RESEARCH REPORT

Insider Data Breach survey 2019

Research commissioned by **Egress**

Independently conducted by **Opinion Matters**

Commissioned by

Table of contents

Executive summary

Over the last five years, headline-grabbing incidents have demonstrated the potential implications of a data breach – from damaged business reputation, to loss of revenue and even company devaluation. According to the 2018 Cost of a Data Breach survey conducted by the Ponemon Institute, the typical data breach now costs a company $3.86M, up 6.4% from 2017.[1]

As the financial impact of data breaches increases, so do the opportunities for employees to leak sensitive data – either accidentally or maliciously. IDC estimates a 300% increase in unstructured data (emails and files) by 2020, as organizations adopt new digitized working practices.[2] As a result, employees are sharing more information digitally, including emails and multimedia content such as audio and video files – creating more opportunities for data breaches to occur.

In efforts to protect and secure this data, organizations continue to invest: Gartner predicts global information security market spend will reach $101.6bn by 2020. Given the significant amount spent on security – and the rise in the cost and opportunity for a data breach, organizations need to be sure that their expenditures are having an impact on minimizing the chances of a data breach.

Despite this investment, statistics from the Ponemon Institute show that all types of insider threats are increasing, with the average number of incidents involving employee or contractor negligence rising by **28%** per organization.

Commissioned by Egress and conducted by independent research company Opinion Matters, the 2019 Insider Data Breach survey gathered responses from 252 U.S. and 253 U.K.-based IT leaders (CIOs, CTOs, CISOs and IT Directors) and 2004 U.S. and 2003 U.K.-based employees to assess the root causes of these employee-driven data breaches, as well as the frequency and impact of such instances.

Moreover, the two surveys dive into the 'intent' behind insider breaches, with a specific look at how employees and executives differ in their views of what constitutes a data breach, what is acceptable behavior when sharing data and who owns company data, in an attempt to explain why insider data breaches continue to rise.

The data shows that there is a disconnect between IT leaders and employees on how each group views sensitive data. This perception gap, combined with the rapid growth in unstructured data and increases in ways for employees to share that data, have the potential to negatively impact an organization's security program.

The results of the research can offer insights that could help to inform the allocation of security budgets and strategies so that investment can be directed to where it will achieve the greatest impact in preventing costly data breaches.

[1]https://www.ibm.com/security/data-breach
[2]https://www.emc.com/collateral/analyst-reports/idc-the-digital-universe-in-2020.pdf

Insider Data Breach survey findings at a glance

IT leaders

79%
of IT leaders believe employees have put sensitive company data at risk **accidentally** in the last 12 months

61%
of IT leaders believe employees have put sensitive company data at risk **maliciously** in the last 12 months

60%
of IT leaders believe they will have an **accidental data breach** in the next 12 months

Employees

92%
of employees say they **haven't accidentally** broken company policy when sharing information

91%
of employees say they **haven't intentionally** broken company policy when sharing information

55%
of employees who intentionally shared data against company rules said their organization **didn't provide them with the tools** needed to share sensitive data securely

IT leaders

46%
of IT leaders believe they will have a **malicious data breach** in the next 12 months

38%
of IT leaders believe **reputational damage** is the greatest impact of an internal data breach

95%
of IT leaders **acknowledge** that insider threats are a concern for their organization

Employees

60%
of employees **don't believe** the organization has exclusive ownership of data

32%
of employees would **consider taking company information** to a new job

29%
of employees **believe they have ownership** of data they have worked on

The IT leader perspective: Insider data breaches are a concern for 95%

Understanding the security threats and data breach risks facing organizations is paramount. But discovering the ‘why’ behind internal data breaches is critical to securing the integrity of an organization — and IT leaders predominantly believe that employees are putting sensitive data at risk, both accidentally or maliciously.

