Egress Data Loss Prevention Report 2021

Defending against **daily data loss**

egress

Inside the report

Summary 3

Introduction 4

Organizations are losing data every day 6

The risk of data loss is rising in 2021 14

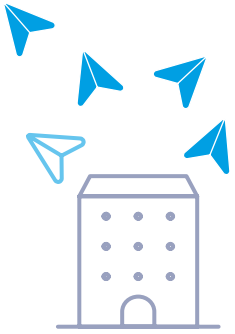
Solving the problem of email data loss 25

At a glance

What's happening?

Go to chapter ▶

95% of organizations say they've **suffered data loss** in the last year



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

83%

of organizations experiencing **email data breaches**

Why is the risk higher in 2021?

Go to chapter ▶

73% of employees **feel worse** because of the pandemic

85% of employees are **sending more emails**

59%

of IT leaders report an **increase in email data loss** linked to the pandemic

The role of technology

Go to chapter ▶

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

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 the past year 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 – the human layer.

Employees who are working from home against the background of the pandemic are subject to more distractions. They are under increased stress and many are more tired than they were before. All these factors increase the likelihood of errors that lead to data loss.

At the same time, the extreme disruption caused by the crisis has provided a wealth of opportunities for cybercriminals to capitalize by ramping up attacks targeting the communications channels that have become even more critical to business continuity. Phishing and ransomware campaigns are in the ascendancy.

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

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 also check in on the health of the human security layer, examining the psychological and practical effects that prolonged home working is having on the workforce, how this affects the potential for data loss and what organizations need to do to help under-pressure employees.

Finally, we 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.

"An under-pressure workforce that is contributing to higher risk of data loss through the channels they rely on when working remotely"

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

Chapter key stats:

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

92%
of organizations **experienced negative impacts** as a result of an email data breach

83%
of organizations experienced an email data breach in **the last 12 months**

24%
of incidents resulted from an **employee sharing data in error**

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 in the past 12 months 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.

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 the past year, 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.

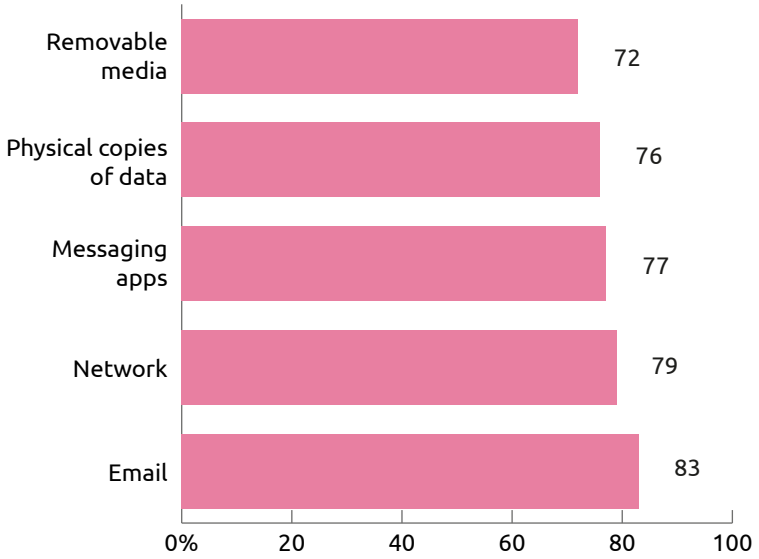
"On average, organizations experience 3.5 data loss incidents every working day"

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 past 12 months. 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 per year. 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 over the last 12 months



How do data loss incidents occur via email?

