IT ISAC

CELEBRATING 25 YEARS OF THREAT INTELLIGENCE SHARING

# The Small and Medium-Sized Businesses (SMBs) Cybersecurity Playbook:

## *10 Practices to Defend Your Business*

2026

# TABLE OF CONTENTS

# INTRODUCTION

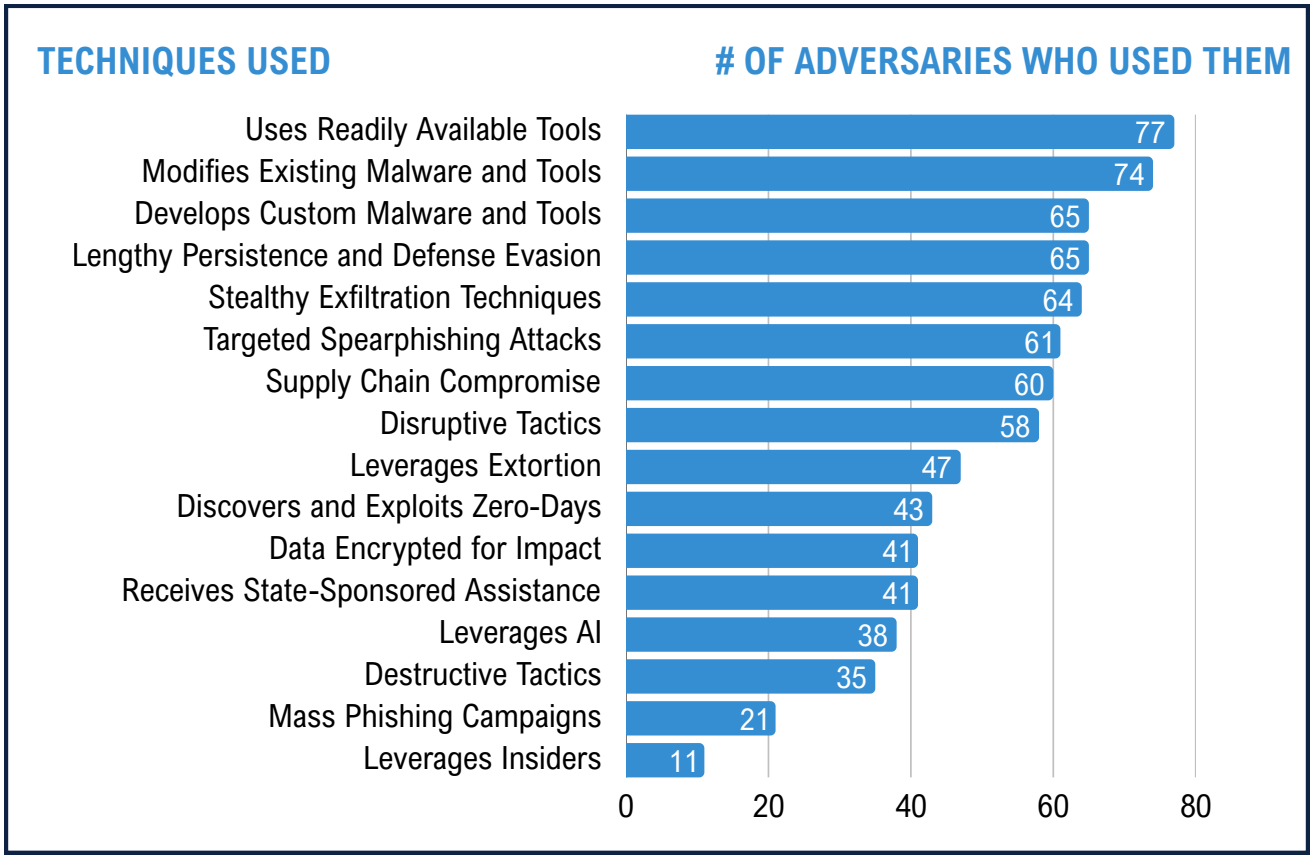
In an era where cyber threats evolve at an unprecedented speed, traditional approaches to cybersecurity must be adapted to mitigate modern dangers. Protecting your organization's assets requires more than just a single firewall or a strong password; it demands a holistic, proactive culture of defense. The interconnected nature of the current digital landscape comes at a cost – vastly expanding threat actors' attack surface, making organizations of all sizes targets for sophisticated cyberattacks.

