Spotlight on cybersecurity strategies for SMBs

Integris.

Why SMBs should reevaluate their cybersecurity posture today

Malicious attackers continue to target smaller companies with cyberthreats, including using email phishing and deepfake scams.

Today's cybersecurity environment is challenging—no doubt. Email security threats such as phishing, quishing, and deepfake fraud continue to target smaller and midsize (SMB) companies and enlist sophisticated tactics.

These attacks also have an outsized impact on smaller companies. According to Mass Data, the success rate for cyberattacks against small businesses averages 67% compared with 23% for large enterprises. Moreover, 78% of SMBs are concerned that a major cybersecurity incident could put them out of business.

Many smaller organizations may have implemented some cybersecurity tools, but they often lack a layered, defense-in-depth approach. Today's best cybersecurity practices require SMBs to think more holistically, creating cybersecurity strategies for all the layers of IT infrastructure, from endpoint security to software applications to network security and end-user risk mitigation.
In what follows, we explore how companies can solidify their cybersecurity posture. Bolstering cybersecurity encompasses a variety of tactics, including email security tools, real-time threat monitoring, employee education and training, and more.

In the articles “Email security threats remain key source of organizational data breaches," and in “Top email phishing scams SMBs can expect in 2026, and what to do about them,” we explore various email security threats, such as phishing, quishing (using QR codes to send users to scamming sites), whaling (sending personalized attacks that target executives), and vishing (creating voice-based messages to dupe recipients into revealing sensitive data or sending money). In both pieces, we outline how threats are morphing and how SMBs can ward them off most effectively with the help of managed service providers (MSPs).

78% of small and midsize businesses are concerned that that a major cybersecurity incident could put them out of business

Next, the article “What can cybersecurity awareness training do for my company?” outlines how integral user education wards off malicious attackers. IT emphasizes how MSPs can help clients train their employees to protect their passwords, employ social media best practices, and recognize the latest cyberattack methods coming to their inboxes. Finally in, “Human risk management: How MSPs protect organizations against a key threat” we explore how, shockingly, human error lies at the heart of some 95% of cyberattacks. We also explore how MSPs can deploy human risk management (HRM), which combines training, monitoring, and policy enforcement to mitigate human error and turn employees into security assets.

We hope this handbook will help you explore key considerations to improve your cybersecurity posture—possibly with help from a managed service provider.

Jeremy Pogue
Director of Security Services
Integris

By Lauren Horwitz

Email security threats remain key source of organizational data breaches

Email security threats hit small businesses hardest. Managed service providers provide tools, training, and AI to prevent breaches, detect threats in real time, and ensure strong cybersecurity hygiene.

Key takeaways:

- Phishing and related tactics like whaling, vishing, and quishing account for more than 80% of email-related security threats, disproportionately affecting smaller businesses, which often have limited resources and expertise.
- Combining tools like multifactor authentication, email filtering, authentication protocols, and real-time threat detection, along with continuous employee training, is essential for defending against advanced email threats such as spoofing, malware, and business email compromise.
- Managed service providers offer real-time threat detection, employee training, and security incident response, making them key partners in helping organizations maintain strong cybersecurity hygiene.

Email is an indispensable tool in office collaboration and communication. But malicious actors continue to pose email security threats that cause significant data and financial losses. Small and midsize businesses (SMBs) are disproportionately affected, suffering an average loss of $328,000 per incident.

Email phishing – in which scammers send fraudulent email messages to trick recipients into revealing personal data – remains a distressingly common email security threat vector. But today, attackers are finding other inventive methods as well. Other tactics include quishing (using QR codes to send users to scamming sites), whaling (creating personalized attacks against executives) attackers target executives), and vishing (sending voice-based messages to dupe recipients into revealing sensitive data or sending money).

According to Zivver's "Widening disconnect between email security and risk management" report, phishing accounts for more than 80% of reported security incidents in 2024. Consider, too, that according to the "World Economic Forum's 2025 Global Cybersecurity Outlook, 72% of respondents cited an increase in organizational cyber-risks, with ransomware remaining a top concern.

"Small and medium-sized businesses are more susceptible to an email vulnerability because of limited internal resources," said Jayson Saumer, product specialist at Integris. "Given the rapid evolution of today's cyberthreats, email security in particular necessitates frequent updates and a high level of specialization to remain current and effective."
That's why organizations need to shore up email cybersecurity strategy, through software tools, policies, and procedures that reflect their industry's data requirements and employee training. Some of these areas may require expert guidance – which is where a managed service provider comes in.

Types of email threats

Table 1: Email threats and solutions to address them

Email threat	Solution
Email phishing. With this type of cyberattack, malicious actors can send fraudulent emails to trick recipients into revealing sensitive personal information, such as passwords, credit card numbers, or other login credentials. Email messages often appear to come from legitimate sources and use deception, such as spoofed sender addresses and fake websites, to steal personal data, creating financial loss or identity theft.	Effectively addressing email phishing involves a combination of strong user habits and robust technical defenses. Key strategies include enabling multifactor authentication (MFA), using strong unique passwords, and being cautious with links and attachments. Additionally, organizations can implement technical solutions like advanced email filtering, anti-malware software, and user training to provide a comprehensive defense against phishing attacks.
Spear phishing and whaling. In these kinds of email security threats, malicious attackers target specific people.	A combined approach merges employee training with tools to identify this tactic. Key solutions include continuous security awareness training to help users spot malicious emails, implementing multifactor authentication (MFA) to add an extra layer of security, and deploying advanced email security solutions with features like secure email gateways and email authentication protocols (SPF, DKIM, DMARC) to filter out threats before they reach inboxes.
Vishing, or voice phishing, is a scam that uses phone calls to steal sensitive information. Malicious attackers scam recipients with faked voice messages – often created with AI – to trick users into sending sensitive data or money.	In an era of largely digital communication, vishing is catching more users unaware. It requires proactive prevention and immediate action if a user is targeted. To prevent vishing, users should be skeptical of unknown callers, never give out personal information over the phone, use call-blocking tools, and register on the National Do Not Call Registry. Victims should change compromised passwords, contact institutions such as banks, and report the incident to the FTC and local authorities.
Malware attachments. Malicious files can be attached in applications such as Word or Acrobat that, when opened, can compromise a user's computer or sensitive data.	Key solutions include using up-to-date antivirus and email filtering tools, with advanced features like sandboxing and attachment restrictions. Just as important, it must be paired with user education on identifying and avoiding suspicious attachments.

