TitanHQ™

# The State of Email Security in 2025

Annual Report

# Table of Contents

# Introduction

Organizations across the world face relentless growth in cyberthreats, as criminal groups leverage new technologies for malicious ends. The application of AI for offensive cyberthreats has threat actors rubbing their hands in glee, and organizations are racing to fight emerging offensive AI with defensive AI. In most years, we see continued evolution in the design of new types of attacks and threats - with recent explorations by threat actors focusing on MFA bypass in phishing attacks, new types of BEC attacks, QR code phishing, and early forays into deepfakes. Incidents and data breaches usually follow.

The past year has been no different, with mammoth incidents and data breaches hitting the headlines. For example (and this is by no means a long nor exhaustive list):

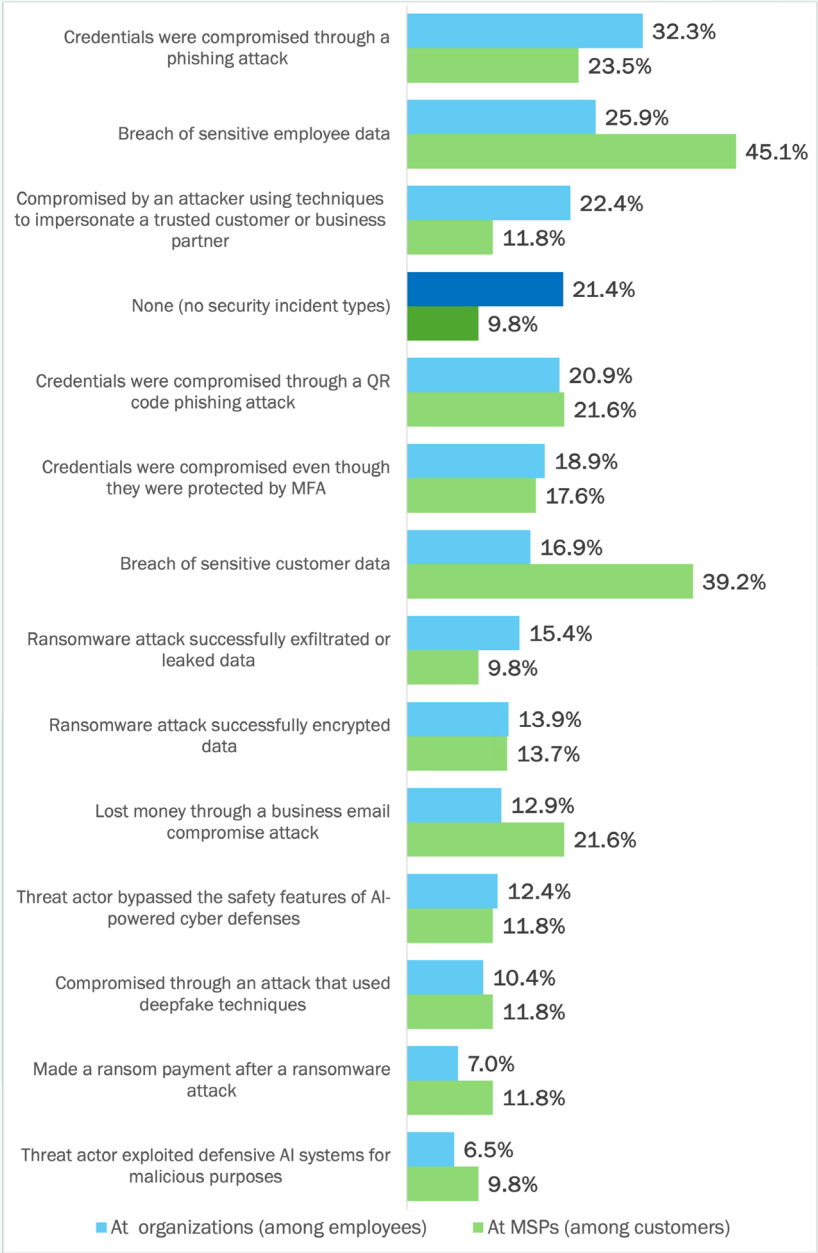
- The deepfake video meeting BEC attack against the Hong Kong office of Arup, which resulted in a US$25.6 million loss.
- The account compromise at Snowflake, resulting in many of its largest customers facing data breaches of tens and hundreds of millions of records.
- The data breach at National Public Data, which compromised 3 billion records from 270 million customers. The firm filed for bankruptcy because the blast radius of the breach was too significant to recover from.
- The data breach at MediSecure, which compromised data on 13 million people in Australia - or around half the population.

The research study we undertook for our annual report investigated the on-the-ground cyberthreat realities for much smaller firms - those with up to 1,000 employees. While the scope of the incidents experienced were less severe that the ones mentioned above, there is still fallout and consequential damages to handle.

## Most organizations were compromised by multiple types of incidents over the past 12 months

**79% of the organizations surveyed for this research experienced at least one of the cybersecurity incident types we asked about in the previous 12 months. Half of organizations experienced between 2 and 4 types of incidents.** Among the MSPs we surveyed, the incident rate was higher, with 90% saying they had customers who were compromised by at least one type of incident over the previous 12 months.

**Figure 1**
**Security incidents over the previous 12 months**
Percentage of respondents



**The most common types of incidents experienced by organizations were (see Figure 1):**

- Employee's credentials compromised through a phishing attack
- Breach of sensitive employee data
- An employee was compromised by an attacker using techniques to impersonate a trusted customer or business partner
- An employee's credentials were compromised through a QR code phishing attack
- An employee's credentials were compromised even though they were protected by MFA

In the survey, we did not assess the root causes of these incident types, such as organizations failing to patch software, the lack of defenses against zero day attacks, and the use of unsecured cloud infrastructure. These precursors, pre-conditions, or posture weaknesses are the starting point for many of the attack and incident trends we see affecting organizations and MSPs.

