Insider Data Breach Survey 2021

Are employees your greatest defense or your biggest vulnerability?

egress

Table of contents

Executive summary

Human layer security: Making people your greatest defense

Insider risk poses the greatest threat to any organization. Every IT leader knows the potential impact of a data breach, but many are worryingly underprepared when it comes to their own people.

That's because insider risk is the most complex cybersecurity issue they have to solve. People create risk every day. They are vulnerable to targeted phishing attacks and being hacked; they make mistakes, such as misdirecting sensitive emails; and they break the rules, often just to make their lives a little easier (and sometimes for personal gain).

Our third Insider Data Breach Survey sums up IT leaders' prevailing attitudes to insider risk and where their biggest concerns lie. We've also gauged the feelings of "insiders" themselves – and found some interesting disconnects between employer and employee when it comes to insider risk.

The findings have raised some thought-provoking discussion around how well organizations are detecting insider breaches, and what impact their handling of breaches is having on employees. We've also explored the ongoing effect of remote working and COVID-19 inspired phishing attacks.

But data breaches aren't just statistics; every data breach has a story behind it. This year, we also asked IT leaders and employees to share their stories, and reached out to industry experts for their views.

As we move into the second half of 2021, IT leaders need to gain a firm grasp on insider risk and put an effective strategy in place to mitigate it. This report should offer you a strong starting point.

"Data breaches aren't just statistics; every data breach has a story behind it"

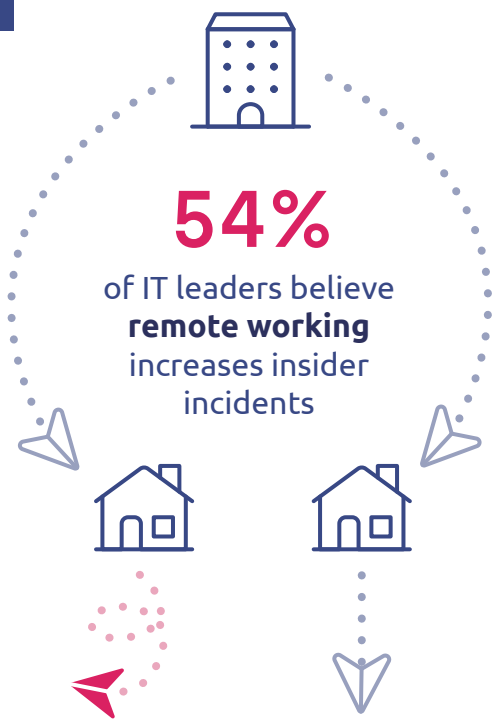
At a glance: what you need to know

94% of organizations had an **insider data breach** in the last 12 months

Human error is the most common cause

But **malicious incidents** worry IT leaders the most

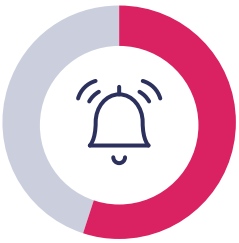
Email is the most **at-risk** vector



54%

of IT leaders believe **remote working** increases insider incidents

97% of employees say they would **report a breach**



This is good news for the

55%

of IT leaders who **rely on employees** to alert them to incidents

89%

of incidents led to **repercussions** for the employees involved

Only

54%

of employees think their organization's security culture **trusts and empowers them**

View from the top

How do IT leaders see insider risk in 2021?

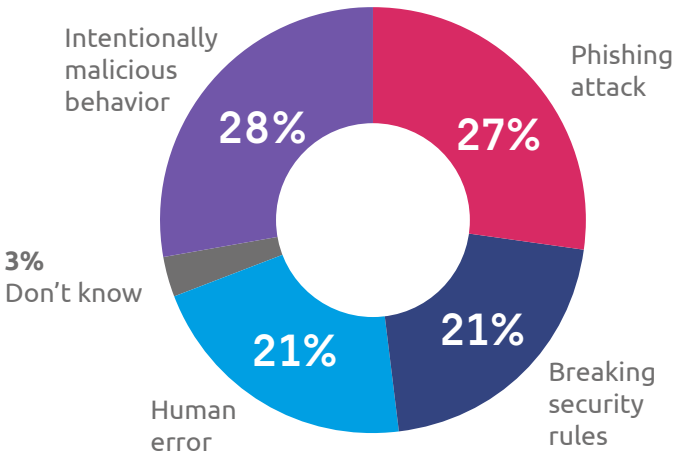
With a fair amount of trepidation! 97% of IT leaders are concerned about insider data breaches – the same percentage as in 2020. It's clear that anxieties aren't easing as time passes, and the figures around breach numbers show that IT leaders are right to be concerned. 94% of organizations have had a data breach in the last 12 months. 84% have suffered a breach directly from human error and almost three-quarters (73%) have experienced a phishing breach.

But what specific incidents are keeping IT leaders up at night? Despite affecting the lowest number of surveyed organizations (66%), malicious insiders worry IT leaders the most. Interestingly, human error came joint bottom of IT leaders' list of concerns – despite being the most common way (84%) in which organizations had been breached.

"94% of organizations have had a data breach in the last 12 months"

Have you (IT leaders) experienced a serious data breach from the following incident?

As an IT leader, which category of insider breach incident are you most concerned about?



Spotlight on malicious insiders

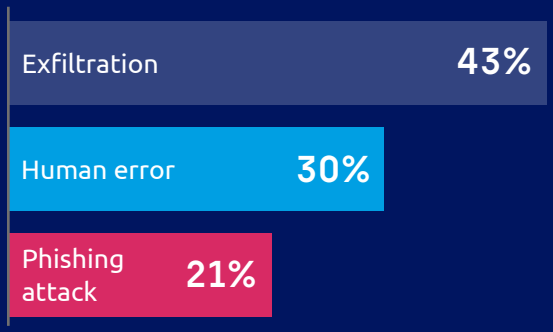
Why are malicious insiders the biggest concern? According to IT leaders, it's not simply the bad taste left by a formerly trusted colleague turning rogue and deliberately doing harm. It's because they believe single incidents of malicious exfiltration will have the greatest negative impact.