Email threat	Solution
Business email compromise. Malicious actors increasingly use these tactics where they impersonate executives or legitimate business partners to trick employees into sending money, providing sensitive information, or making fraudulent transactions.	Key solutions include implementing MFA, email security tools such as DMARC (an email authentication protocol) with a reject policy, establishing strong financial transaction approval procedures, and consistently training employees to identify and report suspicious emails.
Email spoofing. More than 90% of the world's top email domains are vulnerable to email spoofing. With spoofing, a malicious actor can falsify the sender's information in an email header, making it appear to come from a legitimate or trusted source.	The solution to email spoofing involves implementing email authentication protocols such as SPF, DKIM, and DMARC, along with undertaking vigilant user education on how to recognize and report suspicious emails. Anti-spam and anti-virus solutions, keeping systems updated, and enabling MFA are also critical.

The key for organizations to prevent email security threats from having impact on data is to develop strong cybersecurity hygiene. Let's explore the key components–and why managed service providers can help implement.

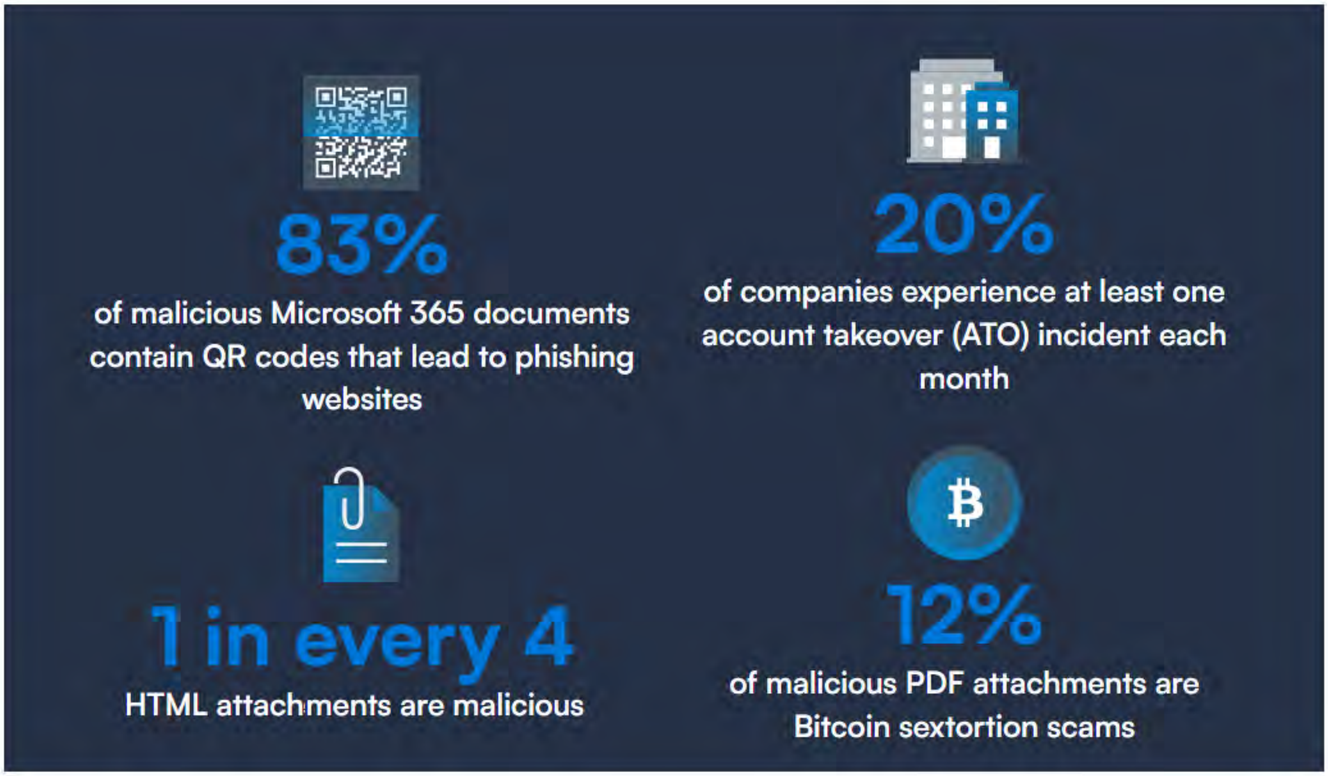

Figure 1: Malicious actors take advantage of various threat vectors, such as QR codes and attachments.
Source: "2025 email threats report," Barracuda, 2025.

Types of email security strategies

Authentication and access controls

Multifactor authentication (MFA). Enforce MFA for all email accounts. With MFA, users are required to provide two or more verification factors to gain access to an account or system, adding extra layers of protection beyond a simple password.

