egress

Koncise
connecting the dots

Email Security Risk Report 2024

INSIDE THIS REPORT

03 QUICK HIT OF KEY FINDINGS

05 EMAIL SECURITY RISK REMAINS HIGH

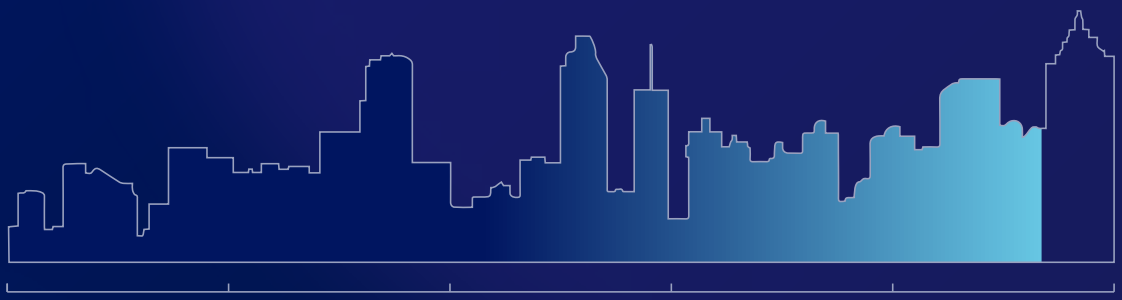
06 GONE PHISHING: HOW CYBERCRIMINALS ARE SUCCESSFULLY TARGETING ORGANIZATIONS

12 COUNTING OUR LOSSES: THE STATE OF DATA LOSS AND EXFILTRATION

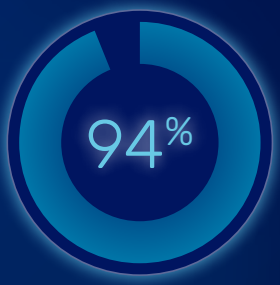
16 IN DEFENSE: IS PERIMETER TECHNOLOGY AND TRAINING MOVING THE NEEDLE?

21 2024: A YEAR FOR CHANGE

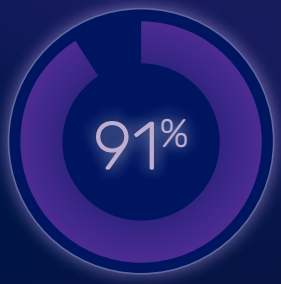
EMAIL SECURITY RISK REMAINS HIGH



94% of organizations experienced incidents



fell victim to phishing



experienced data loss and exfiltration

Top three phishing attacks

Malicious URLs

Malware or ransomware attachment

Attack sent from compromised account

Top three data loss incidents

Reckless behavior to "get the job done"

Human error

Malicious exfiltration

58% suffered account takeover

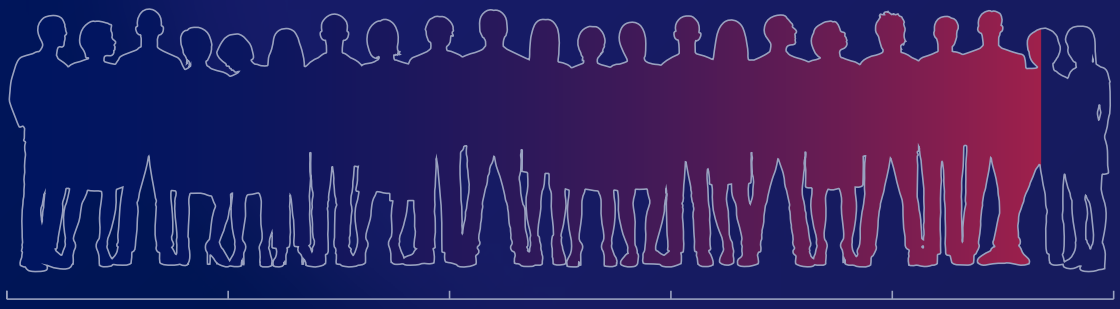
In **79%**, credentials were harvested via phishing

76% enforce internal information barriers

96% were negatively impacted

94%

Traditional approaches are failing



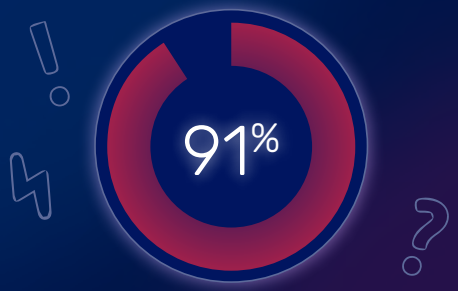
95% of Cybersecurity leaders are stressed about email security

Cybersecurity leaders say that the use of AI within attacks keeps them awake at night

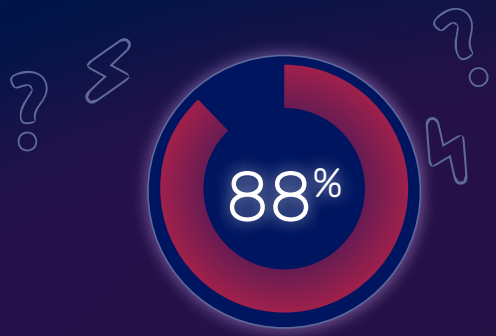
63% Deepfakes

61% AI chatbots

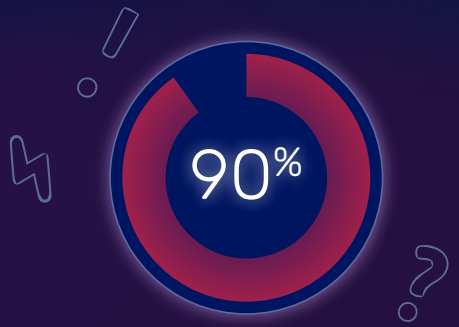
Most have concerns about traditional technology



with their **secure email gateway**



with **Microsoft**



with **static data loss prevention rules**

87% of organizations are considering replacing or have replaced their SEG

And **91%**

are concerned about the effectiveness of training

EMAIL SECURITY RISK REMAINS HIGH

Almost every organization reports experiencing email security incidents - and legacy approaches to technology and training can't keep pace with evolving threats.