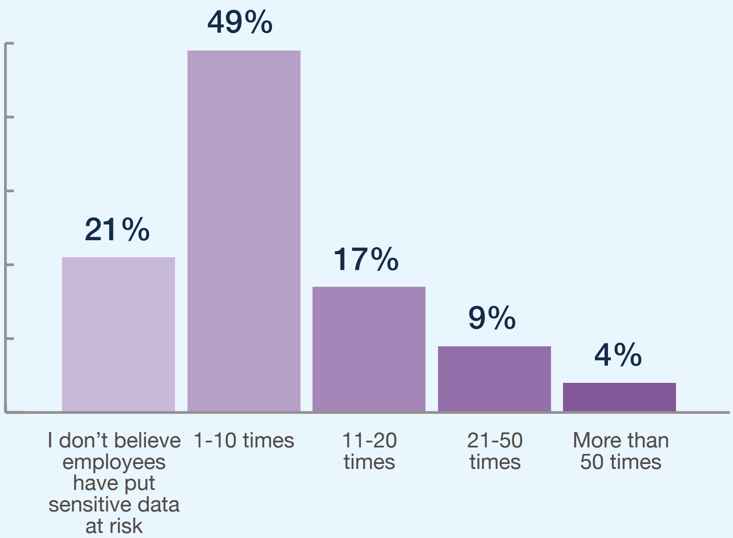
- 79% of CIOs believe employees have put company data at risk accidentally in the last 12 months, while 61% think employees have put company data at risk maliciously
- Overall, 95% acknowledge that insider security threats are a danger to their organization

IT leaders believe that employees are more likely to put data at risk accidentally than maliciously. 61% stated their belief that data had been exposed deliberately compared with 79% who felt that employees had put data at risk accidentally.

Even the ‘curious’ employee can put data at risk by accessing and sharing it without permission. Recently, 60 employees at a hospital in the U.S. were fired for accessing and sharing information on a celebrity patient.

Regardless of intention, IT leaders have a responsibility to provide employees with tools to share and access data securely.

How may times have employees **accidentally** put sensitive data at risk?



How may times have employees **maliciously** put sensitive data at risk?

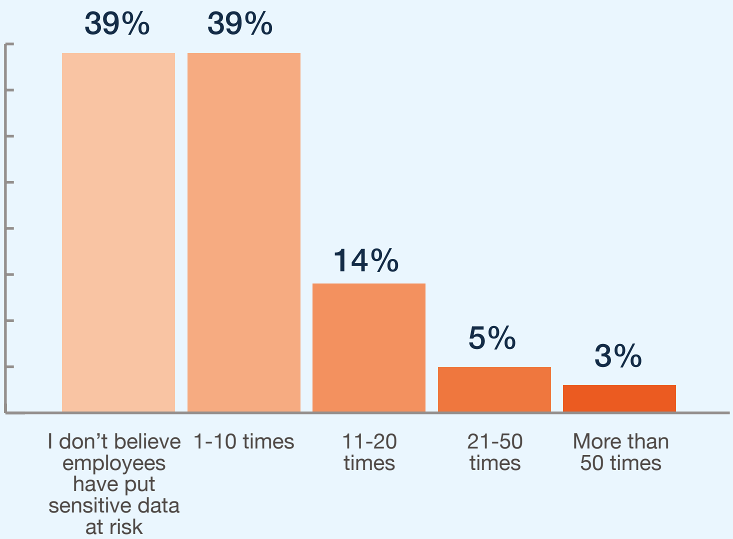


Fig. 1: In the past 12 months, how many times do you believe employees have put sensitive data at risk maliciously or accidentally?

Getting to the root causes of insider data breaches

When it comes to the causes of data breaches — both malicious and accidental — IT leaders give employees the benefit of the doubt and believe they're primarily caused unintentionally by employees rushing and making mistakes (60%). A general lack of awareness was the second leading cause (44%), while 36% believe that a lack of training on the security tools a company uses is the primary driver.

Nevertheless, 30% believe that internal data breaches result from employees leaking data to harm the organization, while 28% believe employees are stealing data for financial gain.