Strong password policies. Strong passwords aren't just long and hard to remember. They use complex, unique passwords that combine uppercase and lowercase letters, numbers, and symbols, require regular password changes, and prohibit reuse. Strong password policies also include mandatory MFA, establishing password expiration rules, and implementing account lockout after failed attempts. Finally, organizations with strong password policies often use password managers, which encrypt passwords in a secure digital vault.

Email content protection

Email encryption. There are two common types of email encryption:

- Encryption in transit (e.g., TLS/SSL/STARTTLS)
- End-to-end email encryption or public key encryption

Organizations with sensitive data – such as law firms' client and case data or banks' customer data – must institute tools to protect this data in transit and at rest.

File-sharing platforms. Additionally, organizations with strong email content protection policies often require secure file-sharing platforms for confidential data, and discourage employees from sharing passwords, credit card information, or personally identifiable information (PII) in unencrypted emails.

Threat detection and awareness

Phishing detection. As Figure 2 indicates, companies expect to address email security threats with AI, using the tech to identify phishing (49%) and produce real-time threat detection and security recommendations (49%). But employees also need continuous training to identify suspicious emails and new scammer techniques.

Anti-phishing tools. According to the forthcoming Integris "2025 technology adoption and spending" survey data, only about a third of 1,500 respondents use email filtering tools (36%) and real-time email scanning (35%). More than half of these respondents (57%), however, also reported an email-based data breach. These kinds of real-time monitoring technologies, paired with employee training, are key for combatting email-based threats. Email filtering and scanning are critical to stay ahead of today's email security threats.

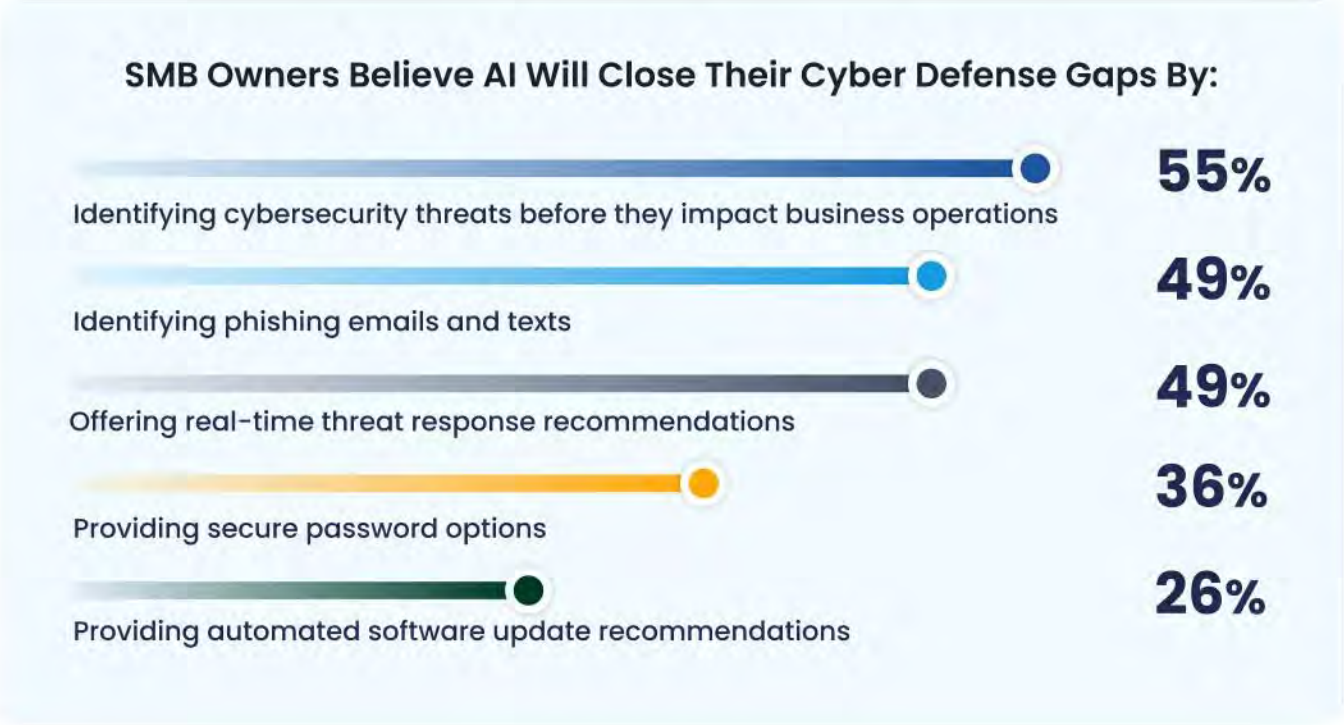

Figure 2: Small and midsize companies see AI as a tool to close the gap on cyberthreats.
Source: VikingCloud, "2025 SMB Threat Landscape Report: Small and Medium-Sized Businesses, Big Cybersecurity Risks," March 2025.

AI-enabled email monitoring. Increasingly, IT professionals see AI as an enabler in tackling malicious threats. Nearly half (49%) of respondents to a VikingCloud survey see artificial intelligence as an effective tool to identify phishing email and texts and provide real-time response recommendations.

Device and endpoint security. Email data is only as secure as the device on which it resides. And indeed, 80% to 90% of all successful ransomware compromises originate through unmanaged devices, according to "Microsoft digital defense report." Organizations must deploy antivirus scanning and anti-malware software on laptops and mobile devices. They should also enforce screen-locking policies and disk encryption and keep all email platforms and operating systems up to date.