There's also personal gain motivating malicious insiders, so their actions are typically well-targeted to harm the organization. This can be the damage done from the incident itself or from further incidents if the data is given to cybercriminals, or some form of payday from hackers, competitors or even nation states.

Three motivations behind malicious breaches worry IT leaders equally:

- Taking data to a new job
- Leaking data to cybercriminals
- Leaking as part of a nation-state attack

As an IT leader, what would have the most negative impact for your business from a single incident?



EXPERT INSIGHT

Steve Williamson, Head of Internal Audit – Information Security & Data Protection, GSK

The malicious breach is different. It's pre-planned. Malicious insiders work out the rules and thresholds of the technical safeguards an organization has in place and identify ways around them to do the maximum amount of damage they can. Typically, they'll have more access to systems and data, and will be targeted in exploiting that access to have the greatest impact or most beneficial outcome for them.

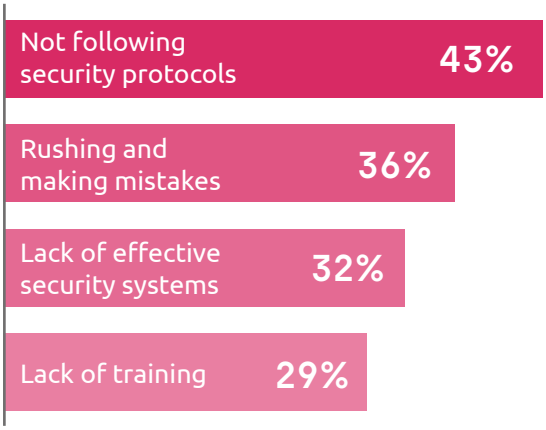
I work for a company that produces blueprints for automobile parts manufactured in China. We had a group of people that started working with us through a local temp company and it turns out they were caught stealing finished blueprints. They were giving the photographs to a competitor of our client!

ANONYMOUS EMPLOYEE, AUTOMOTIVE

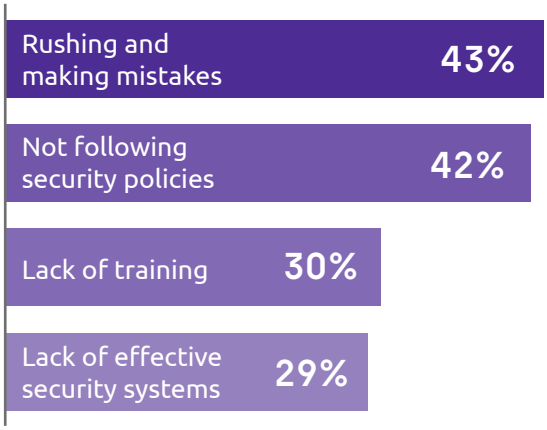
Who's to blame for accidental breaches?

Breaches arising from human error and phishing both require a mistake from an insider – and IT leaders know it! Our findings show that IT leaders put blame at the feet of insiders, rather than deficiencies in their own security systems and training.

What are the top ways an employee would fall victim to a phishing attack within your organization?



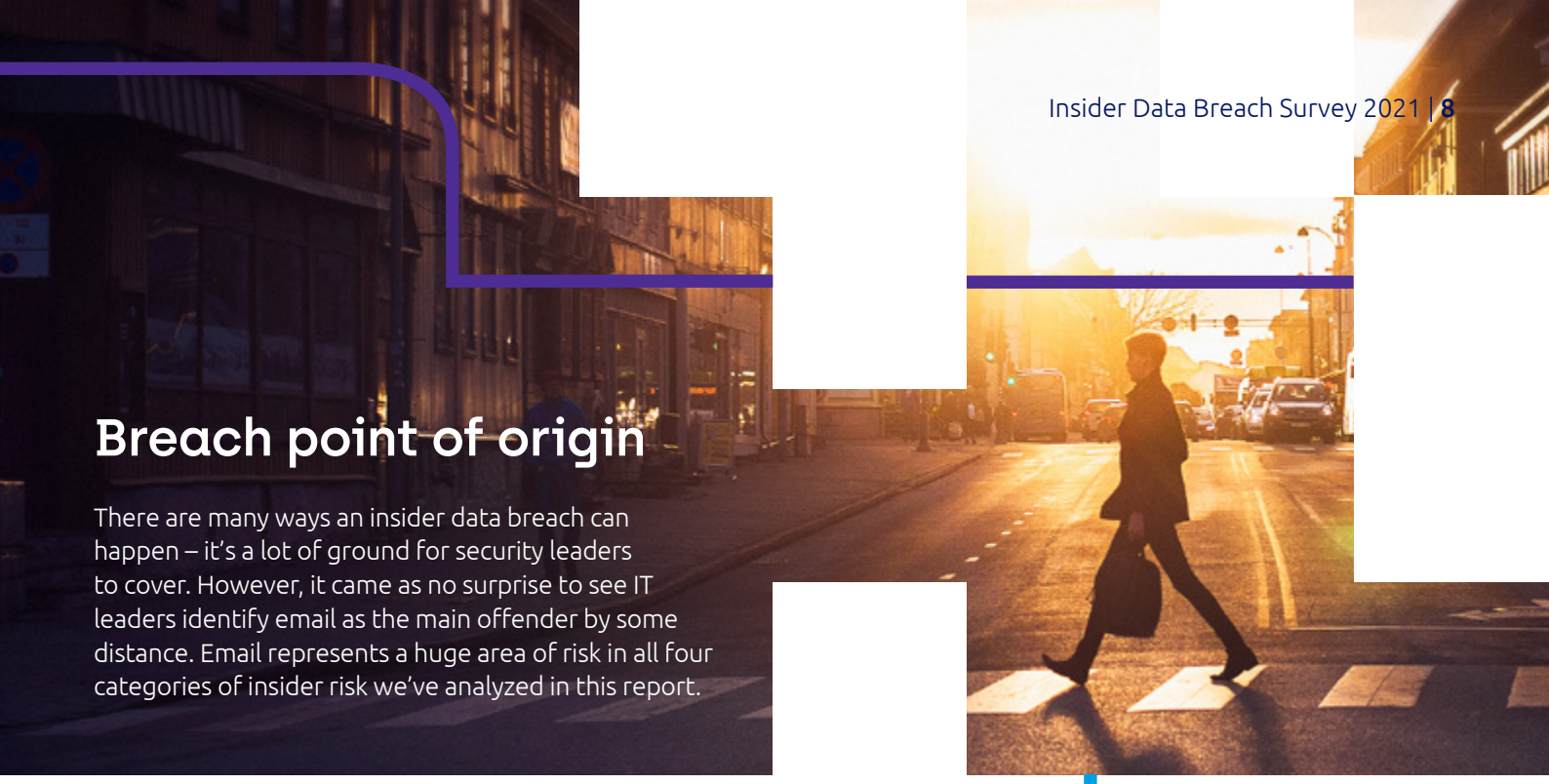
What are the most likely causes of an employee accidentally leaking your organization's data?