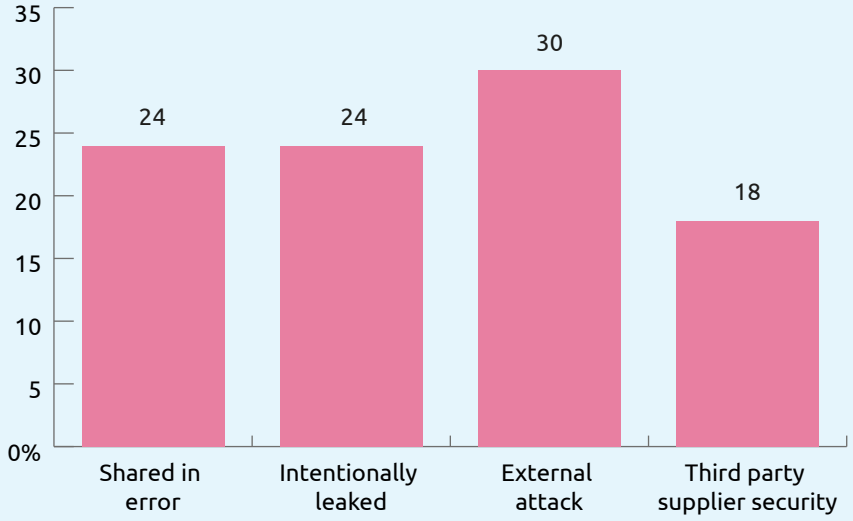
When we look at how email data breach incidents came about, the combination of factors in play paints a graphic picture of the complexity of email data loss risk.

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. COVID-19 disruption has prompted a huge escalation in phishing and ransomware, as cybercriminals take advantage of distracted employees working in less-than-ideal environments.

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

IT leaders reveal the cause of email data loss in their organization over the last 12 months



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. Certainly, in the current climate of economic downturn, job security is under threat for large sections of the workforce and loyalty levels are dropping, 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.

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

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.

Time, money, reputation: what are the impacts of email-activated 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.

"92% of organizations report negative impacts following email data loss"

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."

Read the research

"If a customer cannot trust you with their data, why should they trust you with their money?"

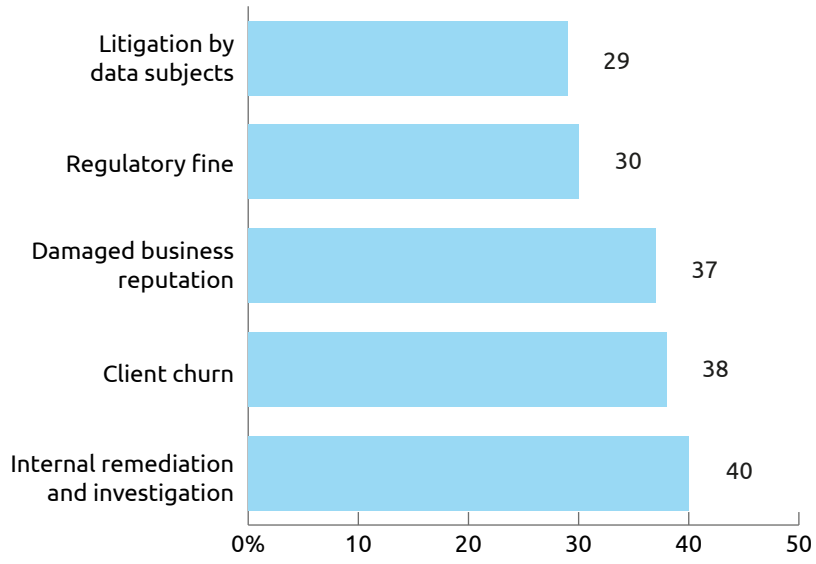
It's understandable that clients are starting to ask more searching questions of suppliers when it comes to security provision. Something needs to be done about those 18% of data loss incidents originating through the supply chain and, for the clients of more than half of our IT Leader respondents, email 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.

IT leaders highlight the impacts of data loss via email for their organization over the last 12 months



"Each email breach incident takes approximately 60 hours to resolve"

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. In fact, they can't mitigate the most common causes of data loss via email.

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% had experienced data loss incidents related to email within the last 12 months, 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. 61% have seen an increase in requests from clients about whether they have email DLP in place in the last 12 months.