Email account management

Least-privilege access. Organizations should limit access to email accounts based on a user's organizational role. Least-privilege access is when organizations give a user or group the minimum level of permissions needed to perform a given task. This default is also key to minimizing data breaches.

User offboarding. When users leave an organization, IT departments should be ready to decommission their email and login credentials. IT staff can set up automated workflows that initiate on an employee's last day of work, such as Entra, for example.

Monitoring account activity. Organizations need real-time insight into account activity and the ability to enable logging and alerts for unusual behavior. AI tools are a clear asset in this regard, and managed service providers are already using AI-enabled email monitoring to detect, mitigate, and even proactively prevent threats.

Email disaster recovery and business continuity

Backup and recovery and email archiving. Email backup provides for disaster recovery and short-term protection of email messages, creating a copy of your emails to restore them after loss.

Email archiving, conversely, is for long-term, tamper-proof storage of all communications, designed for legal compliance, e-discovery, and easy retrieval over extended periods. While a backup can be used for data recovery, it's not the solution for long-term retention and legal purposes because it can be altered or deleted. Archiving focuses on preserving every message for future reference and legal requirements, often using journaling to capture every email in real-time.

User training and policy. While tools and policies are critical to preventing email cyberthreats, human awareness and behavior are by far the most critical aspects of ensuring email security.

But there are persistent gaps in email security awareness training. According to 2024 Hornet data, 25% of organizations still don't offer cybersecurity training. Mimecast estimates, human error contributes to 95% of cyberattacks. Organizations may lack the staff and expertise to develop a robust cybersecurity training program. Regular employee training is a key area in which MSPs can provide substantial added value. They can not only train staff but document clear email policies and develop cybersecurity testing, such as simulated phishing attacks, to improve staff readiness.

How MSPs respond in the wake of an email breach

When an email breach occurs, MSPs follow a structured incident response plan to contain the damage, eradicate the threat, and restore services for their clients. This process is crucial for minimizing downtime, reducing financial losses, and protecting their clients' reputations.

- ✓ **User reporting.** An effective system, such as a "report phishing" button in the email client, allows employees to flag suspicious emails, which helps the MSP detect active threats.
- ✓ **Threat analysis.** Once a potential breach is identified, the MSP investigates the scope of the attack to determine which accounts, systems, and data have been compromised.
- ✓ **Purge malicious emails:** MSPs configure email applications to search for, quarantine, and purge malicious messages.
- ✓ **Reset credentials:** If user passwords have been compromised, accounts must be reset. If a data breach occurs, an MSP may enforce a password reset for all users. MFA is enabled or reinforced for high-risk and newly created accounts. Further, MSPs may use identity threat detection and response (ITDR) to lock down an account automatically if it suspects malicious activity.
- ✓ **Remove persistence mechanisms:** Organizations may not realize that there are backdoor accounts that a malicious attacker has created to maintain access. An MSP can identify and deactivate these accounts.
- ✓ **Patch vulnerabilities:** MSPs can identify the source of the breach–whether through a nefarious link, attachment, or other source, and address vulnerabilities.
- ✓ **Employee communications.** MSPs can also provide alerts about malicious activity and provide guidance to employees to prevent further losses.

MSPs: Your partner can help ward off email security threats

Cyberthreats, including phishing and malware, can strike at any time. MSPs can provide around-the-clock monitoring and management – often with AI-enabled tools – to detect and respond to threats in real time, which is not feasible for most small businesses.

MSPs use a proactive strategy to prevent issues. They deploy advanced tools, perform vulnerability scans, and apply patches to close security gaps before they can be exploited. But if a breach is detected, MSPs can follow a structured process to minimize data loss, identify the source, and alert the organization.

> "Businesses gain access to comprehensive expertise and seasoned professionals when outsourcing email security to MSPs." – Jason Saumer, Integris product specialist

Finally, MSPs are uniquely positioned to develop employee training and education to prevent breaches. Given that humans participate in such a majority of cybersecurity breaches, MSPs can help humans forward organizational cybersecurity hygiene.

“Businesses gain access to comprehensive expertise and seasoned professionals when outsourcing email security to MSPs,” Saumer emphasized. "This allows them to use advanced security tools and methodologies, keeping the latest protective measures against evolving threats, as well as ensuring compliance with relevant regulations.”

Organizations also gain safe access to advanced tools like AI that detect and respond to all types of threats. And MSPs also provide tailored training and testing to ensure that employees safeguard email security and understand evolving email security threats.

Integris offers two tailored options for email security: Core Email Security delivers AI-powered protection against phishing, malware, spam, and email-based data loss prevention, while Advanced Email Security adds reporting and archiving to meet strict compliance and governance needs for regulated industries.

Learn More:
Integris cybersecurity solutions
IT assessments
Responsible IT Architecture framework.

Lauren Horwitz

As Director of Content Marketing at Integris, Lauren brings 18 years of experience in digital publishing and editorial leadership. She specializes in content strategy, SEO, and leveraging data insights to create impactful stories. Lauren has held senior roles at HUMAN Security, Dynatrace, Informa Tech, Cisco.com, and TechTarget, shaping content for technology and business audiences.

By Patrick Dulmage, CISSP, MBA

Top email phishing scams SMBs can expect in 2026, and what to do about them

Malicious attackers have gotten inventive, launching new email phishing scams to trick users out of personal data and money. Here’s what to watch out for in email security.

Key takeaways:

- AI-driven email scams are rapidly evolving, making phishing attempts more personalized and harder to detect.
- Emerging threats like deepfake fraud, vendor email compromise, and QR code phishing are targeting SMBs with sophisticated tactics.
- Layered security – combining AI-powered detection, employee training, and robust verification protocols – is essential to defend against new email scam technology.

