egress

Email **Security Risk** Report

Uncovering inbound and outbound threats in Microsoft 365

AN EGRESS REPORT

Inside the report

Key report statistics at a glance

Email security incidents keep happening

92% of organizations were victims of phishing

85% of ATO attacks started with a phishing email

91% of organizations had an outbound email data breach

Impacts of email security incidents

Phishing attacks

54% of organizations **suffered financial losses** from customer churn

47% experienced **reputational damage**

Data loss

54% of organizations experienced **reputational damage**

48% of incidents resulted in **employees exiting the organization**

Cybersecurity leaders are stressed

99% are stressed about email security

53% say too many phishing attacks get through their SEG

46% say employees skip through training as quickly as possible

INTRODUCTION

Email security risks in Microsoft 365

Organizations remain vulnerable to advanced phishing attacks, human error, and data exfiltration. 93% of the cybersecurity leaders who were surveyed for this report stated their organization had suffered an email security incident in the last 12 months. 99% of Cybersecurity leaders, meanwhile, admitted to being stressed about email security.

This report sheds light on how these incidents happened and the impact they had on the individuals and organizations involved, while also looking at real-world phishing and data loss trends, highlighting the threats of the future, and analyzing the effectiveness of the security measures in place at the surveyed organizations.

While this report examines inbound phishing attacks and outbound data loss and data exfiltration in distinct two sections, it's worth noting that 71% of surveyed Cybersecurity leaders consider inbound and outbound email security as part of a single problem to solve. As a result, the technical controls and security awareness and training (SA&T) programs in place to reduce email security risks are examined together.

The survey data used in this report comes from 500 Cybersecurity leaders, all of whom have deployed Microsoft 365 in their organizations. We've also combined this with anonymized Egress customer data that measures how the reality of inbound and outbound threats to email security matches with what the surveyed Cybersecurity leaders reported.

99% of Cybersecurity leaders are stressed about email security

The phishing attacks targeting organizations

Analyzing phishing risk

92%

of organizations were **victims of phishing**

86%

of organizations were **negatively impacted** by phishing incidents

85%

of ATO attacks started with a **phishing email**

54%

of organizations suffered **financial losses from customer churn**

Which threats are getting through?

Out of our 500 respondents, 92% suffered a successful phishing attack in their Microsoft 365 environment. These phishing attacks got through the existing technical controls in place and the recipient had taken action that enabled the cybercriminal to achieve their aims and a security incident to occur. For our surveyed organizations, malicious payloads were the most common successful attack type, with targeted social engineering and attacks originating from compromised supply chain accounts not far behind.

Top three types of phishing attack that organizations fell victim to:

Phishing involving malicious URL or malware attachment

Social engineering

Supply chain compromise

Supply chain and account compromise causes the most stress

99% of Cybersecurity leaders are stressed about threats to their email security, with phishing attacks sent from compromised supply chain accounts and internal account takeover (ATO) attacks causing the most stress.

Cybersecurity leaders share the current email security threats that cause them stress

Additionally, 60% of respondents said their organization had suffered an ATO attack in the last 12 months, with 83% of them acknowledging that their multi-factor authentication (MFA) protocol had been bypassed as part of the attack. In almost all cases, a phishing email was the initial source of compromise – with 85% stating that their employees' login credentials had been compromised this way prior to the attack.

Microsoft credentials are highly sought after by cybercriminals, as once a legitimate account is compromised, it can be used to further propagate attacks with lower chances of being detected by some types of email security.

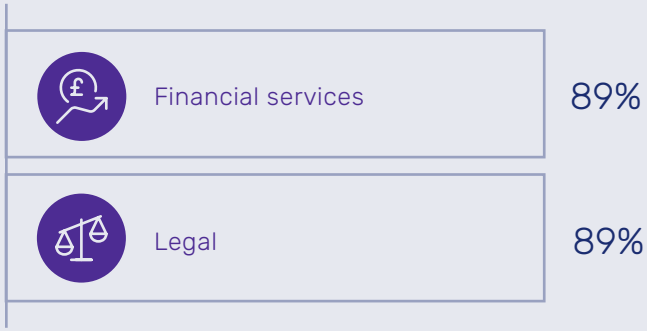
85% of account takeover attacks started with a phishing email

INDUSTRY WATCH

Financial and legal firms are hardest hit by ATO attacks

Industry segmentation of the survey data reveals that **ATO attacks were higher** than average for both financial and legal firms:

Additionally, ATO attacks in both industries were also more likely to **start with a phishing email:**



Real-world attacks: What Egress' platform data tells us

For this report, the Egress team analyzed 500,000 phishing emails that Egress Defend has detected and neutralized in our customers' Microsoft 365 environments. Aligning with the surveyed Cybersecurity leaders, phishing URLs were the most common payload detected (43% of attacks), followed by malicious attachments (18%).

