egress

# Egress **Data Loss Prevention** Report

Defending against daily data loss

AN EGRESS REPORT

# Inside the report

Summary ........ 03

Introduction ........ 04

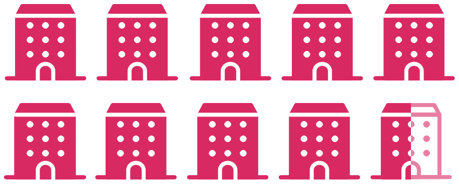
Organizations are losing data every day ........ 05

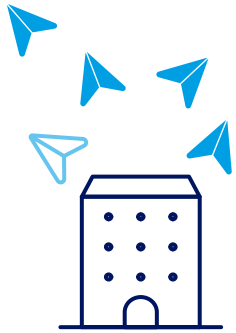
Email remains the most popular (and risky) communication channel for remote workers ........ 12

Solving the problem of email data loss ........ 17

# At a glance: survey results

**95%** of organizations say they've suffered data loss





Data is most likely to be at risk on email, with

**83%**

of organizations experiencing email data breaches

**92%**

of organizations experienced negative impacts as a result of an email data breach

**24%**

of incidents resulted from an employee sharing data in error

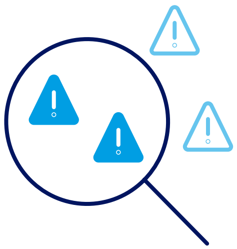
**80%**

of employees use email to share sensitive data with clients and colleagues

**79%** of IT leaders admit to experiencing difficulties using static DLP

**42%**

of IT leaders say that half of all incidents won't be detected by their static DLP tools



**85%**

of employees are sending more emails

# The daily battle against data loss

**IT leaders face an immense challenge when it comes to data loss. The fast, free-flowing exchange of information is vital for successful operations, but the sheer variety of sharing channels available to employees, and the frequency at which they use them, means the risk of data loss is pervasive.**

The challenges of recent years have only served to exacerbate the situation. If the data perimeter was perilously porous when most employees worked in offices, the pivot to remote working has added concerning new dimensions that directly affect the most problematic element of the data security stack

Our latest research, conducted by independent organization Arlington Research among 500 IT leaders and 3000 remote-working employees in the financial services, legal and healthcare sectors within the UK and the US, reveals the true scale of data loss incidents and the damage they do to organizations. We identify the channels employees prefer to use when sharing data and the reasons they give for putting it at risk.

We'll also explore the tools IT leaders have in place to prevent data loss and ask how confident they are that these tools are effective.

Together, these findings reveal an under-pressure workforce that is contributing to higher risk of data loss through the channels they rely on when working remotely. At the same time, the traditional tools deployed to combat data loss are failing to match the risk residing in the remote-working environment.

> The fast, free-flowing exchange of information is vital for successful operations but the risk of data loss is pervasive

# Organizations are losing data every day: the where, how, what and frequency of data breach risk

## How often is data put at risk?

Data risk incidents are ubiquitous in today's organizations. Despite all the technology and training that has been devoted to the problem, data loss is a daily occurrence.

A sobering 95% of the IT decision makers surveyed said that sensitive data had been put at risk in their organization through one or more of the channels used by employees to share information.

These were not isolated events. In fact, on average, each respondent identified an average total of 927 incidents across all channels per year in their organization. That equates to around 3.5 instances of potential data loss every working day in an average working year of 254.  It's a deluge of data loss that threatens to become an unchecked tide of breach risk.

On average, organizations experience 3.5 data loss incidents every working day

## Where does the most risk lie?

Data risk is high across all channels, but some are worse than others. Email led to the most incidents across the highest number of organizations (83%).

### From low risk to high risk: how many organizations are affected?

The risk was lowest from physical data sharing, which is unsurprising in a remote-first world. 72% of organizations were experiencing data risk incidents from removable media such as USBs, CDs and DVDs. Slightly more of a problem was the issue of physical copies of data, such as printouts, going astray. This was reported in 76% of organizations.

It is the pureplay digital channels that are generating most risk, and email comes out in front.