Forecasting email risk for 2026

I think most people in the cybersecurity industry would agree: AI has introduced a revolutionary level of heightened threats coming from email phishing scams. Cheap AI has made it possible for anyone to produce a highly personalized email that's tough to distinguish from a legitimate email from a co-worker, vendor, or even a family member. Now AI can translate convincingly into any language, code custom malware, generate startlingly high-quality voice, video, and audio deepfakes, and so much more. In general, we can no longer trust what we see or hear – and that goes double for our email inbox.

So, what does this mean for the average small or medium-sized business that's just trying to keep its email inboxes safe? Truthfully, it's a bit of a good news/bad news situation. The bad news: Anyone with an ax to grind and a laptop can launch a sophisticated email attack against your company. But here's some good news. The tools we're using to catch cyberthieves are using more advanced technologies, too.

However, before we get into best practices for defense, let's talk first about where the threat landscape stands for today's companies.

Email phishing scams 2026: How threats are changing

According to Mimecast's 2025 State of Human Risk Report, 95% of data breaches involve the human element. Verizon's Data Breach Investigations Report for 2025 breaks it down further, showing that risks coming from third-party vendors doubled to approximately 30%, pointing to a growing sophistication in researched, targeted attacks.

The days of easy-to-spot phishing tactics are over. No more loan requests from "Nigerian princes" or emails sent with egregious spelling errors and bad grammar. "Zscaler ThreatLabz 2025 Phishing Report" backs up this idea. Its analysis indicates that phishing volume declined overall but shifted to more customized campaigns aimed at high-value targets such as human resources, payroll, and finance departments. The report said these attacks were also more likely to use video phishing and CAPTCHAs (photo ID test) to evade filters.

Perhaps that's why cyberattacks in general seem to be getting more devastating. According to the latest FBI IC3 report on U.S. cybercrime in 2024, 859,532 complaints were registered with a total of $16.6 billion in reported losses–up 33% year over year. Of that, $2.7 billion was specifically from business email compromise.

Emerging email phishing scams to watch out for in 2026

Threat no.1: Audio and video deep fake fraud

Deep fakes have gotten publicity lately, mainly because they are frighteningly efficient. Today, scammers can now impersonate the voice and video image of nearly anyone starting with nothing more than a quick voice clip or a stolen headshot. The deep fakes aren't just short, scripted outputs, either. Scammers can have deep-fake live conversations in real time.

One of the most notable examples of this occurred at a Hong Kong finance firm, when a video deep fake version of its CFO convinced the finance department employee to transfer $25.6 million to a series of 15 different overseas bank accounts. The interaction began with an email, which then escalated to a meeting request for a live video call. The employee chatted in real time with a live action deepfake CFO, who claimed to be with the board of directors and needed the money for upcoming investments. The perpetrators – and the money they stole – have never been found.

This scam tech has nearly endless applications. Online guides are circulating the dark web, teaching people how to use deepfake AI to circumvent common "proof of life" checks for financial transactions and cryptocurrency purchases.

Cybercriminals use fake résumés and AI deepfakes to get work-from-home jobs – interacting with HR, IT, and their new co-workers just long enough to dump malware into company systems and steal valuable company data.

In a particularly depressing turn of events, a large number of actors are advertising on the dark web, offering to serve as the live-action talent behind the AI avatars used for deep fake crime. As the tools progress, so will the support industry around these scams.

What to do about deep fake threats

Assume all voice and video requests could be fraudulent. This is especially true if it has the following characteristics:

- involves the transfer of large sums of money
- includes the request for highly sensitive information
- has an element of urgency
- requires circumventing usual protocols or keeping the transaction confidential
- requests funds or information go to a new bank account or email address

Require enhanced verification. For transfers of any kind, require in-person verification by calling the recipient back at a phone number that can be independently verified. During live video calls, the requester should be required to display two pieces of identification. Predetermined code words or challenge questions can also help.

Threat no. 2: Vendor email compromise (VEC)

This complicated fraud starts with an incursion into your vendor's mailboxes. Scammers then lurk in real threads, learning your communication patterns. Then they reply in thread with altered invoices or updated banking instructions. Because it's coming from a trusted inbox, scammers don't even need links or attachments to prompt action.

Payloads from this type of gambit have been enormous. For instance, Reuters reported in 2025 that Ireland's National Treasury management agency, the state body that manages debt and sovereign wealth for the country, lost €5 million in a scam perpetrated by criminals impersonating a known investment partner.

This kind of loss is not surprising. CSO reported that 72% of employees engaged in their test of vendor email compromise – 90% higher than it would be in other kinds of business email compromise.

What to do about VEC attacks:

- Get AI-powered email analytics programs that detect subtle inconsistencies.
- Develop active vendor verification protocols whenever payments or sensitive information transfer is involved.
- Retrain employees on the new protocols, and educate them on social engineering attacks coming from vendor sources.

Threat no. 3: Quishing (QR code phishing) and MFA bypass

QR codes can be the perfect threat vector because they're not considered clickable links by the email filters and security gateways protecting your systems.

Attackers place QR codes in email messages, flyers, or stickers – sometimes covering legitimate codes at parking meters, retail stores, office signage, or of course, emails. When scanned, these codes direct victims to phishing sites that mimic trusted brands like Microsoft, Adobe, Docusign, and even carefully crafted fake payment sites. They then ask for login credentials, payment details, or multifactor authentication tokens.