## The threat landscape is going from bad to worse

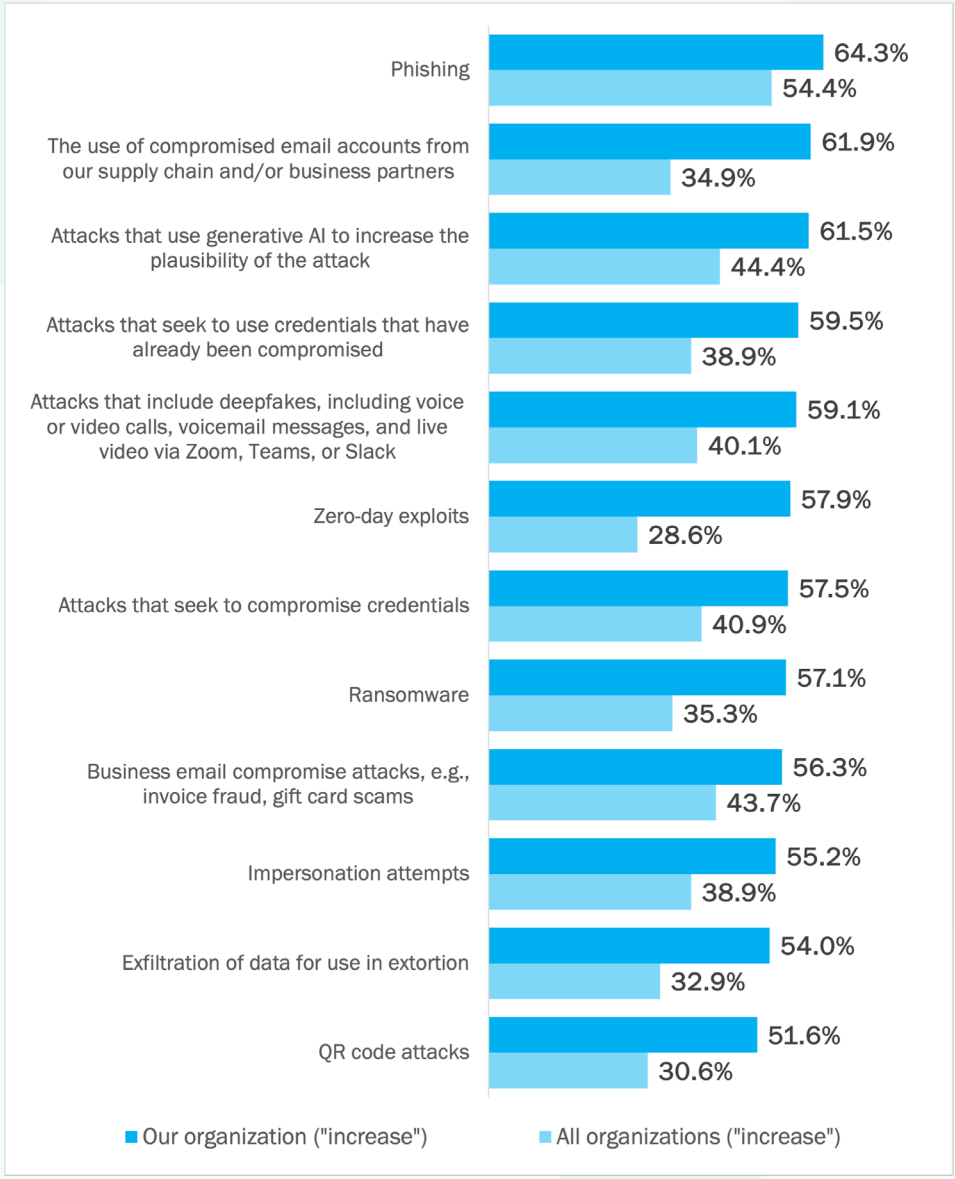
**77% of respondents expect the threat dynamics across a whole range of threat types against their organization to stay the same or get worse over the next 12 months.** In all cases, too, respondents anticipate the intensity of threats specifically against their organization to increase by more than the intensity of threats against all organizations in general.

The top threat types expected to get worse ("increase" in intensity) over the next 12 months are:

- Phishing
- The use of compromised email accounts from our supply chain and/or business partners
- Attacks that use generative AI to increase the plausibility of the attack

**See Figure 2.**

**Figure 2**
**Anticipated change in threat intensity over the next 12 months**
Percentage of respondents



With 77% of respondents anticipating continued degradation in the threat landscape over the next 12 months, making the appropriate response to defend against this growing intensity is critical. Not doing so puts organizations in a progressively worse position as the threat landscape changes and readiness and defenses remain unchanged. See Figure 3.

**Figure 3**
**Decision matrix for email security readiness**

| | | |
|---|---|---|
| **Threat context gets worse or remains the same** | **Worse position with ineffective defenses** | **Either better, neutral or worse position, depending on relative change in the two** |
| **Threat context gets better (less bad)** | **Either better, neutral or worse position, depending on relative change in the two** | **Better protected against threats** |
| | **Organizations don't improve their readiness and defenses** | **Organizations improve their readiness and defenses** |

## Most organizations are investing to strengthen their cybersecurity posture

We investigated how organizations and MSPs were investing in 2025 to strengthen their cybersecurity posture across ten areas. These included protecting against AI-enhanced attacks, protecting against phishing threats, and protecting user identities from attack and compromise.

**Across the ten areas, we asked respondents to rate:**

- Their level of concern with the current cybersecurity posture at their organization. A high rating means they are concerned, usually because defenses are weaker than they should be.
- The level of investment required to bring each area up to an acceptable standard within their organization. A high rating adds evidence that the area remains volatile and is not well enough addressed by the technical capabilities and human risk strategies currently deployed within their organization.
- The level of priority placed on improving the posture of each area in 2025. A high rating signals urgency.

**Across all ten areas, on average, 56% of respondents meet one of three patterns:**

**1. Laggards** playing catchup (high concern, high investment required, and high priority. This is the foremost pattern, occurring an average of 34% of the time for the organizations in this research. Organizations embracing this pattern for a given area acknowledge it as being under-addressed and/or at high risk of compromise.

**2. Risk-averse followers** (high concern, low investment required, and high priority). This is the third most common pattern, where organizations have some spending to do to bring an area up to standard, but relatively speaking, it's not a large spend. In this research, 11% of organizations have already put in the foundational work to strengthen a given area, and are committed to do more over the next 12 months.

**3. Risk-averse leaders** (low concern, low investment required, and high priority). This is the fourth most common pattern, where despite low concern and low investment required, priority is still high. These organizations have already done most of the work required to protect against threats, but are committed to spending more to stay at the forefront of changing defenses. One in ten organizations in this research evidence this pattern.

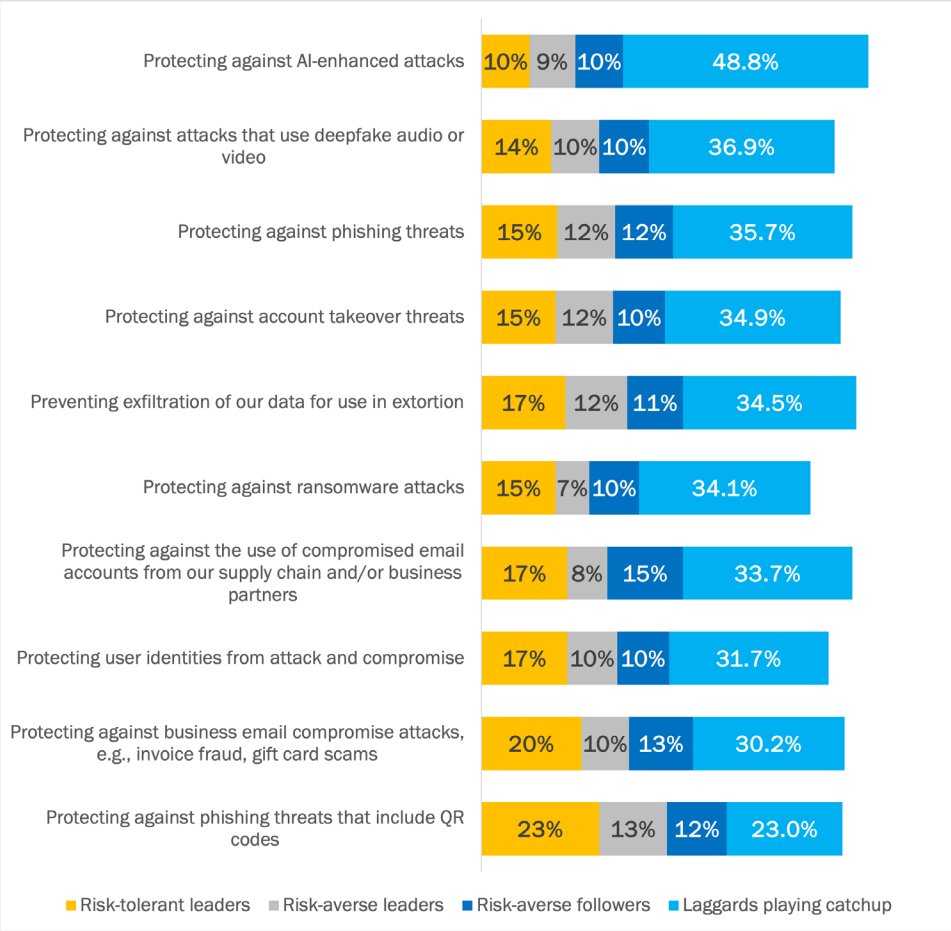
An average of 16% met a fourth pattern - of low concern, low investment required, and low priority. This is the second most common pattern. Organizations in this group have already seen the threats and have spent the funds to address their outstanding issues in previous investment cycles. They are confident their defenses are up to standard **("risk-tolerant leaders").**

**See Figure 4.**

**77%**

**of respondents expect the threat dynamics across a whole range of threat types against their organization to stay the same or get worse over the next 12 months.**

**Figure 4**
**Correlating posture concern, investment required, and investment priority for protecting against security threats in 2025.** Percentage of respondents




**In looking at the combination of these four patterns, the highest priority areas in 2025 are:**

- Protecting against AI-enhanced attacks.
- Protecting against attacks that use deepfake audio or video.
- Protecting against phishing threats.
- Protecting against account takeover threats.
- Preventing exfiltration of data for use in extortion.