Webmail was the most common source of phishing attacks, accounting for over half (53%), likely due to the ease of account creation. Compromised email accounts, including both unknown addresses and trusted supply chain addresses, were the next highest source (28%), backing up the surveyed Cybersecurity leaders' concerns. Finally, phishing domains (e.g. spoofed domains) were the source of the last 19% of attacks.

The Egress team also analyzed the types of phishing attacks detected, separate from their payloads and source. We found that two-thirds (66%) contained a form of impersonation, with the attacker either impersonating a well-known brand, a known supply chain vendor, or a physical mail service (e.g. DPD or UPS).

It is also interesting to note that social engineering was present in 39% of attacks, pressuring recipients to engage. Without advanced anti-phishing technology that uses natural language processing (NLP) it is virtually impossible for organizations to detect text-based social engineering attacks.

Another key problem for organizations is the growing sophistication of phishing emails. Our team classified almost half (44%) of phishing emails as containing complex features specifically designed to evade traditional email security defenses in Microsoft 365.

EGRESS ANALYSIS

From Jack Chapman, VP of Threat Intelligence

Malicious payloads are tried and tested – and cybercriminals will stick to an attack for as long as it works. Native security in Microsoft 365 and traditional SEGs have comprehensive libraries for known attacks and can deal with them very effectively. But while attackers might stick to the same type of payload (URLs and attachments), they will evolve the actual payloads. This combination of proven results and attack evolution means phishing risk continually remains high.

Even harder for traditional technology to detect are text-based attacks that rely on social engineering and attacks launched from trusted compromised supply chain email addresses. It's not just these technologies that struggle to detect them – people do too. It can be easy for recipients to be taken in by highly targeted attacks and those appearing to come from people they trust. Common tactics for these types of attacks can include targeting new employees who might be less aware of organizational processes, impersonating known brands or key leaders within the organization, and putting pressure on recipients to comply with instructions or be responsible for negative consequences.

Phishing threats of the future

Phishing continues to evolve as cybercriminals work to further automate and improve their tactics. Nearly three-quarters (72%) of surveyed Cybersecurity leaders told us that they were concerned about the use of AI to craft better phishing emails and campaigns. There's potential for AI-powered chatbots to rapidly produce an increased volume of highly convincing phishing emails and for deep fake technology to add video and voice capabilities that can be used in combination with text-based phishing and as part of vishing attacks.

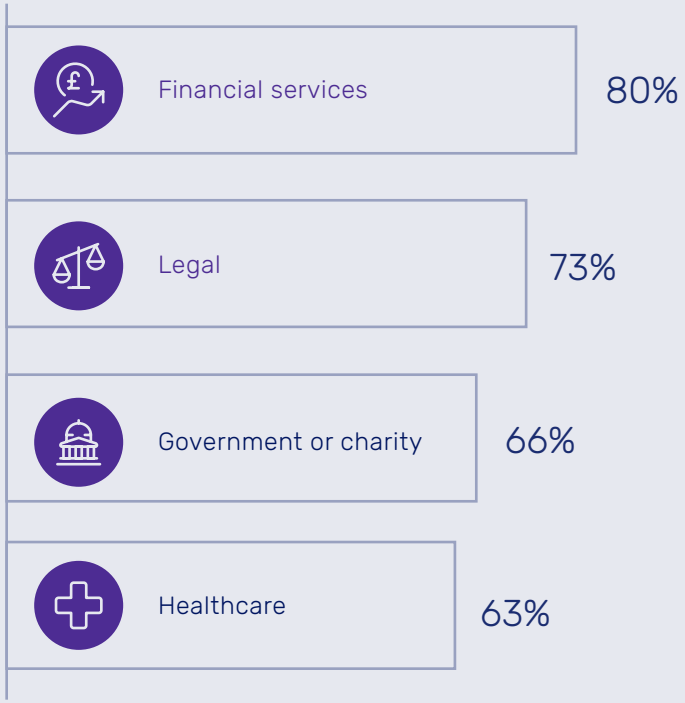
Another concerning trend the Egress team continues to monitor is the ongoing automation of attacks and rising sophistication levels of the toolsets and methodologies available to attackers. This is primarily caused by a maturing crime-as-a-service ecosystem, where criminals have access to better resources, training, and compromised accounts to launch their attacks. They're taking what would previously be months' worth of work, automating it, and selling it to other criminals – greatly lowering the barrier of entry to cybercrime.