QR Code Tiger recently reported on a variety of successful quishing scams, including fake parking tickets in San Francisco, QR codes for stealing credentials at Washington University, fake Microsoft 2FA expiring emails, and more. Online banking pages are particularly vulnerable.

What to do about quishing scams:

- Deploy AI-powered email security solutions that can scan and analyze QR codes embedded in images and attachments for malicious destinations.
- Implement IP filtering and restrict access to sensitive systems from unregistered devices or locations.
- Use advanced endpoint protection and mobile device management to monitor and block access to known phishing sites, even when accessed via QR codes.

Threat no. 4: Polymorphic phishing

Polymorphic phishing is a fancy way of saying that scammers flood the zone with highly personalized and varied messaging. Here's why that causes stress on your security systems.

Scammers start by creating similar but distinct versions of a phishing email as part of a targeted campaign. They then alter elements like the sender's name and address, subject lines, and even the scam email's body text. Artificial intelligence automates this process, creating personalized and convincing messages at scale.

Traditional security tools rely on common patterns and signatures. Polymorphic phishing bypasses these by ensuring no two email messages are exactly alike, preventing detection by block lists and secure email gateways.

Polymorphic capabilities are becoming standard in the automated phishing kits now available to scammers online. Even AI-based approaches to detection, such as natural language processing (NLP) and natural language understanding (NLU) can suffer from polymorphic randomization. Attackers have become creative with many using polymorphic attacks with invisible characters to "break" these systems.

What to do about polymorphic phishing:

- Implement multifactor authentication methods that are resistant to phishing, such as biometrics or hardware tokens, to prevent credential theft even if an employee is tricked by a polymorphic email.
- Extend monitoring beyond email to include SMS, collaboration apps such as teams or Slack, and social media, as polymorphic phishing can charge at multiple channels.
- Combine multiple security layers, including endpoint protection, secure email gateways, behavioral analytics, and threat intelligence feeds.
- Use advanced email security solutions that use artificial intelligence and machine learning to detect subtle inconsistencies and patterns across large volumes of messages. These tools can spot the randomized elements of typical polymorphic phishing and adapt to new attack variants.

Threat no. 5: HTML smuggling

HTML smuggling is an advanced cyber-attack technique that uses legitimate HTML5 and JavaScript features to assemble and deploy malicious payloads directly onto a victim's device. Here's how it works.

Malicious attackers will send a seemingly harmless HTML file through a phishing email. When the victim opens the HTML file in a web browser, an encoded or malicious script is opened. The script is too small to be flagged by security filters, because it's embedded within the HTML file using various JavaScript features. The victim's browser will decode and run the script, assembling the complete malicious payload onto the victim's local machine. JavaScript triggers an automatic download of the completed malware behind the network firewall, which is why network-level security controls fail to detect the threat.

While many users have been trained not to click on links in email messages, AI has made phishing emails much harder to detect overall. Victims may get an email that looks like an order confirmation from a favorite store, or an email from a family friend. The download seems to be generated from a legitimate website. In many cases, they may not know the link they clicked on had a silent script added.

What to do about HTML smuggling:

- Consider advanced security tools such as remote browser isolation (RBI) that can neutralize threats by isolating browsing activity in a secure, remote environment.
- Endpoint detection and response (EDR) tools monitor and detect malicious scripts and suspicious file creation on endpoints.

Preventing email phishing scams: Why every organization should have email encryption as a start

We've discussed a lot of different techniques for stopping scam emails. It's easy to be overwhelmed by the number of techniques and tools that are available to address these problems. So, the best way to get started on your email security is with a best-practice email encryption program.

Look for a tool that offers end-to-end encryption with Smart DLP, which ensures sensitive data is either encrypted or blocked from leaving the organization. The best platforms will integrate natively with Microsoft 365 and Google Workspace, detecting inbound and outbound threats. Choose solutions that provide encrypted archiving, detailed reporting and support for regulatory requirements such as HIPAA for medical data, GDPR for purchase data, and FINRA for financial data.

When you combine the latest email encryption tools with endpoint detection, identity management, user education, and a full cybersecurity stack, you'll be ready to repel most of the scam email that comes your way.

Talk to Integris about our Responsible IT Architecture program

At Integris, we refer to our cybersecurity approach as a Responsible IT Architecture – a program that gives our clients an interlocking set of cybersecurity that aligns with their compliance needs and standards set by the National Institute of Science and Technology (NIST). We'd love to talk to you about what we can do for you.

Contact us today for a free consultation.

Patrick Dulmage, CISSP, MBA

Patrick Dulmage, CISSP, MBA serves as Fractional Chief Information Security Officer at Integris, bringing over 30 years of IT expertise to help organizations align IT initiatives with business goals. With deep expertise in infrastructure assessment, risk management, and cybersecurity best practices, he partners with executive teams to strengthen operational resilience and achieve framework compliance.

By Susan Gosselin, senior writer, Integris

What can cybersecurity awareness training do for my company?

Programmed cybersecurity training can be the best way to fix the biggest cause of data breaches: human error.

Key takeaways:

- Global spending on cybersecurity awareness training is projected to surpass $10 billion by 2027 because 85% of cyberattacks originate from employee inboxes and devices, making staff education a critical defense layer.
- Modern programs deliver short, engaging online modules with monthly updates, teaching employees to spot phishing, create strong passwords, and follow best practices for data protection.
- These programs often include testing, reporting, and compliance tracking, providing proof of good cybersecurity practices for regulators, insurers, and clients.

