



Cybersecurity:

2025 IT TRENDS REPORT FOR SMBs



Table of Contents

Introduction.....	3
Executive Summary.....	4
Managing Cyber Risks	5
Setting IT Investment Strategies	9
Keeping Up with Compliance Changes.....	10
Minimizing Email Cyber Risks	12
Foundational Cybersecurity Investments	14
Post-Attack Disaster Recovery	16
Managing DR Preparedness	17
Conclusion	19

Proactive Cybersecurity Strategies for SMBs

Welcome to the Q2 edition our [2025 IT Trends Report](#), which was based on a survey of 221 small and medium businesses (SMBs) near the end of 2024.

We are ISOOutsource, a managed services provider (MSP) specializing in providing tailored IT solutions for SMBs to enhance their operational efficiency, security, and scalability. We work with hundreds of SMBs to provide managed IT support, system and network administration, cybersecurity services, and strategic IT consulting. With over 30 years of experience, we are committed to delivering flexible, secure, and efficient IT solutions, ensuring that technology catalyzes business growth.

Together with our partner INKY Technology, we've created this Q2 2025 quarterly update providing insights and advice around top IT issues for SMBs. INKY's _ proactively scans inbound, internal, and outbound emails to help eliminate phishing and malware threats, addressing the evolving needs of businesses in today's complex digital environment.

In the 2025 IT Trends Report, SMBs like yours shared their primary interests and issues. This update explores **cybersecurity, disaster recovery (DR), and IT investment strategies for SMBs** in greater detail. Use the headings in the report's table of contents to jump to the sections that interest you.

Why these topics? In our 2025 IT Trends Report, SMB leaders spoke up about the cyber threats that concern them most, including:

- **Data breaches (58%).** Breaches are caused by unauthorized access to sensitive information and can potentially result in regulatory fines, legal action, and irreparable damage to SMBs' reputations.
- **Phishing attacks (46%).** These are deceptive attempts to trick individuals into revealing sensitive information, such as login credentials. Phishing attacks can lead to account takeovers, financial fraud, and malware infections.
- **Supply chain attacks (36%).** Using vulnerabilities in a company's supply chain, such as third-party vendors or software providers, attackers seek to infiltrate networks and compromise or steal data.
- **Ransomware (15%).** This type of attack uses malicious software to encrypt data. Attackers then demand a ransom for the data's release. Until this is resolved, the attack continues to disrupt business.

Executive Summary

In today's digital-first landscape, small and medium-sized businesses (SMBs) face escalating cyber risks and evolving compliance requirements, all while making smart IT investments. This Q2 edition of the 2025 IT Trends Report—based on a survey of 221 small to medium-sized businesses (SMBs) across Washington, Oregon, and Arizona—outlines the most pressing IT priorities and proactive strategies for businesses navigating this complexity.

This report delivers a layered, strategic view of IT needs, grouped into three core categories:

Strategic Initiatives

These sections provide high-level planning advice to help SMB leaders align technology with long-term business goals.

- **Managing Cyber Risks:** Learn how regular audits, employee education, and layered defenses can reduce organizational exposure.
- **Setting IT Investment Strategies:** Discover how SMBs are prioritizing spend based on critical business outcomes and compliance requirements.
- **Keeping Up with Compliance Changes:** With evolving regulatory environments, small to medium-sized businesses (SMBs) need a framework for balancing operational efficiency with compliance requirements.

Proactive Measures

These initiatives can help prevent attacks before they occur by shoring up internal defenses.


- **Minimizing Email Cyber Risks:** Explore tools and techniques—like zero-trust security, behavioral analytics, and AI-enhanced email scanning—to stop threats at the inbox.
- **Foundational Cybersecurity Investments:** Learn which core investments (e.g., MFA, endpoint security, DLP) provide the strongest ROI across verticals.

Reactive Responses

Even with the best defenses, incidents can occur. These sections guide recovery, remediation, and readiness.

- **Post-Attack Disaster Recovery (DR):** Identify steps to detect, contain, and recover from attacks, including lessons from client scenarios.
- **Managing DR Preparedness:** Build a DR strategy with clear recovery time and recovery point objectives to minimize downtime and business impact.

Managing Cyber Risks



Steven Whitacre, Solutions Architect at ISOsource, breaks down his observations of how common threats affect SMBs across industries—and what they should watch out for. As a cybersecurity professional, he sees that in 80% to 90% of cases, organizations that get attacked have internal IT staff. However, if IT staff don't update the software, firewalls, and firmware, or if they reuse passwords, it can make it easy for attackers to gain access and render even sophisticated behavioral security solutions less effective.