The risk of data loss is rising in 2021: pandemic pressures take their toll on the work-from-home-force

Chapter key stats:

85%
of employees are sending more emails **than before the pandemic**

80%
of employees use email to **share sensitive data** with clients and colleagues

73%
of employees are **feeling worse as a result of the pandemic**, making mistakes more likely

60%
of employees are working in environments where **distractions and interruptions** are commonplace

The entire corporate psyche took a major hit in 2020. Transplanted from offices to kitchen tables, board rooms to bedrooms, the workforce became a work-from-home-force overnight. In-person conversations became videocalls and digital channels took the strain as employees strove to keep the wheels of work turning.

As lockdown weeks became months, the initial adrenalin wore off and the implications of long-term homeworking became starkly clear. Unsuitable and uncomfortable working locations, the distractions of caring for and educating children, and the grinding uncertainty around job security and when, or even if, restrictions might be lifted has taken a heavy toll on the morale of the world's home workers.

For a long time, we've known that stressed, tired and unhappy employees make mistakes and raise the risk of data loss, but never has such a uniform effect been exerted on the entire corporate body. Its effects on security and data protection should not be underestimated.

Our research has examined what the office exodus has done to the way employees communicate. What channels do workers prefer using? Which do they dislike, and which do they actively avoid? We also sought to understand what kind of home working set-up they have now, almost a year after the first wave of lockdowns began. Are they still crouched over coffee tables in communal living areas?

And what effect has this had on data breach risk? Has the abrupt change in working habits resulted in more data loss?

Ultimately, how has the pandemic affected people and security?

"85% of employees say they are using email more since they began working from home"

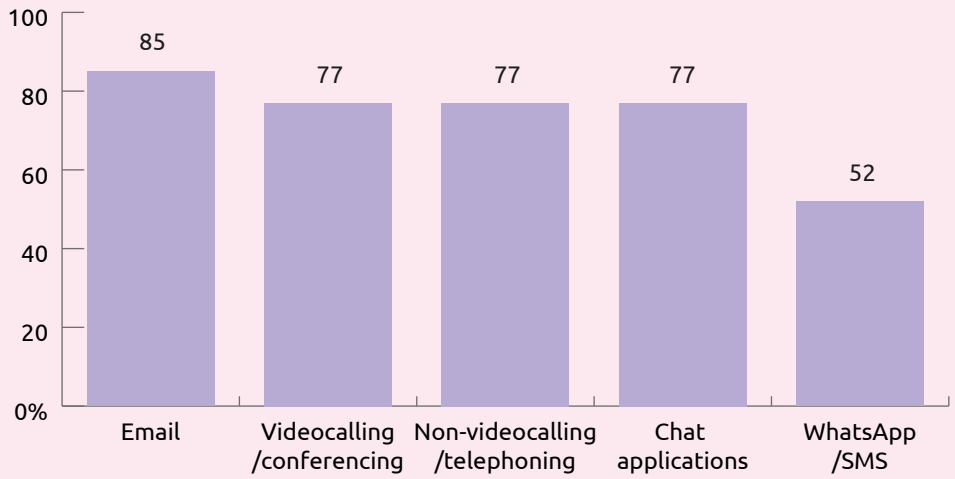
It's good to talk: digital communication surges during COVID-19, particularly over email

Denied the luxury and convenience of meeting in person, employees have naturally turned to digital channels to keep the wheels of work turning. 91% of employees say that they are communicating more frequently through a variety of different channels since they started working remotely. Email has proven the most popular, with 85% of employees reporting they are sending more emails than before the pandemic.

Just over three-quarters of employees say they are using video-calling and chat applications more, and the same number have turned more to conventional phone calls to keep in touch. WhatsApp has seen an upswing in use by 52%.

It appears that, while video-calling and chat applications such as Teams and Zoom have finally come of age during the pandemic, when employees want to be productive, they turn to the technology they are most familiar with: email.

