proofpoint

Compliments of:

www.bytes.co.uk

REPORT

The 2024 Data Loss Landscape

Global cybersecurity insights into departing users, determined attackers and misdirected email

proofpoint.com

INTRODUCTION

Welcome to the inaugural edition of our Data Loss Landscape report. In these pages, we'll explore the current state of data loss prevention (DLP) and insider threats across 12 countries and 17 industries. This is a new category of report for Proofpoint. But we believe it is in keeping with our core principle: that people are a critical variable in data security.

Every year, a handful of vulnerabilities and zero-day attacks create headlines and headaches for security teams. But beyond these technical issues, most analysts recognise that data is typically lost by users rather than system vulnerabilities and misconfigurations. The underlying cause in these cases could be simple carelessness, credentials stolen by a threat actor, or in extreme examples, a malicious insider taking advantage of privileged access to steal valuable data and intellectual property.

Complicating the situation still further are a handful of macro factors affecting organisations of every size. Cloud workflows have changed how data is stored, accessed and synchronised. Hybrid work has multiplied the number of environments in which sensitive data is consumed. Generative AI is absorbing common tasks and confidential data. And resourceful threat actors are constantly innovating to take advantage of any lapses in vigilance and using emerging technologies to improve their techniques.

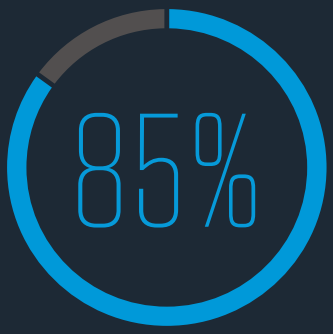
Taking all these issues together, it makes sense to ask: are current DLP approaches holding up against today's challenges? To answer this question, we surveyed 600 security professionals about the current state of DLP around the world. And we've supplemented those answers with data from our own Proofpoint information protection platform to convey the scale of the challenges organisations face in addressing data loss and insider threats.

TABLE OF CONTENTS

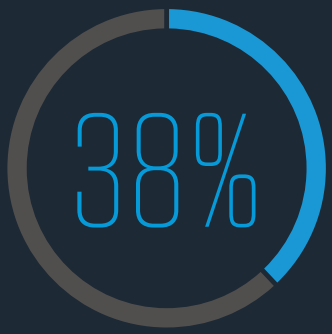
KEY FINDINGS

"Careless users" were the most cited cause of data loss.

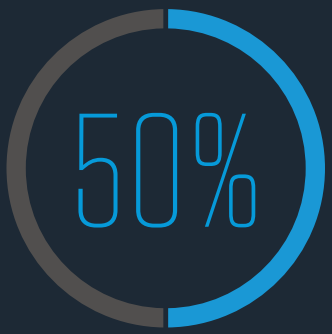
Generative AI is the fastest growing area of concern.



of organisations experienced one or more data loss incidents in the past year.

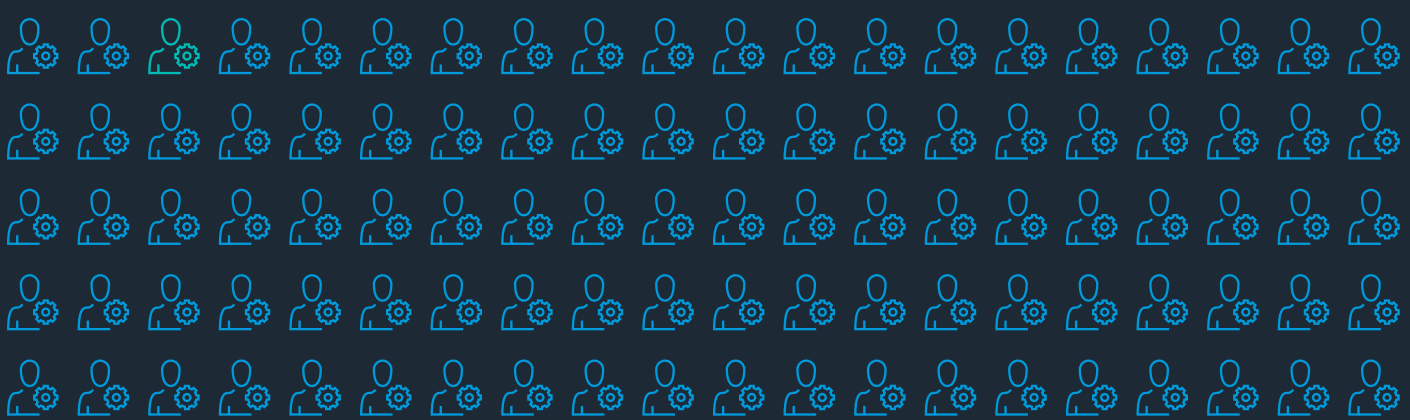


Only 38% of organisations have a "mature" DLP programme.