EXPERT INSIGHT

Rachel Wilson, Head of Cybersecurity, Morgan Stanley

The majority of real-world insider data breaches aren't caused by bad people doing bad things; they're caused by good people trying to get their jobs done. The frenemy that is Outlook autocomplete is the bane of every Security team's existence, because it's a productivity enabler but it's also a top cause of accidental data loss. Similarly, while working remotely, people are sending more data to their personal accounts when they know they shouldn't but they feel they don't have an alternative, for example to get something printed ahead of a meeting or to join a video call from a personal device without realizing there was an attachment in the invite.



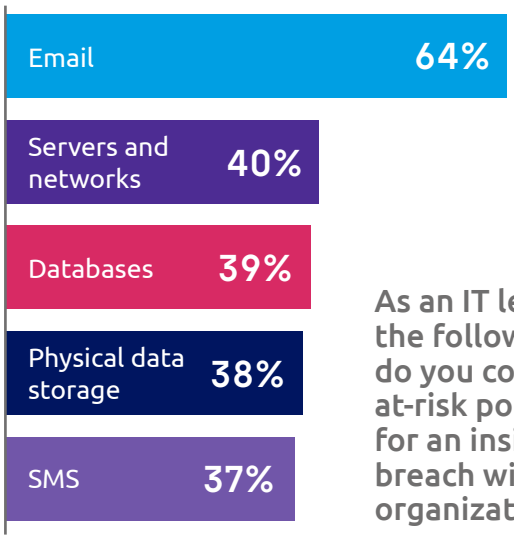
Breach point of origin

There are many ways an insider data breach can happen – it's a lot of ground for security leaders to cover. However, it came as no surprise to see IT leaders identify email as the main offender by some distance. Email represents a huge area of risk in all four categories of insider risk we've analyzed in this report.

Concerned, cautious... and a little fed up

The general consensus from IT leaders is that insider breaches are an ongoing and complex challenge. Despite malicious exfiltration standing out as the number one fear and email remaining the riskiest point of origin, concerns were spread widely in the survey results.

The range of ways each of our four incident categories could happen simply goes to show how complex of a problem insider risk is to solve. But are IT leaders' fears backed up by the opinions of their employees? In the next section, we'll hear what the insiders had to say.



As an IT leader, which of the following channels do you consider to be at-risk points of origin for an insider data breach within your organization?

EGRESS ANALYSIS

Email is still the riskiest channel

It's easy to make a mistake and accidentally misdirect an email – we've all done it. If someone was going to (maliciously or otherwise) exfiltrate data, the chances are they'll simply email it to their personal account. On top of that, email remains the most fertile hunting ground for phishers.

IT leaders clearly recognize email is a problematic channel. But it's fast, familiar, productive – and going nowhere. That means it's not a simple problem to solve, as evidenced by the failure of traditional email data loss protection solutions to stop breaches.

View from the inside

Do employees see themselves as risks?

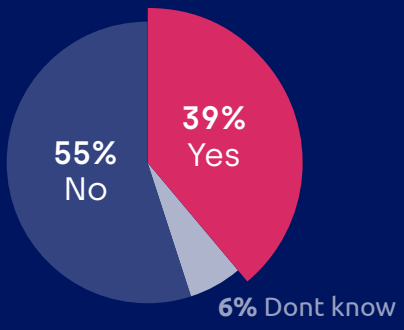
The following stats show an interesting disconnect between how often insiders believe they come across threats and what's being reported by organizations. Only 39% recount having seen instances of accidental email first hand – which is low given the frequency of incidents described by IT leaders.

Phishing is a little higher, with 55% saying they or a colleague have received at least one phish in the past 12 months – although, 73% of respondents also told us they've never fallen victim to a phishing email themselves.

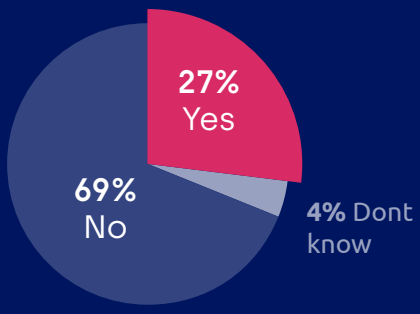
The view from IT leaders is clear. Insider risk is a serious problem, and they're being breached often in a variety of ways. So why are insiders painting a far rosier picture? These stats could serve as a reality check for IT leaders, suggesting that insiders perceive less risk than there actually is.

We asked employees:

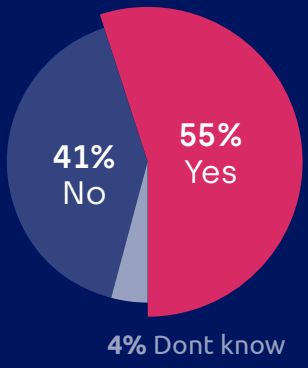
Have you received a recalled Outlook message or an email telling you to disregard an accidental email in the last 12 months?