Of this list of five, the first two are new and emerging threat types that many organizations are ill-prepared for, don't have the right defenses to stop attacks, and have high uncertainty around the extent to which these threats will cause damage. The other three are enduring threat types causing frequent incidents, resulting in unwanted financial costs and reputational losses. Cross-referencing these priority areas with security incidents over the past 12 months shows alignment between common incident types and priorities for 2025.

**See Figure 5**
**Correlating investment priorities with common incident types**

| Investment priority | Reason | Incident types |
|---|---|---|
| Protecting against AI-enhanced attacks | New and emerging threat type - unleashing new attacks with sophistication and speed | |
| Protecting against attacks that use deepfake audio or video | New and emerging threat type - eliminating signals of deception by using high-resolution impersonations | |
| Protecting against phishing threats | Enduring threat type | Credentials compromised through a phishing attack (most common incident type among organizations)<br>Credentials compromised through a QR code phishing attack (fourth most common incident type among organizations) |
| Protecting against account takeover threats | Enduring threat type | Credentials compromised through a phishing attack (most common incident type among organizations)<br>Credentials compromised through a QR code phishing attack (fourth most common incident type among organizations)<br>Credentials compromised even though they were protected by MFA (fifth most common incident type among organizations) |
| Preventing exfiltration of data for use in extortion | Enduring threat type | Breach of sensitive employee data (second most common incident type among organizations) |

# Cybersecurity threats against email

In this section, we analyze five types of cybersecurity threats against email systems:

- BEC attacks
- Phishing
- QR code phishing
- Deepfakes
- Generative AI

We report data from the survey and observations from the TitanHQ team.

## BEC attacks

Business email compromise (BEC) attacks seek illicit financial gain and/or access to sensitive data that can be used for blackmail and extortion. There are multiple types of BEC attacks, including gift card scams, invoice fraud, and payroll diversion.

The latest annual report from the FBI on internet crimes ranks BEC attacks as the second most costly type of attack, after investment scams. Based on the BEC attacks reported to the FBI, total losses for the year were estimated at $2.9 billion across only 21,489 incidents (an average of $137,132 per each). While costly, the incident count for this type of attack in the FBI's annual report has always been among the lowest, highlighting the challenge of detecting infinitesimal threats among the massive collection of messages.

**Specific BEC cases reported to the FBI included:**

- A $50 million loss due to a BEC incident at a construction entity in New York focused on critical infrastructure.
- A $426,000 loss due to a spoofed attorney email in a real estate transaction.

[1] *FBI, FBI Internet Crime Report 2023, March 2024, at https://www.ic3.gov/media/pdf/annualreport/2023_ic3report.pdf*

Another BEC incident resulted in a real estate firm paying $4.9 million to a Hong Kong bank account controlled by a threat actor. A fraudulent invoice had been sent by email from a compromised account at a trusted vendor. While the money was recovered due to the quick intervention of the FBI and law enforcement agencies, many others are not so fortunate. [FOOTNOTE: Coalition, Latest cyber risks and claims trends from Coalition, April 2024, at https://web.coalitioninc.com/download-2024-cyber-claims-report.html]

**BEC attacks are particularly difficult to detect for several reasons:**

- The attacks are very targeted and extremely low in volume. Unlike with mass phishing campaigns consisting of millions of emails, relying on traditional email security defenses to identify common patterns in a BEC attack consisting of several emails only is doomed to fail.
- The email message used for a BEC attack doesn't include weaponized links or malicious attachments that traditional email security defenses are programmed to detect. Both secure email gateways (SEGs) and Exchange Online Protection (EOP) in Microsoft 365 frequently classify BEC attacks as clean because they have none of the telltale malicious signals these solutions were designed to detect.
- If the BEC email originates from a compromised internal email account, it will appear to be coming from a trusted colleague or fellow employee, who may be working in a different location. Traditional email security defenses don't have the ability to consume login geolocation data, which offers critical identifying signals for detecting this type of BEC attack.

Successful BEC attacks impose immediate costs on organizations, due to lost funds. They also impose more significant reputational costs due to the signalling of poor security posture. Finally, they invite additional BEC attempts from other threat actor groups since the organization's control posture has already demonstrated its weakness.

**1/5** **One in five organizations lost money through a business email compromise attack over the previous 12 months.**

**Data points from the survey:**

- Lost money through a business email compromise attack
  - Among employees at organizations - 12.9% (1 in 8 organizations)
  - Among customers of MSPs - 21.6% (1 in 5 organizations)
  - [One in five organizations working with MSPs lost money through a business email compromise attack over the previous 12 months]
- Breach of sensitive employee data
  - Among customers of MSPs - 45.1% - most common incident type
- Breach of sensitive customer data - 39.2% - second most common incident type
- Business email compromise attacks, e.g., invoice fraud, gift card scams - 56.3% of respondents anticipate that the threat level of BEC attacks against their organization will increase in 2025. A further 16.3% expect the current level of threat to continue.

**From the trenches: TitanHQ on BEC attacks**

BEC attacks represent a major threat for organizations. They involve impersonating a trusted executive or partner to trick employees into making unauthorized transactions or revealing confidential information.

TitanHQ's PhishTitan includes BEC protection by analyzing email content and sender behavior to detect and block fraudulent emails. Security awareness training is also provided to educate employees on recognizing and responding to BEC attempts.

## Phishing

Phishing attacks have been a dangerous threat for several decades. Threat actors seek credentials, sensitive data, or a foothold on a device through a malware infection that can be leveraged for illicit gain, lateral movement, and increasingly a subsequent ransomware attack. While only 1% or 2% of intended victims fall for a phishing campaign, that's enough for threat actors, who compensate for a low success rate with a high volume of messages. Repeated success with phishing attacks highlights that threat actors have often found it easier to trick a victim into giving up their account credentials than break into systems using brute force.

**History of phishing**

**Fake email messages asking the recipient to act in a way that was against their own best interest were among the first computer crimes. In the early 1980s on FIDOnet, for example, early threat actors used a text file to queue a command to reformat the recipient's hard drive.** [Footnote: Roger Grimes, The Many Ways You Can Be Phished, January 2021, at https://blog.knowbe4.com/the-many-ways-you-can-be-phished]

**Threat actors are constantly upleveling the phishing playbook. Recent malicious innovations include:**

- Phishing toolkits available for licensing by emerging threat actors, making advanced threat tradecraft available for a small payment. New threat actors require little to no skill of their own.
- Bypass capabilities for multi-factor authentication (MFA). Criminals use a fake site to capture the victim's credentials and MFA code and immediately submit them to the real site, compromising the account despite the identity security precautions the organization has taken.
- New forms of phishing attacks, such as QR code phishing attacks. See the next section for more on these types of attacks.
- The use of AI to enhance phishing attacks, such as improving grammar and spelling, and writing the email in a way to match the email tone of the impersonated sender. Leveraging AI in this way allows threat actors to all but eliminate the warning signs of a phishing email.
- The use of high-reputation email services for sending phishing emails, such as Gmail and outlook.com. Whereas organizations can block known phishing domains based on threat intelligence, few are willing to block Gmail and outlook.com (and others) entirely.
- The use of compromised email accounts from Google Workspace and Microsoft 365 for sending phishing emails. When these accounts belong to clients or suppliers for a given organization, detecting wrongdoing is both extremely difficult and very urgent.