Proactive Steps To Prevent Cyberattacks

The best way to prevent cyberattacks is through regular IT and cybersecurity audits.

Whether you conduct them monthly, quarterly, or biannually, proactive reviews are essential because you can't fix a problem if you don't know it exists. With consistent auditing, you gain the visibility and insights needed to make informed, strategic decisions that protect your business and support long-term resilience.

Some companies offer simple port/service scan reports as the extent of their auditing services. Find an experienced managed services provider (MSP) who can perform full audits, take the time to understand your environment, and provide context and advice around their findings. That way, you have a partner who can help you make informed decisions.

Implementation Of Zero-Trust Security

"The 'Deny Everything First' model is the bedrock of zero trust. Whether it's a firewall policy or an Azure or Microsoft 365 access policy, the first step should always be to deny all permissions, then allow only the permissions you need," says Whitacre.

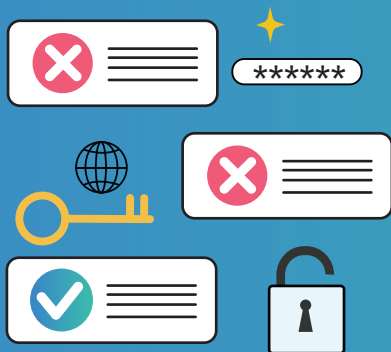
Blocking global IPs can sound smart, but it's tough to maintain. Implementing blanket policies like "Deny connection attempts from China," can be tricky and time-consuming. A better approach would be using a policy like "Deny everyone except Canada." Then, SMBs don't have to worry if providers change IP addresses, or an attacker hops into Germany to bypass their restrictions. For best results, work with an IT team or MSP who can implement user access management for granular control.

The Importance Of Employee Training In Mitigating Cyber Risks

Humans are the weakest link in any security chain. Reusing passwords, clicking unsafe links, or providing too much information over the phone or online are common—and damaging—mistakes that people make.

A solid employee training program and regular refresher courses are paramount to any security program. With this training, employees can help support awareness around security risks, and even help SMBs spot suspicious activity for a quick response to attempted attacks.

As an example of how employees' habits can affect security, we've seen cyberattacks succeed because of reused user names and passwords. In one brute-force/ransomware attack, there were several failed attempts to log into an SMBs' systems via its VPN from many accounts in a row. These accounts got locked for having too many failed attempts. The SMB had several regional networks that were not connected, but the IT admin had reused the username and password for each network. Eventually, the attackers got access via an admin account. The SMB didn't have MFA in place, which would have slowed or stopped the attack.



Protect Against Cyber Risks

- Brute-force Attacks
- Ransomware
- Weak Passwords
- Outdated Software
- User Error
- Insecure Servers

Emerging Threats And How They Affect SMBs

When it comes to new threats, regular IT and security audits are the best defense. "We are seeing more AI-driven attacks. Your average bad guys will use those tools to cast a wider net than they could if they were working manually. Previously, these bad actors tended to set off all the alarms when they gained access. But these days, automation and AI are helping them take things to the next level. These hands-off, automated intrusions are much more challenging to detect, since they adapt to the environment and take advantage of existing tools and applications to avoid detection," says Whitacre. Often, these tools report back to a central command center with the details, and those details are then sold on the dark web. Sometimes the tools simply report back with access information; sometimes, they install back doors to provide persistent access.

Either way, the period between intrusion and malicious activity can be weeks or even months, and you'll never know they are there unless you look for them by auditing and reviewing your organization's security posture.



Industry-Specific Advice

Manufacturing. Many smaller manufacturers rely on older technology. Software companies don't update older technology often, and a dormant technology stack is a prime target for attackers. Prioritize investing in current solutions and having a managed services provider (MSP) perform technology and cybersecurity audits to find and fix security vulnerabilities before attackers exploit them.

Legal services. To better protect client confidentiality in digital communications, firms should know where that data is going and where it resides. It's vital to encrypt any data you send across the Internet—and data stored in your systems. Look into implementing access controls too, to ensure only the people who need to see specific data have permission to do so.

Need Help Identifying Your Cybersecurity Gaps?


Many SMBs turn to an MSP like ISOsource to start with a readiness review.