The 500 Cybersecurity leaders who were independently surveyed for this report made two things very clear: they remain vulnerable to both inbound phishing attacks and outbound data loss and exfiltration, and they are questioning the effectiveness of traditional approaches to email security.

94% of our respondents experienced email security incidents in their Microsoft 365 environment in the last 12 months, which is consistent with our 2023 finding of 93%. Almost all organizations experienced both inbound and outbound incidents, with 94% falling victim to phishing and 91% to data loss and exfiltration.

It's only natural, then, that 95% of Security leaders said they are stressed about email security. Phishing attacks sent from compromised supply chain accounts are the top cause of stress, followed by internal account takeover (from credential harvesting), and wire fraud. Additionally Cybersecurity leaders admit to being kept awake at night by the use of AI in attacks. 63% are concerned about deepfakes and 61% by generative AI and chatbots. Understandably, there's a sense that doing what we've always done is no longer good enough.

For inbound detection, 91% of our respondents that use secure email gateways (SEG) expressed frustrations with them, while 88% voiced concerns with Microsoft's native controls. On the outbound, meanwhile, 83% find static DLP rules unworkable for employees and administrators.

Cybersecurity leaders also have reservations about traditional security awareness training (SAT), with 91% worrying about the effectiveness of their current program.

However, change is coming. 87% of organizations are on the journey to move away from their SEG, either considering or committing to replacing it with Microsoft's controls and integrated cloud email security (ICES) solutions.

In this report, we analyze these risks to inbound and outbound email security, as well as assess the effectiveness of the technical controls and SAT programs our respondents use. All data comes from an independently commissioned survey of 500 Cybersecurity leaders, all using Microsoft 365 as their cloud email platform.

GONE PHISHING: HOW CYBERCRIMINALS ARE SUCCESSFULLY TARGETING ORGANIZATIONS

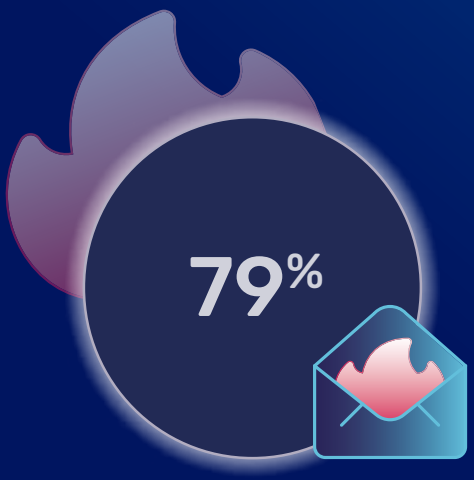
94%

of organizations were **victims of phishing attacks**

of which

96%

were **negatively impacted**



of account takeover attacks **started with a phishing email**

of Cybersecurity leaders say the **use of chatbots in phishing** keeps them awake at night

12 months on and the phishing story's the same

In the last 12 months, 94% of the surveyed organizations have fallen victim to phishing attacks within their Microsoft 365 environments. This remains consistently high in line with last year's report, which found that 92% of organizations had fallen victim.

The **top three attack types** that led to security incidents were:

MALICIOUS URLS

ATTACKS SENT FROM COMPROMISED TRUSTED THIRD PARTY ACCOUNTS

MALWARE OR RANSOMWARE

Compromised accounts continue to put organizations at risk

Compromised accounts remain a significant concern for our surveyed organizations – both at their own companies and within their supply chains.

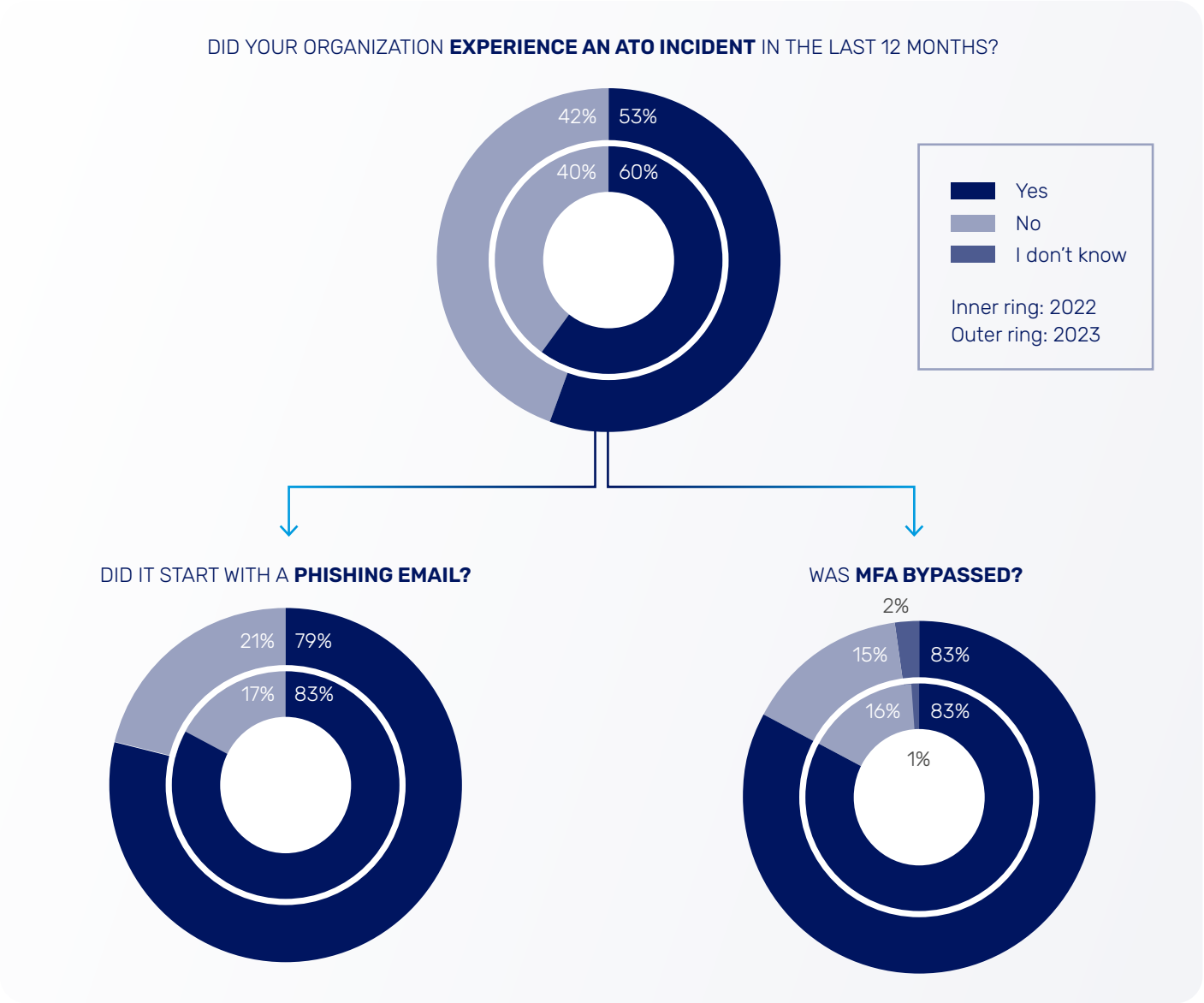
58% of organizations have experienced account takeover (ATO) incidents in the last 12 months. 79% of these started with a phishing email that harvested an employee's credentials, and 83% had multi-factor authentication (MFA) that was bypassed for the attack to succeed. Like many of the findings in this report, these figures paint a consistent picture with our 2023 edition.