72% of Cybersecurity leaders are concerned about the use of AI within phishing emails

INDUSTRY WATCH

Financial and legal firms more concerned about AI and phishing

Cybersecurity leaders from financial and legal firms were overall more alert to the threat of AI within phishing campaigns and emails.



The human and business impacts of phishing

Phishing attacks are taking their toll: out of our surveyed organizations, 86% suffered negative impacts from phishing over the past year. These incidents had repercussions for the individuals involved, as well as for the organization as a whole.

The human cost of these attacks was most commonly disciplinary proceedings, occurring in 39% of incidents. It's worth noting, however, that when combining the 'employee was dismissed, and 'employee voluntarily left' outcomes, almost half (40%) of organizations experienced a loss of talent due to phishing incidents.

The most common, and concerning, impact for organizations was customer churn. 54% of organizations hit by a successful phishing attack ended up losing customers and revenue due to the incident, while 47% said their reputations were damaged.

Cybersecurity leaders share the fallout from phishing attacks for their organizations

The price tag for phishing attacks is larger for financial firms

The financial firms surveyed reported higher than average impacts for both these categories:

63%
Financial loss from customer churn

36%
Financial loss from regulatory penalties

The threats to outbound email security that organizations face

Analyzing human error and data exfiltration

91%

of organizations had an **outbound email data breach**

86%

of organizations **suffered negative impacts** from outbound data loss

64%

of organizations' **information barriers were breached**

48%

of organizations **lost employees** as well as data

How is data being leaked by email?

91% of the Cybersecurity leaders surveyed said data has been leaked externally by email, with three top causes for these incidents.

1. Employees engaging in reckless or risky behaviors, such as sending data to a personal account to work on from home

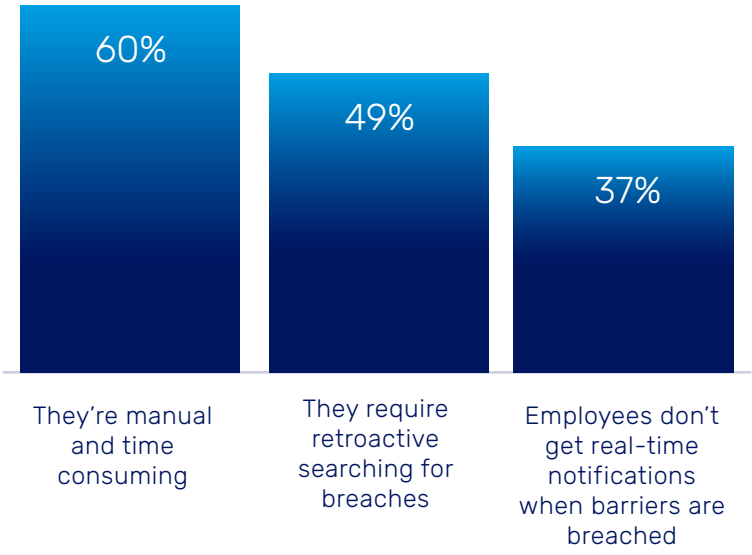
2. Human error, including employees sending emails and files containing confidential information to incorrect recipients

3. Data exfiltration for malicious purposes or personal gain (e.g. taking data to a new job)

Confidential data being exposed internally within the surveyed organizations was also a cause of risk. Three-quarters (75%) said they enforced information barriers internally. Of these, almost two-thirds (64%) said their information barriers had been breached in the last 12 months.

100% of the surveyed Cybersecurity leaders that use information barriers also expressed frustration with them. The chart on the right details the top three.