Causes of insider data breaches

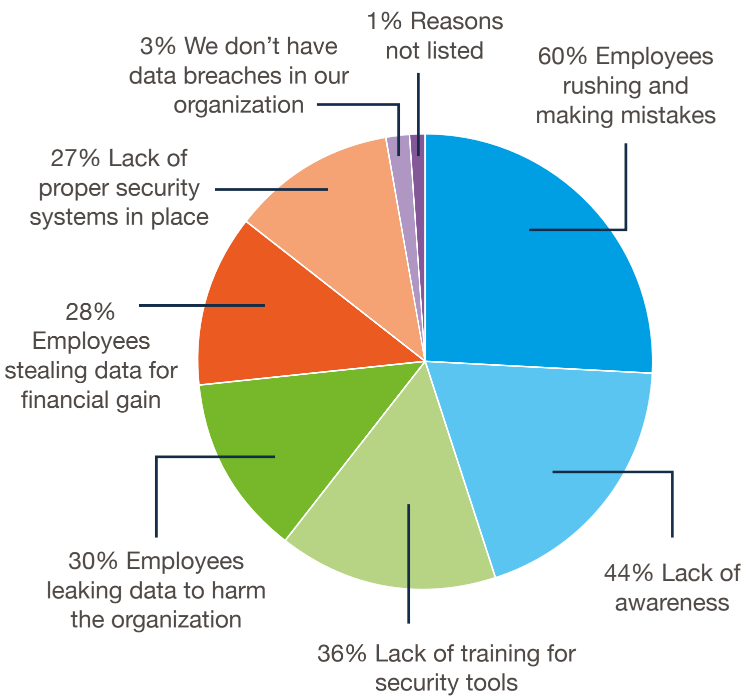


Fig. 2: Which of the following do you believe are the biggest causes of insider data breaches within your organization (whether malicious or accidental)? (Select up to three)

Threat of malicious insider data breaches

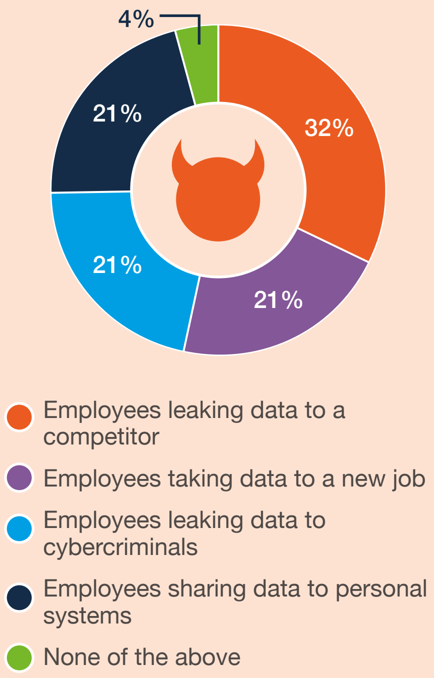


Fig. 3: If an employee maliciously caused a data breach, which of the following would be of greatest concern for your organization?

Where IT leaders believe that data breaches were carried out with malicious intent, the motivations behind the breach can inform the shape of security policy and potentially indicate where budget should be allocated.

Interestingly, when it comes to malicious intentional data breaches, IT leaders are most concerned about those that leak company information to a competitor (32%). Employees taking data to a new job, leaking data to cybercriminals and sharing data with personal systems were the second most commonly cited (21%).

This is why IT leaders need security solutions that provide comprehensive protection for sensitive data, while providing clear audit trails so a log of who is accessing what data is easily available.

Insider data breach: Getting hit where it hurts the most

Employee-driven accidental data breaches are becoming more prevalent every day. Simple mistakes — such as sending an email to the wrong person or falling for a phishing scam – can lead to significant data loss and company damage. According to the IT leaders surveyed, the greatest area of impact by an internal data breach is reputational damage (38%), followed by financial impact (27%) and leaked intellectual property (18%).