Microsoft credentials are synonymous with being 'the keys to the kingdom', enabling cybercriminals to move laterally across systems and networks to exfiltrate data, as well as access email accounts to target customers and suppliers with further attacks.

Our surveyed organizations are hyper-aware of this phishing threat from within their own supply chains. In fact, 51% have already fallen victim to phishing attacks sent from compromised supply chain accounts within the last 12 months.

It's little surprise, then, that our Cybersecurity leaders' are most stressed about attacks sent from the supply chain and ATO attacks.

Half (51%) of organizations have fallen victim to phishing attacks sent from compromised supply chain accounts



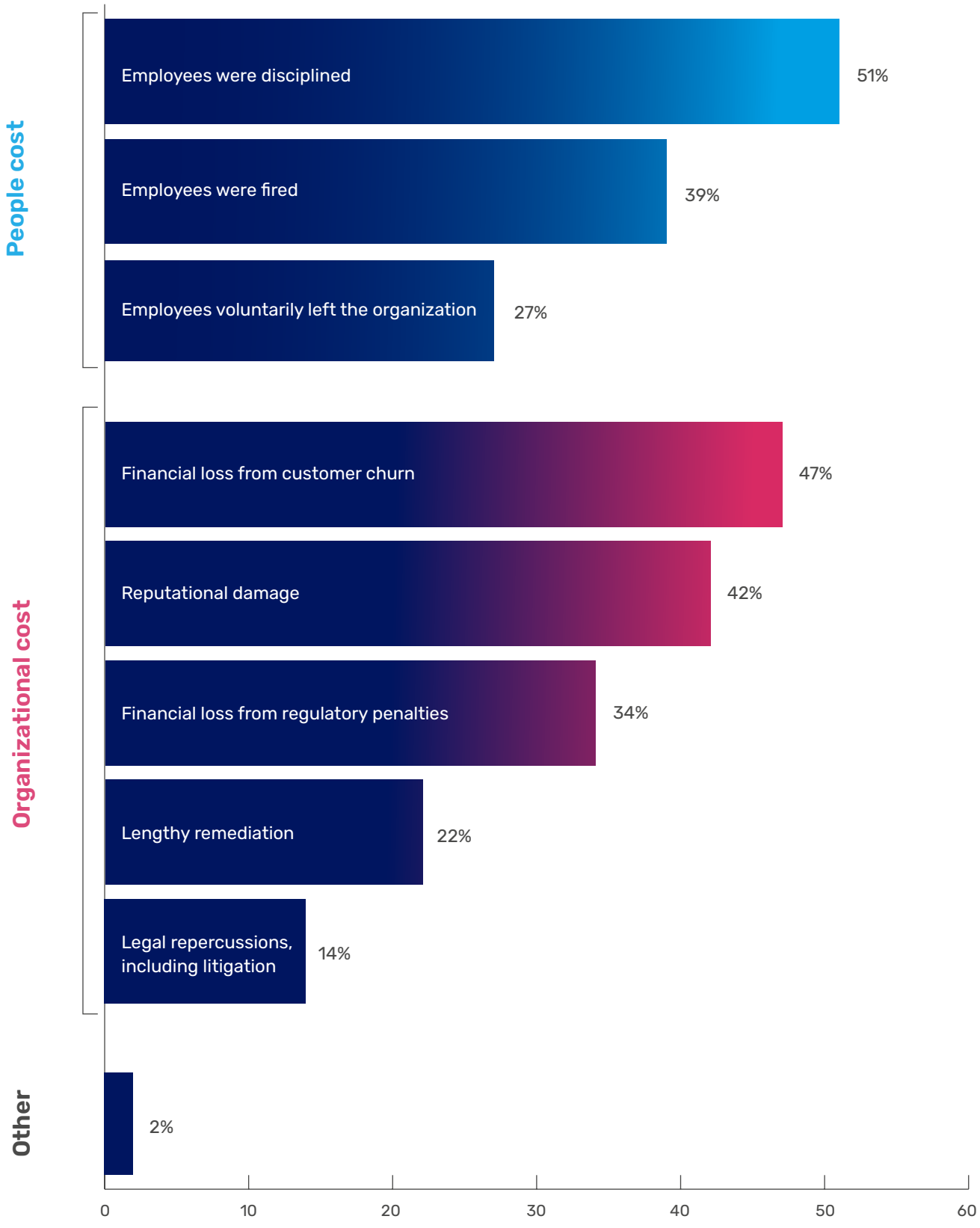
Phishing fallout: the pain is getting worse

96% of surveyed organizations experienced negative impacts from phishing attacks, which is a jump of 10% versus last year's report (when the number sat at 86%).