Cybersecurity leaders share their frustrations with information barriers



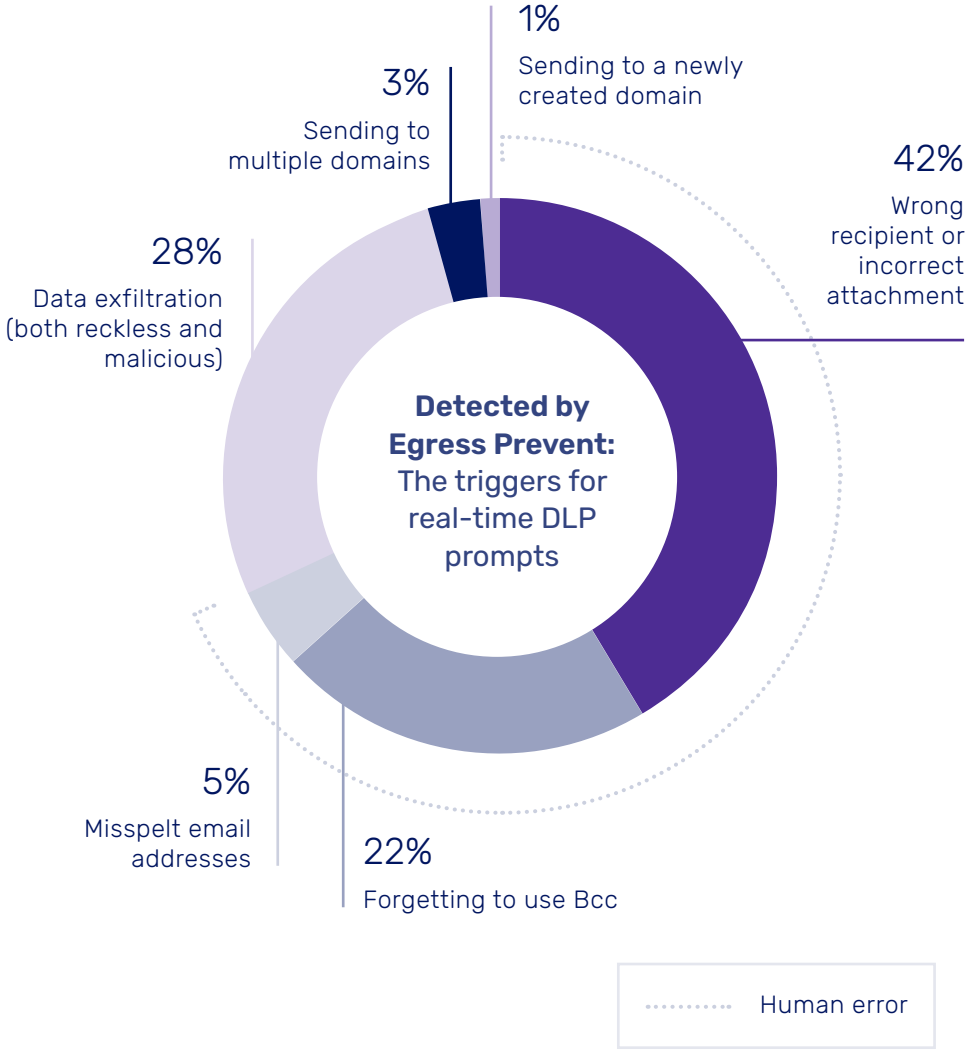
100% of the Cybersecurity leaders that use information barriers expressed frustration with them

Real-world data loss: What Egress' platform data tells us

For this report, the Egress team analyzed the data for over 1.7 million outbound emails within Microsoft 365, examining the types of data loss prevention (DLP) prompts given by Egress Prevent when an outbound email security incident was detected.

Similar to the survey data, data exfiltration was one of the top causes detected. This accounted for 29% of the prompts delivered and included both reckless behavior and malicious exfiltration. However, human error triggered 69% of these security prompts. The most common prompt was for wrong recipients or incorrect attachments (42%), while the third most significant cause detected was failing to use the Bcc, which would expose email recipients to each other alongside any associated confidential or protected information within the body or attachments of an email.

Without real-time intelligent detection and analytics it can be difficult for organizations to get a full picture of what data is being lost unless employees detect and report incidents themselves, with many mistakes passing under the radar.



