy, blogs, and social media posts. Cloud-based AI tools are affordable, making them a smart choice for companies trying to gain an edge while saving money.

³State of Security 2024: The Race to Harness AI, Splunk.com, 2024
https://www.splunk.com/en_us/campaigns/state-of-security.html/





Top IT Investments for the Year Ahead

For 2025, SMBs are focused on:

Enhancing cybersecurity — protecting systems and data from cyber threats through measures like improved security protocols, updated security software, and regular vulnerability assessments.

Improving IT Infrastructure — upgrading and optimizing systems and infrastructure to improve performance, reliability, and scalability. This may include updating hardware, optimizing databases, and improving network infrastructure.

Investing in modern technologies — exploring and implementing modern technologies like AI, machine learning, and big data to improve efficiency, automate tasks, and gain a competitive advantage.

Improving user experience — focusing on user-centered design and improving the usability and accessibility of IT systems and applications.

Data management — implementing robust data management strategies, including data governance, data quality management, and data security measures.

Cloud migration — evaluating and planning for migration to cloud services to improve flexibility, scalability, and cost-efficiency.

Digital transformation — driving digital transformation initiatives to improve business processes, enhance customer experience, and foster innovation.

Developing IT talent — investing in training and development programs to upskill IT staff and address the skills gap.

Our Story

ISOsource is a leading IT consulting and managed services provider based in Washington state, serving over 500 small and medium businesses (SMBs) across the Pacific Northwest, Spokane, and Greater Phoenix for more than 30 years. We offer a range of services, including IT support, cloud solutions, cybersecurity, and strategic IT consulting, with the aim of being a trusted, local, one-stop IT shop. Our team of more than 100 experienced professionals provides flexible and customized IT solutions across Managed IT, Cybersecurity, and Strategy Advisory.

We help businesses Simplify, Save, and Protect by offering tailored IT solutions that streamline operations, reduce costs, and enhance security. Our comprehensive approach ensures that your IT infrastructure is robust, efficient, and aligned with your business goals. Whether you need ongoing IT support, advanced cybersecurity measures, or strategic advice, ISOsource is here to help you navigate the complexities of the digital landscape.

Our Vision

Until now, there has been limited insight into the IT landscape for SMBs, so ISOsource created a framework to measure and report on the specific needs and priorities of these businesses.

Cybersecurity measures are critical, considering that regardless of a business's size, a single cyberattack can cost at least \$200,000, and 60% of businesses shut their doors permanently after being attacked. This report provides an overview of what businesses like yours are facing, how they're addressing these challenges, and where they should focus next to close their IT gaps.





Contact ISOutsource

ISOutsource takes a partnership-first approach to offering SMBs high-quality, cost-effective IT services. We deliver tailored solutions, whether you need to improve cybersecurity or get help with IT budgeting and planning.

Contact us for help with:

- Managed IT Services
- Cybersecurity
- Strategic Advisory Services
- Governance, Risk, & Compliance

www.ISOutsource.com