Healthcare. A single HIPAA violation can result in fines of up to US \$50,000, with repeated violations for "willful neglect without correction" running as high as \$1.5 million per year. No healthcare provider wants to end up on the [HIPAA breach list](#). Protecting patient data adequately requires not just technical controls, but also personnel training and cooperation. Where possible, isolating systems that contain HIPAA data from the rest of the network will go a long way toward protecting your company should a network breach occur.

Business services. Use access controls to help protect third-party data. If somebody can't get to the data, they can't steal it. The challenge is ensuring that only the right people can access that data/location. And whether that data resides in the cloud or behind a firewall, enforcing multifactor authentication (MFA) gives you extra security.

Architecture, engineering, and construction (AEC). Remote project teams and cloud-based software do increase security risks if you don't compensate with user access controls, MFA, strong password policies, regular audits, and a zero-trust security model.

Before, most companies stored their information on a server, on their network, or behind a firewall. There were limited options for an attacker to gain access to that data. Cloud-based services and remote teams have introduced new pathways for a savvy attacker to exploit. Multiple cloud services mean multiple accounts and passwords, increasing the risk of users reusing the same password across services.



Finance and accounting. Since running your company cash-only isn't feasible, securing sensitive financial transactions requires user training and a solid security policy. Financial gain is the goal in probably 95% of attacks, and your employees are an essential line of defense. Alert employees have thwarted plenty of attacks. Having a second person review and verify large transactions is an excellent policy. So is calling to verify requests to change payees' financial institutions or accounts. Direct human communication is best here—more so than with any other department.

Consumer services. To protect customer data without disrupting service, you need a backup and recovery strategy. If you were hit with a cyber incident that deleted everything on your network, how quickly could you get back up and running? Of course, every minute you are down will cost you in lost productivity or client trust. As your organization's needs change, so should your backup and recovery plan; backups aren't a "set it and forget it" type of service. You should review and test them monthly and perform complete disaster recovery exercises annually. It may seem like a lot of effort to prepare for something that might not happen. But if it should happen and you're not prepared, it could be the end of your business.

**ISOsource Supports SMBs
Across Washington, Oregon, and Arizona**
with proactive IT and cybersecurity strategies. If you're unsure
where to start, we're here to help.

Technology. Some excellent data loss prevention Data Loss Prevention (DLP) tools and practices are available to prevent intellectual property (IP) theft in tech firms. These include watermarks, DLP rules to prevent downloading of files or screenshotting of data, and policies to prevent the offloading of data to USB drives.

Nonprofit. Organizations with limited budgets still need to guard against cyber threats. It's a balancing act between security and usability, but when you have a limited budget, you must focus on where you'll get the best value.

There is no one-size-fits-all solution, so SMBs should be prepared to do some planning and decision making. Two companies with the same budget will have different priorities and needs, which means they'll want to allocate those finances differently.

Setting IT Investment Strategies

ISOutsource Security Engineering Manager Charlie Lindsay weighs in on proactive measures SMBs can take to improve their security posture.

How SMBs Are Shifting Their IT Investment Priorities In 2025

SMBs are focusing on data protection, which isn't new for 2025; it's a culmination of where the market has been going for some years. Smaller companies are focusing more on solutions that provide behavioral analysis of users on a network: enhanced detection and response (EDR) platforms like Sentinel and CrowdStrike, along with some firewalls. These solutions can flag certain behaviors linked to data exfiltration, like copying large amounts of files in a short period.

AI is a new priority for SMBs, and they want to use it to improve their security posture and perform behavioral analysis. SMBs are also looking to train AI models to detect these behaviors. In response, software companies are starting to integrate this into their products.

**ISOutsource Supports SMBs
Across Washington, Oregon, and Arizona**
with proactive IT and cybersecurity strategies. If you're unsure
where to start, we're here to help.

Keeping Up with Compliance Changes

David Lukac, Managing GRC Consultant talks about compliance framework issues affecting SMBs.

Q: What key regulatory changes are impacting SMBs in 2025?

A: Here's a quick roundup of regulatory changes to be aware of this year:

PCI DSS 4.0

- New requirements go into effect March 31, 2025.
- Work with your acquiring bank, payment system provider, or International Standard for Organization (ISO) to understand your new requirements and develop a compliance plan.

DORA (EU)

- The Digital Operational Resilience Act (DORA) is the European Union's landmark regulation designed to future-proof the financial ecosystem against cyber threats.
- [Check](#) if DORA applies to your organization.
- Engage ISO or your MSP to assist in building a compliance plan.

NIST CSF 2.0

- There's a new version of the National Institute of Standards and Technology (NIST) standard.
- Assess the benefits of adopting version 2.0 and the timeline for adoption as the new standard matures.

