egress

Fighting phishing:

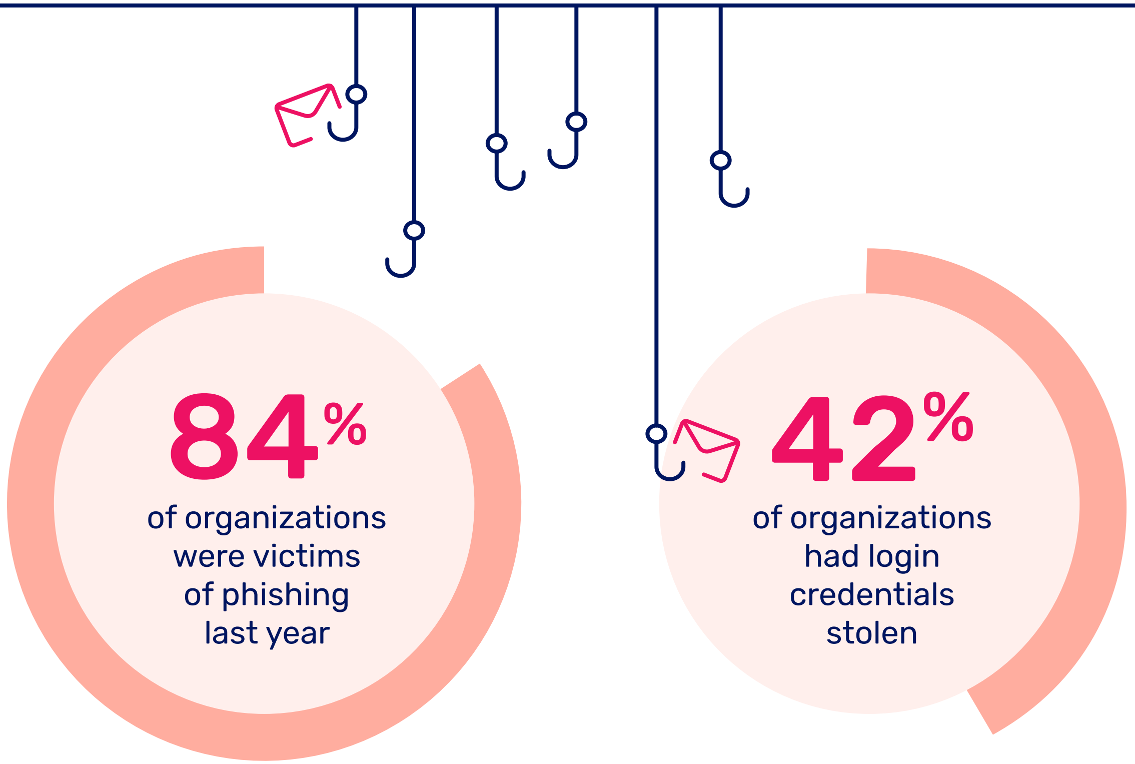
The IT leader’s view

AN EGRESS REPORT

Inside the report

QUICK VIEW: SURVEY RESULTS

Phishing is still a huge unsolved problem



84%
of organizations were victims of phishing last year

42%
of organizations had login credentials stolen

Many organizations suffered financially-motivated attacks:

59%
were hit with ransomware

44%
suffered from payment scams

Organizations are making preparations ahead of future phishing threats:

72%
have taken out cyber insurance

64%
have retained legal counsel to reduce breach impacts

55%
have invested in forensic investigation

Despite the ongoing threats:

Just **23%**

of boards consider ransomware their top security priority

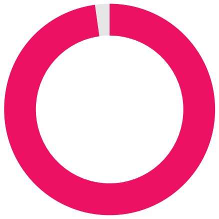
83%

of organizations allocate security budget to dedicated anti-phishing measures

39%

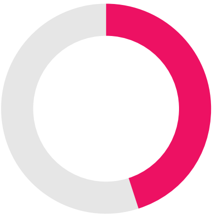
of organizations hit by ransomware paid the ransom