Employees reveal which channels they're using more as a way to communicate while working remotely



We're not ready for our close-up

While the rise in the use of videoconferencing tools for both work and social purposes has been one of the technology themes of the pandemic, our research finds that not everyone is a fan. 29% of employees said they actively use videoconferencing technology but dislike it, and 24% avoid using it altogether. Nor is the workforce convinced about the merits of WhatsApp/SMS, with 39% avoiding it for work purposes.

"When employees want to be productive, they turn to the technology they are most familiar with: email"

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

85% of employees say they are using email more since they began working from home. 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.

Email reigns as the comms channel of choice during COVID-19

Email use has rocketed since the start of the pandemic. Among the 538 IT security professionals who took part in the Egress 2020 Outbound Security Report, 94% said they had witnessed a rise in the volume of outbound email and half of them had seen volumes surge by more than 50%.

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

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.

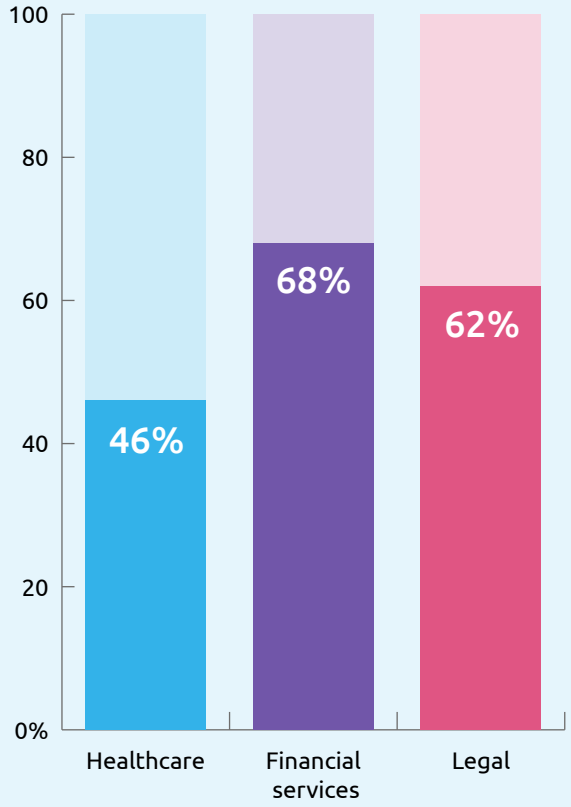
For sharing sensitive data, employees view email as more appropriate than the alternatives. 80% of respondents use email to share sensitive data with clients and colleagues, while fewer than half (45%) would trust confidential information to less formal channels such as WhatsApp.

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 the start of the pandemic.

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



Lockdown's impact on mental health: how is the remote workforce faring?

For a high proportion of the workforce, the certainties of office life – dedicated workspace, predictable hours, reliable IT systems and a focus on work shared with colleagues – have been replaced by the uncertainties of home-working. The fortunate few have dedicated home offices, but most are sharing their workspace with partners and children or housemates as they juggle competing domestic and corporate responsibilities with zero boundaries between work and home life.

Working hours have been extended as commute time has been added to the office day, with little if any screen downtime. Workforce behavior is now very different to what it was a year ago.

While employees struggle to adapt to these changes, businesses are under pressure to perform. Many are pivoting to new approaches, trying to mitigate revenue losses, trimming budgets and restructuring the workforce. As a result, many home workers are being asked to tackle very different tasks and projects to those they would usually undertake. Amid the uncertainty of health concerns, family stresses and job insecurity, the emotional and psychological state of a large section of the workforce is suboptimal.