**64.3%**

**Phishing attacks - highest anticipation of increasing threat levels over the next 12 months**

## From the trenches: TitanHQ on the most common domains used for phishing emails

Based on the quantitative data we capture using our email security tools, the most common domains used for phishing emails are:

- gmail.com
- outlook.com
- hotmail.com
- aol.com
- Anything ending with .jp
- yahoo.com

The use of these services makes it essential that all organizations can identify malicious emails coming from these domains. Blocking the domain entirely is a non-starter because many of an organization's paying customers have email addresses with these services.

**Data points from the survey:**

- Credentials were compromised through a phishing attack - most common incident type at organizations over the previous 12 months.
- Among employees at organizations - 32.3%
- Among customers of MSPs - 23.5% [third most common incident type]
- Phishing attacks - highest anticipation of increasing threat levels over the next 12 months (64.3%). A further 13% expect the current threat level to remain constant.
- Attacks that seek to compromise credentials - second highest anticipation of increasing threat levels over the next 12 months (61.9%). A further 17% expect the current threat level to remain constant.

## From the trenches: TitanHQ on spearphishing attacks

In a recent incident, an MSP faced a sophisticated spear phishing attack targeting their clients. The attackers sent personalized emails to key employees, impersonating trusted partners and including malicious links in the emails. The MSP's support team quickly intervened and reached out to TitanHQ for assistance. By utilizing PhishTitan and SpamTitan, we enabled the MSP to identify and block phishing emails before they reached the recipients. Additionally, the MSP started using our DNS security solution (WebTitan) to block access to the spoofed websites. Recognizing the need for proactive measures, the MSPs team also conducted comprehensive user training and phishing simulation for all clients, educating employees on how to recognize and report phishing attempts. This multi-layered approach neutralized the immediate threat and strengthened the MSP's overall security posture, preventing future attacks.

## From the trenches: TitanHQ on ransomware

Ransomware attacks continue to be a major threat, with attackers encrypting data and demanding payment for its release. These attacks are becoming more targeted and disruptive. The most common attack vector for ransomware to enter a business is via email.

The major trend we see with ransomware is threat actors pivoting from an attachment that needs to be opened to hiding the payload behind a link in the email. Our defense against link-based attacks is called LinkLock - where all links are rewritten and scanned for malicious indicators.

## From the trenches: TitanHQ on phishing email categories

Phishing messages comprise around 1 in every 2,000 emails we see. We group and classify all identified phishing emails to see trends in theme and content. Over the past year, the most popular categories of phishing attempts are invoices, financial account updates (payroll), a request for action, and "follow up." Themes of urgency, confidentiality, and assertion of incompetence occur throughout.

| Phishing email categories | |
|---|---|
| Invoice | **31.91%** |
| Payment / Invoice | **26.07%** |
| Follow Up | **14.01%** |
| Hi / Hello | **5.45%** |
| Action Required | **5.06%** |
| Reply / respond | **5.06%** |
| Available? | **4.28%** |
| Urgent | **3.89%** |
| Accessible? | **1.56%** |
| Confidential | **1.17%** |
| Urgent / Invoice | **0.78%** |
| Bank account update | **0.39%** |
| Account Deactivation | **0.39%** |

## QR code phishing

QR codes proved their value for no-touch web interactions and online ordering during the social distancing restrictions of the covid era. It reintroduced the technology to the masses, providing a simple way of opening a website, placing an order, or starting a transaction. It also posted a large "open for business" sign for threat actors looking for new ways to trick unsuspecting victims and bypass traditional security solutions.

**Threat actors are incorporating QR codes in phishing attacks. For example:**

- By sticking a malicious QR code on top of an existing QR code on a parking meter. When scanned, the malicious QR code opens a nefarious copy of the actual payment site to steal parking monies.
- By sending emails with an embedded QR code to shift the targeted victim out of email on their well-protected corporate device and onto a mobile device with fewer security defenses. The intent with QR code phishing emails is usually to capture account credentials, just as with regular phishing attacks.

QR code phishing attacks in email became a popular threat vector in early 2024. These attacks regularly bypassed the native basic protections in Microsoft 365 and other traditional email security solutions that lacked computer vision technology to identify a QR code in an image and assess the associated link for malicious attributes.

**Data points from the survey:**

- Credentials were compromised through a QR code phishing attack - 1 in 5 organizations experienced at least one of these incidents in the previous 12 months.
  - Among employees at organizations - 20.9%
  - Among customers of MSPs - 21.6%
- QR code attacks - 51.6% of respondents anticipate that these attacks will increase over the next 12 months. A further 25.4% expect current threat levels to remain constant.

**1/5**

**Credentials were compromised through a QR code phishing attack - 1 in 5 organizations experienced at least one of these incidents in the previous 12 months.**

## Deepfakes

Deepfakes leverage AI tools to create images, audio, or videos that trick unsuspecting victims that such media is real. The technology has creative applications in the entertainment industry, for example, by superimposing an actor's face on the person doing a dangerous stunt. It has many malicious applications, too. One of the more commonly referenced deepfake attacks involved the Hong Kong office of a multinational company, which lost $25 million due to a deepfake multi-party video conferencing meeting in which an employee was instructed to transfer money for a secret initiative. [Footnote: Benj Edwards, Deepfake scammer walks off with $25 million in first-of-its-kind AI heist, February 2024, at https://arstechnica.com/information-technology/2024/02/deepfake-scammer-walks-off-with-25-million-in-first-of-its-kind-ai-heist/] Other large businesses in the UK have been targeted too, often with multi-stage attacks using WhatsApp and a voice message using the cloned voice of the organization's CEO and requesting urgent help with a secret transaction. [Footnote: Tom Saunders and Katie Prescott, Deepfake fraudsters impersonate FTSE chief executives, July 2024, at https://www.thetimes.com/business-money/technology/article/deepfake-fraudsters-impersonate-ftse-chief-executives-z9vvnz93l]

It is early days of deepfake attacks. We don't know how far threat actors will push the technology for use in cybercrime, nor do we have sufficient public examples to determine the full extent and shape of this type of attack. Irrespective of what we don't know, 1 in 9 respondents in this research said they had experienced at least one incident over the previous 12 months where a successful attack used deepfake techniques as part of the compromise. Such early success with deepfake attacks will embolden threat actors to experiment with different combinations to see what does and doesn't work.

**Data points from the survey:**

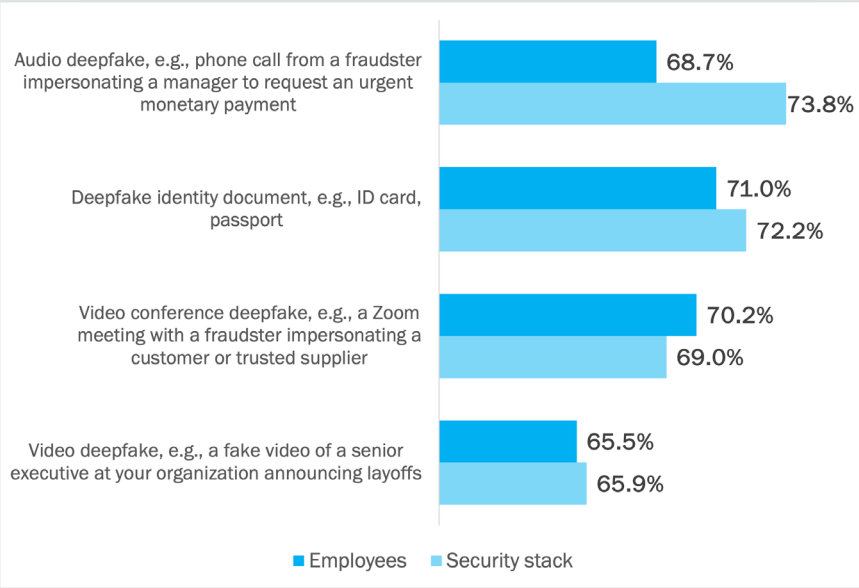
- Compromised through an attack that used deepfake techniques - 11%.
  - Among employees at organizations - 10.4%
  - Among customers of MSPs - 11.8%
- Attacks that include deepfakes, including voice or video calls, voicemail messages, and live video via Zoom, Teams, or Slack - 59.1% of respondents anticipate an increase in the threat level of deepfake attacks over the next 12 months. An additional 19.4% anticipate threat levels to remain constant.