Security awareness training remains popular but IT leaders are dissatisfied with its ability to stop employees falling for phishing:



98%

deliver anti-phishing training



Yet **45%**

switch providers every year

39%

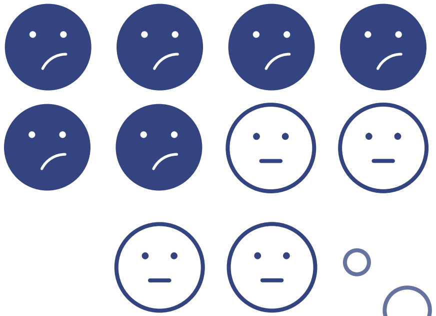
conduct training monthly

72%

switch providers within three years

89%

of IT leaders voiced frustrations with their secure email gateway (SEG)



64%

think SEGs require too much admin and are too expensive

Phishing challenges in 2022

2021 was dominated by cybercrime. The Allianz Risk Barometer places cyber incidents as the most important global business risk for 2022.

Ransomware hit headlines as critical infrastructure such as Colonial Pipelines was targeted, and it also became a daily worry for businesses of all sizes. Then Log4j helped attempted cyberattacks reach their all-time high according to Q4 2021 data from Check Point Software. We saw the average cost of a data breach rise to its highest in 17 years, jumping from $3.86m to $4.24m according to IBM's Cost of a Breach Report.

Against this backdrop, phishing was pervasive throughout 2021 and a constant thorn in organizations' sides. Cybercriminals continue to exploit the increased attack surface available as companies have rapidly transitioned to hybrid and fully remote working.

This report gives insight into the experiences of 500 IT leaders from medium-to-enterprise-size businesses with phishing over the past year. It details the main attacks they've seen hit their organizations and where their perceived weak spots are. The report also includes first-hand quotes to give you an understanding of how phishing is directly impacting your peers across a variety of industries.

Cybercriminals continue to exploit the increased attack surface available as companies have rapidly transitioned to hybrid and fully remote working.

> *An employee at my organization was tricked into opening a link to download malware, as they believed it was a legitimate request from a supervisor. The organization was offline for about two weeks and many of our clients were affected.*
>
> Legal industry CISO, USA, (500 employees)

Which phishing attacks are IT leaders seeing?

Our data shows 84% of the organizations surveyed have suffered a phishing attack in the last 12 months. This is a 15% increase from our 2021 'The real and rising risk of phishing' report.

According to Ponemon Institute's 2019 State of Cybersecurity Report, 66% of small to medium sized businesses experienced a cyber-attack during 2019. Our survey data shows a percentage increase of 26%, with 83% of small to medium sized businesses (under 1,000 employees) experiencing a breach.

INDUSTRY WATCH

FINANCIAL SERVICES

70% of surveyed financial services firms experienced a ransomware attack.

That's **16% more** than in the legal industry and **19% more** than general businesses.

$91,240
the average ransom that financial firms paid in 2021.

#1 Threat: Ransomware

According to Cloudwards research, global ransomware cost $20bn in 2021 and affected 37% of all organizations. Our survey found ransomware to be **even more** prevalent, with 59% of our surveyed organizations falling victim over the past 12 months.