Have you received an email from someone pretending to be a senior employee in the last 12 months?



Have you received a phishing email in the last 12 months?

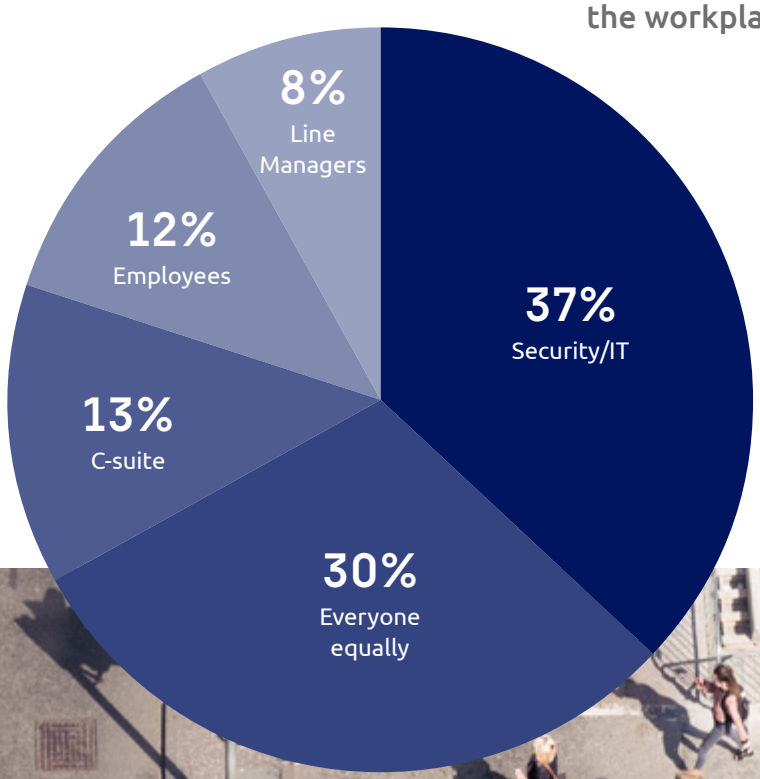


> **Someone fell for a phishing attack and ended up sending personally identifiable information (PII) to an outside source. Luckily, it was their own PII and not a client's or someone else's in the company, so we narrowly avoided a major incident.**
>
> ANONYMOUS IT LEADER, LEGAL

Whose data is it anyway?

IT leaders would think (and hope) that data security is seen as an organization-wide effort. However, it can be an interesting debate as to who has the ultimate responsibility for securing data. Our respondents were divided on the issue – suggesting employees simply aren't clear on where the final responsibility for securing data lies.

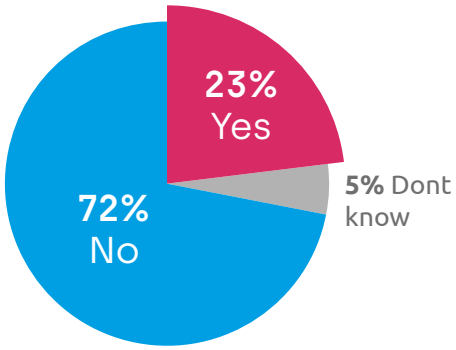
We asked employees: Who has the greatest responsibility for securing information and data in the workplace?



Would you take data to a new job?

Given deliberate exfiltration was the biggest worry for IT leaders, they'll be pleased to hear that 72% of insiders believe a person should not be allowed to take data with them to a new job. However, for Security teams, the quarter (23%) of employees who think they are entitled to take data with them remains a concern.

We asked employees: If a person moves to a new job, should they be allowed to take data with them?



INDUSTRY WATCH

Interestingly, only 15% of legal employees believe that everyone in an organization has an equal responsibility to secure data.

Does that suggest those of a legal mindset would prefer to see clearly defined rules and regulations around data security responsibility?

Legal employees were outliers in other categories too:

46%
think they should be able to take data with them to a new company

48%
have received an email pretending to be a senior employee from their company

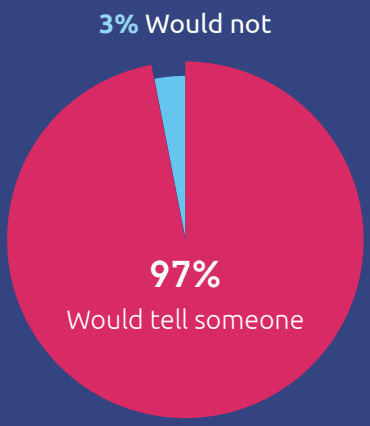
57%
have received an Outlook recall message or email telling them to disregard a misdirected email

Can we trust insiders to do the right thing?

According to our respondents, the answer is a resounding yes. When asked if they would report themselves or a colleague for a data breach, almost every respondent said that they would. Should IT leaders take employees at their word? The question is: how far can we trust what people say they would do?

"97% of insiders say they would report a breach"

If you caused a data breach, would you inform someone internal (line manager, HR, IT, Security, a colleague)?



What about if a colleague caused the breach?

EGRESS ANALYSIS

Prevention beats reaction

From our findings, it would appear insiders believe they would do the right thing if they knew they had caused a breach. In a real-life scenario though, people can panic and stay quiet, hoping the incident will come to nothing if they don't act. It's therefore imperative to create a security culture where incidents are caught before they happen, and before the damage is done and remediation is required.