EGRESS ANALYSIS

From Jack Chapman, VP of Threat Intelligence

People making mistakes or taking risks in the name of getting the job done happen far more frequently than malicious exfiltration. When someone sends an email to the wrong recipient or attaches the wrong file, typically they've spent time and energy composing the email body. This is perceived as the 'trickier' part of sending an email, with people focused on getting the right tone and selecting the right words to get their message across. Adding the recipients and file attachments is perceived as 'easier' – after all, the person knows before they start writing the email who they want to send it to. Concentration can lapse during this part of the task and productivity tools can also be more of a hindrance than a help, with Outlook autocomplete suggesting commonly contacted emails and recent file attachments. With the click of a button, the wrong recipient and file can be quickly selected, with the sender often none the wiser that they are about to make a mistake.

Unlike human error, when people behave recklessly with data, they know what they're doing contravenes security processes but they choose to do it anyway. Sometimes they might not realize or acknowledge how 'serious' this action is, and frequently justify their behavior through social proof (e.g. other, often more senior or long-tenured employees acting the same way) or cost-benefit analysis (with the benefit to the individual or organization perceived as outweighing the risk). This is seen by the one-third (33%) of Cybersecurity leaders who said an employee had exfiltrated data 'for work purposes', with the employees likely believing that getting their jobs done was more important than preventing data being sent to personal email addresses.

Finally, malicious data exfiltration typically occurs less frequently but can do significant damage. Most malicious insiders know the parameters they operate within (e.g. what access they have to which systems or what's being centrally monitored by the Cybersecurity team) and try to work around them for maximum gain and impact.

The human and business impacts of data loss

86% of surveyed organizations suffered negative impacts from outbound email incidents, which is the same percentage as those that suffered negative impacts following a successful phishing attack. The most common impacts of outbound incidents, however, varied versus inbound.

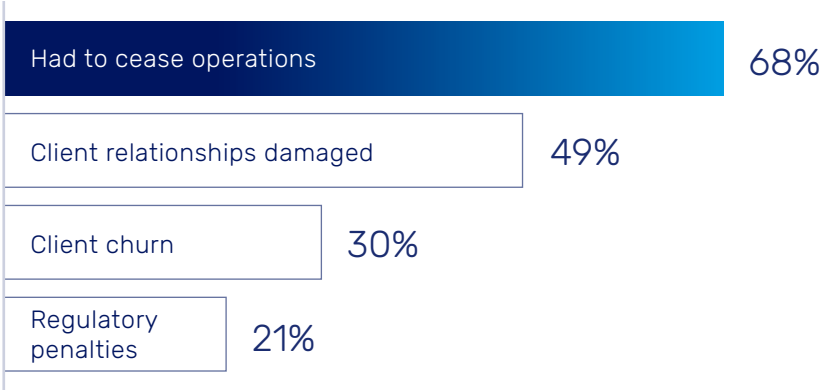
Employees being disciplined following an outbound email security incident was slightly higher at 41%. Again, similar to inbound attacks, almost half of organizations saw employees (48%) exiting the company following an incident, with 27% dismissed and 21% leaving voluntarily.

The most common outcome overall was reputational damage, which impacted 54% of surveyed organizations. It was also more common for organizations to experience financial losses from regulatory penalties following outbound incidents at 49% (versus 30% for phishing).

Additionally, organizations that experienced internal email security incidents when their information barriers were breached also reported negative outcomes. Operational inefficiency occurred for over two-thirds (68%) of these organizations, almost half (49%) reported that client relationships were damaged, and just under one-third (30%) said they experienced client churn.

Cybersecurity leaders share how outbound email security incidents have impacted their organizations

Cybersecurity leaders highlight the impacts following an internal breach of information barriers



What are organizations doing to lower their risk – and is it working?

Understanding the inbound and outbound email security defenses organizations have in place

73%

of organizations **enforce email security** with their supply chain vendors

58%

of Cybersecurity leaders say their SEGs are **ineffective against misdirected emails**

53%

of Cybersecurity leaders are concerned that too many **phishing attacks bypass their SEG**

46%

of Cybersecurity leaders worry that **employees skip through training**

Both the survey data and Egress' platform data shows that organizations are vulnerable to advanced phishing attacks, human error, and data exfiltration.

92% of organizations have been victim of phishing attacks, while 91% have experienced an outbound email data breach. Egress' platform data shows that almost half (44%) of phishing emails are classed as 'technical', meaning they've been specifically engineered to bypass signature-based defenses and over one-quarter (28%) were sent from compromised legitimate domains. At the same time, 69% of DLP prompts were triggered by people making mistakes.

The thoughts shared by Cybersecurity leaders align with the overall market trend of layering email security solutions for the best defense, with the introduction of integrated cloud email security (ICES) solutions to deliver intelligent behavior-based security to address advance threats.