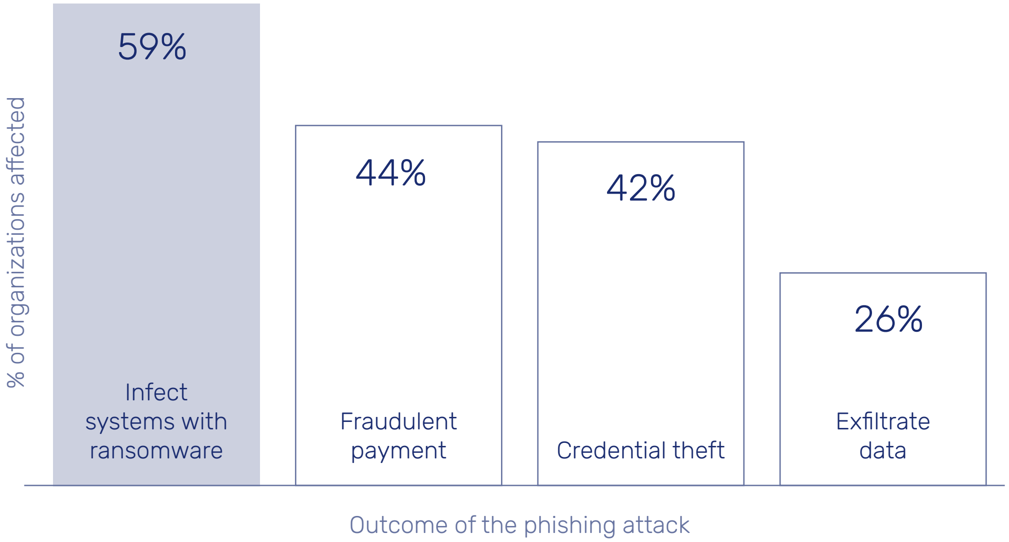
For the organizations affected, there was a relatively even split between ransomware being deployed through two key tactics:

- People clicking malicious links (52%)
- People opening malicious attachments (45%)

There is a clear need for organizations to invest in the right defenses: ones that can detect ransomware through either tactic.

The chart on the right show the attacks being reported by IT leaders. However, it's important to remember that many instances of credential theft and data exfiltration can go undetected and unreported. Ransomware attacks and fraudulent payments are far more likely to be noticed and reported.

IT leaders reveal the outcomes of the phishing attacks their people fell victim to in the last 12 months

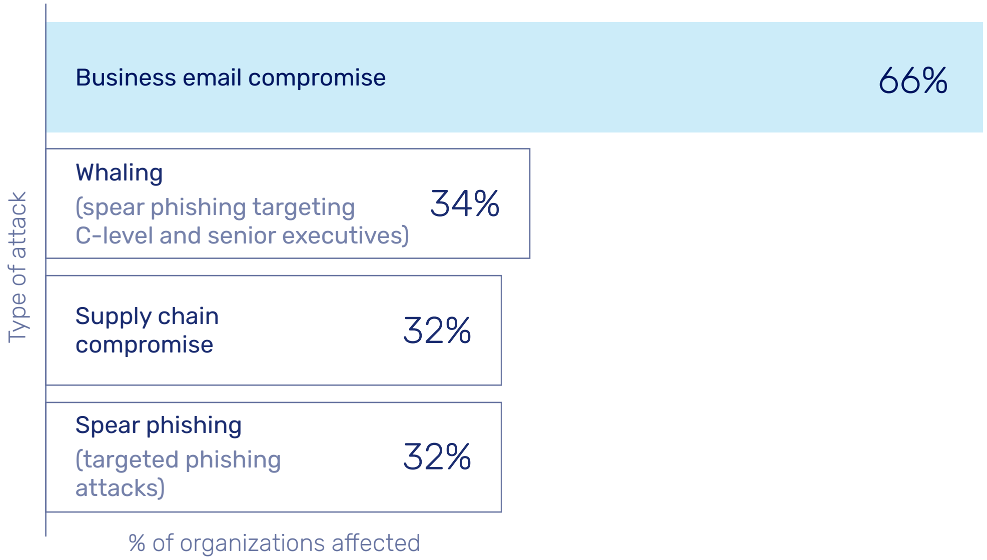


Insiders are losing organizations' money and credentials

Of the organizations we surveyed, 44% said a fraudulent payment had been made in the last 12 months, while 42% acknowledged that people had entered their credentials into phishing websites. It's important to note that all these attacks originated with a phishing email. And of course, there are likely to be many more undetected and unreported instances of credential theft within an organization.