People are caught up significantly in this fallout. In 74% of organizations, the employees involved were disciplined, dismissed, or voluntarily left. In fact, disciplinary action was the most common outcome for all organizations, occurring in just over half (51%).

There was also an organizational cost for 79% of the companies we surveyed. Phishing hurt the bottom line in 64%, with financial losses related to customer churn the most common outcome at 47%. Reputational damage caused pain for 42%, as organizations managed the impact with customers and suppliers alike.

CYBERSECURITY LEADERS SHARE THE FALLOUT FROM **PHISHING ATTACKS**



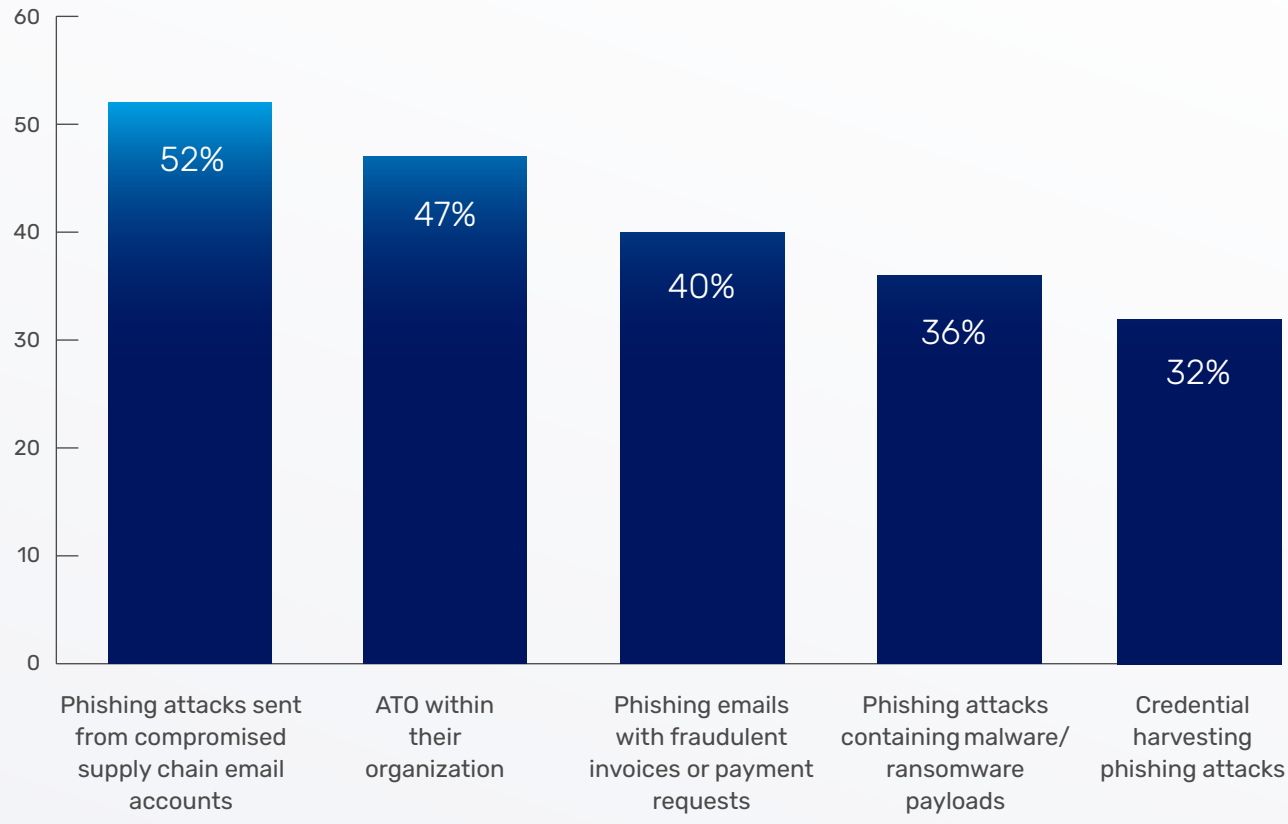
Everybody is stressed about phishing – and AI in the hands of cybercriminals obviously isn't helping

95% of our Cybersecurity leaders admitted that they're stressed about email security – and phishing concerns dominated the list of their worries. The top stressor is attacks sent from compromised supply chain email accounts, which worries just over half of our Cybersecurity leaders (52%), closely followed by account takeover (ATO) attacks in their own organization (47%).

In 2023, it was impossible to talk about cybersecurity and phishing without talking about AI. Large language models (LLMs) and generative AI enable cybercriminals to easily create targeted and sophisticated phishing emails, as well as generate malware.

Cybersecurity leaders say that the use of AI within attacks keeps them awake at night, with 63% concerned specifically about deepfakes and 61% losing sleep over AI chatbots being used to create phishing campaigns.

CYBERSECURITY LEADERS SHARE THEIR **STRESSES ABOUT PHISHING**

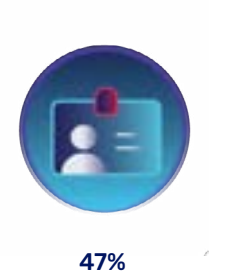


CYBERSECURITY LEADER'S TOP CONCERNS AROUND **AI USE**

63%
DEEPFAKES

61%
AI CHATBOTS

52%
SUPPLY CHAIN COMPROMISE



47%
ACCOUNT TAKEOVER

Expert analysis

JACK CHAPMAN, VP OF THREAT INTELLIGENCE

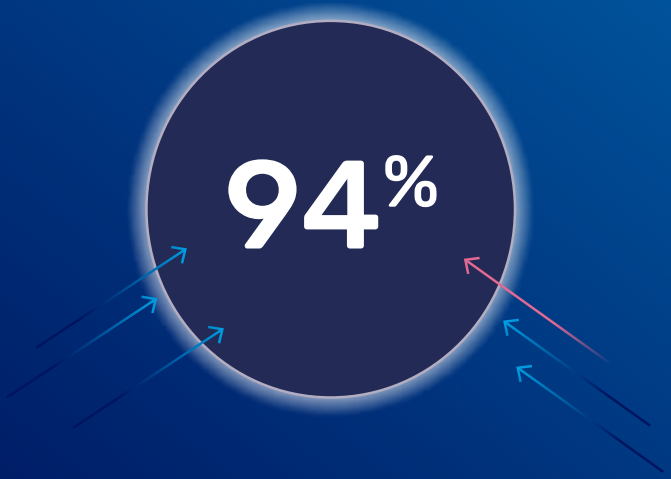
Phishing attacks are increasingly sophisticated, which makes them harder for both traditional perimeter defenses and employees to detect - and our Cybersecurity leaders know they're vulnerable.