Security culture: The human cost of handling breaches

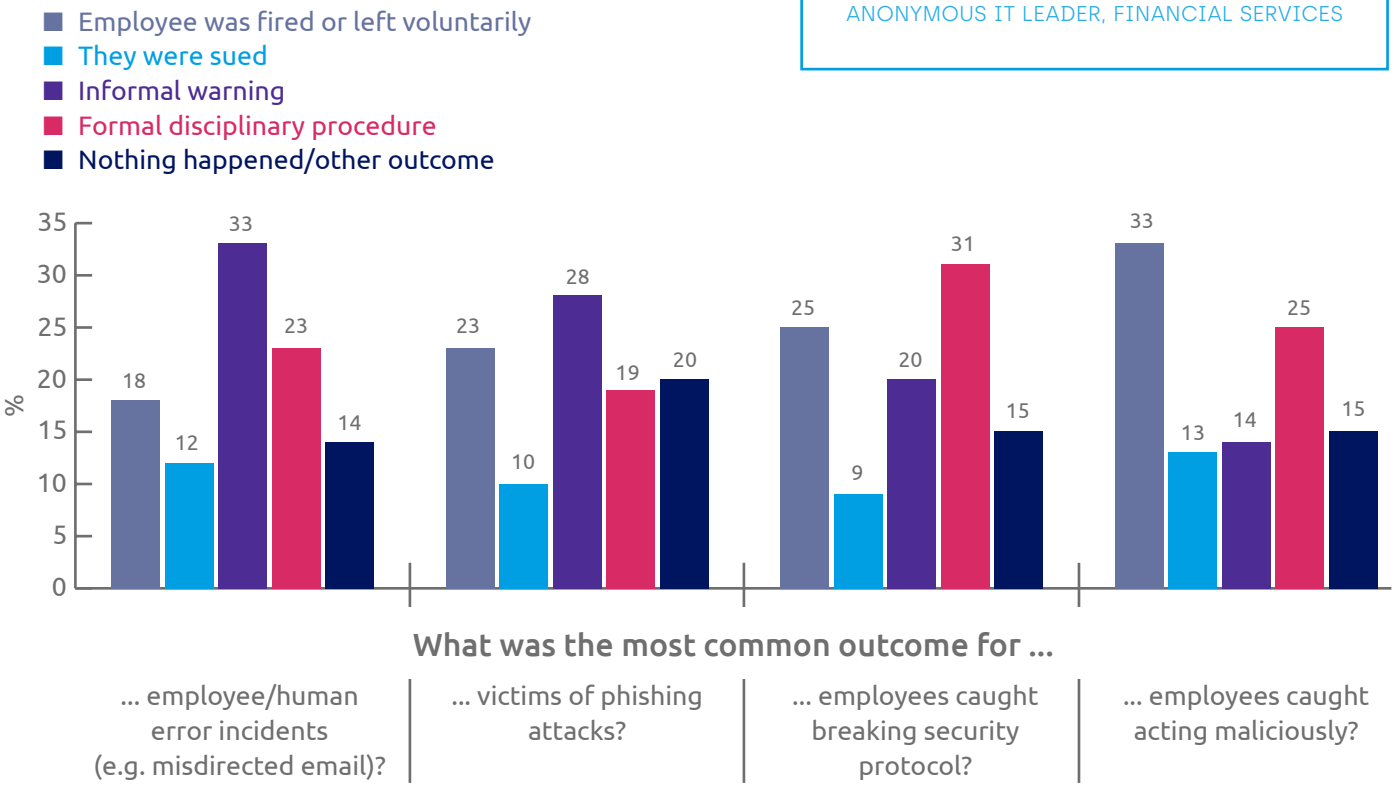
"In 23% of organizations, employees who were hacked via a phishing email were fired or left voluntarily"

Does a data breach always lead to dismissal?

A worrying amount of insider data breaches do end up with the individual in question losing their job or choosing to work elsewhere. When we consider that 84% of organizations experienced at least one breach (some many more) arising from a mistake, 18% is a high amount of cases to result in a dismissal. It's also concerning that almost one-quarter (23%) of phishing victims end up changing jobs – for a mistake.

We actually caught an employee selling data to a competitor. He was copying it onto a physical USB and caught by a colleague. He was dismissed and we ended up taking legal action against him.

ANONYMOUS IT LEADER, FINANCIAL SERVICES



EXPERT INSIGHT

Lisa Forte, Partner,
Red Goat Cyber Security LLP

Balancing morale with breach remediation

When it comes to intentional insiders, those who deliberately and purposefully compromise your security, appropriate measures may include suspension and ultimately taking the drastic action to fire them. They may well have broken the law and violated their terms of employment. These situations are clear. There is one victim and one perpetrator.

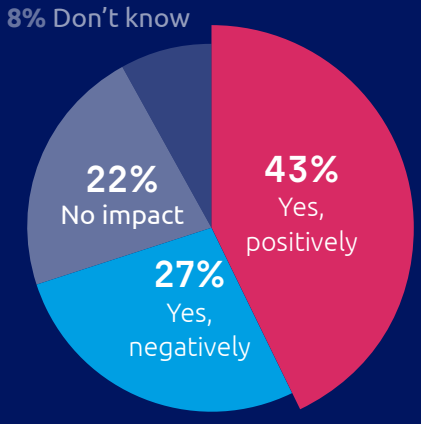
Where the correct action becomes less clear is when the insider makes a mistake, is distracted and clicks on something they shouldn't or simply sends an email to the wrong "Lisa" in their address book. Punishing people for mistakes will cause more damage in the long run.

If you fire or discipline an employee because they made a mistake, the knock-on consequences to your security culture could be catastrophic. Employees could stop reporting mistakes due to the fear of some draconian punishment coming their way. These errors may go unnoticed which is far more dangerous than ones you know about and can remediate.

Investing in stopping these mistakes in the first place is key. Ensuring employees are well trained, supported and know the importance of reporting incidents and mistakes will leave you far better off than taking a hard line.

> I was approached by a colleague who had been the victim of a phishing email along with myself, and we were very embarrassed (needless to say). Reluctantly, we reported the entire incident to our IT Department.
>
> ANONYMOUS EMPLOYEE, FINANCIAL SERVICES

Do you think your organization's overall response to any insider security incidents has impacted how employees who were not involved in the incident perceive your organization?



Thumbs up or down for security culture?

When asked to describe their organization's approach, responses from employees were positive overall. This implies that insiders are on board with their organization's security efforts – even if the outcome of a breach does tend to be negative for the individual involved.