Stolen credentials remain a popular commodity, either for infiltration by the original hacker, supply chain phishing, or for selling on the dark web to others. Credential theft often goes undetected and provides cybercriminals with the keys to unlocking an organization. This enables them to exfiltrate sensitive data and launch further attacks into both the victim's organization and to their customers and supply chain.

IT leaders categorize the type of attacks that led to payment scams in their organizations



> *We were attacked via an innocuous-looking email where the recipient didn't use best practice to avoid clicking on an unknown link. They ended up downloading ransomware that compromised some of our supply chain data – but we were very lucky it didn't compromise any patient data. Solving the issue required extensive training and changes to how we manage our pharmacy supply chain issues.*
>
> **Healthcare CISO, USA, (1,000 employees)**

Business email compromise is a persistent (and expensive) problem

Business email compromise (BEC) is a phishing attack that uses a compromised business account. This makes it dangerous, as the compromised account has legitimate communication history and passes authentication checks.

According to IBM, BEC is the most expensive form of phishing attack, costing organizations an average of $5.01m per breach. The FBI's Internet Crime Report shows that BEC scams made over $1.8bn in 2020, which was more than any other type of cybercrime.

Because BEC attacks are carried out in combination with sophisticated phishing tactics, they're more likely to pass undetected through secure email gateways (SEGs) and lead to breaches. Finance teams in particular need to be wary of urgent email requests from vendors or senior executives that sound unusual or try to break normal processes.

Eighty-four percent of organizations have fallen victim to an email attack in the last 12 months.

EGRESS ANALYSIS

What makes BEC so dangerous?

"The main concern with BEC is how it can bypass traditional security solutions and augment other phishing techniques. This attack vector is so successful as it immediately builds credibility for the attacker by using compromised business email accounts. This is powerful when combined with other attack techniques.

"These methods allow the attacker to fool both the technical solution as well as human perception. This raises the sophistication of the attack vector and increases the likelihood of attackers achieving their goals. Given the clear success attackers are having, there is no doubt this trend will continue to increase."

Jack Chapman,
VP of Threat Intelligence

How are organizations defending against phishing?

Most IT leaders are aware that email presents a large attack surface in their organizations. Our findings show 20% of organizations spent over 100 hours remediating phishing attacks during the past year. We had a wide range of responses from IT leaders regarding how much they spent on anti-phishing – with some spending a large amount of their security budget.

Despite 83% of our respondents spending a portion of their security budget on dedicated anti-phishing measures, it's clear from previous data in this report that many attacks are still getting through. So, we also asked IT leaders what business measures they were taking to prepare for the event of falling victim to an attack.

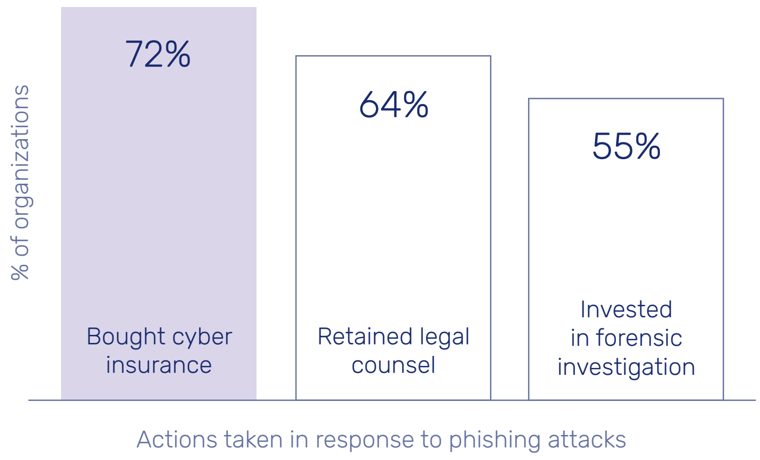
Business measures that prepare for attacks

Taking out cyber insurance is a logical reaction to phishing threats, as it offers financial security against the immediate attack and with the cost of remediation.