Large language models (LLMs) and generative AI have dominated discussions this year, with fears that chatbots that can mimic natural human interactions will be used to produce targeted phishing campaigns at scale. It's currently impossible to prove chatbots are being used this way - but given how cybercriminals generally take every advantage they can get, I'm confident it's happening. Organizations can't afford to be left behind but must ensure their defenses keep pace.

Added to this, the threat from the supply chain is currently sky high. Phishing emails sent from compromised accounts can get through the reputation-based domain checks carried out by traditional perimeter defenses, and if combined with a credible phishing email, there's every chance an employee will fall victim.

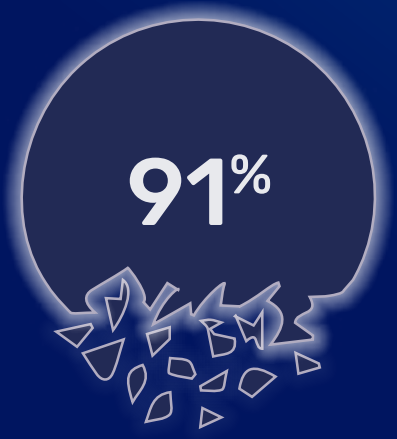
Cybersecurity leaders appear to be taking a tough stance on those employees who are caught out by phishing attacks, with negative outcomes for the people involved happening in 74% of organizations. I would caution them, however, to work with employees. It's a very lucky opportunist who receives a phishing email at the exact time they want to hurt their employer. In my experience, people who fall victim have genuinely made a mistake. In today's world, organizations owe it to their people to provide the right technology to detect advanced attacks and SAT programs that genuinely increases their understanding of real threats, reducing phishing risk for the long term.

COUNTING OUR LOSSES: THE STATE OF DATA LOSS AND EXFILTRATION



experienced incidents caused by **data loss and exfiltration**

of organizations had **information barriers breached**



of organizations experienced **negative fallout**

of people involved **were impacted**

Outbound email is a source of breaches for almost every organization

91% of the surveyed Cybersecurity leaders stated their organization had experienced security incidents caused by outbound email data loss within Microsoft 365 in the last 12 months.

Overall, these incidents were result of employees breaking the rules or making mistakes while simply trying to get their jobs done, with the top three causes:

EXFILTRATING DATA FOR WORK PURPOSES, SUCH AS SENDING DATA TO PERSONAL ACCOUNTS

ACCIDENTALLY SENDING EMAILS AND FILES TO AN INCORRECT RECIPIENT

EXFILTRATING DATA FOR PERSONAL GAIN, FOR EXAMPLE TAKING DATA TO A NEW JOB

This picture matches identically with last year's report, with the same number of organizations reporting incidents and correlating them to these top three causes.

There also remains significant risk of internal breaches of confidentiality within an organization. Of the 76% that enforce information barriers internally, half (51%) have had them breached.