What best describes your company's security culture?

EGRESS ANALYSIS

Is the human cost being counted?

Everyone creates risk. It's why 97% of IT leaders are concerned about insider data breaches, and why you'll struggle to find someone who hasn't been caught out by a phishing scam, misdirected an email, or broken security policy. So, is a security culture where employees lose their jobs for honest mistakes truly an effective one?

There has to be an element of accountability – especially when it comes to malicious or deliberately reckless behavior. However, for truly accidental mistakes, there are better ways to operate. We believe there should be more accountability on the employer side to protect employees with the right technology.

INDUSTRY WATCH

Legal employees were more likely (21%) to find their security culture too controlling than surveyed employees from other industries.

> A colleague opened a risky email, but it was a set-up from the hospital to see if employees would click those types of emails and she did. She was fired directly.
>
> ANONYMOUS HEALTHCARE EMPLOYEE

How much visibility do organizations have over insider risk?

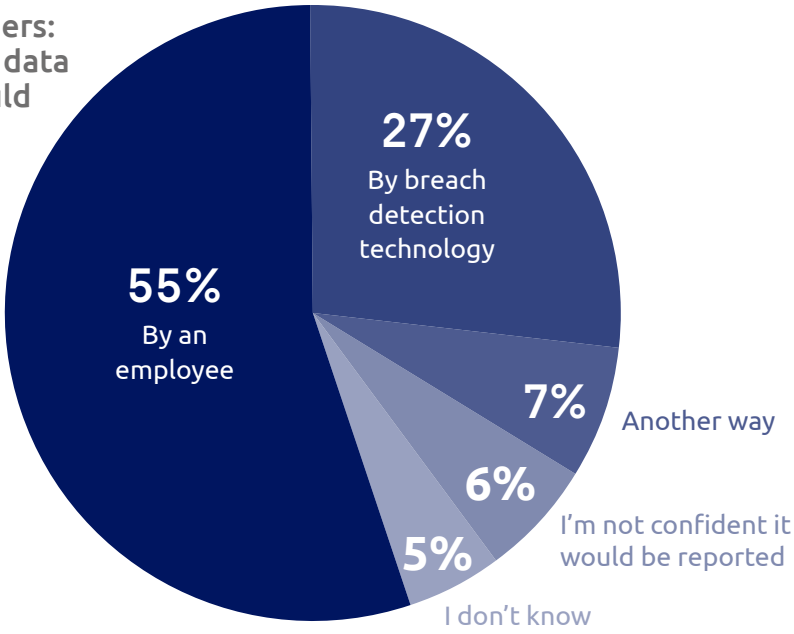
A reliance on self-reporting

We've seen evidence that insiders tend to (or at least claim to) do the right thing after being involved in a data breach. And based on our survey findings, IT leaders clearly trust in their employees more than their breach detection technology. However, is it really effective or fair to rely on insiders to self-report?

Even if reporting and visibility is good within an organization, there's still a large elephant in the room. The breach has happened. Catching a breach early can sometimes mitigate the impacts, but often, the damage has already been done. IT leaders need better visibility before breaches occur – not just after the incident.

> **One of our employees clicked on a phishing link but thankfully they didn't download anything. They reported it to the IT team who took over from there and managed to avoid what was nearly a very serious data breach.**
>
> ANONYMOUS IT LEADER, FINANCIAL SERVICES

We asked IT leaders: In the event of a data breach, how would you be alerted?

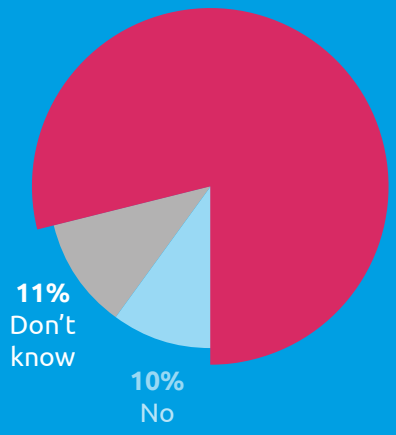


"Only 27% of IT leaders say they would be alerted to an incident by their breach detection technology"

How much help are employees getting?

We wanted to know how employees rated the cybersecurity training and technical controls within their organizations. Mostly, they seem to believe their security training is effective and that the right tools are in place to protect them. But if that's the case, should we really be praising controls and systems that let so many data breaches slip through the net?

We asked employees: Does your organization have the right technical controls to ensure you don't cause a breach?



We asked employees: What best describes your security training?

EGRESS ANALYSIS

Good technology can be trusted

It's worrying to see just how little faith IT leaders have in their breach detection software. Is it really fair to put that much pressure on employees to always detect and report their mistakes? It's one of the reasons why insider risk isn't reducing year on year.

A better way would be for intelligent technology to aid the natural good sense of employees, helping them towards smart security decisions before incidents occur. It's simply not good enough to only gain visibility over breaches after the damage is done – and expect the people most at risk of punishment to come forward and admit their mistakes.

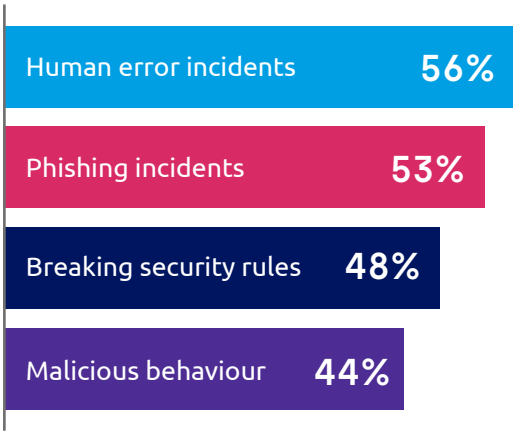
Remote work: A game changer

The new way of working

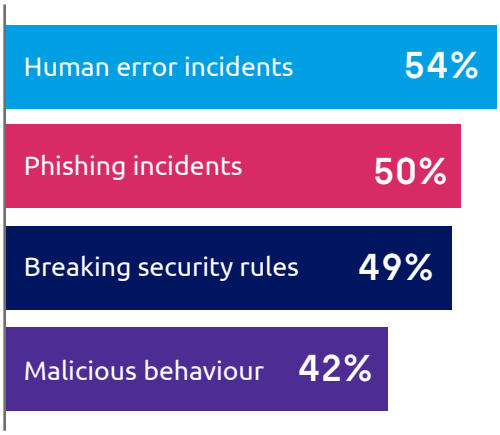
There might have been a point in 2020 when sceptics could have claimed remote working was a temporary and forced solution, and that we'd all be returning to offices en masse post-pandemic. It would be hard to find many who share that opinion now.