Global spending on employee cybersecurity awareness training is predicted to exceed $10 billion by 2027, up from around $5.6 billion in 2023, according to the latest estimates from Cybersecurity Ventures. Why? Because more companies than ever are realizing employees are their best defense against hackers. In fact, industry analysts estimate that about 85% of the hacks come directly through employee inboxes and devices.

Cybersecurity awareness training has earned its place as a key part of a company's defenses. Fortunately, the cybersecurity industry has responded with training programs employees can complete online in quick, easy, and continuously updated lessons. Best of all, they're affordable, scalable, and easy to implement–even for small organizations. Here's what you can expect when you start shopping for security awareness training programs.

What is cybersecurity awareness training?

Cybersecurity awareness training is all about teaching your team how to keep your company's data safe from cyberthreats. It covers everything from spotting phishing emails and creating strong passwords to understanding malware and following best practices for data protection. By making sure everyone is up to speed on these topics, you can greatly reduce the risk of cyberattacks and stay compliant with regulations. Regular training helps build a security-first mindset, which is crucial for protecting both personal and company data in today's digital world.

What would a cybersecurity awareness training program look like at your company? Let's get into it.

How does cybersecurity awareness training work?

Most modern cybersecurity awareness training programs are delivered online in short training modules employees can watch on their work devices. New lessons come out monthly, and are delivered in fun, engaging videos. They highlight some of the latest tricks malicious attackers are using to lure employees into giving up protected data, sharing passwords, or clicking on bogus links that deliver malware into company systems. When employees finish watching the lessons, many programs will prompt them to take a quick test to prove that they've understood the material. The "grades" and completion certificates for these courses are then stored in the company's systems and usually attached to their human resources files.

The best programs will offer a company portal which will allow network administrators the ability to onboard/offboard users, store testing data, and generate company wide reports and tracking data. These reports provide crucial third-party attribution for your good cybersecurity practices. Regulators, cyber-risk insurers, potential vendors, and customers may ask to see these reports as part of routine cybersecurity reviews of your company. With programs like these, you'll be one step ahead of the game.

How much does cybersecurity awareness training cost?

Estimates for cybersecurity awareness programs will vary widely. We recommend having a trained IT manager from your staff or managed IT service provider secure a custom quote from reputable training companies. The cost of your program will depend on these factors:

- The number of employees, or "users," who will be taking the training
- The timeframe of its use – most cybersecurity awareness programs are billed on a yearly basis
- The complexity of the program

Most companies can expect to pay anywhere from $8 to $25 per user per year for a cybersecurity training program. Most providers will also charge a "setup fee" to get started which can run several hundred dollars. Once you've started a program, we recommend you stay with it, year after year. This ensures new employees get up to speed quickly, and existing employees stay up to date on the latest threats.

What does cybersecurity awareness training cover?

The best training programs teach employees how to be discerning internet citizens who can spot common traps and tricks hackers use. They'll use real-world examples ripped from the headlines to show what not to do. Rather than overwhelm, these training programs show how breaches can be avoided with a few common-sense strategies, and empower employees to be the front line of defense for their companies. Here's just a few of the topics you can expect to be covered.

Email safety
Employees learn how to spot spoofing, social engineering, malware, and phishing attempts. They will be given simulations to see if they can properly identify and respond to email scams and hacking attempts. Your team will learn how to tell suspicious URLs from good ones, how to verify a sender's address and identity, and how to protect confidential or proprietary information.

Safe online behaviors
From securing devices to the risks of installing unapproved software, your cybersecurity awareness training will cover unintentionally risky behaviors your employees do that could lead to a breach. From clicking on the wrong links, to accepting cookies and tracking software, employees will learn how to stay safe when they're surfing the web.

Social media compliance
What can you say and not say about the company you work for on social media? What social media sites are engines for thieves and disinformation? How can you avoid sharing personal information on social media that can give thieves clues to your passwords? A good social media fair use policy can help your organization set a code of conduct that will keep everyone safe.

Password hygiene
As part of any cybersecurity awareness training, employees need to learn about how dangerous certain behaviors are, like password sharing, weak password changes, and reusing passwords for multiple applications. Most trainings will also explain two-factor authentication, and why a double login is necessary.

Cybersecurity trends
What are the latest tools thieves are using to launch cyberattacks? Your entire team needs to understand just how sophisticated cyberattacks have become so they can learn to avoid them. Cybersecurity awareness training will cover threats, both new and existing. It will also cover best practices to identify and prevent potential breaches.

Interested in getting a training program started at your company?

Integris can help. We offer training programs for small and mid-sized companies, delivered by the industry's most trusted training vendors. We'd love to help you install, administrate, and monitor your training program. Contact us today for a free consultation.

Susan Gosselin

As a Senior Writer at Integris, Susan brings a wealth of experience in business journalism and communications. She has covered IT topics and trends for providers like Iconic IT and ProCoders Ukraine, as well as business publications including TechnologyAdvice.com, Datamation.com, and The Lane Report.

By Lauren Horwitz, Director of Content Marketing, Integris

Human risk management: How MSPs protect organizations against a key threat

Managed service providers can help organizations with a key cybersecurity risk: human behavior. Learn how an MSP is best positioned to provide human risk management strategies.

Key takeaways:

- Human error causes some 95% of cyberattacks. Managed service providers (MSPs) can deploy human risk management (HRM), which combines training, monitoring, and policy enforcement to mitigate human error and turn employees into security assets.
- MSPs deploy HRM tools such as risk assessments, configuration enforcement, phishing simulations , dark web monitoring, and continuous observation to identify vulnerabilities, close security gaps, and strengthen compliance.
- By offering training, strategic guidance, and best-practices frameworks, MSPs help organizations build a proactive security culture that reduces human risk, improves resilience, and stays ahead of emerging threats.

