Insider Data Breach Survey 2020

Research commissioned by **Egress**

Independently conducted by
Opinion Matters

Opinion matters

Commissioned by:
egress

Table of contents

Executive summary 3

Insider data breach survey findings at a glance 4

Insider breach risk: the view from the top 5

Concerned, cynical and conscious of compliance 5

Breach causes: why the rise in cynicism? 6

What data is most at risk? 7

Breach impact: financial reality bites 8

Insider data breach risk: behind the scenes 9

How and why do employees cause data breaches? 10

Whose data is it anyway? 12

How IT leaders tackle insider breach risk 13

Looking ahead: insider data breaches in 2020 14

Summary 15

About Egress 16

Methodology 16

Executive summary

The world has changed. The implementation of GDPR in 2018 was just the opening act in a global transformation of data privacy laws. As companies continued to hit the headlines for non-compliance in 2019, we saw regulators such as the UK's Information Commissioner's Office (ICO) flex new powers by issuing intentions to fine on a scale that left the security community reeling.

Now more than ever, no one wants to be part of the security team at the next company under investigation by regulators.

Headlines frequently focus on external attacks, but the risk from employees accidentally or intentionally leaking data is significant and arguably more difficult to confront. Increasing volumes of unstructured data and a wealth of sharing tools make it easier than ever for employees to cross the company policy line and carry out actions such as taking data with them to new jobs or downloading it to personal systems to work from home.

Preventing insider breaches – whether intentional or accidental – and protecting sensitive data while still ensuring employees remain productive is a complex challenge for IT leaders (including CISOs) to solve.

The second **Egress Insider Data Breach Survey** explores how IT leaders view that challenge, and compares how they and employees working in non-security functions perceive data risk, responsibility and ownership.

In our 2019 report, we found significantly high levels of concern amongst IT leaders over insider data breach risk – although a large percentage of employees denied causing data breaches. We also discovered a disconnect between how employees and IT leaders view data ownership.

In the 12 months since that survey, have organisations managed to move the dial and develop a more effective approach to managing insider breach risk?

This year we have expanded the study to include IT leaders and employees from the Benelux region, as well as the US and UK, to give a broader perspective on insider data breaches in different regions, and although we evolved some of the questions and industry sectors surveyed, the trends coming through were quite clear.

The risk from employees accidentally or intentionally leaking data is significant and difficult to confront.

Insider data breach survey findings at a glance

IT leaders

78%
of IT leaders say employees have put data at risk **accidentally** in the last 12 months

75%
of IT leaders say employees have put data at risk **intentionally** in the last 12 months

97%
of IT leaders acknowledge that insider breach risk is a concern for their organisation

Employees

71%
of employees say they or a colleague haven't **accidentally** shared company information externally

68%
of employees say they or a colleague haven't **intentionally** broken company policy when sharing data

45%
of employees said they had received an outlook recall message or email asking them to disregard an email sent in error

IT leaders

57%
of IT leaders rely on employee reporting to alert them to an **intentional** breach

59%
of IT leaders rely on employee reporting to alert them to an **accidental** breach

41%
of IT leaders think financial fallout would be the greatest impact of a breach

Employees

46%
of employees said they or a colleague **intentionally** breached company policy by taking data to a new company

31%
of accidental breaches were caused by accidentally sending data to the wrong person

41%
of employees don't believe the organisation has exclusive ownership of data

Insider breach risk: the view from the top

Concerned, cynical and conscious of compliance

97% of IT leaders surveyed admitted to being concerned about insider data breaches. Up 2% from 2019, this widespread worry shows nothing has happened to reassure IT leaders in the past 12 months that this problem is going away.

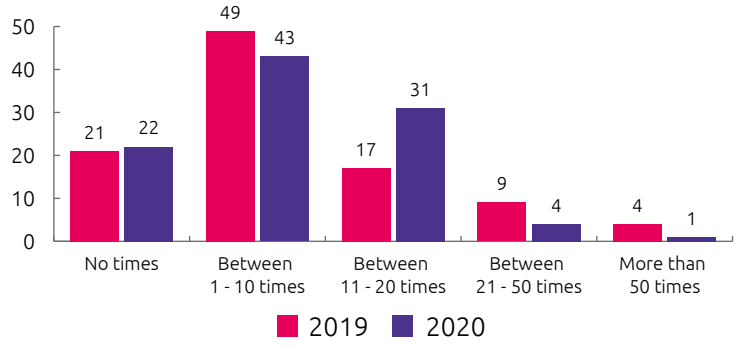
This anxiety is reflected in IT leaders' estimates of how often staff have put data at risk over the last year:

78% say employees have put data at risk **accidentally**

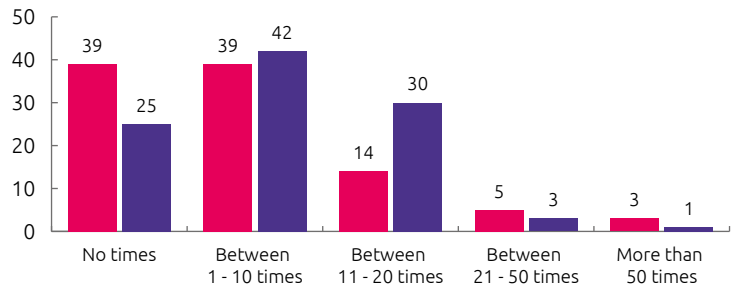
75% say employees have put data at risk **intentionally**

The proportion who believe employees have put data at risk accidentally has remained stable since 2019, but there has been a notable 14% jump in the percentage of IT leaders who think employees have deliberately put data at risk.

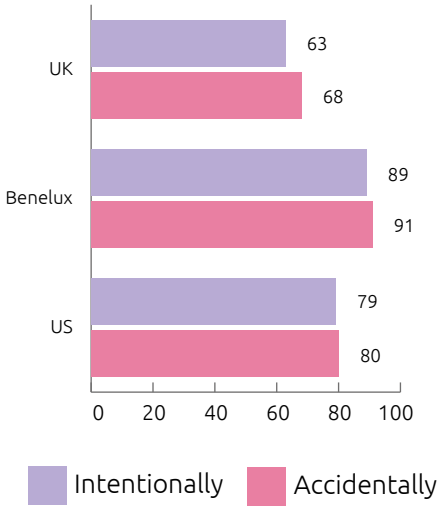
How many times have employees accidentally put sensitive data at risk in the last 12 months? (%)



How many times have employees intentionally put sensitive data at risk in the last 12 months? (%)



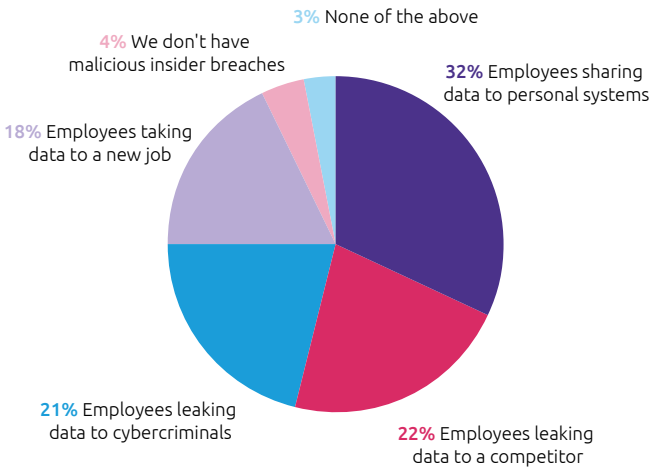
IT leaders who believe employees have put data at risk, by country (%)



Breach causes: why the rise in cynicism?

This increase in cynicism points to a more nuanced understanding by IT leaders that even employees with the best intentions – those who are just trying to get the job done – can still intentionally breach company policy and put data at risk. And IT leaders recognise this, believing that staff sharing data to personal devices is the most common type of intentional risk.

When thinking about intentional insider breaches, which of the following would most likely be the cause in your organisation? (%)



Mobility matters

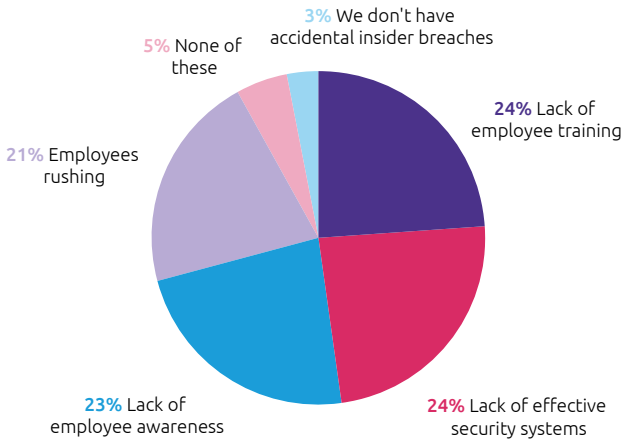
As employees become ultra-mobile and the boundaries of the workplace are less defined, the complexity of safeguarding data increases. IT leaders are trying to protect a moving, growing, changing target but the frequency of breaches suggests they are failing.