However, insurance payouts to cybercriminals, particularly for ransomware demands, often fund further attacks and put organizations at greater future risk of repeat attacks.

The fact 64% have retained legal counsel and 55% have invested in forensic investigation in preparation for phishing attacks shows how seriously IT leaders are taking the threat of phishing and the potential fallout of an attack.

IT leaders share the actions their organizations have taken to prepare for phishing threats



Ninety-eight percent of companies surveyed conducted some form of cybersecurity training over the past 12 months.

Training as an anti-phishing defense

Out of our surveyed organizations, almost all (98%) carried out at least some form of phishing cybersecurity training. Fifty-five percent of IT leaders said they carried out training a few times a year, while 38% have monthly training.

Forty-five percent of our surveyed organizations change their training supplier on a yearly basis. This suggests they're constantly trying to find a more effective training supplier, for example with newer or better content. Or it could mean they don't feel the training is working.

> *An email chain had been compromised between a buyer and their supplier. The attack got through the supply chains' systems and piggy-backed onto an ongoing email conversation. It included a malicious link, which our employee presumed was safe due to it being from a supplier, so the link was opened. Retraining was sent out to the entire organization.*
>
> **UK, Financial Services, (10,000 employees)**

EGRESS ANALYSIS

Phishing training – is it worth it?

"Why are successful attacks still so prevalent after all this training? The truth is cybersecurity training is limited in its effectiveness. It's a lot to expect people to be constantly vigilant to the threat of phishing.

"Phishing attacks are carefully designed to move us away from 'Type 2 thinking' where we're measured and working in a slow, calculated way. More people would catch a phishing attacks if they really stopped and thought. But phishing plays on our psychology to shift us into 'Type 1 thinking' where we act quickly and intuitively, working on autopilot instead.

"Perhaps it's the approach to cybersecurity training in general that needs to change? An alternative is to put security technology in place that can detect phishing threats while also offering real-time insight into why certain emails are blocked – catching people in that 'Type 1' state where they're about to do something risky without thinking."

Jack Chapman, VP of Threat Intelligence

Spotlight on ransomware

Ransomware was the most common outcome for the surveyed organizations that fell victim to phishing (59%). However, only 23% of CISOs said ransomware was the number one cybersecurity priority for their board. This is surprising, given the potential for ransomware to lock down entire systems and leave a business wide open to future attacks and blackmail.

Ransomware was the most common outcome for the surveyed organizations that fell victim to phishing (59%).

Research from Cybereason shows that 80% of organizations struck by ransomware end up suffering another attack – and 46% are targeted by the same cybercriminals that hit them in the first place. There's also **no guarantee the hackers didn't exfiltrate your data to sell** or use for future blackmail before decrypting it.

A FinCEN Report on Ransomware Trends in Bank Secrecy Act Data found that as much as **$5.2bn** worth of outgoing Bitcoin transactions could be connected to payouts involving the 10 most common ransomware variants.

How are ransomware victims chosen?

Cybercriminals can carry out their own research into organizations or they can choose from a wide range of open-source intelligence (OSINT) available for purchase on crime-as-a-service marketplaces. Factors for choosing a victim will include:

- What security defenses do they have in place?
- Is there a known entry point for an attack?
- Have they paid a ransom before?

When choosing an ideal victim, cybercriminals often find out whether a target has cyber insurance. Out of our surveyed organizations, 72% have put cyber insurance in place as a preventative measure to mitigate phishing attacks. A common tactic is to set a ransom just below what an insurance firm will pay out, as hackers know their ransom will be covered under the terms of the insurance and is more likely to be paid.

Only 23% of CISOs said ransomware is the number one cybersecurity priority for their board.