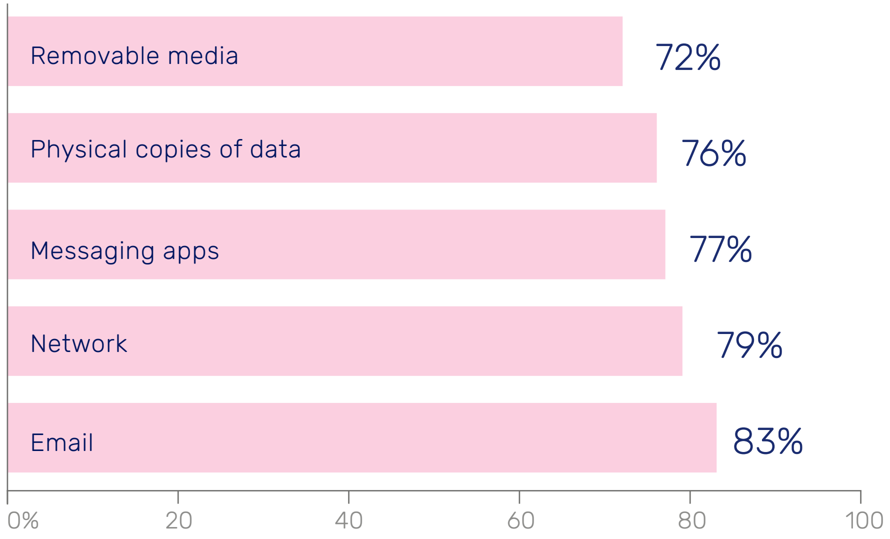
Unsurprisingly, given their rapid adoption over recent years, message apps including Teams and SMS were a source of incidents for 77%, while 79% reported data loss incidents arising from the network, such as malware initiated by third parties.

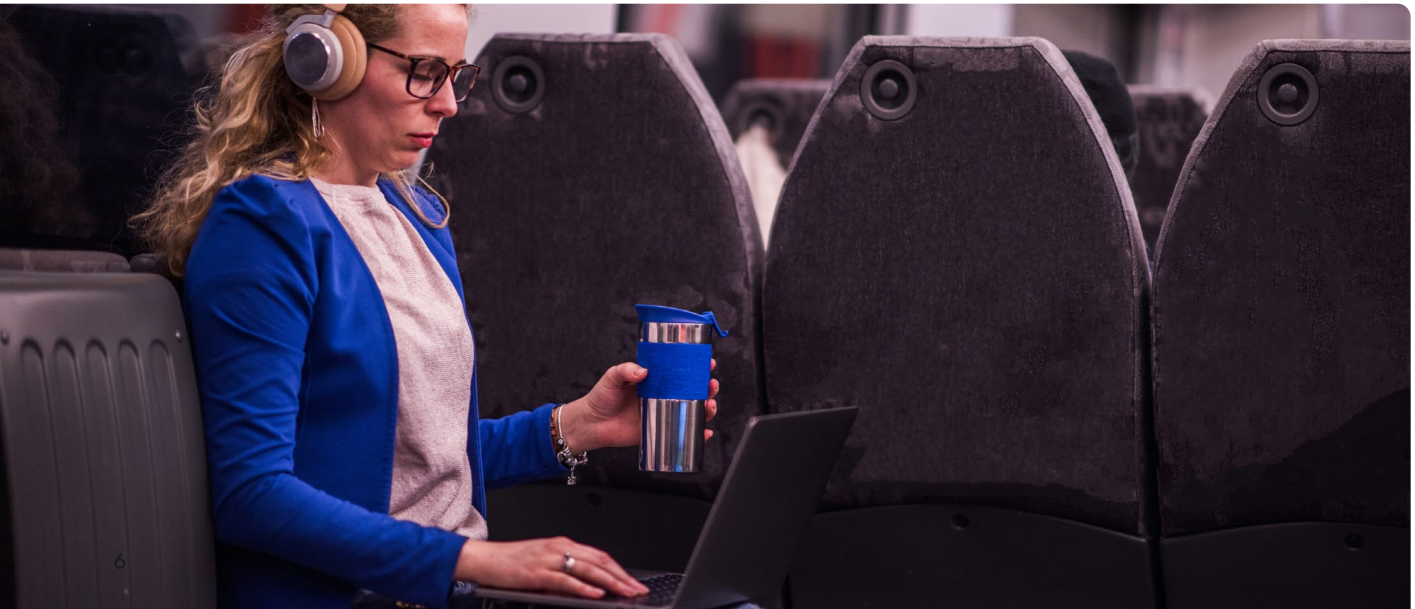
By far the most common vector for data risk resides in email systems. 83% of IT leaders said that sensitive data had been put at risk via email. In the legal sector the problem is particularly endemic, with 90% of respondents saying data was exposed in this way.

So what does that mean in real terms? The data reveals that an organization with between 100 and 249 employees experienced an average of 178 incidents that put data at risk via email within a 12 month time period. That equates to approximately one incident per user, per year.

As we will discover, the rate at which email use is rising and its importance in the employee communications hierarchy means that high risk in this channel should be a significant red flag for IT leaders.

**IT leaders reveal how data has been put at risk in their organizations within a 12 month time period**





## How do data loss incidents occur via email?

When we look at how email data breach incidents came about, the combination of factors in play paints a graphic picture of the complexity of email data loss risk.