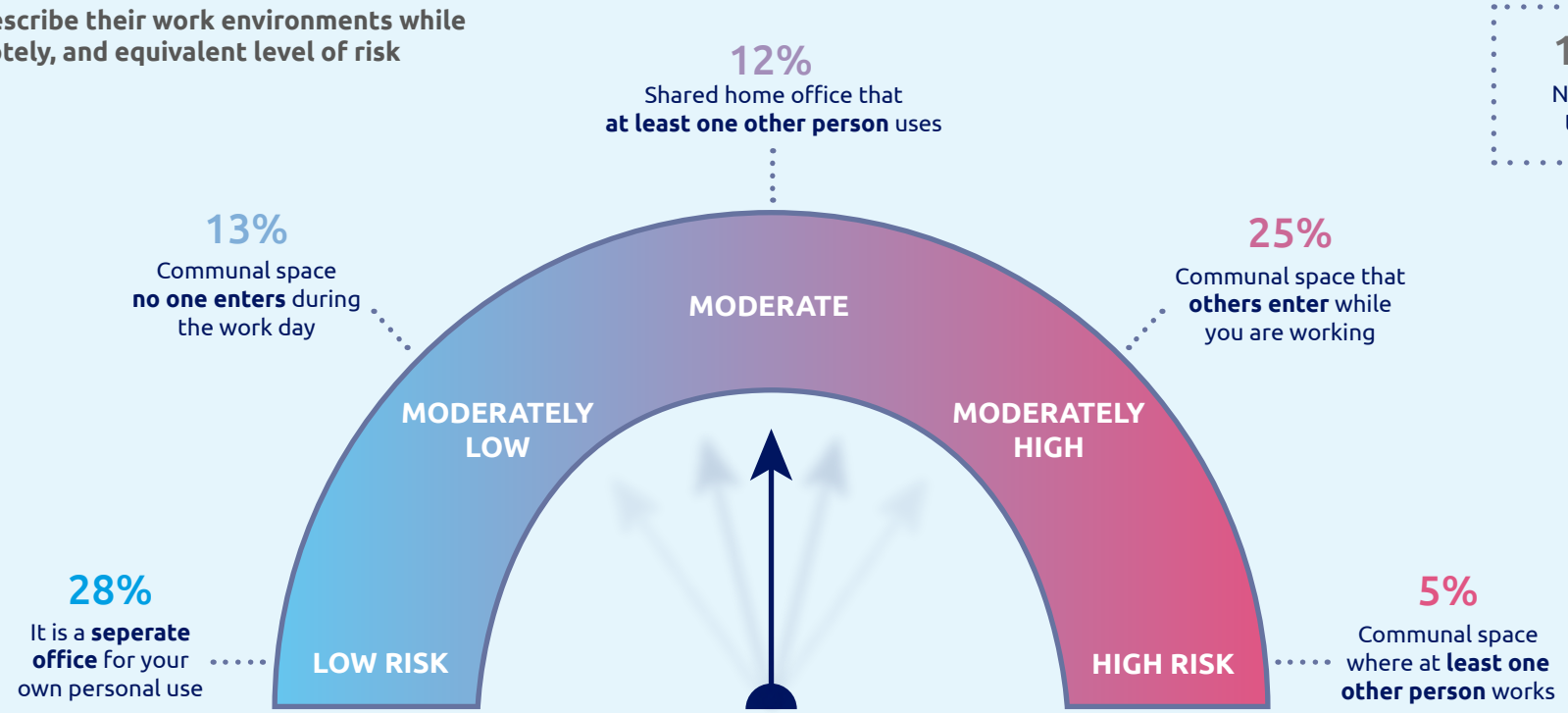
This translates to an increased likelihood that employees will make mistakes when completing everyday tasks such as sending emails, which ultimately translates into data loss risk.

In fact, when asked what factors are driving the increased data loss they're experiencing, a fifth (19%) of IT leaders point to employees being distracted in the home working environment. Almost one-quarter believe stress or tiredness is playing a part, while 23% identify the effects of job uncertainty on employee loyalty, saying that employees are taking data with them when they were made redundant or moved to a new job.

Employees agree.