Native controls in Microsoft 365

In addition to Exchange Online Protection, which comes as standard with the Exchange Online mailboxes used by the surveyed audience, almost half (48%) have deployed Microsoft Defender and nearly two-thirds (63%) have deployed Microsoft Defender ATP.

Over half (53%) of the surveyed Cybersecurity leaders worry that the native controls they'd deployed can't stop the most advanced phishing attacks, such as zero-day attacks, while 47% say that too many phishing emails end up in employees' inboxes. Top of the outbound email security concerns was stopping employees from accidentally emailing the wrong recipient or attaching the wrong file.

SEGs within Microsoft 365 environments

Similar to Microsoft, SEGs deliver signature-based detection of known phishing threats, quarantine and remediation functionality for inbound attacks, and static rules-based DLP protection for outbound email.

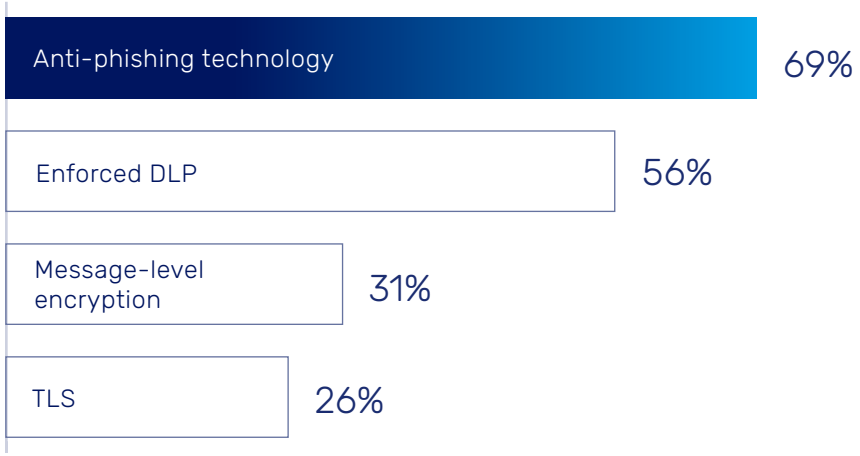
98% of Cybersecurity leaders that use a SEG acknowledged concern about mitigating email security risks. Top of the list was an inability to prevent accidental data loss from misdirected emails and wrong file attachments (58%), with 53% worried that too many phishing emails end up in employees' inboxes. Half (50%) of Cybersecurity leaders also stated that their SEG takes a lot of administrative time to manage.

Almost half (47%) of Cybersecurity leaders from financial firms were concerned their SEG couldn't stop the most advanced phishing attacks, such as zero-day attacks, and they also had above-average concerns about accidental data loss with almost two-thirds (64%) believing their SEG couldn't prevent people from emailing the wrong recipient or accidentally attaching the wrong file.

Securing the supply chain

73% of the surveyed Cybersecurity leaders said their organization enforces email security with their supply chain. This is likely a response to the fact that phishing attacks sent from compromised supply chain accounts were the third most common inbound attack that these organizations had fallen victim to and the top cause of email security stress. As it's typically difficult for traditional email security technologies to detect phishing attacks sent from compromised supply chain addresses, cybercriminals are known to target these organizations before leapfrogging to their ultimate target.

Cybersecurity leaders share the email security requirements they enforce with supply chain organizations