Almost one-quarter (24%) of incidents resulted from an employee sharing data in error, perhaps through a misdirected email or by clicking on the wrong file when choosing an attachment. And the larger your organization, the more your employees make mistakes. Data shared in error is the cause of more than one-third of incidents among enterprises with 1000-4,999 employees and a concerning 47% of incidents in those with more than 10,000 people on the payroll.

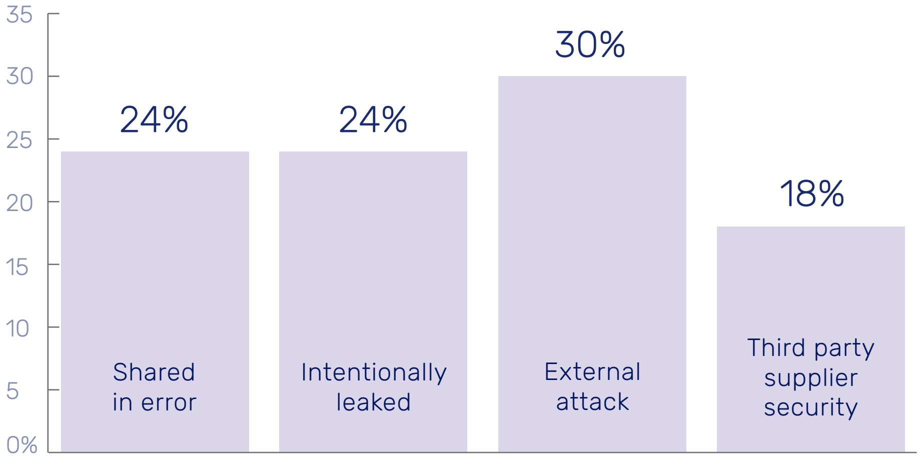
Almost one-in-three (30%) incidents were the result of external attacks such as phishing and malware campaigns that prey on recipient vulnerability to gain access to data and networks.

It is clear that inadvertent employee mistakes are contributing significantly to breach risk.

### Employee loyalty is under strain

Intentional leaks accounted for a further 24% as employees deliberately choose to share data in a way that is not secure – whether that's with the best intentions of getting the job done, or with less honest motives such as removing data to take to a new job.

**IT leaders reveal the cause of email data loss in their organization within a 12 month time period**



Certainly, in the current climate of economic downturn, job security is under threat for large sections of the workforce and loyalty levels may be dropping, potentially making employees more likely to appropriate data for their own career objectives.

### Supply chain vulnerabilities are leading to breaches

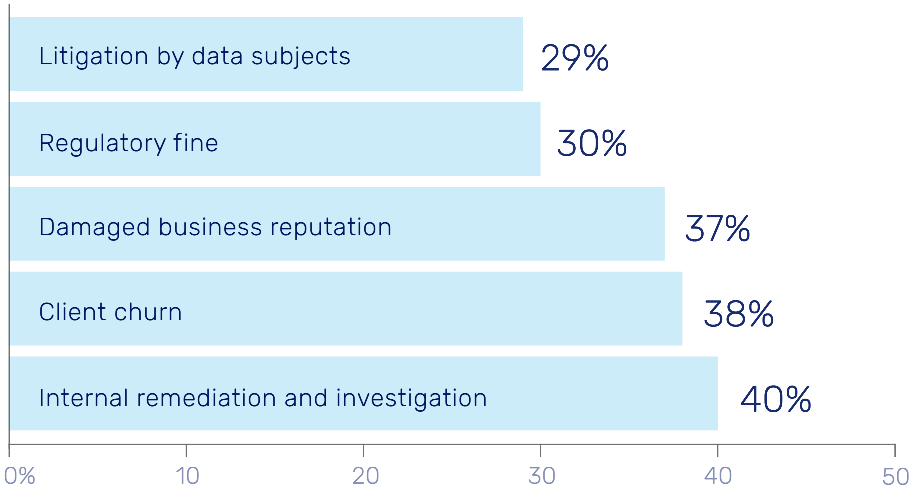
Adding an unwelcome dimension to the email risk and regulatory compliance environment is the fact that almost one-fifth (18%) of email-activated data breaches arose from weaknesses in third party supplier security. This is highly concerning due to increasingly robust data protection and privacy regulations that mean organizations, as data controllers, are in an exposed position of legal liability for breaches that occur via third party suppliers who act as data processors.

## What types of data are most at risk via email?

The picture doesn't get any rosier when we look at the types of data that are most often exposed to unauthorized access. 95% of IT leaders say that both client and company data is at risk on email.

Organizations believe they are doing slightly better at protecting their clients' data than they are at protecting their own, with two-in-five (41%) IT leaders saying their own company's sensitive data is the most at risk, while only 23% think client data is more exposed. However, with 31% of respondents saying both types of data are equally at risk there is scant room for confidence in either client confidentiality or corporate data protection.