Greatest **area of impact** from insider data breach

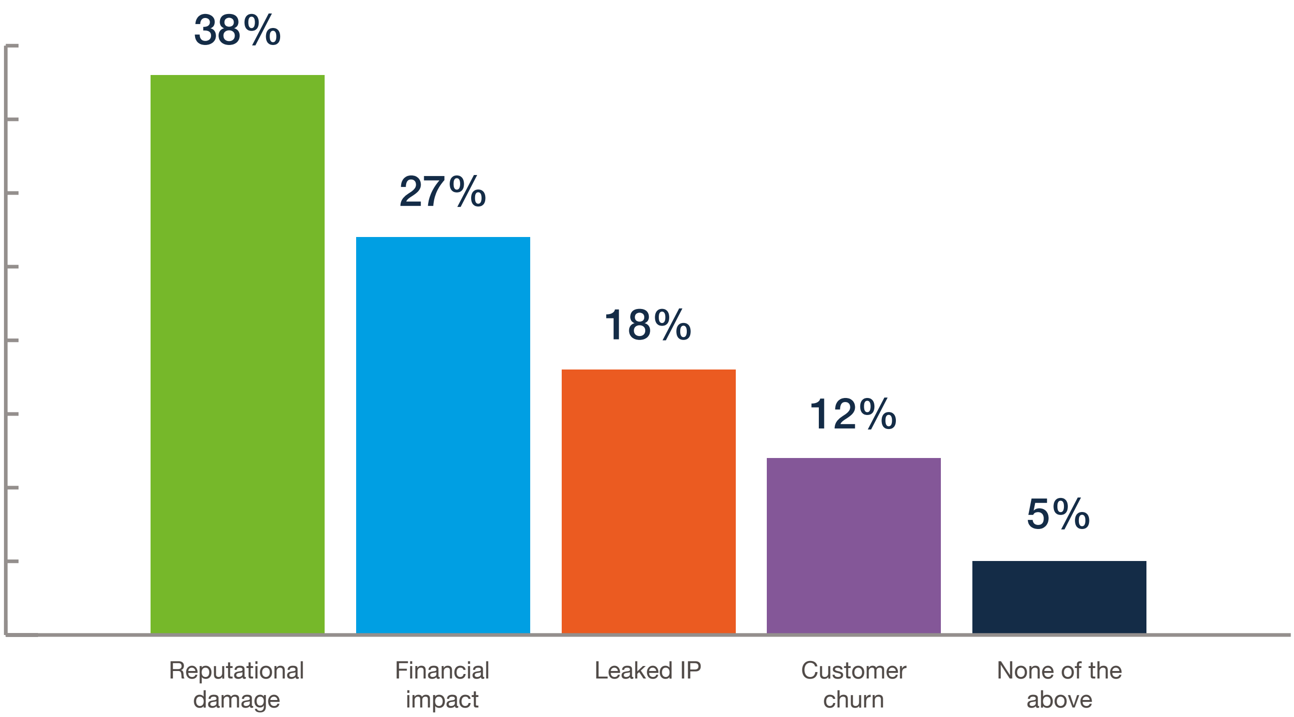


Fig. 4: Which of the following would be the area of greatest impact if an internal data breach occurred at your organization?

Fears for the future

In light of their experience to date, IT leaders anticipate breaches in the next 12 months. 60% believe it's likely that they'll suffer an accidental data breach, while 46% believe their organization will be victim to a deliberate breach with malicious motivation.

The employee perspective: No company policies being broken

As part of the overall study of insider data breaches, the research also surveyed 2004 U.S. and 2003 U.K.-based employees to assess the root causes of these employee-driven data breaches, as well as the frequency and impact of such instances.

The results show a significant disconnect between the IT leader and employee perspectives of insider data breaches.

- While 61% of IT leaders believe employees have maliciously breached data at some point, 94% of U.S. employees and 87% of U.K. employees claim they have **not** intentionally broken company data sharing policies.
  - A small percentage (2% in the U.S. and 5% in the U.K.) state that they've maliciously broken policies two-to-five times in the last year.
- Similarly, 95% of U.S. and 90% of U.K. employees believe they have never accidentally caused a data breach.
  - A recent Egress survey on data privacy in the U.S. found that 83% of companies have suffered an accidental data breach.[3]

Egress analysis:

This perception gap points to a major challenge for businesses. Insider data breaches are viewed as frequent and damaging occurrences that are of major concern to 95% of IT leaders, yet the vectors for those breaches – employees – are either unaware of, or unwilling to admit, their responsibility.

While the majority of employees were hesitant to admit to being the cause of a data breach, those that did own up to intentionally sharing sensitive data showed a worryingly blasé attitude towards company information.