The number of small and medium-sized businesses (SMBs) in the United States grows every year. According to a 2025 report from the U.S. Small Business Administration, there are 36.2 million small businesses in the country – these businesses account for nearly 46 percent of private sector employment. Yet SMBs often bear the brunt of a harsh reality: the economics of cybersecurity heavily favor the attacker. Because it is fundamentally more expensive to defend a network than it is to exploit one, many SMBs find themselves at a structural disadvantage. Unlike large corporations with expansive resources, these businesses must protect their data and infrastructure with limited capital and staff; they must strategically maximize their resources to survive an adversary that only needs to succeed once.

The Information Technology Information Sharing and Analysis Center (IT-ISAC) was founded to help close this kind of gap. As a member-driven community of leading IT companies, IT-ISAC enables members to share threat intelligence, analyze adversary behavior, and collectively strengthen defenses across the sector. That same collective defense mission drives this guide: translating the threat intelligence our members rely on into practical, accessible guidance for the SMBs that form the backbone of the U.S. economy.

To meet these challenges, we have created this SMB Cybersecurity Playbook, which outlines 10 security practices to help organizations strengthen their defenses. In creating the guide, we leveraged the analysis contained in our IT Sector Cyber Threat Report, released earlier this year. The report highlighted the top threats within the IT sector, identified over 330 adversaries, and analyzed the 77 most impactful actors to the industry. From that analysis, we identified the most common tactics, techniques, and procedures (TTPs), and built this guide of security practices to help combat against those.

Even though a technique may have been used less commonly, it does not make it less relevant. This list gives us a baseline on common adversary techniques and can help organizations prioritize their resiliency efforts.




While no network is entirely immune to breach, the following security practices offer a practical, effective way to manage risk. Many of these improvements are easy to deploy and low-cost or free, but can represent the difference between a secure operation and a major incident. Implementing even a few of these practices will reduce your organization's exposure and improve its ability to recover should an incident occur, making you a more difficult target for opportunistic attackers.

## SECURITY PRACTICE #1: Attack Surface Reduction

*Every open door is an invitation. Give attackers less to work with.*

Attack surface reduction is the process of shrinking the total number of entry points an attacker can exploit. For SMBs, this isn't just about erecting firewalls but rather about setting good digital hygiene practices. The Verizon 2025 Data Breach Investigations Report highlighted that 12% of all reported breaches were the result of basic web application attacks. Unused applications, unmonitored ports, and more provide extra entry points for attackers to exploit. By removing what you don't use, attackers are forced to work significantly harder to find a way in, shrinking their possible targets and keeping your system safer.

The most effective strategies for attack surface reduction cost just your time and attention. Organizations can begin by taking an inventory of assets and entry points – anything that would make the network vulnerable to attack. Servers, software applications, connected devices, user accounts, and more all provide potential paths for attackers to slip in. Free tools are available to scan for open doorways in your network, such as Microsoft Defender. If a service doesn't have a clear purpose, disable it.

**Enforce a Least Functionality Policy**

Limit the apps, programs and software on workstations to just what's needed for the job – no superfluous applications or pre-installed third-party software, etc. Remove administrative rights from standard users and ensure all newly downloaded applications are approved by your IT team.

**Configure Default Settings**

Audit the default settings on your current suite of apps to ensure each is as secure as possible. This includes switching off Office macros, and disabling outdated communication protocols like SMBv1 or TLS 1.0, which are often exploited in modern ransomware.

**Shield Public Assets with a Firewall**

Public-facing websites and applications can be shielded with a web application firewall. Using free tiers of providers like Cloudflare can hide origin IP addresses from attackers and automatically filter out common attacks before they reach your servers.

## SECURITY PRACTICE #2: Data Loss Prevention

*Stopping the breach is important, but so is stopping the data from leaving.*

While cybersecurity practices typically focus on keeping attackers out, data loss prevention focuses on keeping your most valuable assets in. Traditional cyberattacks orchestrated by threat actors are not the only ways in which information can slip out of your organization's grasp – it can be as simple as an employee accidentally sending an email with sensitive data to the wrong recipient.