**IT leaders highlight the impacts of data loss via email for their organization within a 12 month time period**



## Time, money, reputation: what are the impacts of email data loss?

Organizations are paying a considerable price for email data leaks. 92% have suffered negative outcomes following a material incident.

The first and most obvious hits are the immediate costs of breach identification and remediation. This takes time and resources, with insight from Egress client consultations indicating that each email breach incident takes approximately 60 hours to resolve.

A breach of data is undoubtedly also a breach of client trust and the predictable result is customer churn. The legal sector is particularly exposed to client churn, with more than 40% identifying this as an impact of email data losses. Given that this sector is also the most likely to experience these incidents in the first place, the compound effect on corporate revenues is likely to be significant.

It's understandable that clients are starting to ask more searching questions of suppliers when it comes to security provision. Something needs to be done about those 18% of data loss incidents originating through the supply chain and, for the clients of more than half of our IT Leader respondents, email DLP software appears to be the answer. 56% of respondents have experienced an increase in clients asking whether DLP software is in place. This rises to 62% in the legal sector and 68% in the financial services sector.

Related to direct client churn is the general impact on business reputation when a company suffers a breach. These are the potential customers you'll never convert because they don't believe you can be trusted with their data. 37% of IT leaders say their organization has experienced reputational damage following a breach and the figures are higher still in Financial Services, at 47%. This is not surprising; if a customer cannot trust you with their data, why should they trust you with their money?

Litigation is also a growing risk. As individuals realize the true value of their personal data, they appreciate the damage caused when it is compromised and are increasingly disposed to take legal action. Currently more prevalent in the UK, where 31% of IT leaders say their organization has been subjected to litigation from breach victims, anecdotal evidence indicates that this is a rising trend.

Law firm Pinsent Masons notes that "litigation risk significantly heightens in correlation with the severity of the security breach. Controllers can be almost certain of litigation where there has been regulatory enforcement in respect of the incident." For the 30% of respondents who have faced regulatory action following a data breach, this should be a concern.

95% of IT leaders say that both client and company data is at risk on email

EGRESS ANALYSIS

## Brand damage and litigation risk lingers after data losses

The natural result of stricter data protection regulations is more rigorous pursuit of those who violate them. Apart from the penalties handed down by regulators – which in themselves are punitive – there is also the growing threat of class action lawsuits.

Anyone with a social media account in the UK will have seen organizations advertising to victims of mega-breaches such as the British Airways incident to recruit them to mass legal action. Each time one of their adverts is served, BA's reputation as a trusted carrier is tarnished a little further, quite apart from the compensation costs it could face should these suits succeed.

The rising trend for litigation is being noted among law firms. Research from the Cyber Team at Pinsent Masons found that "in cases where data subjects are notified about a data security breach, 20% have resulted in actual or threatened claims from data subjects."

## IT leaders with Microsoft 365 environments are more concerned about data loss

With more than 200 million active monthly users, Microsoft 365 is the go-to productivity platform powering organizations. There's no denying that it is intuitive and flexible – popular with users and IT teams alike – but its native email security tools are not a cure-all for data breach prevention.

96% of IT leaders running Microsoft 365 within their organization were worried about client and corporate data being put at risk on email. Our research also showed 85% have experienced data loss incidents related to email, with 26% caused by misdirected emails and 24% by intentional exfiltration.

72% of IT leaders at organizations using Microsoft 365 think employees are more likely to leak data by email when they are using a mobile device. The same percentage also believe flexible and remote working will lead to data losses in the future, and 64% have experienced data loss via email since the start of the pandemic, compared with 28% in organizations that don't use Microsoft 365.

These incidents are also causing problems for IT leaders, with 93% reporting negative impacts from email data breaches, including client churn, regulatory action, litigation and application of internal resources for remediation.

## The limitations of Microsoft 365's email DLP

The integrated email DLP security in Microsoft 365 is built using static rules, and consequently cannot identify the incidents that arise from employee behavior. The majority of mistakes are made when they are stressed or tired, such as an erroneous address auto-complete, the wrong file being attached, or replying to a spear phishing email. And, while static rules can enforce encryption and send permissions on a policy basis, they cannot easily cope with the nuances that mean a user is permitted to email financial data to one employee at an external organization but not another, whose address they may have selected in error. Achieving this requires the maintenance of complex sets of rules for each individual and quickly becomes a significant overhead.

This was reflected in the frustrations of IT leaders, with 43% saying they require high levels of administrative overhead to maintain and 38% say they have had to alter rules to make them more workable for staff.

Despite this, organizations using Microsoft 365 need to find a way to improve DLP because it is becoming a common client concern. 56% have seen an increase in requests from clients about whether they have email DLP in place in the last 12 months.