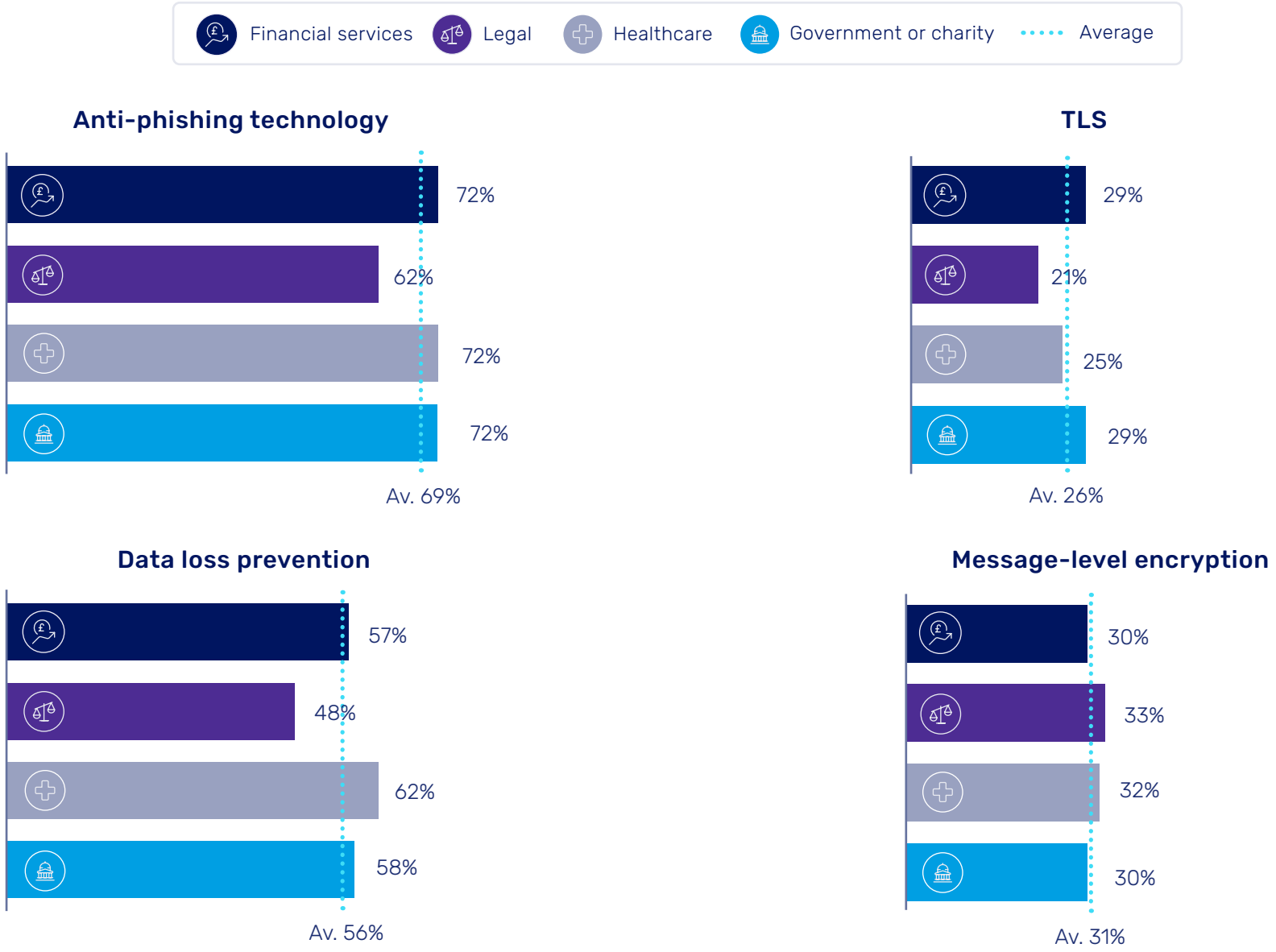


It follows, then, that anti-phishing technology was the most common requirement pushed onto supply chain organizations, occurring in 69% of the surveyed organizations. Outbound email security received patchier coverage, with 56% enforcing DLP, falling to less than one-third for message-level encryption (31%) and TLS (26%).

The survey respondents worked for organizations operating in financial services, legal, healthcare, and government and charities. While there was broad overall consistency between those in financial services, healthcare, and government and charities, legal firms were an outlier and generally enforced less security with their supply chains. Legal respondents scored 5-12% below average across three of the categories. Healthcare organizations were also 8% more likely to enforce email DLP with their supply chains than average, and 12% more likely when compared to legal firms.

73% of the surveyed Cybersecurity leaders said their organization enforces email security with their supply chain

Cybersecurity leaders show which email security requirements they enforce with their supply chain (split by industry)



The role of training

Almost all (98%) of the surveyed organizations carry out security awareness and training (SA&T). The most popular regularity was monthly (39%) but many organizations also train weekly (29%) and fortnightly (13%). Financial firms were 10% more likely than average to train weekly rather than monthly versus the average.

Yet 96% aired a concern or limitation with their SA&T programs. Over half (59%) acknowledged there was an element of box-ticking to it, stating it was necessary to carry out for compliance purposes. 46%, meanwhile, felt employees weren't engaging properly with program content and were instead skipping through as quickly as possible. Again, Cybersecurity leaders from financial firms shared stronger reactions. Operating in a highly regulated industry, almost three-quarters (71%) said their program was delivered for compliance purposes, while over half (54%) said employees skip through exercises.