For SMBs, the stakes are high, especially those including personally identifiable information (PII), can lead to not only loss of trust but also regulatory fines. And those in the United States are especially at risk of losing big. According to the 2025 Cost of a Data Breach Report by IBM Security, breaches can cost an organization in the U.S. as much as $10 million, compared to the global average of $4.44 million – a financial hit that has the potential to close a growing company's doors.

Implementing a data loss prevention strategy does not require massive resources. The first step involves data discovery and classification: understanding what you have and what you need to protect most. Pinpoint where the most sensitive information lives, including credit card details, proprietary information, and employee and customer data. Once identified, apply the principle of least privilege access, which means ensuring that employees only have access to specific data necessary for their daily tasks. In limiting access, the effects are likewise limited if an employee's account is compromised or if they decide to go rogue.

Beyond this, there are several other high-impact, low-cost changes and implementations your team can make to prevent and mitigate data loss:

**Leverage Existing Ecosystems**
Many organizational tools, such as Microsoft 365 or Google Workspace, have basic data loss prevention features baked in, such as the ability to set DLP rules for Google Drive and the free version of Microsoft Purview. Utilizing these features is a cost-effective way to put an extra layer of security on your data.

**Enforce Endpoint Encryption**
Ensure all laptops use built-in encryption, such as BitLocker for Windows Pro/Enterprise/Education editions or FileVault for Mac. This ensures that if a device is left somewhere or stolen, the data remains unreadable.

**Disable USB Ports**
Leverage administrative tools to block the use of unauthorized external hard drives and thumb drives on company computers.

## SECURITY PRACTICE #3: Phishing Prevention

*Don't get reeled in. If it smells phishy, it probably is.*

Phishing remains a persistent threat to businesses because it targets people, rather than software. For an SMB, a single successful "hook" can lead to business email compromise (BEC), ransomware attacks, or credential theft. Verizon's most recent data breach report shows that 60% of breaches involve a human element, with phishing as the primary attack vector. These attacks range from wide-net campaigns across an organization to spearphishing, which is targeted messages disguised as correspondence from a trusted source like a vendor or internal colleague. The IT-ISAC's own analysis of the 2025 IT sector cyber threat landscape showed 79% of threat actors utilized spearphishing techniques to try and coax sensitive information out of employees.

The evolution of phishing has moved beyond simple emails to include smishing (SMS phishing) and vishing (voice phishing), creating multiple channels for attacks. AI tools can also be used to replicate voices, video, and increasingly sophisticated scripts to try and cause employees to slip up.

The simplest, most resourceful-conserving way to mitigate phishing is to train employees on how to spot the hook:

**Look for Alarming Headlines**
Attackers tend to use urgent language or impersonate well-known companies to make you act without thinking.

**Watch for "Familiar" Faces**
Business email compromise (BEC) is a common form of attack in which attackers impersonate trusted parties or even have compromised a known contact. Trust your gut: if anything seems off or suspicious, call (do not email) the person to confirm they contacted you before sharing any sensitive information.

## SECURITY PRACTICE #3: Phishing Prevention

There are a few other tactics your organization can put in place to flag suspicious emails and make reporting them easier.

**Enable External Email Warning Banners**
Configure your email platform to automatically tag all incoming messages from outside the company. This simple, free configuration provides a nudge for employees to scrutinize links and attachments more carefully when the sender is external.

**Deploy DNS Filtering**
Use a free domain name system (DNS) filtering service to block malicious websites at the network level. If an employee accidentally clicks a phishing link, these services act as an automated safety net by preventing the computer from ever connecting to the known fraudulent domain.

**Implement a One-Click Reporting Process**
Set up a dedicated mailbox (for example, phish@yourcompany.com) and encourage employees to report suspicious emails immediately. Reducing the time between an email arriving and your team being alerted can prevent a single click from turning into a company-wide breach.

**For more on how to recognize and report phishing, check out our phishing-specific blog here.**

## SECURITY PRACTICE #4: Managing Insider Threats

*Not every threat comes from the outside, some already have a key.*

Attacks do not always come from unknown attackers invading from remote locations – sometimes the threat originates much closer to home. Insider threats are anyone with authorized access to your network, whether that's employees, former staff, or third-party contractors. Insider threats can fall into two categories: those that are from malicious insiders and those that are from negligent insiders. The 2025 Insider Risk Report from Fortinet finds that 77% of organizations experienced insider-driven data loss over an 18-month period, whether intentional or not.