CMMC

If your manufacturing company has government contracts related to military information, [check](#) to see if recent changes in Cybersecurity Maturity Model Certification (CMMC) affect your organization.



How To Choose The Right Cybersecurity Framework For Your Business

Start by understanding the legal/regulatory and contractual/business requirements that affect your business. You should also understand the risks of acceptance—which risks and requirements affect your organization.

From there, define your risk acceptance position.

Select a framework and maturity level. Then, build your cybersecurity framework around a particular regulation. Keep in mind that this is more than checking boxes on a compliance form. It's an ongoing commitment. Without investing in internal compliance, informing and educating employees, and maybe engaging an MSP to help, organizations can't hope to meet security framework standards—they might as well not bother adopting a framework.

That's a high-level explanation. Organizations can adjust their approach depending on their size, resources, and industry.

Best Practices For SMBs At Different Security Maturity Levels

Keep your program alive. Most companies come to us when a new client or lawyer requires them to meet specific requirements. We help them comply and build a program for them. However, they won't remain compliant unless they continually work on their own, with an MSP, or with ISO to update their policies and educate employees on them.

The Industries That Are Seeing The Most Regulatory Pressure For Compliance

Currently, any organization that's taking credit card payments is under the most pressure. They should stay compliant with PCI 4.0.

How To Balance Regulatory Compliance With Operational Efficiency

SMBs must build and operate a risk-driven cybersecurity and compliance program. Smaller businesses can reduce regulation to only the parts that apply to them and build your compliance program around that.

The other aspect is to make security tasks part of your regular operational routines.

Minimizing Email Cyber Risks

Proactive Protection Against Cyber Risks

Zero-trust is a security framework that assumes no user or device is trustworthy by default, whether they're inside or outside the network. Every access request must be authenticated, authorized, and continuously validated. This reduces the chance of a breach by filtering out the less-determined attackers and limiting their lateral movement across your network if they do manage to get in.

Zero-trust frameworks protect remote/hybrid users by enforcing MFA policies, verifying device health, and limiting access with the least privilege principle. These are all things that support industry standards like HIPAA, PCI-DSS, and others.

Endpoint security protects individual devices (laptops, phones, servers, etc.) that connect to SMBs' networks. It includes antivirus, firewall, device encryption, patching, and often endpoint detection and response (EDR). This kind of solution stops malware early by detecting threats before they spread with real-time scanning. It automatically patches and updates endpoints to close security vulnerabilities quickly—even when employees use personal devices for work.

To underscore the importance of updating software and systems, an ISOsource security expert says he frequently sees the aftermath when SMBs don't apply patches or upgrade to new versions of software. Attackers often get into a network via brute-force attacks. Once inside one particular SMB, attackers found an older version of the organization's backup software and used it to create new admin accounts on the domain. With those new admin accounts, they set up a command center on one of the organization's internal servers, spreading their access across servers and networks. They started offloading as much data as possible and then deployed robot encryption. Thankfully, in this case, the SMB had cloud backups in addition to its onsite backups. Attacks like these are common. What we see at ISOsource is that, outside of email compromises, 75% of attacks are enabled by outdated apps and firmware.

Behavioral security solutions are another top investment. These solutions monitor systems, such as networks, for suspicious activities. As an example of how these solutions can help, an ISOsource security expert cites a cyberattack on an SMB. The SMB was providing remote access to employees through an RDP gateway that was not protected by MFA. The attackers seemed to have had a list of user accounts, and they were trying various passwords until they got locked out of each account. When they finally did get access, the SMB's MSP responded quickly enough that there were no more compromises. If this SMB had a behavioral security solution, it could have detected the attack before any servers were taken offline.

Email security solutions are also a valuable defense, especially as Phishing remains the most common cyberattack vector, according to **INKY's 2023–2024 Email Security Annual Report**

INKY's 2023–2024 Email Security Annual Report



Behavioral security solutions analyze email traffic in real time, using machine learning to identify malicious links or attachments by comparing them to large threat samples and patterns. Because of how fast new threats and threat categories are emerging, INKY added Generative AI Detection to its email platform this year.

Generative AI Detection goes a step further, to see past the various techniques used in phishing attacks, such as urgent language, misleading links, and malicious attachments. The solution understands how all these things add up to criminal intent—even if the wording that cybercriminals use doesn't include the usual markers that signal danger (such as emotional appeals and urgent deadlines).

INKY's GenAI detects the true meaning behind the words, which is more effective than relying on outdated pattern samples.