Altogether, 73% of employees are feeling worse as a result of the pandemic. More than one third (34%) say they feel more tired since they started working remotely; 39% feel more stressed. One-fifth (21%) feel under more pressure to be productive. While organizations accept that, at any one time, there will always be pockets of the workforce that are feeling disenchanted for a variety of reasons, to see nearly three-quarters struggling with the situation they are experiencing is – like so many features of the pandemic – unprecedented.

Employees describe their work environments while working remotely, and equivalent level of risk



Addressing the issue from a management support perspective is complicated because, while the cause is the same, the individual circumstances of each employee and their home working set-up differ widely.

28% of respondents are fortunate to have a separate office for personal use to minimize distractions, while a further 12% share a home office space with at least one other person. One-quarter of remote workers are occupying a communal space that others enter during the working day and a further 5% are sharing that communal space with at least one other person. 13% have succeeded in banishing others from the communal space they are using during working hours.

This means that three-in-five employees (60%) are repurposing domestic spaces and are working in environments where distractions and interruptions are commonplace. It's something we've all experienced – children and pets making unexpected cameos on video calls, delivery drivers turning up in the middle of an important presentation, and children demanding help with schoolwork just when we're trying to meet a critical deadline. Denied the luxury of being able to concentrate on the job at hand, we all make mistakes, and email mistakes are the easiest (and often costliest) of all.

"73% of employees are feeling worse as a result of the pandemic"

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, such as helping with home school. 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.

"Denied the luxury of being able to concentrate, we all make mistakes"

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.

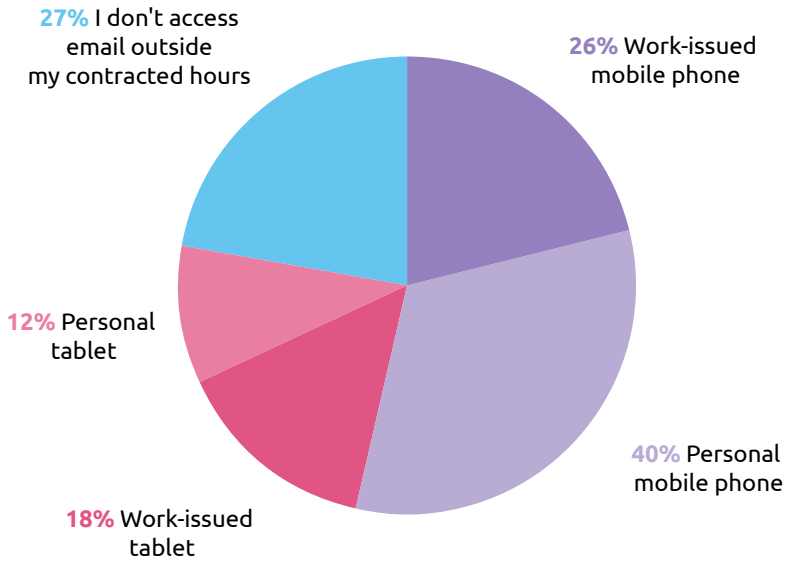
Employees in the legal sector are the most likely to be burning the midnight oil, with 93% saying they open their inbox at unorthodox times.

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". 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 working from home during the pandemic. One-quarter (24%) said that they are normally doing something else at the same time they are replying to emails.

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



"Employees who access emails out of hours are almost 2.5 times more likely to say that they feel tired as a result of working from home during the pandemic"

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. Among those feeling more tired due to the pandemic, this rises to 61%, and in the legal sector the figure is 69%.

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.

"46% of employees feel pressured to email outside of work hours"

The COVID-19 remote workforce is not OK

Aside from highlighting the very real increase in the risk of data loss that these working practices create, the responses to our survey also offer sobering insight into the unsustainable habits employees have adopted and the destruction of healthy work boundaries they have suffered due to the pandemic.

Businesses are undeniably under pressure to survive the commercial impacts of the crisis, but they are putting employees under considerable strain as they do so. Aside from the rise in significant data loss incidents that we expect to see over the coming months, the corporate world is surely storing up psychological debt that will eventually be called in - in the form of employee burnout and mental health crises.