On small teams especially, it can feel awkward to restrict access or monitor activity. Yet this lack of oversight is exactly what insider threats exploit (intentionally or unintentionally). Whether it's a disgruntled employee taking a client list to a competitor or a well-meaning manager using an unsecured personal cloud drive to "get work done faster," the result is the same, sensitive data leaves your control. Because these individuals already have legitimate credentials, traditional perimeter defenses like firewalls often fail to trigger any alarms.

Managing this risk doesn't require expensive surveillance software, but a culture of accountability and least privilege. By ensuring that employees have access only to the specific files and systems necessary for their current role, you significantly limit the impact of any single compromised or rogue account. Furthermore, having a clear offboarding process is critical. Far too many breaches stem from a simple oversight of a former employee's email or VPN access that was never deactivated, leaving a digital back door open long after they've left.

Implement these mitigations to protect your team from insider threats:

- **Enforce the Principle of Least Privilege Access:**
  Restricting the access of your users to *just* the window that they need to see, and nothing more, mitigates a number of different threats – not just ones from the inside. Conduct a quarterly access audit to ensure that staff can access only the data they need for their specific jobs. Use the built-in permission settings in your online workspace to restrict admin roles to only one or two people and move sensitive folders (like HR or Finance) into restricted-access silos.

- **Establish a Standardized Offboarding Checklist:**
  Create a formal protocol for when an employee or contractor leaves. This should include immediate revocation of access to email, cloud storage, and internal apps, as well as the remote wiping of any company data from personal devices used for work.

## SECURITY PRACTICE #5: Malware Detection

*Not all malware is known, and its customization is getting easier to create.*

Malware is the catch-all term for malicious software, including viruses, ransomware, spyware, trojans, and anything else designed to break in, lock you out, or steal what's yours. Traditional antivirus software is no longer something that can be set up and forgotten about. In the past, security tools relied almost exclusively on signatures – a digital fingerprint of known viruses. In the modern age, attackers have pivoted to leveraging AI and other tools to keep organizations and antivirus software on their toes.

Effective detection now requires a shift towards endpoint detection and response (EDR). Unlike traditional antivirus software that looks for what a file is, EDR looks at the file's activity. An EDR tool can detect suspicious behavior and automatically terminate processes, stopping malicious entities like malware strains in their tracks. With a shocking 88% of SMB breaches involving ransomware, according to the 2025 Verizon Data Breach Report, defending against this breed of attack is all the more important.

Fortify your organization against malware with these steps:

**Upgrade to Modern Protection**
EDR tools don't have to break the bank. If you are already a Microsoft 365 subscriber, ensure you are utilizing Microsoft Defender for Business (included in Business Premium), which provides EDR-level protection rolled into your existing suite of tools. Google also provides endpoint management tools which are rolled into many of their Workspace editions; for Mac users, the standard is Jamf Protect. If you have no baked-in endpoint management tools, there are a range of effective EDR products available for purchase at a low cost.

**Implement Tamper Protection**
Modern security software often has a "tamper protection" toggle that prevents malware from disabling your antivirus. Enabling this feature is free and blocks one of the first steps a malware script takes after gaining a foothold on a device.

**Automate Weekly Vulnerability Scans**
Free, open-source tools are available that can scan your network for unpatched software. Finding and patching the holes in your software before malware can crawl through them is a high-impact, zero-cost defensive move. Don't worry, we'll go over patching in more detail later in this guide (Security Practice #9!).

If managing malware detection on your own feels overwhelming, consider partnering with a managed service provider (MSP). An MSP is a third party that provides 24/7 monitoring and incident response for your team for the cost of a subscription. There are many affordable options; for some businesses, outsourcing to an MSP may be the most cost-effective way to stay secure without the overhead of an extensive IT department, or the time cost of keeping up with these tools yourself.