Concerns around deepfake attacks echo the general level of concern around the abuse of AI, especially the ability to identify what is authentic and what is not. AI in general and deepfakes in particular put sophistication in attack design on hyperdrive.

Detecting and stopping deepfake attacks relies on well-trained employees and the security stack used by an organization. On average, 69% of respondents are highly confident employees can detect and stop such attacks, and 70% are the same related to their current security stack, leaving almost one in three who are not highly confident. There is work to do across the board to strengthen both human and technical protections - ensuring that organizations have a layered security approach, AI-powered deepfake detection methods, and effective security awareness training.

Across the four types of deepfake attacks we asked about in this research, the attack with the lowest confidence level is a video deepfake (e.g., a fake video of a senior executive announcing layoffs). However, even if such a video can be detected on a platform like Youtube, the financial and reputational damage done is likely to be extremely high before it can be stopped. See Figure 6.

**Figure 6**
Confidence to detect and stop deepfake attacks: Employees and security stack. Percentage of respondents indicating "very confident" or "extremely confident"




As mentioned above, it is early days in the unfolding story of deepfake attacks. Many of the respondents to this survey claim not to be too worried about different types of deepfake attacks, probably because they haven't experienced the full blast of deepfake attacks yet, or that they believe their organization isn't in the crosshairs.

**Industry data: the cost of impersonation scams**

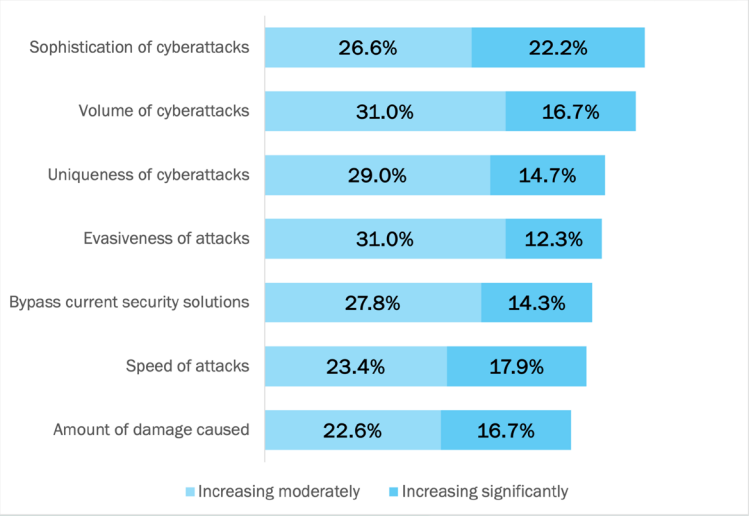
**While we don't know the full extent of deepfake criminal activity, the costs of impersonation scams in general are significant. Coalition, a cyber insurance company in the United States, said that 56% of its claims start from an email inbox. This is made up of funds transfer fraud and business email compromise attacks - both of which rely on impersonation. [FOOTNOTE: Coalition, Latest cyber risks and claims trends from Coalition, April 2024, at https://web.coalitioninc.com/download-2024-cyber-claims-report.html]**

## Generative AI

Compared to two years ago, the respondents in this research say that offensive AI used by threat actors has had the largest impact on the sophistication, volume, uniqueness, and evasiveness of the cyberattacks they experience. It is not expected to get any better over the next 12 months, either, with 61.5% of respondents anticipating an increase in the threat level of attacks using generative AI to increase the plausibility of attacks. A further 15% expect the current threat level to remain constant. Sophistication and plausibility go together - by removing the identifiable signals in an email message that it's a scam. Common signals include grammatical errors, differences in writing tone and style used by the threat actor in impersonating a sender, and spelling mistakes. See Figure 7.

**AI** | **offensive AI used by threat actors has had the largest impact on the sophistication, volume, uniqueness, and evasiveness of the cyberattacks they experience**

**Figure 7**
**Impacts of adversarial AI threats**
Percentage of respondents




Both AI in general and generative AI make it easier for threat actors to launch successful attacks. For example:

- Generative AI can be used to create phishing messages with no easy warning signals of fraudulent intent.
- Generative AI can be used in writing phishing messages that align the tone and language with how a nominated sender would normally write.
- Generative AI allows a threat actor to create several orders of magnitude more phishing campaigns in the time it previously took to prepare one campaign. This increases both the volume and speed of attacks.

**79%**

**79% of respondents say that email security solutions that include defensive AI capabilities are "very important" or "extremely important" to their cybersecurity posture in 2025.**

**From the trenches: TitanHQ on AI-enhanced cyberattacks**

Attackers are increasingly using artificial intelligence to automate and enhance their attacks. This includes AI-powered phishing, deepfake scams, and sophisticated malware.

At TitanHQ, we see increased use of AI in email attacks. This includes:

For email targeted at our customers - the use of AI tools to translate malicious emails to the native language of the intended recipients.

For email targeted against TitanHQ - the use of AI tools to translate malicious emails in Irish.

Our support team is extremely vigilant for these types of emails - both those targeting our customers and those coming directly to TitanHQ team members. We automatically gather all threat intelligence collected across our customer base for analysis via TitanHQ's generative AI and other ML technologies. With appropriate controls, this data is used for training our ML models to enhance future detection performance so we can counteract the changing dynamics of AI-enabled cyberthreats. We're fighting on the front lines against offensive AI so our customers don't have to.

We asked respondents in this research to indicate the emerging innovation that offers the greatest potential boost to email security at their organization over the next 12 months. Straight up, 47% of respondents said "AI." AI in general was in first place, and AI specifically for threat detection (including behavioral analytics) was in second place. Respondents have noticed the coming tsunami of AI-enabled cyberattacks and view AI-powered email security and other cybersecurity solutions that leverage AI as essential counterdefenses.

## AI is highly important to cybersecurity posture in 2025

79% of respondents say that email security solutions that include defensive AI capabilities are “very important” or “extremely important” to their cybersecurity posture in 2025. This received the highest ranking; it’s the overall summary statement of the four innovations we asked about. Having defensive AI capabilities in email security solutions means, for example:

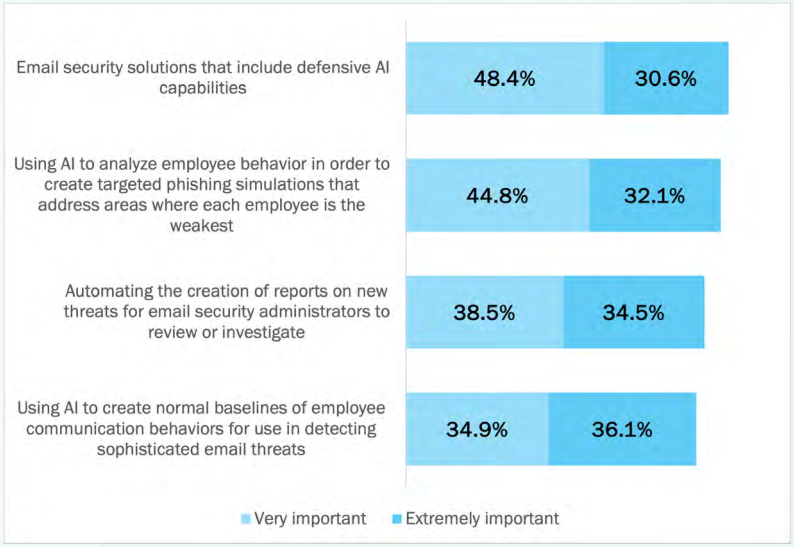
- Fighting AI-enabled attacks in real-time with AI-powered defenses. AI-driven security solutions detect, analyze, and mitigate threats faster.
- AI-powered security solutions predict threats by analyzing vast amounts of threat intelligence to identify patterns and anomalies. This allows AI-powered security to adapt to new attack methods faster, and eliminates the need for manual tuning of detection rules.
- Automated incident response reduces human error among cybersecurity professionals. This means that AI amplifies and safeguards human capabilities.
- AI automates repetitive security tasks, improving response times. Handling the repetitive basics in cybersecurity with machine precision contributes to freeing up cybersecurity professionals to focus on more strategic cybersecurity activities.