According to the survey:

- 55% of employees who shared data intentionally claim they did so because they didn't have the security tools necessary to share information safely.
  - This points to employees' determination to 'get the job done', even if that means deliberately sharing data insecurely.
- 23% of employees who shared data intentionally stated that they took information with them when they left the company to go to a new job.
  - Regionally, this was one of the biggest gaps between U.S. and U.K. respondents – 29% of U.K. employees stated they have taken data to their next job, compared to only 11% of U.S. employees.
- 13% of employees who intentionally shared or removed data did so as an act of defiance because they 'were upset at the organization'.

[3]https://www.egress.com/news/data-privacy-survey-2019

Who owns company data?

One of the most startling reasons given for intentional data breaches came from the one-in-five respondents who felt that the data belonged to them, and therefore they had the right to share it as they wished. This concerning evidence of employees' proprietary attitude to company data is underlined by the fact that only 40% of respondents agreed that data is exclusively owned by the organization and not by teams / departments or individuals.

A proportion of employees seem to be working under the misconception that the data they collect, manage and distribute belongs to them personally or to their department and that, as a result, they may choose how and with whom it is shared.

The research also indicated a generational divide in attitudes towards data ownership. Younger employees (aged 16-24) were less likely to agree that the organization is the exclusive owner of company data (33% agreed), compared with 51% of those aged over 65.

Overall, this finding may shed light on why IT leaders think employees are putting data at risk more than employees think they do: employees do not view company data ownership with the same perspective as IT leaders, therefore they simply don't see the associated risks. They may not even believe that they have done anything wrong in sharing data insecurely.

This highlights that user education around data ownership should be a priority for organizations. Employee responsibility for the protection of companies' intellectual property must be made clear through policies, HR contracts and ongoing training.