# SECURITY PRACTICE #6: Adversary Eviction

*If they can't stay, they can't prey on your data.*

Adversary eviction involves removing an attacker who has already successfully infiltrated a network and is lying in wait to strike. Keeping the “dwell time” – the period an attacker remains undetected while establishing a presence in the network and gathering information – low is essential, as the longer the dwell time, the bigger the damage. Though the median dwell time is 11 days, according to Mandiant’s 2025 M-Trends Report, for small businesses without round-the-clock monitoring, it can stretch into weeks or months.

During this time, attackers can deploy backdoors that allow them to return, even after passwords have been changed. They are also increasingly using legitimate administrative tools, such as PowerShell, to stay longer, making them almost invisible to standard antivirus software once they’ve gotten a foot in the door.

The goal of eviction is to achieve a clean slate. This involves identifying every compromised account, persistent remote access tool, and corrupted backup. Kicking out adversaries in part will often accelerate their attack, triggering ransomware to burn the evidence before they lose access entirely. This is why a coordinated, decisive eviction is often safer than a piecemeal approach. For an SMB, this means not just deleting a malicious file, but resetting the entire digital perimeter simultaneously.

Rid your system of long-term dwellers by taking the following steps:

**Perform a Global Password and Token Reset**
If a breach is confirmed, a single password change isn't enough. Use administrative consoles to revoke active sessions for all users and force a global password reset. This kills the tokens that allow attackers to stay logged in without needing a password.

**Audit and Disable Administrative Accounts**
Attackers often create a new, innocuous-looking service account to maintain access. Regularly export your user list to a spreadsheet and verify that every account with admin privileges is tied to a current, known employee. If you don't recognize the account, disable it immediately.

**Isolate and Rebuild via "Known Good" Backups**
Never trust a machine that was touched by an adversary. Use the 3-2-1 backup rule (3 copies of data, 2 different media types, and 1 copy stored offsite) to restore systems to a point in time before the earliest evidence of the breach. Reimaging a compromised laptop from a clean backup is often faster and much safer than trying to clean the infection manually.

## SECURITY PRACTICE #7:
## Third-Party Risk / Supply Chain Vendors

*Know your neighbors, as security is only as strong as your weakest vendor.*

Defending against supply chain attacks starts with a simple reality of knowing exactly what and who you are connected to. These attacks occur when a hacker targets a partner or software provider to gain a backdoor into your business, rather than attacking you directly. Because you can not protect what you do not know you have, visibility is your most important resource. For any technology-reliant business, maintaining a living inventory of every third-party vendor, software provider, and service touching your network is non-negotiable. This includes everything from your core accounting software to the remote tools used by your managed service providers.

To stay ahead of these attacks, you apply the principle of least privilege access. This means tightly limiting vendor remote access to specific times and roles rather than leaving a permanent open door into your network. Ideally, this access should be routed through a dedicated VPN or a simple access management tool that lets you revoke their key instantly once the job is done. By ensuring that vendor access is disabled as soon as it is no longer needed, you eliminate a massive amount of risk to your operation without requiring a significant financial investment.

Lastly, stay informed and inquisitive. You should be an active participant by subscribing to vendors' security alerts and monitoring resources like CISA's Known Exploited Vulnerabilities (KEV) catalog. Don't be afraid to ask your partners the hard questions. If a vendor cannot confirm they use multi-factor authentication (MFA) internally or refuses to discuss their incident history, they are a liability. Utilizing free resources, such as the IT-ISAC's Critical SaaS SIG whitepaper on shared responsibility, can help you understand and ensure that when a product is delivered, you know exactly which security features you need to enable yourself.

## SECURITY PRACTICE #7: Third-Party Risk / Supply Chain Vendors

**Aggressively Apply Least Privilege Access to Vendors**
Never grant always-on access to third-party service providers. Manually enable a dedicated VPN account or remote desktop session only for the duration of a specific maintenance window, then disable it immediately afterward.

**Inquire About Your Vendor Security**
Before renewing a contract or signing a new SaaS provider, require answers to three specific questions:

- Do you require MFA for all user accounts?
- Have you experienced a security incident or breach in the past 24 months? If yes, provide the summary report.
- Is the product "Secure by Default," with high-risk features configured securely out of the box rather than requiring customer hardening?