The shift to flexible working may have a psychological impact, too. As employees work outside the physical walls of the company – especially in their home environment – there's a risk that they develop a more proprietary attitude to the data they work on.

Other perceived motivations for intentional breaches are less benign, including 18% believe employees take data with them to new jobs – but as later figures show, this is a more widespread problem that IT leaders realise.

The relatively even split of IT leaders' opinions on the likely causes of accidental data breaches indicate how they view the complexity of this problem. Often, this can be a 'moving target' - with causes such as employees rushing, and the effectiveness of awareness and training campaigns influenced by a variety of external and psychological factors that can change not just day-to-day, but hour-by-hour. Additionally, one-quarter of IT leaders (24%) don't believe technology is providing an adequate safety net to catch employees' mistakes.

When thinking about accidental insider breaches, which of the following would most likely be the cause in your organisation? (%)



Egress analysis:

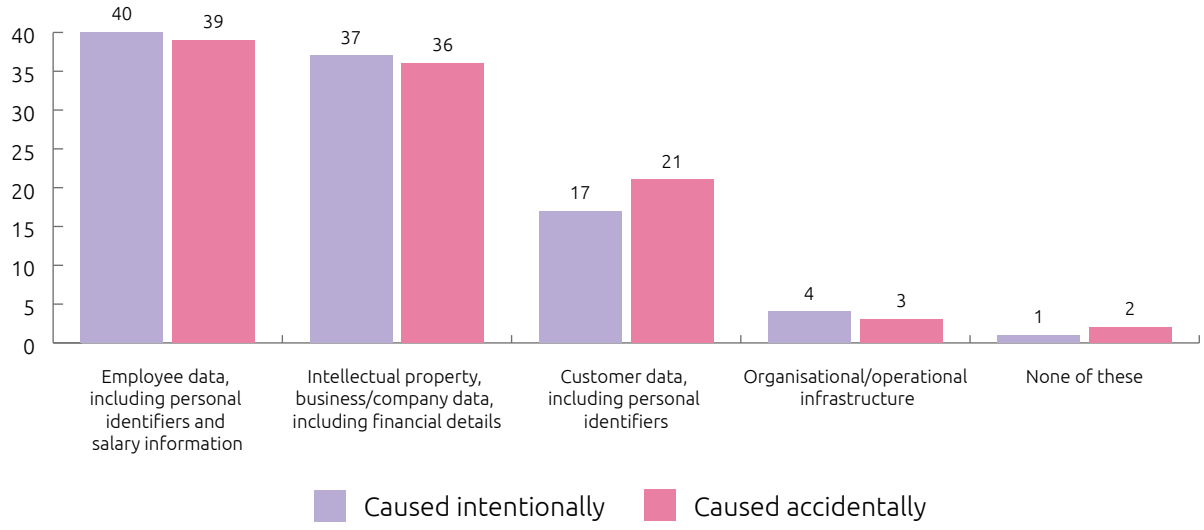
The spread of causes and motivations for insider data breaches points to the wide range of 'personalities' that commit these incidents - from harassed workers just trying to get the job done, to calculating individuals sharing data for personal gain. All present risk but, as they exhibit different behaviours, they require prevention strategies and solutions that can respond dynamically to their individual actions. Understanding these different personas is key to directing resources effectively.

What data is most at risk?

Devising an effective data loss prevention strategy requires IT leaders understand what types of data are most vulnerable from which type of internal breach.

Top of the list for both accidental and intentional internal breach risk is employee data, including personal identifiers and salary information, closely followed by company intellectual property. Interestingly considering the current regulatory climate, customer data including personal identifiable information (PII) was ranked third.

Which of the following company information do you feel is most vulnerable to an internal data breach? (%)



Breach impact: financial reality bites

Regulation is designed to provide a powerful push for businesses to act the right way by making non-compliance suitably punitive. This year's insider breach survey shows that message is hitting home with IT leaders.