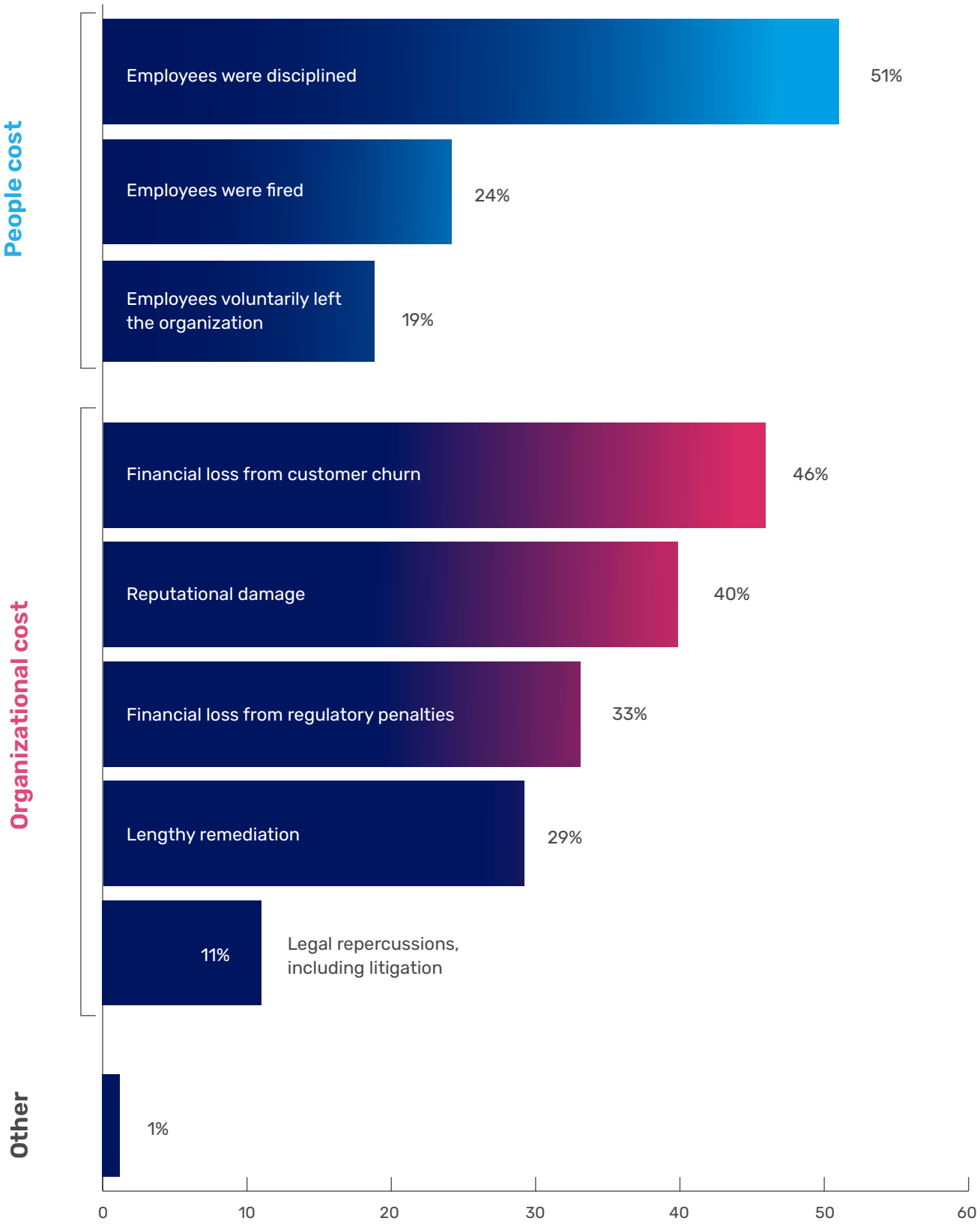
The damage caused by outbound incidents

As with phishing attacks, more organizations are being negatively impacted by security incidents caused by data loss and exfiltration this year than last year. 94% of the surveyed organizations reported being adversely affected, which is an increase of 8% from last year's report.

Again, taking actions against employees was the most common outcome. 67% of people were disciplined, let go, or chose to leave the organization. Employees being disciplined was the most common outcome, happening in 51% of organizations. This is a jump of 10% compared to our 2023 findings, when 41% of organizations reported employees were disciplined and reputational damage was the top impact at 54%.

Negative outcomes for the organization affected 75% of those surveyed. 57% experienced financial losses in some capacity, and this year, revenue lost from customer churn (46%) has overtaken reputational damage (40%).

THE CONSEQUENCES OF **DATA LOSS AND EXFILTRATION**



Every organization that had its internal information barriers breached experienced disruption and damage. Over half (58%) had to cease operations while incidents were investigated, impacting organizational efficiency and the bottom line. In 49% of organizations, client relationships were damaged from breached confidentiality, and just under one-quarter (22%) lost customers.

THE **NEGATIVE IMPACTS** OF BREACHED INFORMATION BARRIERS

58%

CEASE OPERATIONS

49%

DAMAGE TO CLIENT RELATIONSHIPS

22%

CLIENT CHURN

11%

FINANCIAL LOSSES FROM REGULTORY PENALTIES

Expert analysis

JACK CHAPMAN, VP OF THREAT INTELLIGENCE

Without visibility into human risk, organizations are unable to quantify risk and prevent email data loss.

It's interesting that for the second year running, our Cybersecurity leaders have reported intentional rule breaking as the top cause of outbound incidents. When we analyze data from the Egress platform, however, human error is the greatest risk, such as accidentally misdirecting an email to the wrong recipient or attaching the wrong file.

So much can pass under the radar when implementing email DLP manually. Static rules are fundamentally unworkable at the scale they need to predict and prevent organizational-wide data loss. They create too much friction and, even if they didn't, it would be impossible to cater for every use case. Similarly, reviewing audit logs requires administrators to understand and identify every way that data can be lost. This makes it far easier to spot rule breaking, breached information barriers, or even malicious exfiltration - for example, someone sending something to a personal email address or to a colleague in another department when they're not allowed to do so. There's a clear-cut line in all these incidents.

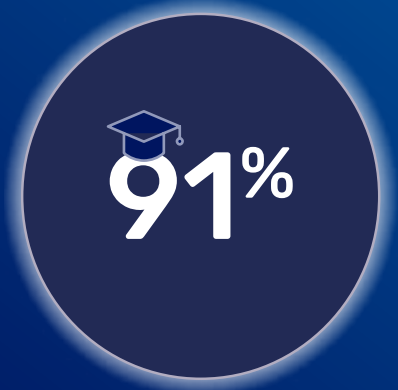
Operating in this way, DLP is wholly too reliant on people, and we're seeing the impact. Almost every organization we've surveyed has experienced incidents – but alarm bells are ringing for me because based on these findings versus what I see when we increase organizations' visibility. I predict the problem is far worse than they know.

IN DEFENSE:
IS PERIMETER TECHNOLOGY AND TRAINING MOVING THE NEEDLE?

of Cybersecurity leaders **expressed frustration with their SEG**

of Cybersecurity leaders are **considering or have already replaced their SEG**

of Cybersecurity leaders are **concerned about the limitations of static email DLP**



of Cybersecurity leaders **worry about the effectiveness of traditional training**

Perimeter detection and static DLP technology are not enough

Our findings have demonstrated that almost every organization remains vulnerable, with 94% experiencing email security incidents in their Microsoft 365 environments – and almost all falling victim to both phishing attacks (94%) and human error and data exfiltration (91%).

As anticipated, they're also being adversely affected by these incidents, with 96% experiencing negative fallout following a successful phishing attack, 94% suffering negative consequences from an external outbound breach, and 100% impacted by breached information barriers.

This is despite the fact that all have some level of perimeter phishing detection and 94% have static email DLP enforced.

87% of Cybersecurity leaders are considering replacing their SEG or have already done so

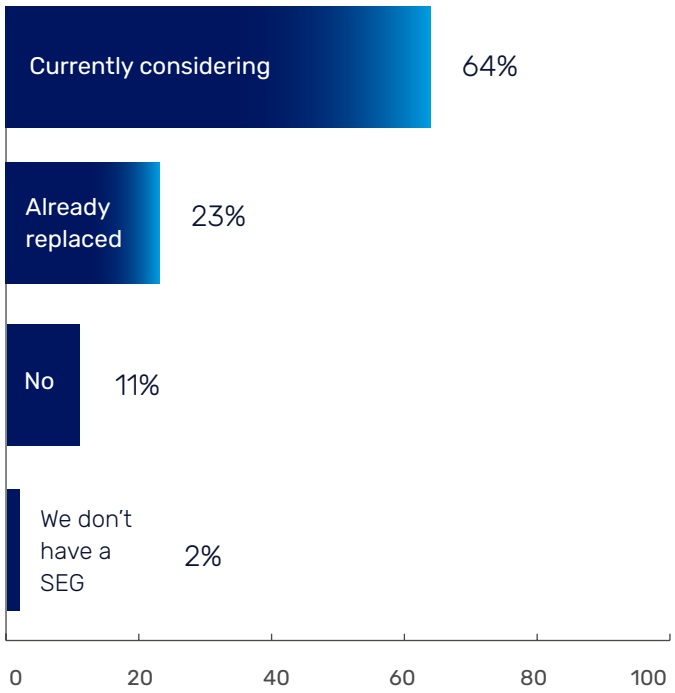
SEG reality

In recent years, Microsoft has developed its inbound email security defenses, bringing them more in line with the detection capability available in SEGs. In turn, this overlap in security functionality is increasingly leaving organizations questioning the value of their SEG.