Managed service providers (MSPs) are well positioned to help organizations with a central cybersecurity vulnerability: human risk. In fact, email and collaboration security provider Mimecast estimates human error contributes to 95% of cyberattacks. And according to the "2024 Insider Threat Report," 48% of organizations reported that insider attacks have become more frequent over the past 12 months.

Just as organizations have to focus on external risks, they have to develop strategies for addressing internal cybersecurity risks. As a result, human risk management (HRM) is becoming a key approach to safeguarding companies against internal threats.

Organizations have come to recognize that they need HRM strategies to address human risks to cybersecurity. According to the same survey, 95% of respondents say that their organization is using AI to help defend against cybersecurity attacks and/or insider threats.

What is human risk management?

Human risk management is the practice of identifying, measuring, and reducing security risks that human behavior causes, such as clicking on phishing links or mishandling data. When successful, HRM mitigates human error and nefarious activity by combining security training, behavioral analysis, and policy enforcement to build a stronger security culture.

When formalized, the discipline of human risk management identifies human behavior that creates cybersecurity risk, such as these activities:

- ✓ clicking on phishing links in emails
- ✓ mistakenly sharing sensitive data with unauthorized recipients
- ✓ using or sharing weak passwords
- ✓ failing to update security patches
- ✓ connecting to unsecured Wi-Fi networks
- ✓ neglecting configuration drift and change management
- ✓ attempting to access or share privileged company information
- ✓ inadvertently leaving systems with critical data exposed due to misconfiguration

How MSPs help organizations deploy human risk management

MSPs offer critical expertise, tools and strategies, and training to deliver HRM. MSP methods include continuous monitoring, personalized training, and automated responses, enabling organizations to effectively transform an organization's workforce from a risk to a resilient security asset.

MSPs can mitigate this key source of vulnerability. They can identify individual risk, automate personalized security awareness training, run phishing simulations, and monitor exposed credentials on the web.

MSPs also manage identity and access management policies, assess risk through continuous monitoring and analysis, and provide visibility into security gaps to reduce vulnerabilities, reduce client risk, and foster a stronger security culture.

Key areas in which to deploy human risk management

Risk assessment. Through regular assessments, vulnerability scans, and platforms that provide real-time data and human risk dashboards, MSPs can uncover an organization's specific security blind spots and vulnerabilities – addressing these areas with policy and training if necessary.

Continuous monitoring. MSPs provide ongoing observation and analysis of an organization's environment to detect risk indicators and ensure that security controls are functioning correctly. Monitoring also encompasses visibility into employee actions, identifying patterns that might indicate malicious intent, such as unusual access attempts or data exfiltration attempts.

Identity and access management (IAM). According to a recent Cisco Duo report, 69% of respondents say that they lack visibility into identity vulnerabilities and 55% are into access management. IAM is a key area where MSPs can help organizations develop strategies and deploy solutions.

Compliance support. By helping clients adhere to regulations and manage security policies, MSPs mitigate risks of noncompliance, which can lead to fines, legal issues, and reputational damage.

Training and education. MSPs use human risk management platforms to assess user knowledge gaps and deliver customized, automated training programs. This helps to build a proactive security mindset, rather than a reactive one.

Phishing simulation. According to DeepStrike data, 36% of attacks begin with phishing. By automating and deploying regular phishing simulations, MSPs can gauge employee resilience to new attack techniques and provide immediate feedback and targeted training.

Dark web monitoring. MSPs can proactively monitor the dark web for stolen user credentials – acquired via third-party data breaches. MSPs can notify affected customers and take action to protect exposed accounts.

Policy management. MSPs simplify and streamline the process of managing security policies by using tools that auto-generated policies and also automate notifications and approvals, ensuring that users are consistently aware of and adhere to security standards.

Best practices-driven cybersecurity framework. Integris has developed a framework to ensure that an organization's cybersecurity platform is integrated, and proactive.

The Responsible IT Architecture (RITA) framework monitors current and emerging threats by identifying and finding the patterns in bad actors' behavior–so your cybersecurity strategy can anticipate and stay ahead of malicious attacks.

Strategic guidance and support. MSPs act as trusted advisers and support partners, guiding clients on where they should focus their security efforts and developing strategies to mitigate human error.

Only 6% of respondents to the Mimecast survey say that their organization's security policies are continuously updated based on emerging trends. This is where organizations can benefit from the work of MSPs – who stay abreast of novel strategies from malicious attackers.

Considering a new approach to HRM

If your organization hasn't taken a proactive approach to identifying, addressing, and mitigating human risk management, the status quo is dangerous.

Malicious attackers are becoming more sophisticated and rely on an engaged employee base to test and deploy new tactics. Now is the time to consider an IT assessment to understand your points of vulnerability and where human risk management – and potentially an MSP to help you build an HRM strategy – plays a part.

If your organization needs to reduce the human element in its cybersecurity posture, consider human risk management.

Learn more:
Integris cybersecurity solutions
IT assessments
Responsible IT Architecture framework.

Lauren Horwitz

As Director of Content Marketing at Integris, Lauren brings 18 years of experience in digital publishing and editorial leadership. She specializes in content strategy, SEO, and leveraging data insights to create impactful stories. Lauren has held senior roles at HUMAN Security, Dynatrace, Informa Tech, Cisco.com, and TechTarget, shaping content for technology and business audiences.

Integris.

About Integris

Integris is a national leader in future-ready managed services, delivering innovative solutions that drive digital maturity for small to midsize businesses.