Employee motivation for intentionally sharing data - regional breakdown

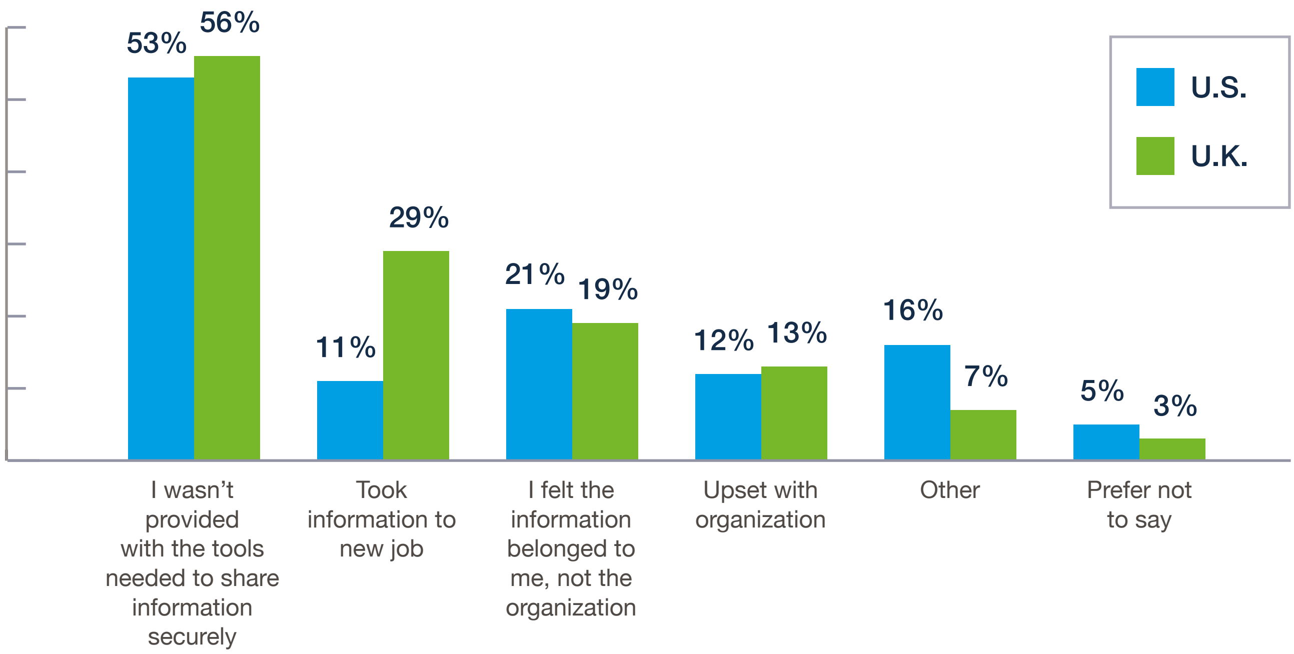


Fig. 5: On occasion(s) where you have intentionally shared or removed company information against company rules, what was your motivation for doing this?

Stop accidents from happening

Accidents happen, but accidental data exposure represents a significant risk. The explosive growth of unstructured data in email, messaging apps, and collaboration platforms has made it incredibly simple to share information. As a result, it's easier than ever before for employees to accidentally share company information in a manner that does not conform to corporate or regulatory policy.

- 45% of employees who accidentally shared information sent it to the wrong person, while over one-third shared information that they were unaware shouldn't be shared (35%).
- Employees who have accidentally shared information also put data at risk by exhibiting poor security practices: 27% have clicked on a phishing link, while 12% responded to a spear phishing email and shared data.

The Insider Data Breach survey 2019 also looked into the mentality behind the accidental breaches. According to the survey:

- 48% of employees who accidentally shared data believe they caused an accidental data breach by 'rushing.'
- 30% blamed a high-pressure work environment.
- While 29% claimed they did it because they were tired.

Employees' reason for **accidentally sharing** company data

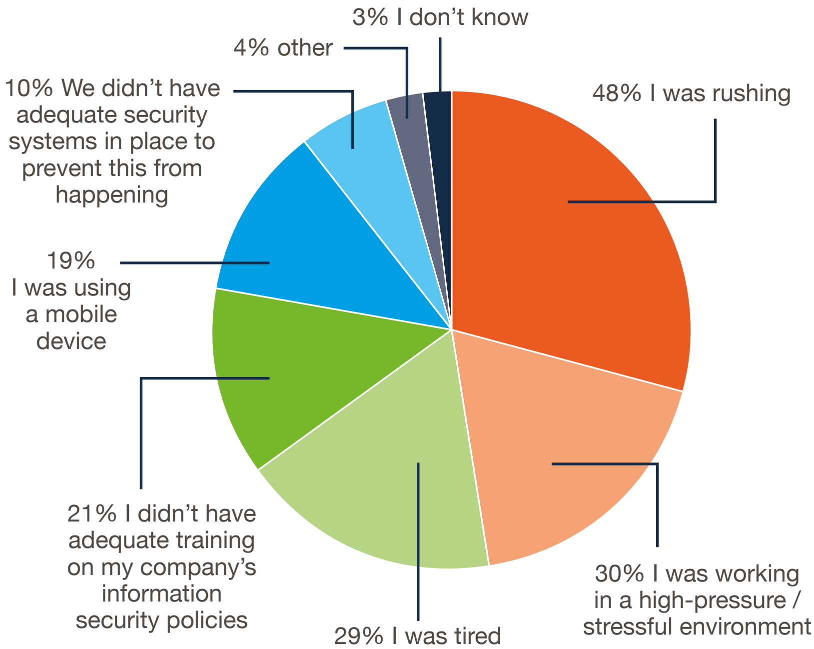


Fig. 7: Why do you think this incident happened? (Tick all that apply)