# Email remains the most popular (and risky) communication channel for remote workers

85% of employees say they are using email more than ever before, largely thanks to an increased amount of time spent working remotely. Almost two-thirds have increased their email frequency with colleagues, while 36% are sending more emails externally to clients.

Among respondents in the legal sector, this trend was even more marked, with 91% relying on email more overall and 50% using this channel more with clients.

Why, with so many alternative methods available, does email retain its position as the communication channel of choice?

Put simply, workers feel more productive when they use email. It allows for the formulation of measured and detailed responses to client and colleague queries and requires less thinking on your feet than instant channels. It is free of the visual and audio cues that need to be managed during video and/or phone calls. And, crucially, it allows users to share data linked to the topic of discussion and provides a ready-made audit trail.

How many times does a phone or video call conclude with the words "I'll send you an email about it"?

Email is undoubtedly the central pillar of business communication and it is supplemented, not supplanted, by alternative channels.

> Email is undoubtedly the central pillar of business communication and it is supplemented, not supplanted, by alternative channels

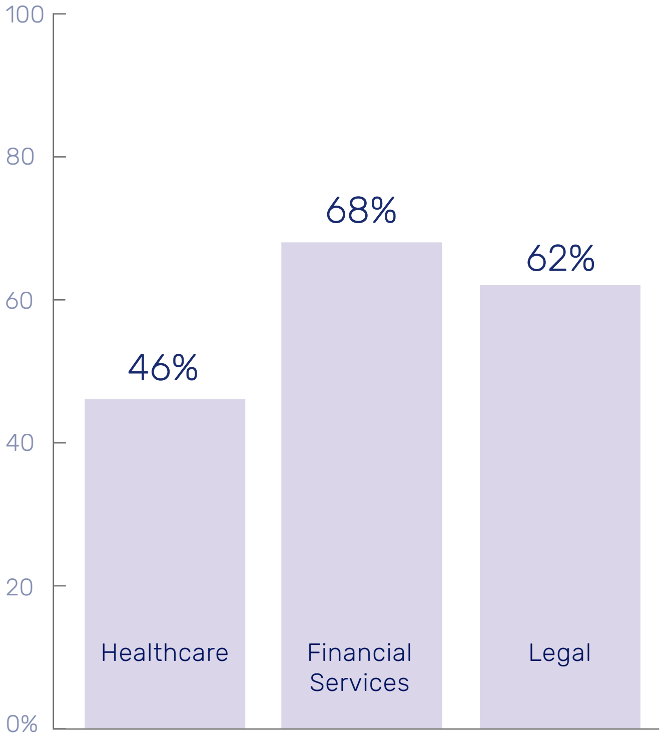
For sharing sensitive data, employees view email as more appropriate than the alternatives. 80% of respondents use email to share sensitive data with clients and colleagues, while fewer than half (45%) would trust confidential information to less formal channels such as WhatsApp.

Respondents from the legal sector are even more committed to email as a sensitive data-sharing platform, with 88% saying this is the channel they use.

### Data leakage via email is on the rise

The more emails employees send and the greater the stress they are under, the more the risk of errors rises. So it's not surprising that 59% of IT leaders have noted an increase in data leakage via email since large sections of their workforce began working remotely.

**IT leaders reveal an increase in data loss via email since remote working became widespread across different industries**



46% of employees say they feel most productive when using email

## The psychology of email errors

Email is not a difficult tool to use. In fact, it has been engineered to be easy to use, with most email clients now suggesting recipients through autocomplete and some even predicting the next sentence to be written. Email is familiar, functional and, as this research has shown, people feel productive when they are using it. How hard can it be to make sure the right message with the right file attachment gets to the right person?

In theory, not hard at all. Reality, however, is very different.

Individual employees are rarely totally alert and focused 100% of the time, and certainly no organization would realistically anticipate their entire workforce to act like this en masse. Plus, right now, circumstances are far from ideal; employees are feeling even more tired, stressed and under pressure than usual. This is when skills-based errors creep in for even the most well-meaning and conscientious worker.

Rushing to send a time-sensitive email before the kids need help logging on to remote lessons, it is more likely that the sender won't notice that they've added the wrong recipient to the address field or attached the wrong file. And they may not even realize they've made a mistake, especially if they've immediately switched to a completely unrelated activity. The error will often only come to light if the unwitting recipient queries why they've received the mail, or if no response is received from the intended recipient.

Email errors also often arise from the way we view the different elements of the process of writing and sending an email.

We see the tone, structure and content of the message itself as the primary activity; the part requiring time, focus and brain power. When it comes to the "easy part" of selecting recipients and file attachments, our concentration wanes – perhaps we start thinking about the next task on our busy to-do lists – and we don't spot that autocomplete has suggested the wrong recipient, or that we've picked the wrong attachment from the "recent files" list. With a click of the send button, our painstakingly crafted email is winging its way to the wrong person and the data within it has been exposed.