Foundational Cybersecurity Investments

Charlie Lindsay, Security Engineering Manager at ISOsource, provides insights on the upfront investments SMBs should make in cybersecurity.

The Most Critical Cybersecurity Investments For SMBs

When you consider that INKY's 2024 Annual Report found that \$534 Billion was lost to data breaches in 2024, it's critical for any business to protect its information and systems. There are many ways to do this.

The security investments you make will vary based on your data and how you store and access it. For example, SMBs that are in sales collect personally identifiable information (PII) and process credit cards. So, identify and classify your data to indicate what should be protected based on your company policies and industry compliance requirements.

The best approach requires acknowledging that security comprises layers: data management, access management, incident and contingency planning, risk management, systems and software protection, user training, vulnerability assessment and remediation.

Technology, like endpoint security, firewalls, data classification, and DLP, applies across all seven security layers and can be used effectively by all companies and verticals. Take DLP, for example. Companies' implementation of DLP is determined by where their data sits in relation to the employees accessing it: whether they store their data in SharePoint sites, online cloud services, or file servers on-premises. And whether users are connecting across a VPN or from on-site at one location or many across geographies.



"How we value data is relative. A law firm might classify client data as highly sensitive and implement many safeguards on it, but a data-mart company that collects some of that same information and sells it—they have no incentive to protect it in the same way. Your company decides how sensitive its data is, based on its mission and the regulations it must meet," says Lindsay.

Securing Internet Of Things (IoT) Devices And Supply Chain Networks

It's common for manufacturers to use industrial equipment that isn't current, regularly updated, or subjected to security practices. Manufacturers should isolate that equipment from the rest of their network and only allow access to it by the systems that need to interact with it. This applies across verticals. The most restricted access is what works best.



Foundational Cybersecurity Investments

- Technology: endpoint security, firewalls, data classification, and DLP
- Manage equipment
- Classify and control data at granular level

The Best Method For Investing In Secure Document Management In The Legal Industry

SMBs should classify and control data at the most granular level. "I encourage anyone in the legal industry to use DLP to set rules and access limits on their data, when it's in their network or travels outside it. Determine and control who needs access and use policies to enforce that," says Lindsay.

In a highly regulated industry, sometimes law firms' client data is subject to those clients' industry regulations. If you represent a healthcare provider whose patient data is involved in a case, you must follow HIPAA standards to keep that patient data safe.

Post-Attack Disaster Recovery

Charlie Lindsay, Security Engineering Manager at ISOsource, covers what to do after a cyberattack.

Steps To Take In A Data Breach, Ransomware, Or Other Attack

"I'll start by clarifying that an attack is ongoing until you've remediated it. Remediation is the restoration of affected systems and getting any compromised or stolen data back," says Lindsay.

With that in mind:

- **STEP 1** is identifying that your systems have been breached.
- **STEP 2**, call your cyber insurance provider, if you have one.
- **STEP 3**, let your internal IT team work to contain the attack. Don't ask an outside company at this point, or it could void your insurance policy.
- **STEP 4**, recover any missing or compromised data from your backup and DR systems.
- **STEP 5**, do a root cause analysis for what happened. What attack vectors were in play, and how can you close them?
- **STEP 6**, close your security gaps.

How SMBs In The Manufacturing Industry Can Address Production Downtime Risks

Much of this advice applies to many industries:

Identify which systems are the most and least critical and spend most of your energy protecting the most critical systems. This is a business decision, so business leaders should decide how much money and effort should be allocated to backing up each system. They must understand the impact of a system's downtime on their business, including any contractual requirements around delivery of products and services. It's a balancing act of determining acceptable losses. You could back up all your data every 30 minutes, but that cost grows exponentially with the need for secure storage space for every backup.

When deciding how vital each system is, consider an acceptable recovery time for it, that is, the time between the system going down and when it recovers. So that would be a DR plan based on:

Recovery point objective (RPO)

how much data loss you can tolerate within a period most **relevant to your business before significant harm occurs.**

Recovery time objective (RTO)

the amount of time the business can tolerate having a system be down and how much time they can afford to spend trying to recover their data to restore operations.

Managing DR Preparedness

David Lukac, Managing GRC Consultant at ISOsource, talks about DR planning and how SMBs can mitigate risks.

Best Practices Emerging In SMB Disaster Recovery Planning

“SMBs are focusing on cloud recovery solutions now. Even if you store your data on-premises or in a secondary data center, you can find a provider who will recover your information in the cloud at a lower cost than building a [cold, warm, or hot recovery site](#),” says Lukac.