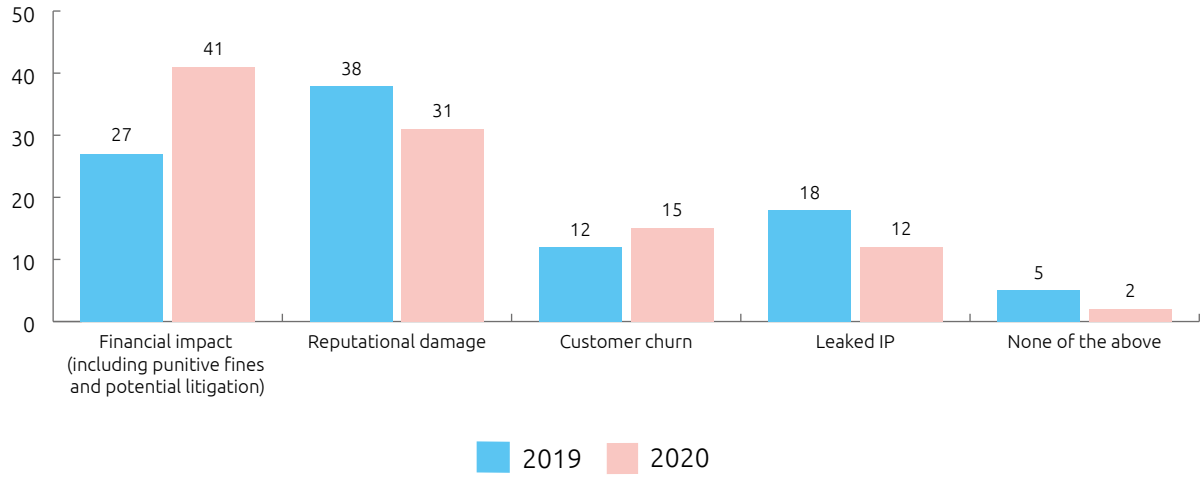
41% say financial damage would be the area of greatest impact following an internal data breach, increasing from 27% in 2019 when IT leaders were most concerned about reputational impact.

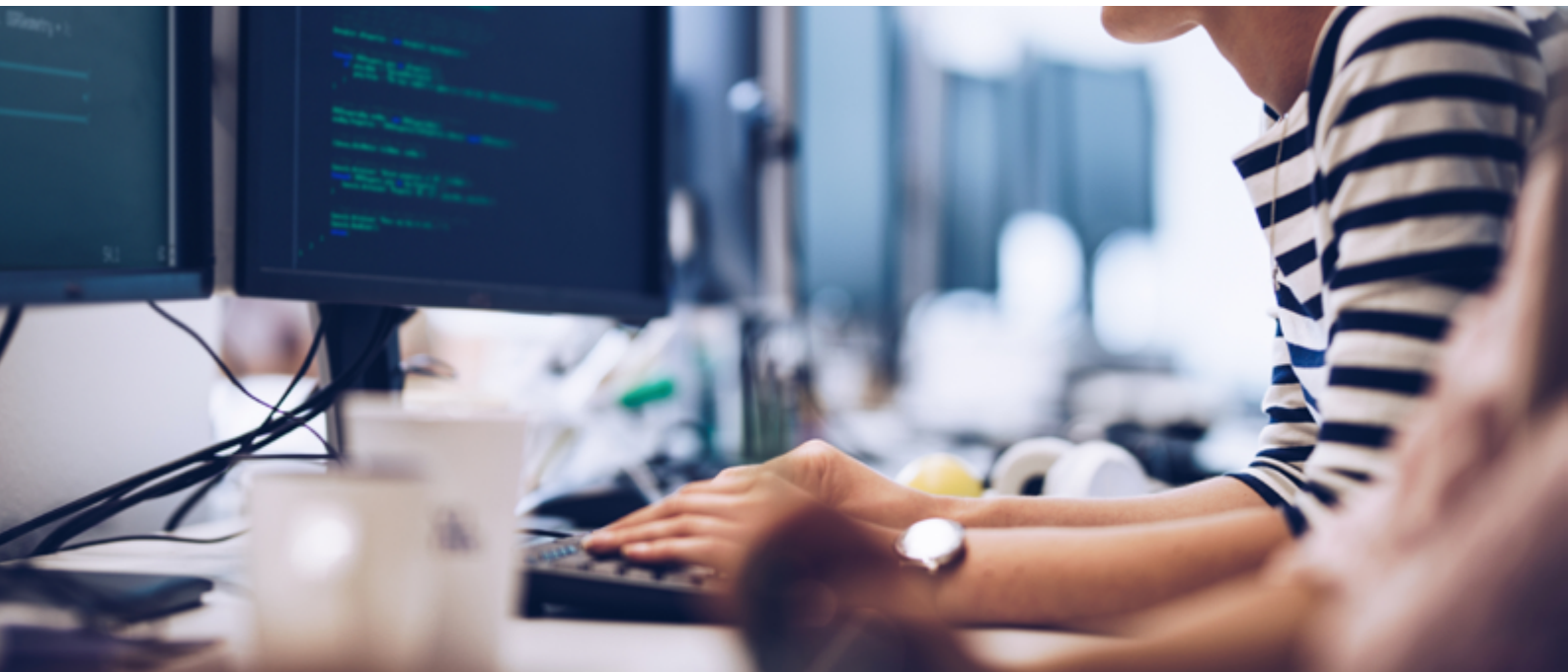
This is a predictable result of the introduction and enforcement of stringent data privacy legislation. In the UK, the ICO has fired a shot across the bows by pressing for unprecedented penalties for British Airways and Marriott Hotels for non-compliance with GDPR. For US IT leaders, the newly implemented California Consumer Privacy Act (CCPA) from January 2020 brings with it a penalty structure that means fines could eclipse even those available to GDPR regulators. The direction of travel for privacy regulations worldwide is clear: non-compliance comes with a considerable price tag attached.