## Blurred work-life and technology boundaries raise data loss risk

It is not just the physical location that has changed for office workers, their technological and temporal environment has changed too. Many are now working on mobile devices and at unusual hours as they fit their work commitments around family duties. This is ringing alarm bells for IT leaders, among whom over two-thirds (67%) believe that data loss via email is more likely to happen when employees use mobile technology.

They are right to be concerned.

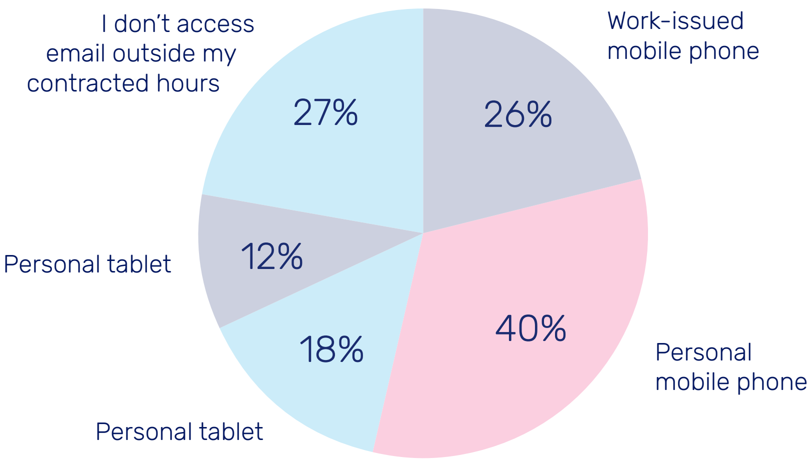
73% of the employees we surveyed access work emails outside their contracted working hours and 45% do so on personal devices rather than work-issued hardware. Just under two-thirds (66%) use either a personal or work-issued mobile phone to check work emails out of hours.

Employees in the legal sector are the most likely to be burning the midnight oil, with 93% saying they open their inbox at unorthodox times.

The risks here are both technological and circumstantial.

First, accessing emails on mobile devices, especially small smartphones, increases the chances of so-called "fat finger error".

**Employees reveal the devices they use to access email outside of contracted working hours**



When navigating on tiny touchscreens, it is easier to select the wrong recipient or file and harder to spot the mistake once it has been made. Spear-phishing attacks are also more difficult to identify, as mobile email clients default to display names only and the opportunity to spot an erroneous address is lost.

Second, employees accessing emails out of hours are less likely to be fully focused on what they are doing and more likely to be tired. In fact, our research found that employees who access emails out of hours are almost 2.5 times more likely to say that they feel tired as a result of remote working. One-quarter (24%) said that they are normally doing something else at the same time they are replying to emails.

### The always-on culture remains rife

Overall, just under half (46%) of employees feel pressured to send and reply to emails outside of working hours.

Perhaps unsurprisingly, it is employees who have been issued with a mobile phone by their employer who feel under most pressure to be available after hours, with almost three-in-four (74%) saying they feel obliged to respond to emails.

When sending email replies, the out-of-hours scenario affects how employees respond. A conscientious 39% try to respond as quickly as possible, but almost one-quarter (24%) are normally doing something else at the same time and not concentrating fully on the task at hand.

Emails encroaching on personal time makes 17% feel stressed by the effect on their work-life balance.

All these factors are common ingredients in the recipe for a human-activated email data breach.

> 56% of IT leaders have had clients ask if email DLP tools are in place at their organization

### Rising risk awareness in a remote-first future

It seems clear that more flexibility over employees' primary location will be a key feature of the future workforce. Companies will aim to become more resilient towards future disruption and right-size their office estate to accommodate a smaller in-house workforce, realizing the associated cost savings.

For IT leaders, this requires a close look at security risk around remote workers, and the signs are concerning. 68% believe that a remote and flexible workforce makes it harder to prevent email data breaches. This rises to 72% in organizations using Microsoft 365, indicating that its native security tools are not capable of mitigating against breaches that originate in human behavior.

There is no doubt that something needs to be done. As organizations become more aware of their responsibilities for data protection and liability for data losses caused by suppliers, they are asking questions about the security tools those suppliers have in place. Our survey data shows 56% of IT leaders have had clients ask if email DLP tools are in place at their organization. Among those that have noted an increase in email data leakage due to remote working, this figure jumps to 76% - perhaps a sign that a reputation for poor data protection is starting to influence decisions among their client bases.

# Solving the problem of email data loss

Inaction is not an option for IT leaders faced with the constant threat of data loss and its consequences, but finding a workable and reliable solution to the challenge of human-activated email data breaches has not proved easy.