Employees' method for **accidentally sharing** company data

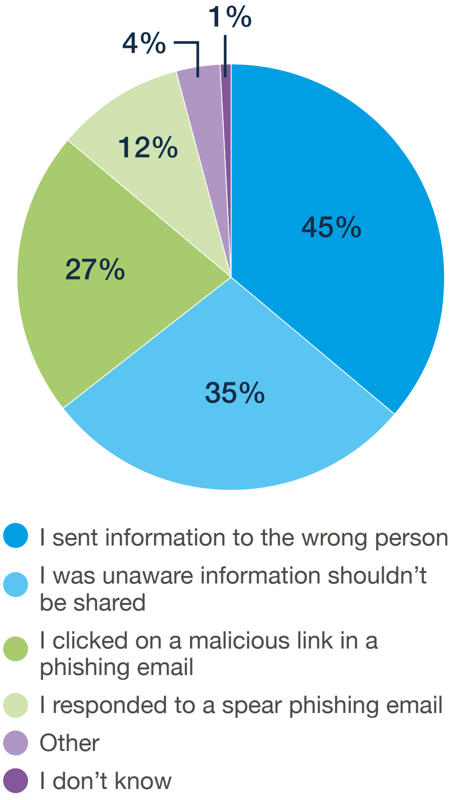


Fig. 6: How did you accidentally share the company information? (Tick all that apply)

The ubiquity of email, and the growing use of FTP sites and file sharing services like Dropbox and Slack mean that employees have more vectors and tools available to share information than ever before. Combined with automated features like Outlook's auto-insert, the opportunities for accidental data breaches are growing exponentially.

Security spending needs to align with the collaborative workflow across an organization, anticipating the most likely path for accidental breaches and mitigating them before they happen.

Summary

IT leaders are rightfully concerned by insider data breaches and believe that there is a likelihood of them occurring in the near future at their organization. Despite this recognition and understanding of the root causes, they still can't seem to prevent them from actually happening. The result is loss of brand equity; heavy compliance fines; and potentially lost revenue, lost customers and lost competitive advantages.

The Insider Data Breach survey 2019 highlights the clear disconnect between IT leaders and employees in terms of their understanding of data ownership and what is appropriate behavior when sharing information – a potential reason for this ongoing rise in data breaches.

When employees do recognize that they may have caused a breach, they attribute it to a high-pressure work environment, rushing to get a job done, and poor training.

Equally concerning, 60% of employees don't believe the organization has exclusive ownership over data, favoring instead departments and individuals.

> "60% of employees don't believe the organization has exclusive ownership of data, favoring instead departments and individuals."

The research also highlights that attitudes towards data ownership and responsibility vary significantly between generations. In today's multigenerational workplace, this has implications on the design of training / user education programs, which should be tailored to the profiles of the employees.

This disconnect shows that policy-driven decisions are not enough to secure data and that 'employee trust' should not be used as a foundation for security.

At the heart of the problem is the growth of unstructured data – the data that employees use and interact with continually to do their jobs. Compounding this issue is the explosion of data sharing tools that employees use both inside and outside of corporate perimeters, and the fact that employees do not place the same value on company data as their C-level counterparts.

As a result, IT leaders need to enforce data policies with security tools that are intuitive and easy to use, provide broad support to both end-users and the business, and automate the enforcement of regulatory and corporate data policies.

Appendix

Commissioned by Egress and conducted by independent research company, Opinion Matters, the Insider Data Breach survey 2019 gathered responses from 252 U.S. and 253 U.K.-based IT leaders and 2,004 U.S. and 2,003 U.K.-based employees to assess the root causes of these employee-driven data breaches, as well as the frequency and impact of such instances.

"The results of the survey emphasize a growing disconnect between IT leaders and staff on data security, which ultimately puts everyone at risk. While IT leaders seem to expect employees to leak data – they're not providing the tools and training required to stop the data breach from happening," said **Tony Pepper, CEO and co-founder, Egress**. "Technology needs to be part of the solution. By implementing security solutions that are easy to use and work within the daily flow of how data is shared, combined with advanced AI that prevents data from being leaked, IT leaders can move from minimizing data breaches to stopping them from happening in the first place."

> "By implementing security solutions that are easy to use and work within the daily flow... IT leaders can move from minimizing data breaches to stopping them from happening in the first place."
>
> **Tony Pepper, CEO and co-founder, Egress**

Opinion matters

About Opinion Matters

Opinion Matters is an award-winning insight agency whose consultants create bespoke market research solutions for businesses, organizations and agencies worldwide. Opinion Matters is an expert in creating concepts, implementing and managing projects, analyzing results and reporting. As communications specialists with a wealth of experience in research, PR and marketing, Opinion Matters unlocks information that helps its clients hit the right note in understanding and communicating with their market.