Like most things in IT, DR plans and technology change, so review your contracts every time you renew. I’ve seen companies sign off on DR contracts that mention backup technology they’re no longer using, such as tapes.

Examples Of Cyber Risk Mitigation

We are seeing SMBs mitigate cyber risks by:

Adopting cybersecurity product packages. This includes products from Microsoft, CrowdStrike, and INKY. Your MSP can help you choose which services and features you need and deploy them to best meet your business needs.


Building a cybersecurity program using a solid framework.

The security frameworks you adopt will vary depending on your industry, but they include:

- Center for Internet Security (CIS) top 18 controls
- ISO-27001 / ISO-27002
- NIST Cybersecurity Framework (CSF)
- CIS Critical Security Controls (CIS-CSC)
- PCI-DSS

These frameworks help you identify your organization’s IT maturity and guide you toward your security goals.

Using conditional access policies. These policies restrict access from geographic locations where employees do not have legitimate use. You can use features and options from the cybersecurity product you chose, like Microsoft 365, to support these policies.



Enforcing MFA. “MFA adds an extra layer of security to help protect against cyberattacks like phishing. By requiring additional authentication when users access your systems, attackers will need more than just a valid username and password; they’ll also need access to that user’s smartphone, email account, authentication app, etc.,” says Lukac.

How To Structure A Backup And Recovery Strategy

There are a few options, including:

- **Air-gapped backups.** SMBs can store backups of critical data offline, in storage that isn’t accessible from public networks or is behind a software partition.
- **Cloud backups.** When data, apps and resources are backed up in the cloud, SMBs can easily restore them to their primary data center or cloud provider if these resources are ever lost or compromised.
- **Paying as much attention to recovery planning and testing as to backups.** It’s good to back up your data, but you won’t know that your backup plan works unless you test it. Testing can reveal the unexpected, like problems with your backup power system. It can help find weaknesses and areas to improve and verify just how long it will take to recover from various scenarios, like IT failures, natural disasters, and cyberattacks.

The Role Of Automation In Disaster Recovery

SMBs should automate backups and backup validations. This can reduce manual errors, recovery time, and overall efficiency.

SMBs should also assess the value of automating their recovery activities depending on the assumed frequency/time-criticality of the data they need to recover. For example, a company that provides a ticketing service for venues and groups involved in events (like concerts) would consider keeping this service online to be highly critical—without the service, they can’t sell or accept tickets at events. This type of company can justify investing more money in more frequent backups and faster recovery than, say, a marketing agency that can delay creating a client presentation for a day or two if needed.

Common Misconceptions Or Mistakes Around Disaster Recovery

SMBs shouldn’t rely on SaaS providers to protect all their data in all situations. While Microsoft and other providers might enable you to recover documents from 30 to 60 days ago, that doesn’t protect you when, for example, a disgruntled employee alters a bunch of files on their last day with the company, the data gets corrupted, or your organization was the target of a cyberattack. You should have a comprehensive backup plan for all your critical data, whether it’s in a cloud service or not.

Conclusion

In conclusion, the Q2 2025 IT Trends Report highlights the critical importance of proactive cybersecurity, resilient disaster recovery planning, and strategic IT investment for SMBs. To effectively mitigate cyber risk and ensure business continuity, organizations must prioritize regular security audits, comprehensive employee training, and a multi-layered approach to cybersecurity that encompasses network, endpoint, and data protection.

Equally important is staying ahead of regulatory shifts and emerging threat vectors by embracing AI-driven threat intelligence and scalable, cloud-based solutions. These capabilities are essential for navigating the rapidly evolving IT landscape and driving sustainable growth.


Finally, fostering a culture of security awareness and continuous improvement will position small to medium-sized businesses (SMBs) for long-term resilience and success in an increasingly digital and interconnected world.

**ISOutsource Supports SMBs
Across Washington, Oregon, and Arizona**
with proactive IT and cybersecurity strategies. If you're unsure
where to start, we're here to help.

Looking Ahead to Q3 2025: IT Investments, Cloud, and AI Emerging Technologies

As we move into Q3 2025, staying updated on IT investments, cloud computing, and AI emerging technologies is crucial. Growth in IT spending, driven by advancements in AI and cloud services, will offer new opportunities for businesses to enhance their technological capabilities. Embracing innovative AI solutions and leveraging scalable cloud platforms will be key to maintaining a competitive edge and achieving sustainable growth. This will help SMBs level the playing field against enterprise businesses.

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