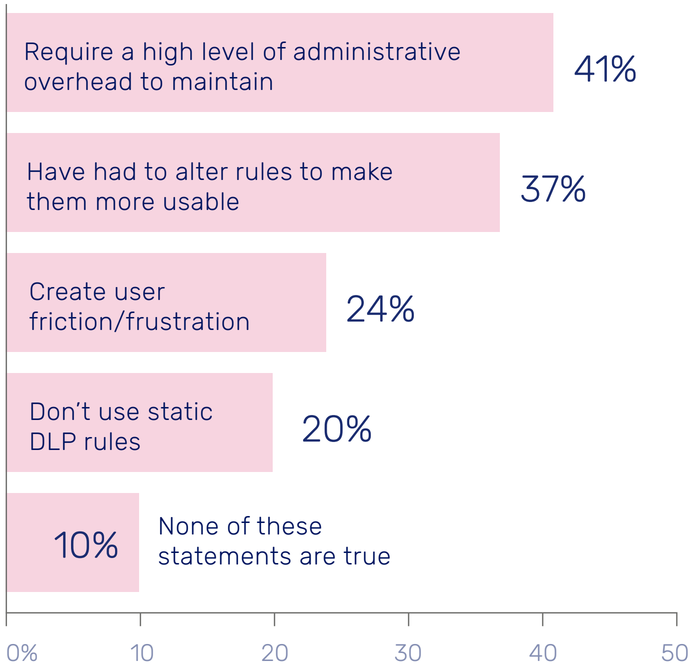
Traditional approaches to preventing data loss via email have centered on the implementation of rules-based static DLP tools and reliance on the native security tools in email clients such as Microsoft 365.

Static DLP rules are designed and administered by security teams, and theoretically can be configured to stop sensitive data from being emailed to unauthorized recipients. The content of messages and files is scanned according to the rules in place and, if an email violates the selected criteria, action is taken. The email may be blocked or quarantined, the sender may be asked to modify its contents or verify the recipients, or encryption might be mandated.

However, static rules and native security tools are not capable of detecting context-driven incidents such as an employee selecting the wrong recipient, attaching the wrong file, or the failure to use Bcc.

79% of IT leader respondents have deployed static email DLP rules in a bid to mitigate risk, but they are by no means a cure-all for breach prevention and 79% have experienced difficulties resulting from their use.

**IT leaders acknowledge the difficulties they have using static email DLP**



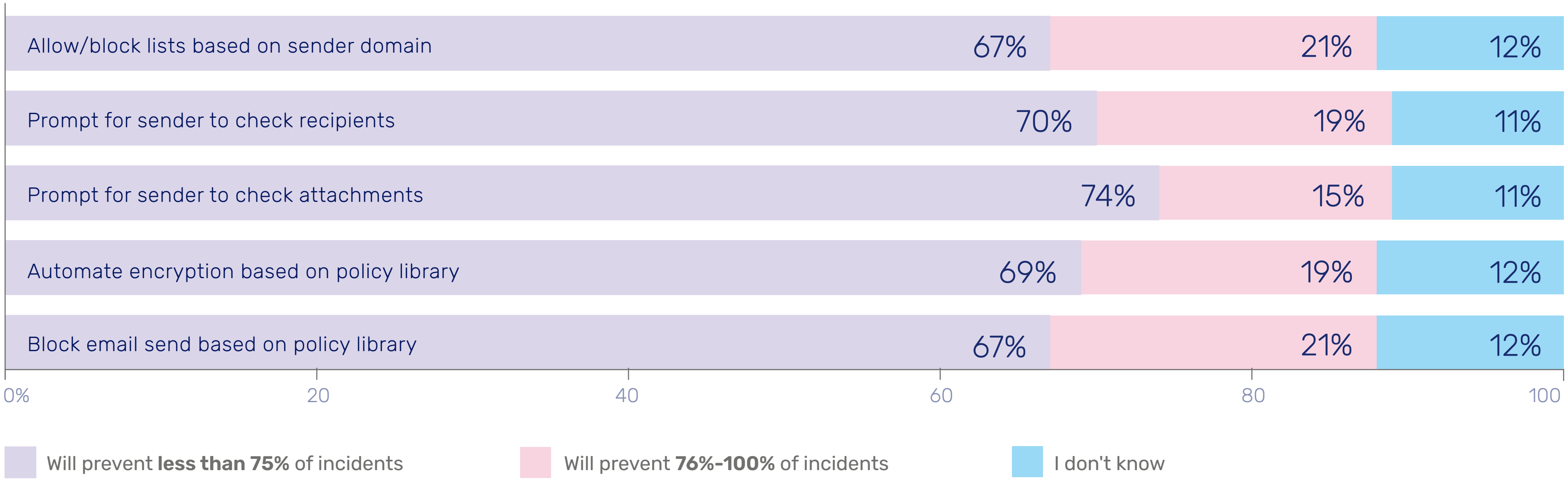
The main complaint from IT leaders is the high level of administrative overhead associated with maintaining static DLP rules to ensure that they are adapted to manage emerging risks. 37% of respondents said they had to alter rules to make them more usable, putting productivity ahead of security in a bid to up employee efficiency. Keeping users happy is also a consideration, with almost one-quarter of IT leaders saying that DLP rules create user frustration. This impacts productivity and reduces the usefulness of email as a communications tool which, given its central role in corporate communications, is a significant negative.