Changing global concern

Concern about financial impact is highest in the US, with 43% saying it is the area of greatest concern. This drops to 33% for Benelux IT leaders, who remain most worried by reputational impact (34%).

Which would be the area of greatest impact if an internal data breach occurred at your organisation? (%)





Insider data breach risk: behind the scenes

IT leaders have grown more suspicious of employees, and our survey of employees working in non-security functions shows this is justified. This year we amended our question, asking respondents whether they **or a colleague** had broken company policy. The rationale was to encourage greater honesty in responses through shared responsibility around breach incidents.

27% of employees say they or a colleague have accidentally shared or leaked company information externally. This is a major change from last year where only 8% admitted personal responsibility.

This picture is also reflected in intentional data breaches: **29% of employees say they or a colleague have intentionally shared or leaked company information externally**. Last year, just 8% admitted personal responsibility.

Despite an increase in admissions when employees are not asked to bear sole responsibility for an incident, there remains discrepancy between the number of incidents reported by employees and IT leaders.

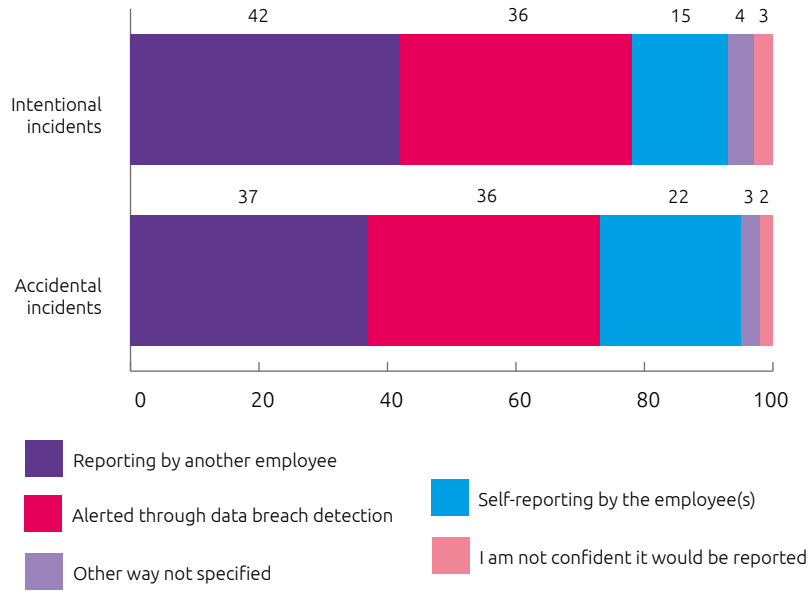
But who is right? Do IT leaders have an unreasonably negative view of employees, or are employees unwilling to admit (even in an anonymous survey) the truth about how they and their colleagues treat data?