Remote working and the knock-on effects on data loss are here to stay – and it's a concern for IT leaders. 56% believe remote working has had a direct impact on human error incidents in the past 12 months, and 54% believe it will make preventing breaches harder in the future.

We asked IT leaders: Did remote work due to the pandemic increase data breach incidents over the last 12 months?



We asked IT leaders: Will hybrid/ full-time remote working make it harder to prevent insider data breaches in the future?

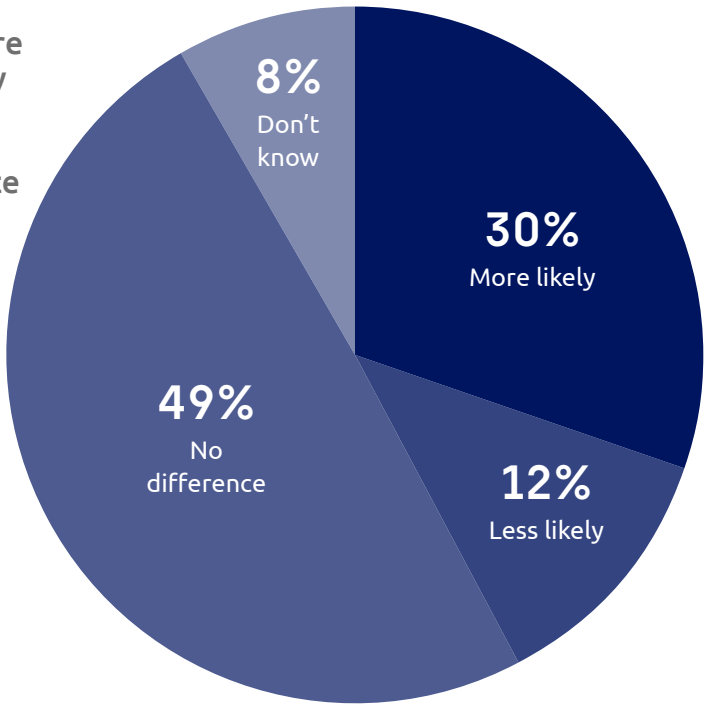


"56% of IT leaders believe human error data breaches increased due to remote working in the pandemic"

A remote work disconnect

Interestingly, remote workers themselves have a lot more confidence in their own breach-prevention skills. 61% believe they are less (or equally) likely to cause a breach at home compared to the office. Given the frequency of data breaches throughout 2020 and 2021, IT leaders might argue this confidence is misplaced. There is an interesting disconnect here, and it's one businesses will need to figure out with many employees actively pushing for the option to work remotely.

We asked employees: Are you more or less likely to cause a data breach while remote working?



> The most serious insider data breach for us would be employees sending proprietary company data into personal devices and emails. I think the employees are doing it unintentionally, trying to make their life easier in a work-from-home environment.
>
> ANONYMOUS IT LEADER, FINANCIAL SERVICES

INDUSTRY WATCH

FINANCIAL SERVICES

Our findings show IT leaders in FS have been hit particularly hard by the impacts of the pandemic and remote working. During the pandemic:

69%
think human error incidents increased (plus, 63% think it'll be harder to prevent human error incidents due to remote working in the future)

65%
think employees falling for phishing attacks increased

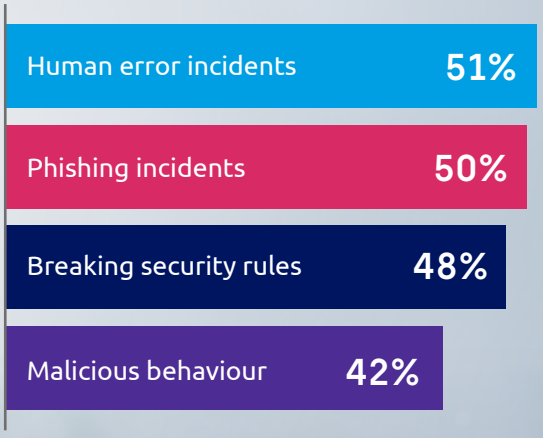
65%
think incidents of employees not following procedure increased

> **Someone emailed customer info to their home computer so they could work remotely. They wrongly assumed it wasn't a big deal.**
>
> ANONYMOUS EMPLOYEE, FINANCIAL SERVICES

More mobile devices = more breaches?

It's not surprising to see human error as the number one concern around remote working. One key factor could be the devices people are using in less-than-ideal home setups. It's much harder to spot phishing attacks on mobiles, and far easier to make 'fat-fingered' mistakes on smaller screens. With unsecured home networks and easily downloadable shadow IT in the mix too, it's a clear problem for many IT security teams.