Although the majority have chosen to deploy static email DLP rules, there is low confidence in the extent to which they will effectively prevent breaches.

Analysis of key features of static DLP tools shows that only around one-in-five IT leaders believes the tools in place will prevent between 76-100% of incidents.

That leaves up to three-quarters (74%) of respondents who believe the static email DLP tools they use are less than 75% effective.

**IT leaders rate the effectiveness of their static email DLP tools to prevent data breaches**



These remaining IT Leaders accept that a minimum of 25% of data loss incidents will be undetected, and an alarming average of 42% overall say that half of all incidents won't be detected by the DLP tools they have in place.

This general lack of confidence indicates that IT leaders are well aware of the limitations of legacy static DLP technology. It is not equipped with the intelligence required to detect and prevent the incidents where the root cause lies in human behavior.

Where security and DLP are user led rather than automated by set rules, we still run into problems because they rely on people to make decisions. You can either take a sledgehammer approach of prompting on everything, which for the vast majority of employees will lead to click fatigue; or you can trust people will always make the right choice when it comes to adding recipients, attaching files and applying security. However, while training can help employees be more aware of the ways they can protect data, prevent breaches and avoid phishing attempts, humans are not and will never be infallible, especially when they are experiencing external distractions and pressures.

An alarming average of 42% say that half of all incidents won't be detected by their static DLP

Consequently, IT leaders need a more intelligent approach to email security and DLP or they will face a continuously rising tide of email data loss.

Intelligent DLP uses contextual machine learning and bases its activity on comprehensive analysis of a user's behavior patterns and relationships with senders and recipients. Armed with constantly updated analytics, intelligent DLP detects the abnormal behaviors that lead to security breaches, including instances such as selecting the wrong email address via autocomplete, or when an attachment containing sensitive financial data is being directed to a recipient that would not usually receive such information. When a genuine risk is detected, the user is alerted so they can correct their mistake before they hit "Send".

Similarly, intelligent DLP can automatically apply the appropriate level of encryption based on email and attachment content and the risk associated with the recipient's domain, eliminating the need for users to make decisions on encryption and taking the responsibility entirely out of their hands.

Together, this intelligent approach to preventing unintentional errors and automating email protection lift the burden of security responsibility from the shoulders of employees and put organizations in control of the data they share.

## Data sharing doesn't have to result in data loss

Email remains the trusted and universal productivity aid that it has always been, but with it come the data protection risks that have always existed.

If businesses don't act now to contain email data loss, we will see a rising tide of incidents putting reputations and revenues at risk.

Where, how and when employees work has undergone permanent change, and security professionals need to adapt their defenses and protective measures to fit the new environment.

Legacy DLP solutions are not working and more must be done to support employees and automate data loss prevention and information protection. It is time for the power of contextual machine learning to be applied to the problem, to restore confidence for employees, employers and clients that data sharing doesn't have to result in data loss.

# The combined value of Microsoft and Egress

Together, Microsoft's cloud-native email security capabilities and Egress' advanced email protection capabilities help organizations optimize their email protection investments and reduce human activated risk by:

- Reducing unnecessary email infrastructure cost and complexity by avoiding duplication of functionality between cloud-native capabilities and secure email gateways (SEGs)
- Complementing cloud-native security features with modern techniques like AI and natural language processing to stay a step ahead of sophisticated threat actors
- Bringing the once disparate activities of inbound and outbound email protection together into a unified model
- Turning users into allies by educating and guiding them in non-intrusive and mutually beneficial ways

Book a demo

### Egress Defend

**Detect and defend against advanced phishing attacks**

Learn more

### Egress Prevent

**Prevent human error and data exfiltration**

Learn more

### Egress Protect

**Send and receive encrypted email**

Learn more

**Inbound** threat protection

**Outbound** threat protection

## 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.

**www.egress.com** | EgressSoftware

© Egress Software Technologies Inc 2023. 1616-0123

## Methodology

Data for this report came from a survey conducted by independent organization Arlington Research. Respondents were 500 IT leaders and 3,000 remote-working employees in the financial services, legal and healthcare sectors within the UK and the US. IT leaders were defined as people with decision-making roles for choosing IT solutions within an organization. Researched was conducted in 2021.

egress