IT leaders need to hope that the latter is not the case because, incredibly, employee reporting appears to be a pillar of breach detection strategy.

Alarmingly 59% of IT leaders rely on employee reporting for accidental breaches and 57% rely on them for intentional incidents.

Breach detection systems were the second most likely way IT leaders think they'll be informed about an incident, with 37% selecting this for intentional breaches and 36% for accidental.

How IT leaders think they will be notified of an insider breach (%)



At higher risk: Legal professionals are significantly more likely to say they or a colleague had put data at risk.

56%
said they or a colleague had **accidentally broken** company policy

57%
said they had **intentionally** done so

Owning up: Employees are most likely to tell their line managers about data breaches

66%
said they would report **their own mistake** to their line manager

60%
said they would report a **colleague's mistake to their own manager**

Showing greater trust: UK IT leaders think

33%
of employees will self-report **accidental** breaches

20%
would self-report **intentional** incidents

How and why do employees cause data breaches?

The vectors and underlying causes of breaches provides timely insight into insider breach risk.

The global rise in phishing attacks is inevitably taking its toll, with 41% of employees saying they were tricked into clicking a malicious link. Almost one-third (31%) admitted to simply making a mistake by sharing information with the wrong person, for example via email - although as 45% of those surveyed said they'd received an email in error, it's surprisingly this figure isn't higher.

Only 8% of employees reported accidentally leaking data because they didn't know better - most likely showing the success of global regulatory campaigns to improve awareness.

Senior personnel were far more likely to fall prey to phishing attacks – 61% of directors said they'd caused a breach in this way. Conversely, clerical workers were more likely to have sent information to the wrong person – 44% had done this compared to 20% of directors.

In the UK, employees are almost as likely to send an email in error (35%) as they are to fall foul of a phishing email (37%). Meanwhile, phishing was a bigger issue in Benelux (46%) and the US (44%).

Why are accidental breaches happening? Hint – it's often not for the reasons IT leaders think!

The reasons employees give for sharing data vary depending on whether the breach is accidental or intentional – and the answers show that IT leaders' views are sometimes wide of the mark.

Just 8% of employees think accidental breaches happen due to inadequate security systems, versus 24% of IT leaders. Similarly, 5% of employees blame inadequate training - but, again, 24% of IT leaders believe this is the primary cause of incidents. IT leaders also put more emphasis on people rushing and making mistakes (20%) than employees (15%).

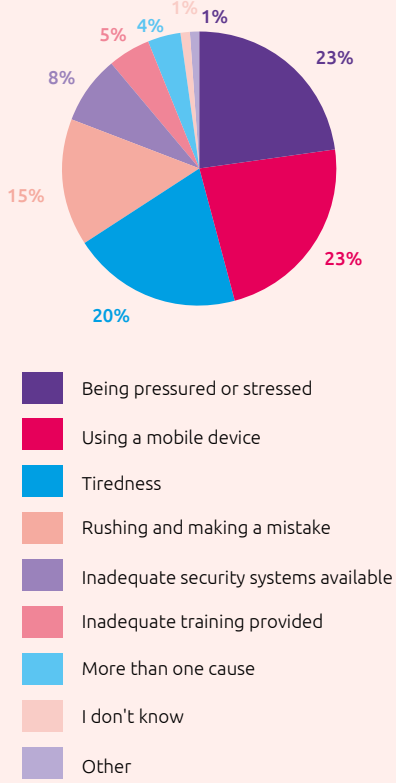
Industries with above-average risk of sending data to the wrong person

37%	35%	34%
Healthcare	Financial Services	Government

Worryingly, employees in these sectors are most likely to be dealing with highly sensitive personally identifiable information (PII), including special category data.

How data breaches have happened, according to employees (%)

Why data breaches have happened, according to employees (%)



Intentional data breaches – departing employees take data out of the door

Only 18% of IT Leaders think that the most likely cause of an intentional data breach is employees taking data to a new job. In contrast, almost half (46%) of employees who said they or a colleague intentionally breached company policy in the last year had done so by taking customer and/or project data to a new company. This points to a critical need for diligence around employees leaving the company, so sensitive data doesn't leave the building when they do.