Three additional innovations follow closely behind:

- Creating better human risk management defenses by using AI to create targeted phishing campaigns based on an individualized assessment of employee behavior. This allows weaknesses to be addressed for each employee individually, shifting training from generic to highly personalized.
- Speeding email incident response interventions by the security team by automating the creation of threat reports for review or investigation. Security team members can focus on handling threats, not trying to figure out what is happening.
- Enabling a fundamentally different way of identifying threats in email. By baselining the normal communication patterns of each employee, deviations and anomalous activity can more easily be detected. Many sophisticated types of threats - BEC, for example - are virtually impossible to detect with traditional email security solutions that look for malicious links and attachments. In BEC attacks, they simply aren’t present.

**See Figure 8.**

**Figure 8**
The importance of AI to cybersecurity posture in 2025
Percentage of respondents

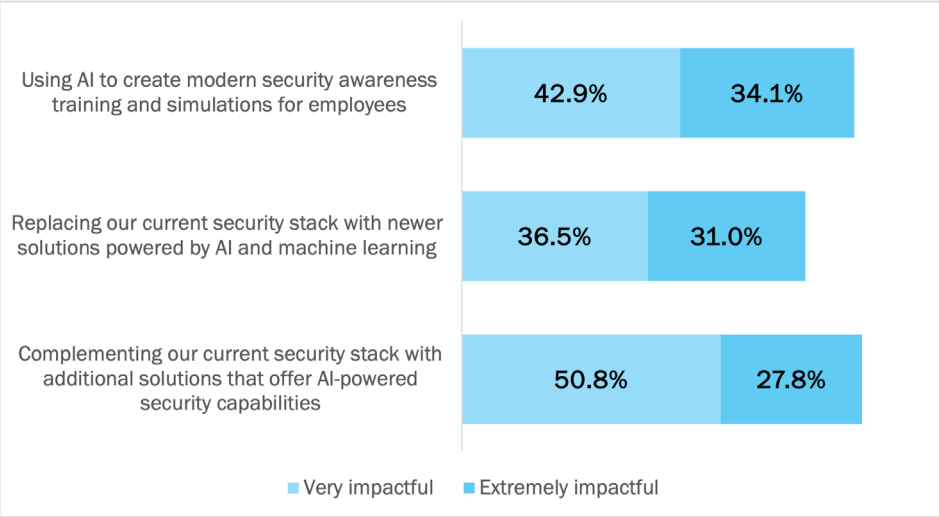



## The impact of AI strategies on the security stack in 2025

For most of the respondents in this research, exactly how different AI strategies will affect their security stack over the next 12 months is still a matter of internal discussion / debate. In alignment with the importance of human risk management in Figure X above, the strategy that’s expected to have the highest level of impact is focused on human risk management - specifically, the use of AI to create modern security awareness training and simulations for employees (34.1% giving this an “extremely impactful” rating).

**AI** | **the emerging innovation that offers the greatest potential boost to email security at their organization over the next 12 months. Straight up, 47% of respondents said “AI.”**

**Figure 9**
Key use cases for AI-powered email security solutions
Percentage of respondents




Two strategies focused on the technical composition of their security stack received close ratings. The predominant mindset for 2025 is:

- Organizations will replace their current security stack with newer email security solutions powered by AI and machine learning if their current stack does not measure up. Almost all email security vendors are racing to bring AI into their solutions; some are moving faster than others. If incumbent vendors aren't fast enough, organizations will jump to different vendors.
- Organizations will complement their current security stack with additional solutions that offer AI-powered security capabilities. This creates a multi-level defensive posture for the organization, although there are cost implications of running too many solutions. Almost all organizations are running - and need to run - at least two email security solutions because Microsoft 365's native capabilities doesn't catch everything. However, running too many solutions in parallel is cost-prohibitive for most - once costs for licensing, resourcing, and management overhead are factored in. Options where one solution covers more of the problem domain in a single platform helps to address these cost concerns.

## The top 12 trends evident in TitanHQ's data

1. Spoofing attempts increased dramatically in 2024, becoming the second most common type of malicious email caught by PhishTitan (TitanHQ's integrated cloud security solution for Microsoft 365). Organizations relying solely on Microsoft 365's native protections are in trouble.
2. Social engineering phishing emails is the number one vector seen by TitanHQ for all types of attacks.
3. Traditional malicious emails that include weaponized URLs are declining in popularity among threat actors. Modern email security solutions are able to assess embedded URLs for malicious intent, thus preventing the message from reaching its intended recipient.
4. Phishing emails are predominantly sent in the morning. Threat actors hope to catch people in transit using email on phones where scanning for malicious signals is harder.
5. Most phishing emails come from free email providers, such as Gmail and Yahoo.
6. When people join a business, they are a particular target for threat actors. We see evidence of LinkedIn profiles being monitored and new joiners getting social engineering and spoofing emails supposedly from executives.
7. While auto remediation of email threats is growing rapidly in popularity, a large portion of our customers still prefer to add a security warning banner to emails because they feel this both protects and educates users.
8. End users offer an additional layer of defence - making any email security system better. For example, people need education around reporting suspicious emails via the TitanHQ add-in for Microsoft Outlook.
9. The most popular categories of phishing attempts are invoices, financial account updates (e.g., change of bank account for payroll), a request for action, or a follow-up task.
10. Russia and China are known hot spots for malicious activity. We have seen a sharp increase in malicious activity coming from domains in Japan and Poland. The .jp top-level domain is very highly used for phishing attacks.
11. Domains ending with .ai and .io are growing in popularity by malicious actors.
12. "Subject line name" spoofing is on the rise, particularly for mobile phishing attempts. This type of spoofing attack puts the name of the impersonated sender in the subject line.

# Email security strategy

In this section, we investigate how the organizations in this research are approaching the technical and people aspects of their email security strategy.

## Organizations rely on a multi-level stack of technical protections

**93% of respondents recognize that email presents an area of ever-changing threat requiring constant vigilance and up-to-date solutions. This recognition aligns with the findings we explored earlier in this report:**

- That 80% to 90% of organizations experienced at least one incident type over the previous 12 months, with most experiencing between two and four different types of incidents.
- That a whole range of cyberthreat types are anticipated to intensify over the next 12 months, such as phishing, supply chain account compromise, and attacks enhanced with generative AI.

In response, the organizations in this research are pursuing a multi-level / defense-in-depth approach. 89% of respondents assert that the native basic native capabilities in Microsoft 365 offer sufficient protection for their organization. This means Exchange Online Protection (EOP), which is bundled at no additional cost for all Exchange Online customers.

However, despite this assertion, 98% of organizations using Exchange Online Protection (EOP) indicate that leveraging third-party complementary advanced solutions is highly important for protecting against phishing, business email compromise, and other advanced email threats in 2025. Third-party complementary advanced email security solutions that work with Microsoft 365 provide the second most important line of defense for the organizations in this research.