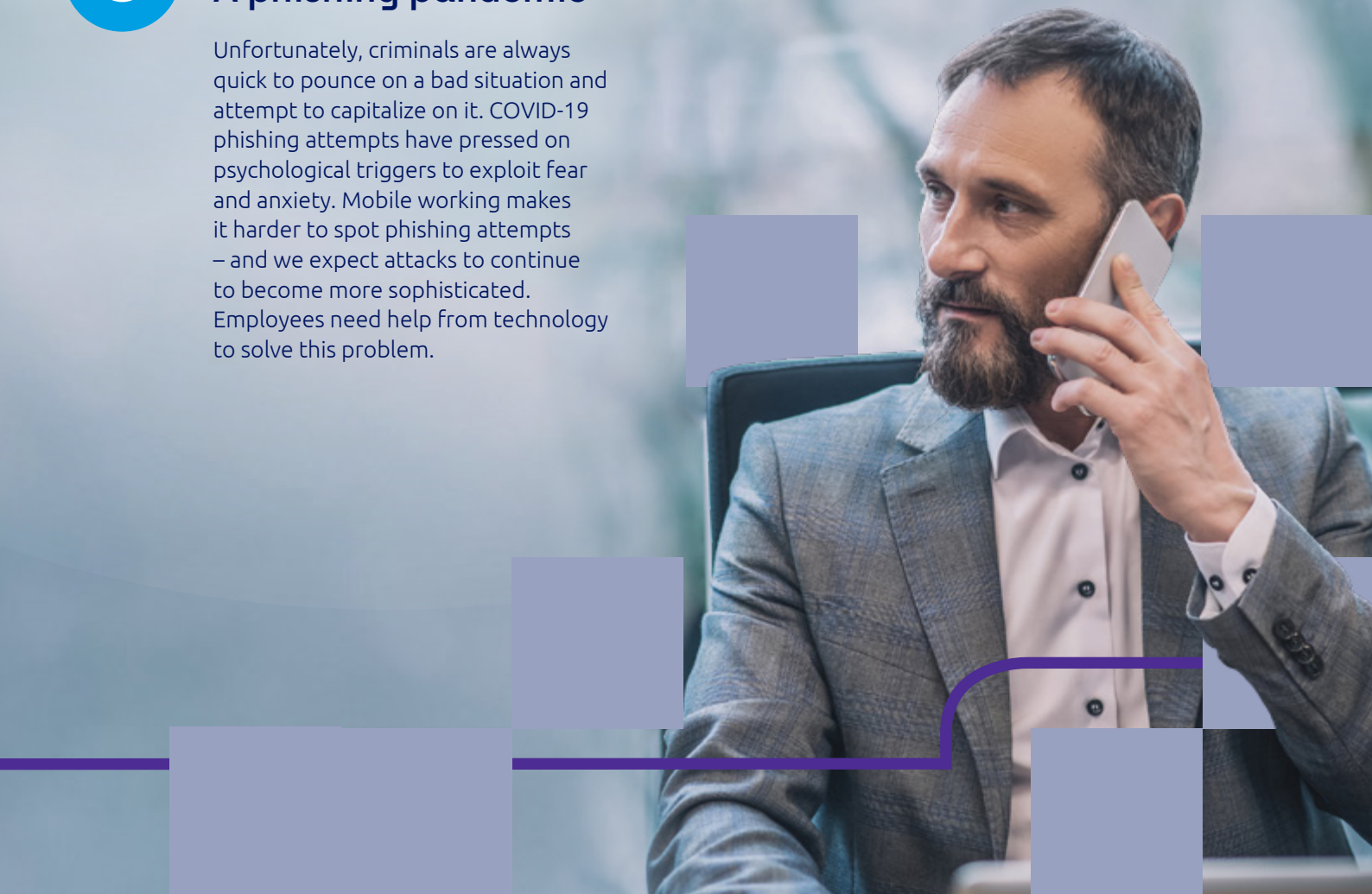
We asked IT leaders: Do you think using mobile devices (e.g. phones and tablets) makes it more difficult for you and your team to prevent the following security threats?



EGRESS ANALYSIS

A phishing pandemic

Unfortunately, criminals are always quick to pounce on a bad situation and attempt to capitalize on it. COVID-19 phishing attempts have pressed on psychological triggers to exploit fear and anxiety. Mobile working makes it harder to spot phishing attempts – and we expect attacks to continue to become more sophisticated. Employees need help from technology to solve this problem.



Solving insider risk

Are insiders security risks or your greatest defense?

Our findings have shown generally people want to do the right thing and are on board with creating an effective security culture. Most employees (72%) believe deliberately removing data from a business is wrong, and nearly every respondent (97%) said they would self-report a data breach.

However, even if employees know breaches are wrong and are willing to admit their mistakes – it doesn't stop the fact that the breaches have occurred. And by that point, the damage tends to have been done.

So, how do organizations harness the good security sense of their employees to stop breaches before they happen? The answer is to turn insiders into your security defense using intelligent technology.

Human layer security

We can mitigate insider risk by offering employees intelligent tools that truly help them. Human layer security uses machine learning to deeply understand the behavior of each individual user, meaning it can detect the context-driven incidents that lead to breaches.

Egress' human layer security platform works in the background, only intervening when people are genuinely at risk of being hacked, making a mistake, or breaking the rules. Our traffic-light based prompts are usually all an insider needs to make smart security decisions, although we can also block risky behavior and exfiltration attempts. A comprehensive analytics function then gives IT leaders full visibility into these risks and employees' behavior.

Human layer security treats people as part of the solution, not part of the problem. It doesn't only offer warnings, it teaches and raises security awareness, helping insiders to understand the warning signs of human-activated data breaches. Insider risk can be solved – organizations simply need to arm their employees with human layer security.

Find out more about **Egress Intelligent Email Security Software**

1

Egress Defend

Detect and defend against targeted phishing attacks

This email shows very strong signs of phishing

2

Egress Prevent

Stop email data breaches before they happen

You wouldn't normally include janed@gmail.com with the other recipients on this email

3

Egress Protect

Send and receive secure, encrypted email

Unprotected

Encrypt email and attachments

4

Egress Respond

Understand, monitor and report on the security of your email flows

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 surveys for this research paper were carried out independently by Arlington Research. 500 IT leaders (defined as someone who has decision-making power over IT solutions within a business) and 3,000 employees were surveyed. Respondents were equally split across the healthcare, finance, and legal industries, and split 50/50 across the US and the UK.

egress

www.egress.com | info@egress.com | 0203 987 9666 | @EgressSoftware