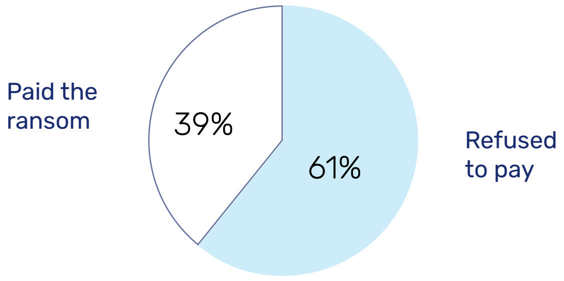
> *An employee received an email from an external prospect that seemed to contain legitimate business information – but when they opened the attachment, ransomware was downloaded. The employee was unaware that their personal information, including email credentials, had been compromised and continued using their account. This allowed the cybercriminals to have continued use of their account to send malicious links to internal and external participants.*
>
> **Financial Services CISO, USA, (5,000 employees)**

To pay or not to pay?

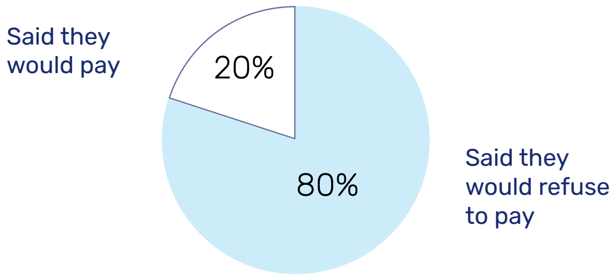
Organizations struck by ransomware find themselves in a difficult catch-22. Pay the ransom for the key to decrypt their files or rebuild their entire affected IT system from scratch. This shows why incident response planning and back-ups are so important. Some businesses believe the best idea is to pay and then they will at least be left alone in the future. Unfortunately, this is wishful thinking.

The truth is: once ransomware has struck, it can be a huge problem to overcome. Prevention is the best defense. By stopping ransomware at one of the most common points of delivery (email phishing), you can stop someone clicking the link or attachment to download it in the first place. This breaks the kill chain much earlier and closes off the easiest and most productive way for cybercriminals to get ransomware into your system.

The majority of CISOs surveyed refused to pay a ransom. Of the surveyed organizations who received ransom demands in the last 12 months:



Unaffected CISOs appear to underestimate the likelihood of paying a ransom. Of the surveyed organizations who were not hit by ransomware:



The truth is: once ransomware has struck, it can be a huge problem to overcome.

EGRESS ANALYSIS

Why is ransomware so prevalent?

"In the past, a cybercriminal would have needed at least moderate coding and hacking skills to create ransomware and carry out an attack. Today, it's as simple as making a credit card payment and sending an email. Wannabe hackers can access the crime-as-a-service marketplace and buy readymade ransomware and phishing kits for easy delivery into organizations. This greatly reduces the barrier to cybercrime – and that's partly to blame for the increase in ransomware.