Of the organizations we surveyed that use a SEG, 91% expressed frustration with it. The top inbound concern is that too many phishing emails end up in employees' inboxes, while the top outbound concern is that it isn't effective in stopping misdirected emails and files.

Likely as a result of Microsoft's security developments and limitations in both inbound and outbound threat detection, 87% of Cybersecurity leaders are considering replacing their SEG or have already done so.

CYBERSECURITY LEADERS SHARE WHETHER THEY ARE CONSIDERING **REPLACING THEIR SEG**



Native controls in Microsoft 365

100% of the organizations we surveyed use Microsoft 365 with a minimum of Exchange Online Protection (EOP) deployed to detect phishing attacks. As noted, Microsoft has enhanced its native security capabilities to the point of significant overlap with SEGs – but, as acknowledged by our Cybersecurity leaders, organizations need enhanced defenses to stop the broad spectrum of email security threats.

88% of those surveyed shared concerns with the Microsoft security controls they have deployed, with the top inbound one being that it can't stop the most advanced phishing attacks, such as zero-day and business email compromise (BEC). Again, similar to SEGs, the top outbound concern was being ineffective at stopping employees from accidentally emailing the wrong person or with the wrong file attached.

88% of organizations have concerns with the Microsoft security controls they have deployed

The limitations of static DLP and Outlook autocomplete

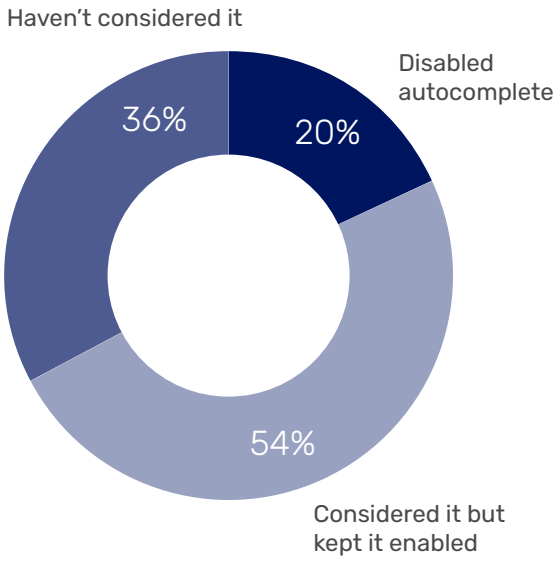
Outbound email security remains a manual process driven by administrators. 94% use static email DLP rules and 51% are reliant on reviewing audit logs to detect breaches.

Of those using static rules, 100% expressed frustration with them, with the most common complaint being the need to alter rules to make them more usable for employees. Cybersecurity leaders also noted they require a high level of administrative overhead to maintain.

In general, Outlook autocomplete is seen as the culprit for most misdirected emails, with people quickly clicking on suggested names and adding incorrect recipients. As a result, three-quarters (74%) of Cybersecurity leaders have considered turning autocomplete off, but only 20% have actually gone through with it.

Pressure continues to build on organizations to preserve client confidentiality on email, with 69% saying they've seen an increase in customers requesting email DLP to be enforced.

CYBERSECURITY LEADERS TELL US WHETHER THEY'VE **CONSIDERED DISABLING OUTLOOK AUTOCOMPLETE**



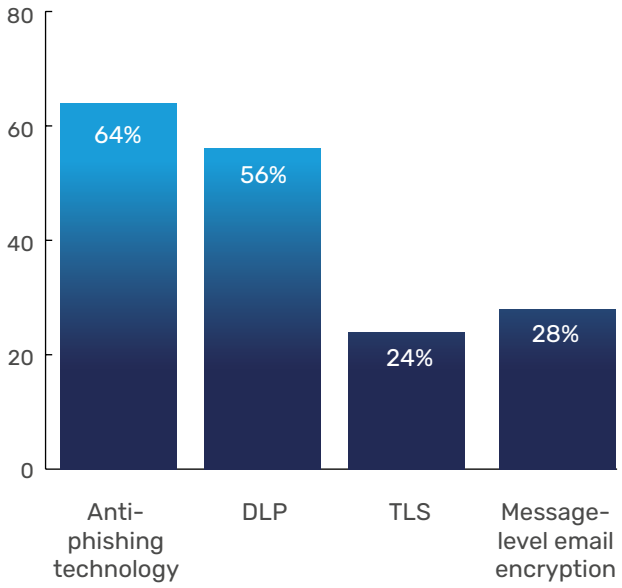
Stress with the supply chain

The customer to supplier to customer cycle continues, with our Cybersecurity leaders putting pressure on their suppliers to uphold inbound and outbound email security.

As we saw earlier in this report, our surveyed Cybersecurity leaders are hyper-aware of the threat that compromised supply chain accounts poses to their organizations. 51% told us that their organizations had been victims of successful phishing attacks sent from compromised supply chain accounts in the last year, and it was their top cause of stress.

It's logical, then, that 82% of Cybersecurity leaders enforce email security requirements with their supply chain, with anti-phishing technology as the most requested defense (64%). Data loss prevention, however, is hot on its heels, with 56% of Cybersecurity leaders enforcing this with suppliers.

CYBERSECURITY LEADERS SHARE THE TYPES OF **EMAIL SECURITY THEY ENFORCE**



Traditional training isn't moving the needle

As could probably be predicted, 100% of the organizations we surveyed carry out SAT. Over half (59%) train employees weekly or monthly, while just under one-third (30%) conduct training quarterly.