EGRESS ANALYSIS

From Jack Chapman, VP of Threat Intelligence

People need real-time teachable moments that engage them at the point of risk to tangibly reduce the number of security incidents that occur and augment SA&T.

Unlike generic warnings and prompts (e.g. 'Caution External Email' applied to every inbound message), real-time teachable moments are delivered through intelligent email security solutions and designed to prompt people only when a risk is detected. That way, people don't get over-exposed to them but can see the value they add to their work lives, with in-the-moment nudges helping them to engage in good security behaviors. Augmenting Microsoft 365 with real-time teachable moments lets an organization layer their security training in a more engaging way. SA&T is being reinforced by more intelligent email security tools that can intervene in the moments when someone is about to make a mistake, without relying on them having perfect memory recall of the training exercise.

Stopping more threats to email security in Microsoft 365

The data throughout this report reveals that advanced email security technology is now table stakes for doing business. Despite investments to date in traditional email security and SA&T, organizations remain vulnerable to phishing, human error, and data exfiltration.

99% of Cybersecurity leaders are stressed about email security. 92% of organizations have been the victims of successful phishing attacks and 91% of organizations have experienced outbound email data loss in the last 12 months. 85% of account takeover attacks start with a phishing email. 66% of organizations that deploy information barriers have had them breached. 86% of organizations have been negatively impacted by email security incidents.

The only way to change this narrative is by using intelligent email security solutions.

As noted, Microsoft's native security helps organizations reduce their risks and their offering has evolved to the point that many Cybersecurity leaders have consolidated around it. However, it's recognized by governments and cybersecurity advisories globally that email security requires a layered approach.

New ICES solutions use intelligent technology to deliver behavior-based security. This approach is proven to provide additional security and controls to stop more targeted threats within Microsoft 365 environments, including business email compromise, phishing emails sent from compromised supply chain accounts, invoice and payment fraud, and impersonation attacks. Intelligent technology can also be used to prevent outbound email data breaches caused by human error, risky behavior, and malicious data exfiltration, going beyond static rules-based DLP for tangible real-time risk reduction.

Taking this approach and layering an ICES solution into their Microsoft 365 environment is the only way for organizations to combat the threats to email security they face now and to protect them for the future.

Egress and Microsoft 365

An intelligent approach to detecting advanced inbound and outbound threats by email

Seamlessly integrated into Microsoft 365, Egress' contextual machine learning not only detects advanced inbound and outbound threats that Microsoft and secure email gateways miss, but also transforms employee education using real-time teachable moments.

This approach is the only way modern enterprises can surface actionable intelligence and tangibly reduce today's email security risks.

When a threat is detected, Egress' intelligent technology provides a combination of interactive heat-based warning banners and prompts directly within the mailbox. Leveraging behavioral psychology best practices, these real-time alerts offer a clear explanation of risk at the exact moment people need it most. By using these teachable moments, Egress is proven to sustainably reduce risk through eliminating interactions with phishing emails and correcting human error and risky behaviors before security incidents can occur.

Egress provides a single holistic view of data and trends for both inbound and outbound email security. We surface organizational and human risk insights that matters most, allowing you to act quickly to effectively manage areas of risk and remediate threats. Offering integration with leading SIEM and SOAR platforms, Egress delivers immediate time to value when protecting against human activated risk.

Request a demo **Learn more**

About Egress

Our mission is to eliminate the most complex cybersecurity challenge every organization faces: insider risk. We understand that people get hacked, make mistakes, and break the rules. To prevent these human-activated breaches, we have built the only Human Layer Security platform that defends against inbound and outbound threats. Using patented contextual machine learning we detect and prevent abnormal human behavior such as misdirected emails, data exfiltration and targeted spear-phishing attacks. Used by the world's biggest brands, Egress is private equity backed and has offices in London, New York and Boston.

Methodology

The survey data for this report was compiled from 500 Cybersecurity leaders, including CISOs and CIOs, from the US, UK, and Australia, and working in the financial services, legal, healthcare, and government or charitable sectors. All respondents used Microsoft 365 as their operating system and were responsible for email security. The survey data was supplemented by platform data generated by Egress Defend and Egress Prevent.

www.egress.com | EgressSoftware

egress