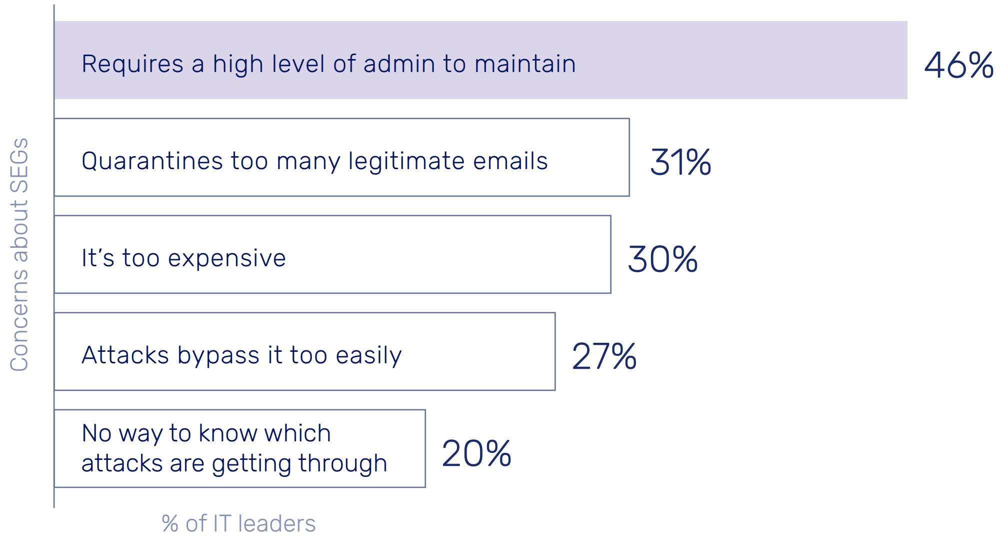
"Cybercriminals are also increasingly taking a 'poison the well' approach, exploiting vulnerabilities in supplier or open-source code that they can use to propagate attacks against multiple victims. The SolarWinds (2020) and Kaseya (2021) attacks are two high-profile examples of cybercriminals using a supplier's own software to target their customers."

Jack Chapman, VP of Threat Intelligence

Limitations of SEGs

Out of the IT leaders we surveyed, 89% have at least one issue with the performance of their SEGs. Nearly half (46%) found they required a high level of admin to maintain. This is often down to administrators having to update static rules and blocklists, rather than it automatically adapting to detect the latest threats. The chart below details the specific challenges they’ve been experiencing.

IT leaders share their opinions on their SEGs



> *We had a series of emails from someone posing as one of our vendors. Due to remote working and staff shortages, no-one had questioned their authenticity and allowed the person (or people) to gain access to sensitive data on our central database system. We were able to shut the system off within 24 hours, but some key information had already been compromised.*
>
> **Financial Services CISO, UK, (5,000 employees)**

Complementing the SEG: Integrated Cloud Email Security

A new category of email security solution has emerged to complement the SEG, which industry analyst Gartner calls Integrated Cloud Email Security (ICES). These solutions use advanced threat detection techniques, such as machine learning and natural language processing. The best solutions go beyond simply blocking known threats, instead protecting and educating people in real time.

Findings in IBM's Cost of a Breach Report showed that organizations with AI-based security solutions experienced a significant reduction in the costs associated with a data breach. They found that AI security solutions cut breach costs from $6.71m to $2.90m.

2022 will be a year when many organizations re-evaluate the capabilities of their anti-phishing defenses to judge how effective they are against modern threats.

EGRESS ANALYSIS

Is a SEG enough on its own?

"Phishing attacks (and cybercrime tactics in general) are constantly evolving. They use many sophisticated techniques to evade detection by email security controls. Traditional SEGs provide excellent email hygiene by filtering spam and malware. However, SEGs are reactive and they struggle to deal with both links and payloadless attacks.

"ICES solutions can detect attacks that often slip under the radar of SEGs. The best solutions are easy to set up and integrate with existing controls, meaning they tend to show their value quickly. In 2022 we expect more businesses will choose to either augment or replace SEGs with ICES to gain true peace of mind against phishing threats."

Jack Chapman, VP of Threat Intelligence

>> Top three takeaways

As we look on to 2022, here are the top three takeaways from our survey results:

1

84% of businesses were hit with successful phishing attacks last year – a 15% increase from our 2021 ‘The real and rising risk of phishing’ report.

2

Ransomware is a problem for businesses of all sizes, with 59% being hit in 2021. IT leaders are preparing for attacks by getting cyber insurance (72%) and retaining legal counsel (64%).

3

89% of IT leaders have at least one frustration with their SEG.

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

This survey was carried out by Arlington Research, in partnership with Egress. 500 IT leaders were interviewed from a range of industries, with an equal number of respondents coming from the UK and US.

www.egress.com | EgressSoftware

egress