**1/2** | **Half of organizations experienced between 2 and 4 types of incidents.**

The fundamental reason why is that Microsoft 365's native security is slower to detect emerging and dangerous attack types, such as QR code attacks, Office 365 password reset scams, invoice fraud, fabricated email threads, and more. These types of attacks result in compromised credentials, account takeover, data breaches, and heavy financial and reputational losses. No organization wants to be the victim of these attacks due to insufficient protections in Microsoft 365. Email is such an important channel of communication that a multi-level defensive posture is critical for all organizations.

## Human risk management

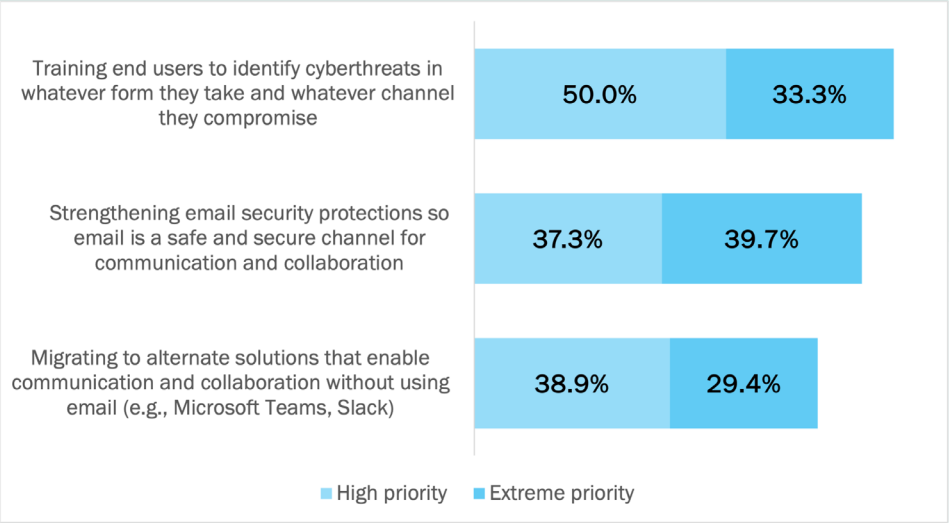
In this section, we look at the human risk management strategies that organizations are pursuing to strengthen protections against cyberthreats. Threat-aware, security-competent people are a significant part of the efficacy of cybersecurity posture.

## Organizations want threat-aware employees and strong technical protections

Communication is the lifeblood of organizations. It enables coordination and collaboration - fundamental underpinnings of modern productivity. But to work, communication systems must be secure - from outside tampering and insider threat. For the organizations in this research, priorities for creating secure communication without degrading productivity are shown in Figure 10 below. Priorities are:

- Having threat-aware, security-competent end users who can identify cyberthreats anywhere, anytime, any channel. It's not just about knowing a phishing email message when you see it; it's about sensing the threat signals and knowing how to respond across all situations and channels.
- Strengthening email as a place of work and communication so it is a safe and secure channel. This means doing everything possible to stop current and emerging threats from making it through to end user inboxes. It means having the incident response capabilities and skill set to rapidly remediate identified threats before they become incidents.
- Migrating communication and collaboration into alternate solutions that don't use email. This offers a potential answer to the immediate threats of email, but threat actors have already demonstrated their ability to compromise new solutions, too. For instance, the compromise of Microsoft 365 account credentials gives access to Microsoft Teams, too, not just Exchange Online.

**Figure 10**
Priority of strategies for secure communication without degrading productivity. Percentage of respondents




## Strategies for human risk management

Across six areas related to creating a strong security culture, we asked respondents to rate:

- Their level of concern with each area at their organization. A high rating means they are concerned, usually because defenses are weaker than they should be.
- The level of investment required to bring each area up to an acceptable standard within their organization. A high rating adds evidence that the area remains volatile and is not well enough addressed by the technical capabilities and human risk strategies currently in use within their organization.
- The level of priority placed on improving the posture of each area in 2025. A high rating signals urgency.

**Across all six areas, on average, 60% of respondents met one of three patterns:**

13. **Laggards playing catchup** (high concern, high investment required, and high priority). This is the foremost pattern, occurring an average of 42% of the time for the organizations in this research. Organizations embracing this pattern for a given area acknowledge it as being under-addressed and/or at high risk of compromise.

14. **Risk-averse followers** (high concern, low investment required, and high priority. This is the third most common pattern, where organizations have some spending to do to bring an area up to standard, but relatively speaking, it's not a large spend. In this research, 11% of organizations have already put in the foundational work to strengthen a given area, and are committed over the next 12 months to do more.

15. **Risk-averse leaders** (low concern, low investment required, and high priority). This is the fourth most common pattern, where despite low concern and low investment required, priority is still high. These organizations have already done most of the work required to protect against threats, but are committed to spending more to stay at the forefront of changing defenses. An average of 7% organizations in this research evidence this pattern.

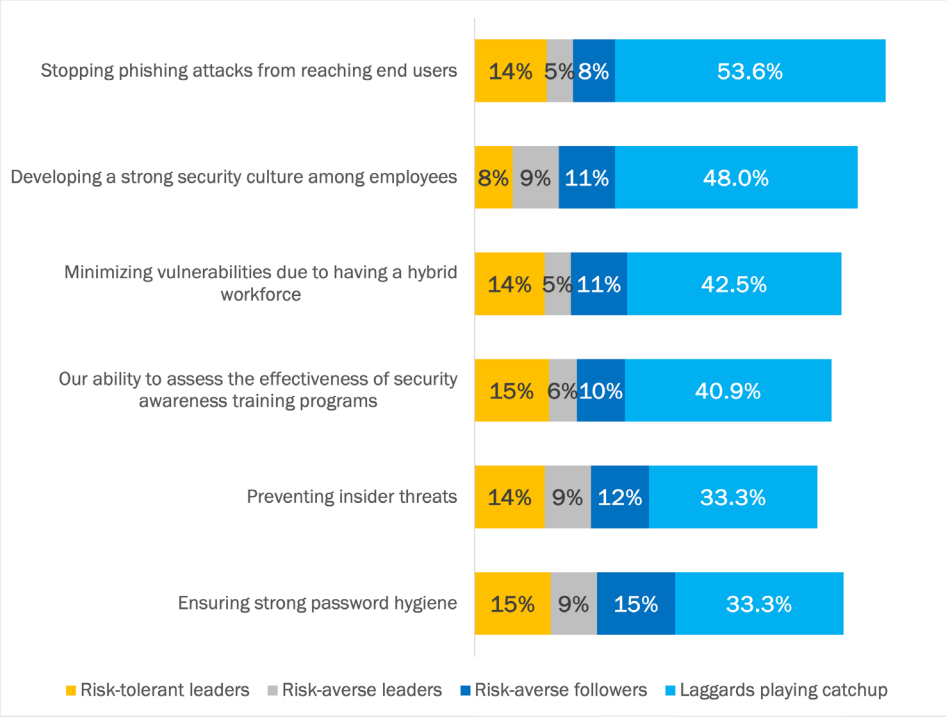
On average, an additional 13% of organizations evidence a fourth pattern - of low concern, low investment required, and low priority. This is the second most common pattern in the data. As we said earlier, organizations in this group have already seen the threats and have spent the funds to address their outstanding issues in previous investment cycles. They are confident their defenses are up to standard (risk-tolerant leaders).

**See Figure 11.**

**79%**

**93% of respondents recognize that email presents an area of ever-changing threat requiring constant vigilance and up-to-date solutions.**

**Figure 11**
**Correlating posture concern, investment required, and investment priority for human risk management strategies in 2025**
Percentage of respondents




**Across these four patterns, the highest priority areas for 2025 are:**

- Ensuring phishing attacks don't reach end users. Phishing attacks that resulted in credential compromise was the most common incident type among organizations over the previous 12 months.
- Developing a strong security culture among employees. This highlights, for example, the priority around developing threat-aware, security-competent end users who can identify cyberthreats anywhere, anytime, any channel.
- Reducing the threat scope against an organization, especially with the vulnerabilities due to having a hybrid workforce.