Employers need to act now to implement the technological solutions that help employees avoid mistakes, but also to effect a cultural shift that prioritizes wellbeing, reaching inside their workers' homes to set realistic expectations about working hours and responsiveness that allows employees the freedom to switch off and recharge.

"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

Over the past year there has been much debate about the shape of the post-pandemic workplace. It seems clear that more flexibility over employees' primary location will be a key feature. 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 not good. 68% believe that a future remote and flexible workforce will make 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. In the last 12 months 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 home 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

Chapter key stats:

79%
of IT leader respondents have **deployed static** email DLP rules

and...

79%
have **experienced difficulties** resulting from their use

42%
of IT leaders say that half of all incidents **won't be detected** by their static DLP tools

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.

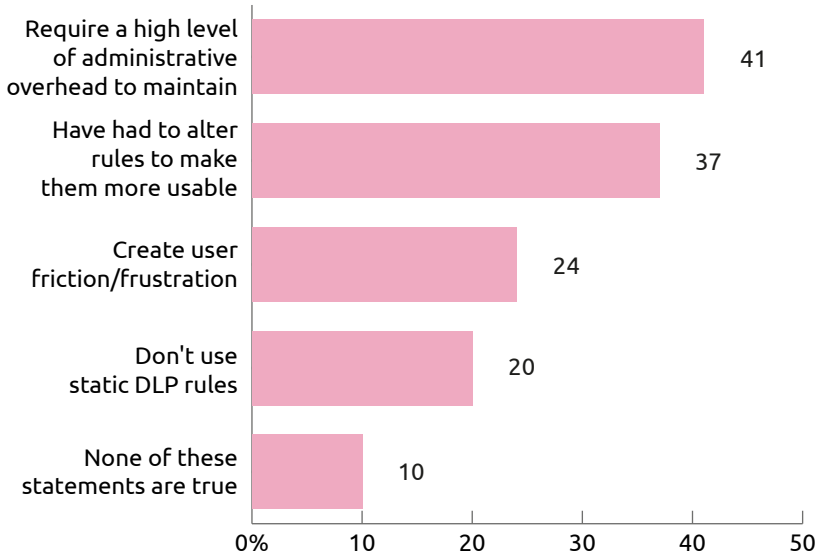
Traditional approaches to preventing data loss via email have centered on the implementation of rules-based static DLP tools and reliance on the native security tools in email clients such as Microsoft 365.

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.

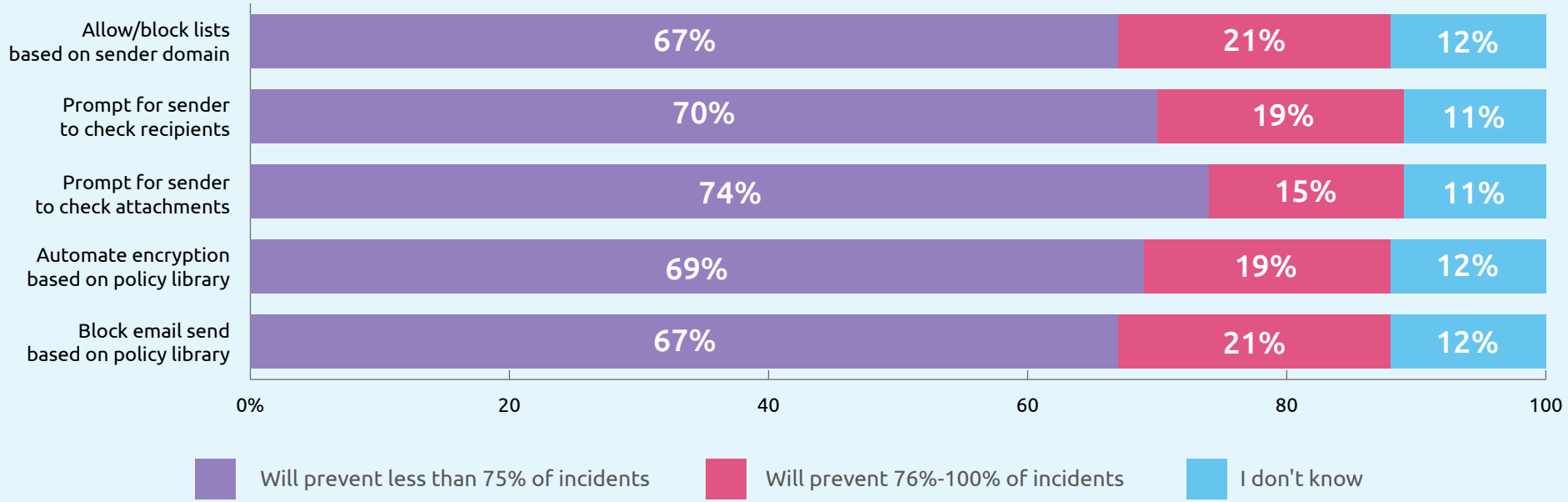
Although the majority have chosen to deploy static email DLP rules, there is low confidence in the extent to which they will effectively prevent breaches.