**Subscribe to Automated Vulnerability Alerts**
Monitor the pulse of your supply chain for free by subscribing to CISA's Known Exploited Vulnerabilities (KEV) Catalog and vendor-specific security advisories, as well as your specific software tools' security alerts. Staying informed allows you to patch or disconnect a compromised service before an attacker can utilize the exploit against your specific instance.

# SECURITY PRACTICE #8: Multi-Factor Authentication (MFA)

*One lock isn't enough. Add another.*

Your password is a key that provides open access to highly sensitive information and critical systems. However, in today's threat landscape, even complex passwords or passphrases are only a baseline defense. By layering MFA over your accounts, you transform a simple entrance into a high-security vault. According to the Microsoft 2025 Digital Defense Report, MFA remains the most effective deterrent against identity-based attacks, potentially blocking over 99% of unauthorized access attempts.

Organizations are moving beyond passwords and are requiring additional parameters. MFA acts as an essential secondary barrier, requiring not just what you know (a password or passphrase) but something physical, such as a smartphone app or a dedicated hardware security key. This ensures that even if an attacker manages to obtain a password through a data breach or phishing site, they would still need physical access to a user's mobile device or token to gain entry. For small businesses, this is a cost-effective way to increase defenses without a massive overhaul of existing infrastructure.

While any MFA is better than none, not all methods are created equal. Text message-based (SMS) MFA is a good starting point, but it can be vulnerable to advanced techniques like SIM swapping. Application-based MFA, such as Microsoft Authenticator or Google Authenticator, is even better because it relies on encrypted, time-based codes or push notifications that are much harder for a remote attacker to intercept. Transitioning your team to these phishing-resistant methods creates a stronger lock than a simple password.

**Audit and Enable MFA Everywhere**
Review every business-critical account including email, cloud storage, and financial portals – and toggle on MFA. Most modern platforms include MFA in their base subscription tiers at no additional cost. Prioritize accounts with administrative privileges, as these are high-value targets for attackers. Need more information on how to get it done? Check out our one-pager on the topic.

**Standardize on Authenticator Apps**
Move your workforce away from SMS-based codes and toward authenticator apps. This removes the risk of middleman attacks that can intercept text messages. For your most sensitive accounts (like your primary domain admin), consider investing in a one-time purchase of a physical security key, such as a YubiKey, for the highest level of protection.

**Adopt Managed Passphrases**
Encourage the use of long, memorable passphrases instead of complex passwords that are hard to remember. To make this manageable, provide your team with a low-cost or free-tier password manager. This ensures that passwords remain unique across all services, preventing a single leak from causing a domino effect throughout your entire business.

## SECURITY PRACTICE #9: Patching

*Every unpatched system is an open invitation.*

In almost all businesses, software is the backbone of operations, but even the most robust applications can harbor hidden vulnerabilities. The speed at which attackers exploit these weaknesses is skyrocketing. The "time to exploit" — the window between a patch release and active exploitation — has shrunk to mere days, or in some cases, within 24 hours of disclosure, according to a 2025 threat landscape report from Fortinet. This makes unaddressed vulnerabilities some of the most dangerous entry points for cybercriminals.

The exploitation of known vulnerabilities remains a top-three entry vector for breaches, proving that many businesses are simply not patching fast enough to stay ahead of the curve. With the addition of emerging technologies like Anthropic's Mythos Model and Project Glasswing, vulnerability discovery and disclosure is going to increase exponentially, adding further strain to patch management processes.

To counter this, organizations must maintain a rigorous patch management cycle to ensure that software, firmware, and drivers are consistently hardened. For an SMB, the goal is to eliminate the window of opportunity. When patches are delayed due to compatibility testing, be prepared to implement temporary mitigations or isolate high-risk systems. Regularly monitoring vendor security advisories and the CISA Known Exploited Vulnerabilities (KEV) Catalog is a critical, zero-cost habit that ensures you aren't caught off guard by a zero-day threat.

### DID YOU KNOW?

A "zero-day" is a software flaw that attackers discover before the vendor does — meaning developers have had zero days to build a fix. Until a patch is released, every system running that software is exposed, and attackers know it.