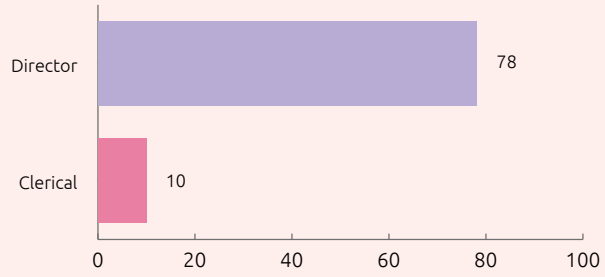
26% of these employees intentionally took a risk and shared data against company rules because the company hadn't provided the tools needed to share information securely, while one-in-ten (11%) were upset with the company and wanted to cause deliberate harm.

Directors disrespecting data protection

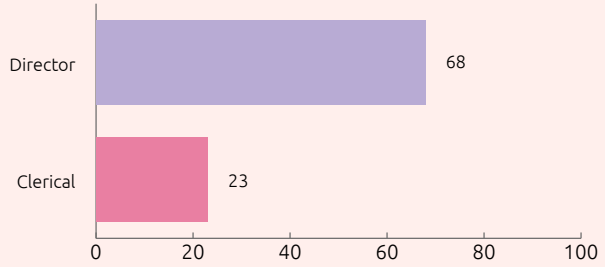
Despite their seniority, director-level staff set the wrong tone for data protection – they are more likely to intentionally leak data and far less likely to believe employees are responsible for securing it.

Almost half of employees who said they or a colleague intentionally breached company policy in the last year had done so by taking data to a new company.

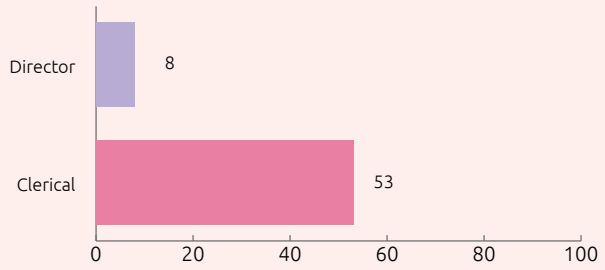
Employee has intentionally shared data against company policy (%)



Employee has taken data to a new job (%)



Belief that everyone has equal responsibility for securing data (%)



Whose data is it anyway?

The grey area of data ownership and responsibility

Understanding employees' views on data ownership and security responsibility sheds useful light on why they act how they do and - consequently why insider breach risk is so difficult to manage.

- Only 59% of employees recognise that the organisation has ownership of its data.
- 41% of employees said that the departments and teams that created the information own it. This figure rose to 61% among directors who clearly take a more proprietorial view over the data they generate.
- More than one-fifth (22%) felt that any employees of the organisation had data ownership - not just those who created it.

Despite this proprietorial approach, a discrepancy arises when employees are asked who's responsible for securing company data. Just 37% of employees felt that everyone has equal responsibility for keeping data safe - so while they want to own data, they don't want to share the security burden.

The more senior the employee, the less likely they are to accept data protection liability – just 8% of directors believe everyone shares responsibility, compared with 53% of clerical staff. Directors and business owners are much more likely to delegate the greatest responsibility for information security to IT departments or the C-suite.

And incongruously, even though line managers are the most likely to be the first to hear about an internal data breach, just 8% of individual employees believe that the greatest responsibility for data protection lies with them.

Egress analysis:

These findings show serious a disconnect between beliefs about where data ownership and security responsibility lie. Organisations must articulate clearly that, while departments such as IT have an operational role in providing data security tools and the C-suite should ensure effective policies are in place, all employees share equal responsibility to protect data.

How IT leaders tackle insider breach risk

High penalties for data breaches and the intensive risk environment mean IT leaders need a strategic arsenal of complementary tools. Yet patchy deployment of those tools traditionally associated with mitigating insider risk reveals they are cherrypicking their solutions - perhaps due to shortcomings in the traditional static technology stack.

As well as a foundation of static technology, IT leaders also require solutions that can respond dynamically to employees' changing behaviours and motivations in order to stop breaches of security before they happen.