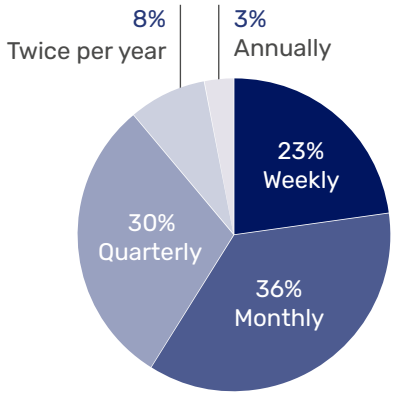
For most, however, it seems that SAT involves a degree of box-ticking.

For 88% of Cybersecurity leaders, meeting compliance requirements is a primary driver for their SAT programs. Additionally, most organizations only offer a limited degree of personalization, with 74% using either out-of-the-box modules or tailoring based on the organization as a whole. Only 19% of organizations deliver SAT that reflects on the department or team that employees work in, and just 9% tailor to the individual employee.

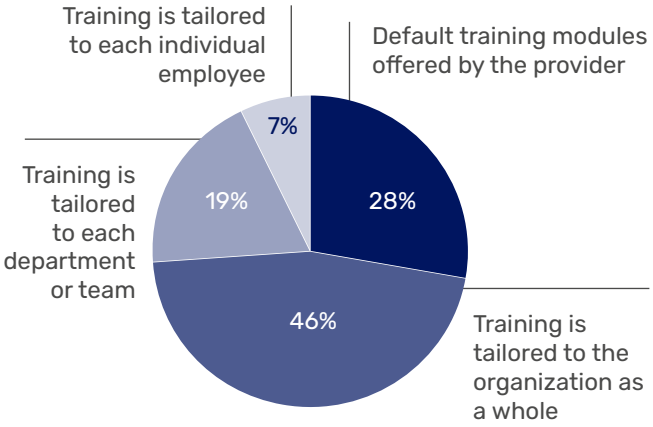
91% of Cybersecurity leaders have doubts about the effectiveness of their traditional SAT programs. The top concerns are that employees skip through training as quickly as possible and that they find training annoying.

For most organzations it seems that SAT involves a degree of box-ticking

CYBERSECURITY LEADERS EXPLAIN **HOW REGULARLY THEY CONDUCT SAT**



CYBERSECURITY LEADERS SHARE **HOW SAT IS TAILORED IN THEIR ORGANIZATIONS**



Expert analysis

JACK CHAPMAN, VP OF THREAT INTELLIGENCE

This isn't a case of 'if it ain't broke, don't fix it'. Organizations urgently need to adapt their approach or find themselves in the same position next year.

Microsoft has made it virtually impossible for SEGs to differentiate their email security. Some organizations will continue to see value in other specialist use cases (such as archiving and journaling) but for most, Microsoft's anti-phishing capability means that that won't also need a SEG.

However, it's not a silver bullet. Due to the overlap in detection functionality, advanced attacks that can get through a SEG can also bypass Microsoft, such as zero days, business email compromise, and phish sent from compromised legitimate accounts.

At the same time, organizations remain vulnerable to outbound data loss and exfiltration, with no reliable and scalable way to detect attacks. People will always make mistakes and they won't know they've done so until it's too late (if they notice at all). Without significantly improved visibility, organizations won't be able to meaningfully address the problem.

Ultimately, is it really fair to expect employees to detect phishing attacks that have made it through at least one layer of detection technology or to never make a mistake? Especially when they're being trained using generic programs that aren't tailored to the actual threats they face.

Organizations urgently need to enhance their detection capability to stop more advanced threats and ensure that training is highly tailored and relevant, based on the way they use email and the actual threats they face.

2024: THE YEAR FOR CHANGE

Organizations need to switch gears in their approach to email security - or face the same incidents and impacts as before.

Many of the findings in this year's report are worryingly consistent with our 2023 edition. Organizations remain vulnerable to advanced phishing attacks, human error, and data exfiltration.

Without change, organizations will face another year of security incidents and negative impacts.

People are at the center of the issue. Without someone acting on a phishing email, adding the wrong recipients, or choosing to break the rules, these incidents wouldn't happen.

Organizations are responding to this by disciplining and dismissing employees. This year, the human cost of both inbound and outbound incidents was higher – but this is likely going to create more problems than it solves.

Instead, Cybersecurity leaders should prioritize approaches that work with and for their people.

Managing human risk on email requires technology that protects employees from advanced threats and adapts to meet them in the moment of risk – such as when they're faced with a phishing email or about to make a mistake. It's also crucial that training is highly relevant to the risks they face and, as a result, far more engaging than out-of-the-box modules or SAT that's tailored to an entire organization.

The shift in attitude towards SEGs shows that Cybersecurity leaders are embracing change, but many may have to accelerate their timelines in 2024 to truly reduce email security risks.

STOP ADVANCED PHISHING ATTACKS AND DATA LOSS IN MICROSOFT 365

People are organization's biggest risk – and they're most vulnerable when using email.

Request demo

Learn more

To empower organizations to manage human risk on email, Egress takes a new approach to behavioral-based threat detection and response. We've architected a single cloud-based intelligent platform that eliminates the advanced inbound and outbound threats that get through Microsoft 365's native controls and secure email gateways (SEGs).

The world's first cloud email security platform to use an adaptive security architecture, we automate threat detection and response for advanced phishing attacks, data loss, and data exfiltration.

Combining contextual machine learning and AI, we use zero-trust and pre-generative modeling to provide the highest efficacy of inbound threat detection, while leveraging social graph and pretrained deep neural networks to detect human error and data exfiltration. Our products are easy to deploy and provide immediate time to value. Egress also offers a powerful combination of contextual banners and prompts that provide in-the-moment education when people need it most.

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.

About Egress

Egress is the only cloud email security platform to continuously assess human risk and dynamically adapt policy controls, preparing customers to defend against advanced phishing attacks and outbound data breaches before they happen. Trusted by the world's biggest brands, Egress is private equity backed with offices in London, New York, and Boston.

www.egress.com

egress