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.

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.

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



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.

As our research has shown, the workforce is under extreme pressure right now that shows no sign of letting up any time soon. 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.

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

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. We have known for a long time that tired, stressed and distracted employees make mistakes, but never has the entire workforce been facing these problems simultaneously in the way it is now.

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, at the very point when organizations need to do their utmost to ride out difficult economic conditions.

Where, how and when employees work is undergoing 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.

"Legacy DLP solutions are not working and more must be done to support employees"

Human layer security with Egress Intelligent Email Security

Empowering your people to be your greatest security asset – wherever they're located

Egress offers the only human layer security platform that is designed to prevent breaches and protect sensitive data. Our intelligent technology combines contextual machine learning and powerful encryption, empowering employees to remain productive while being totally secure. We can detect and prevent accidental data loss and intentional exfiltration in real time, while also automating email security to reduce the risk to data in transit and at rest.

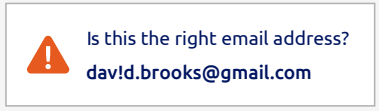
Our analytics technology accurately demonstrates risk reduction through using Egress, as well as areas for targeted remediation, and enables administrators to run thorough compliance reporting.

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

1

Egress Prevent

Stop email data breaches before they happen



Contextual machine learning is used to deeply understand individual user's email patterns and detect the abnormal behaviour that puts data at risk.

Learn more

2

Egress Protect

Send and receive secure, encrypted email

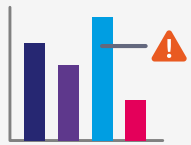
Automating security and authentication relative to risk, our encryption reduces friction for senders and recipients.

Learn more

3

Egress Investigate

Understand, monitor and report on the security of your network



We empower administrators to accurately measure risk, and maintain local and international regulatory compliance.

Learn more

Want to find out how our intelligent technology can help you? The Egress Team would be happy to discuss the top benefits of our solution for your organization, including:

- **Enhancing service delivery to your clients**
- **Supporting your employees however and wherever they work, including on mobile**
- **Ensuring corporate and compliance data privacy requirements are met**
- **Making email security a competitive differentiator**
- **Protecting your employees from career-limiting mistakes**

Talk to us today

About Egress

Our mission is to eliminate the greatest risk to every business – the insider threat. To achieve this Egress has built the world's only Human Layer Security platform that empowers your people to remain secure while being highly productive.

Using patented contextual machine learning, Egress is trusted by the world's biggest brands to prevent human error and protect against malicious or reckless behavior on email without any administrative overhead. Funded by FTV Capital and Albion VC, Egress is headquartered in London with offices in Toronto and Boston.

www.egress.com | info@egress.com | @EgressSoftware

egress