Organizations are pursuing multi-dimensional training

Around 50% to 60% of respondents say that five security training strategies have become more important within their organization in 2025 than two years ago. For the highest rating of increasing importance ("increasing significantly"), offering security awareness training to educate employees on emerging high risk cyberthreats, such as deepfakes, is the priority over the other four strategies (23.8% versus 19.3% on average).

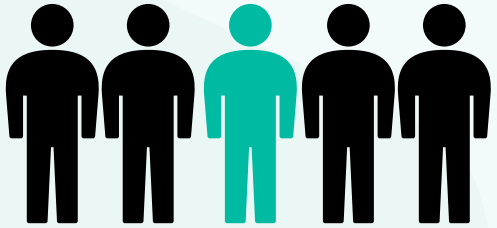
Overall, the strategies differ by who they focus on (cybersecurity professionals versus employees) and their nature (scenarios and simulations versus training). Both groups of individuals are essential in developing a threat-aware, security-competent culture. And both types of interventions - training for cultivating awareness plus scenarios and simulations to assess knowledge in action - are critical. See Figure 12.

**Figure 12**
**Importance of security training strategies in 2025**
Percentage of respondents

## What organizations want from an email security solution

The highest rated purchase factor from an email security solution for the respondents in this research is that it is effective against email security threats (41.7% ranking this "extremely important"). This includes the ability to prove that it's effective, both for the IT professional at an organization seeking budget approval and for MSPs positioning their services to customers. The inclusion of both technical and human risk management capabilities ranks second, measurability is third, and integration option is fourth. The initial, upfront cost of the solution has the lowest rating for "extremely important" but the highest rating for "very important." Price remains important, but is dwarfed by the primacy of technical capability to stop email security threats.

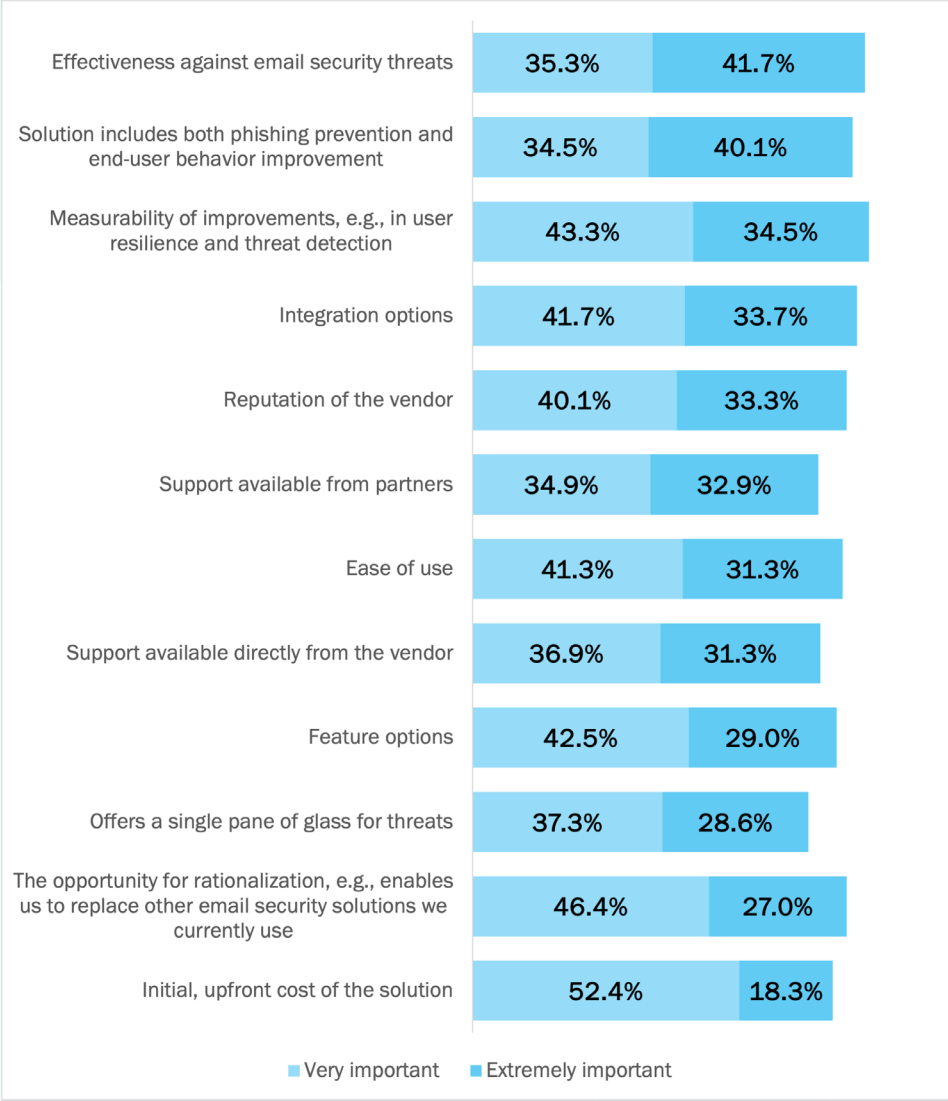
**See Figure 13.**



Credential compromise through a phishing attack was the most common incident type at organizations over the previous 12 months.

**1 in 5 organizations experienced credential compromise in the previous 12 months.**

**Figure 13**
**Importance of purchase factors for email security solutions**
Percentage of respondents



# Conclusion

This research makes it clear that smaller businesses (with fewer than 1,000 employees) and MSPs need to strengthen their email security protections - as AI-enabled attacks increase and the threat level of a whole set of email threats intensifies. Strengthening email security protections encompasses both technical protections that leverage defensive AI capabilities as well as human risk management investments that create threat-aware, security-competent end users who can identify cyberthreats anywhere, anytime, across any channel.

| Type of organization | |
|---|---|
| End-user organization | **79.8%** |
| Managed service provider | **20.2%** |

| Job role | |
|---|---|
| Owner or managing director | **15.9%** |
| CISO, or some other role that has this responsibility | **11.9%** |
| Security director or VP | **16.7%** |
| Security administrator | **2.0%** |
| Information security director or VP | **9.5%** |
| CIO, or some other role that has this responsibility | **6.7%** |
| IT manager, director or VP | **34.1%** |
| IT administrator | **3.2%** |

| Geography | |
|---|---|
| United States | **38.1%** |
| Canada | **7.9%** |
| European Union | **23.8%** |
| United Kingdom | **30.2%** |

# Methodology

This white paper was commissioned by TitanHQ and conducted by Osterman Research. 252 respondents in security roles were surveyed during February 2025. To qualify, respondents had to work at organizations with between 100 and 1,000 employees, or at an MSP (managed service provider) and be responsible for several aspects of the email security strategy at their organization. The surveys were conducted in three countries and the European Union. The survey was cross-industry, and no industries were excluded or restricted.

**All respondents used Microsoft 365.**

Microsoft 365 (E3)- **29%**
Microsoft 365 (E5) - **58.70%**
Microsoft 365 (a plan other than E3 or E5) - **12.30%**

| Industry | |
|---|---|
| Agriculture, forestry or mining | **0.8%** |
| Computer hardware or computer software | **6.0%** |
| Data infrastructure or telecom | **5.6%** |
| Education | **2.8%** |
| Energy or utilities | **6.0%** |
| Financial services | **7.5%** |
| Government | **0.8%** |
| Healthcare | **6.3%** |
| Hospitality, food or leisure travel | **6.7%** |
| Industrials (manufacturing, construction, etc.) | **11.9%** |
| Information technology | **11.1%** |
| Life sciences or pharmaceuticals | **5.6%** |
| Media or creative industries | **4.4%** |
| Professional services (law, consulting, etc.) | **9.5%** |
| Public service or social service | **1.2%** |
| Retail or ecommerce | **6.3%** |
| Transport or logistics | **7.5%** |

TitanHQ.com