## SECURITY PRACTICE #9: Patching

If a patch is not available or cannot be installed immediately, prioritize containment. Be prepared to isolate the affected machine by temporarily disconnecting it from the internet or segmenting it from the rest of your production network. This "digital quarantine" keeps your core infrastructure safe while you wait for a permanent fix. Staying current is not just a maintenance task, it is one of the most effective defensive barriers you can build.

**Automate Everything Feasible**
Enable automatic updates for operating systems and browsers. For Linux environments, use free tools like unattended-upgrades to ensure security patches are applied without manual intervention, drastically reducing your exposure window.

**Monitor Threat Intelligence for Free**
Subscribe to CISA's KEV Catalog and vendor-specific security mailing lists. Knowing which vulnerabilities are being actively exploited in the wild allows you to prioritize the emergency patches over routine updates.

**Establish a Quarantine Protocol**
Ensure your team knows how to quickly isolate a compromised or vulnerable asset via VLAN segmentation or a physical disconnect. Preventing "lateral movement" – where an attacker that has already entered your network attempts to infiltrate deeper – is the difference between one compromised workstation and a company-wide ransomware event.

# SECURITY PRACTICE #10: Employee Training

*A trained employee is a security asset. An untrained one is a risk.*

Despite robust technical defenses, the human element remains the most targeted link in the cybersecurity chain. Careless or uninformed employees remain the top insider threat concern for 73% of security professionals heading into 2026. A single staff member's mistake can bypass even the most expensive firewall, making comprehensive and ongoing training a business necessity rather than a simple compliance checkbox.

Effective training is frequent, engaging, and relevant to the modern threat landscape. One-off annual slide decks or videos are largely ineffective. Organizations are moving toward ongoing microlearning modules — short, targeted lessons that take five minutes or less and focus on current trends, such as AI-driven social engineering or deepfake voice scams. By keeping security at the forefront of the daily workflow, you foster a culture of vigilance where security becomes second nature.

Ultimately, the goal of training is to transform your staff from a vulnerability into an active part of your detection system.

**Implement Microlearning and Teachable Moments**
Swap long annual seminars for monthly five-minute briefings. Use free resources like CISA's toolkits or SANS OUCH! newsletters to provide timely tips. When an employee fails an internal test or makes a minor error, provide immediate, constructive feedback rather than punishment to reinforce the correct behavior.

**Gamify Phishing Simulations**
Use low-cost simulation platforms to send fake phishing emails to your staff. This gives them a safe environment to practice spotting red flags. Recognize and reward the top reporters – those who consistently flag test emails – to reinforce security habits.

**Continuous Re-Testing and Validation**
Training is not a one-time event. Implement a recurring retesting schedule in which employees who struggle with specific concepts (such as identifying deepfake audio or spotting lookalike domains) are automatically enrolled in targeted follow-up drills. This ensures that the learning "sticks" and allows you to track measurable improvement in your organization's resilience over time.

# CONCLUSION

Maintaining your organization's cybersecurity is not a static goal to be reached, but a continuous cycle of adaptation and improvement. The security practices outlined in this guide combine to form a multi-layered defense designed to mitigate the threats posed by today's evolving adversaries. It is important to move away from reactive measures and develop a proactive security posture to protect not just your team and data, but your customers as well.

Adopting these practices allows your organization to substantially lower its risk and recover faster from incidents, all without requiring a massive overhaul of your budget or staff. These are small adjustments that can yield big impact, protecting your most valuable assets and ultimately saving your business significant time and money.

And of course, we would be remiss not to mention joining an ISAC as another safeguard against cyber threats in your organization's sector. ISACs expand a small cybersecurity team's network of defenders, acting as a force multiplier through collaboration with hundreds of peer analysts. The IT-ISAC has helped IT sector organizations defend by providing a platform for information sharing and producing its own timely cyber threat reporting for over 25 years.

Every proactive step you take strengthens both your own posture and the stability of the entire network. Sharing knowledge helps to create a more secure landscape for the sector as a whole. We defend better when we defend together.

**Information Technology - Information Sharing and Analysis Center (IT-ISAC)**

Founded in 2000, the IT-ISAC is a non-profit organization that augments member companies' internal capabilities by providing them access to curated cyber threat analysis, an intelligence management platform, and a trusted forum to engage with senior analysts from peer companies.

**Learn more at IT-ISAC.org or email us at membership@it-isac.org.**