Technologies deployed to mitigate insider risk: IT leaders cherrypicking solutions reveals a lack of effectiveness of the traditional stack

50%
Anti-virus

48%
Email encryption

47%
Secure collaboration software

46%
Anti-malware

41%
Static DLP

41% of employees believe the departments and teams that create information own it.

Looking ahead: insider data breaches in 2020

Considering the complexity of the insider breach challenge and the frequency of incidents, we might expect IT leaders to have robust technology stacks, be proactively implementing new solutions, and have zero reliance on their unpredictable staff reporting every breach incident. Worryingly, this is not the case.

In fact, the statistics point to a very uncertain 2020 and a sense that insider data breaches will continue to rise:

- 78% of IT leaders acknowledge data was put at risk accidentally in the last 12 months, while 75% said it had happened intentionally
- The most likely way IT leaders are currently alerted to data breaches is via the uncertain route of employee reporting
- 24% believe ineffective systems are at the root of accidental breaches
- Employees have a proprietary attitude to data ownership
- More than one-quarter of employees who breached company rules intentionally felt they weren't provided with safe sharing tools
- Insider breach mitigation technology is inconsistently deployed

So why are IT leaders taking this approach? Does this derive from a sense of resignation to the perceived inevitability of insider data breaches? Are they, in effect, adopting a risk posture in which at least one-third of employees putting data at risk is deemed acceptable?

Resignation to insider data breaches is not justified. Ethical obligations and the potentially crippling financial penalties and reputational damage demand more is done to prevent employees from making mistakes or intentionally putting data at risk - especially given powerful developments in the technologies available to mitigate common breach vectors, such as misdirected emails and spear phishing attacks.

It seems IT leaders should re-examine their approach and investigate building out their technology stack and security strategies, or face having their confidence shattered as the year unfolds.

97%

of IT leaders acknowledge that insider breach risk is a concern for their organisation

Summary

The **Insider Data Breach Survey 2020** reveals the dial on mitigating insider data breach risk has not moved in the last 12 months. Concern among IT leaders is greater than ever and employees' perception gap persists over who owns data and who has responsibility for securing it. The survey also illuminated significant inconsistencies between IT leaders' views of current insider breach risk and their expectation of how they will manage it in future.

Employees have been revealed to exhibit different 'breach personas' informed by their roles and seniority in the organisation: from careless clerical staff sending accidental emails, to devious directors whose proprietary view of data cultivates a cavalier approach. As business culture is set by the tone from the top, directors and business owners who fail to protect data are giving the wrong message to their employees.

Also of major concern must be the staggering 46% of employees who said they or a colleague breached company rules on data sharing because they took information to a new job. Ultimately, IT leaders need to be more proactive to stop data from simply walking out of the door.

Now more than ever, consistent technology use and greater visibility of insider breach risk vectors is needed, so IT leaders are no longer relying on their own, often unreliable, employees to alert them to a breach.

Yet while more than three-quarters of IT leaders believe employees put data at risk in the past 12 months, there seems to be no attempt to change policy or adopt new technologies. So, without impetus to improve, we will most likely be looking at the same story of frequent breaches and confusion over data ownership in 12 months' time.

Without impetus to improve, we will most likely be looking at the same story in 12 months' time.

About Egress

Our vision is for a connected world in which people communicate efficiently and securely. To achieve this, we provide human layer security to protect individual users and stop breaches before they happen. Our patented technologies are built using leading-edge contextual machine learning and powerful encryption that mitigate modern risks in ways that other solutions simply can't achieve.

Today, we provide intelligent email security and collaboration solutions that prevent accidental and intentional breaches, protect sensitive data, and equip CISOs and their teams with the detailed reporting required for compliance purposes.

Egress is headquartered in London, with regional offices in the UK, the US, Canada and the Netherlands.

Methodology

This research was commissioned by Egress and undertaken by independent research organisation Opinion Matters, in December 2019. 528 IT directors, CIOs, CTOs and CISOs in companies with 100 employees or more were surveyed in the UK, US and Benelux. 5001 employees in companies employing 100 people or more (but not those working in the IT / tech / legal departments) were surveyed in the UK, US and Benelux.

Note: In 2020 the survey was expanded to additional countries and targeted to gain responses from specific vertical markets. Therefore, findings are not always like for like comparable due to sample variation. This should be taken into consideration when the report refers to data from each survey.

www.egress.com | info@egress.com | 0844 800 0172 | @EgressSoftware