Data loss is disruptive: over 50% reported business disruption as a consequence.

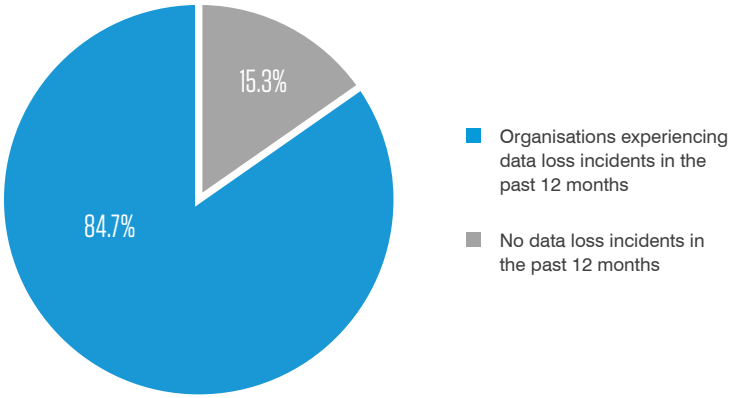
1% of users are responsible for 88% of data loss events.



Data Loss Is a People Problem

The vast majority (85%) of organisations polled in our survey experienced at least one data loss incident in the past year, showing just how widespread this issue has become. The mean number of incidents per organisation was just over 15, amounting to more than one incident a month. While these findings are not surprising given the shift to hybrid work, accelerated cloud adoption and high rates of employee turnover, they are sobering and illustrate the scale of the problem. In fact, 10% of respondents reported more than 30 separate incidents apiece. English-speaking countries enjoyed slightly lower rates overall. But even the country with the lowest percentage – the United Kingdom – still had 73% of respondents reporting at least one incident in the past 12 months.

Organisations Experiencing Data Loss Incidents



The prevalence of data loss across countries and industries begs an obvious question: what's causing all these incidents? Our survey provides a surprising answer, with "careless users" (including general employees, IT workers and contractors/vendors) selected by more than 70% of respondents. Examples of carelessness include:

- Misdirected emails
- Visiting phishing sites
- Installing unauthorised software
- Sharing sensitive files publicly
- Emailing personally identifiable information (PII) to a personal email account
- Any other unintended user exposure of systems or data

WHAT IS A CARELESS USER?

Data loss isn't always the result of deliberately malicious activity. Sometimes mistakes are made. Of course, with data loss it doesn't matter if the door was kicked down by an intruder or left open by a careless employee – the consequences can still be severe.

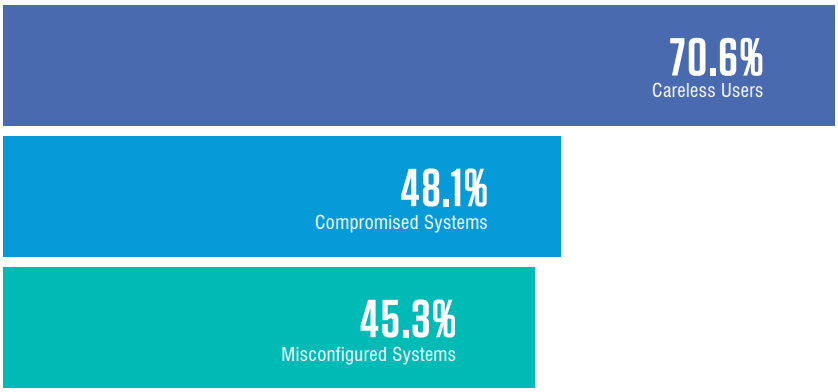
In February 2023, around 14,000 employees of the **Liverpool NHS trust in the U.K.** found out that their personal data had been shared with hundreds of NHS managers and 24 people outside the organisation. In an apology letter to victims, the trust's chief executive explained that a spreadsheet file with a hidden tab had been attached to an email. Although the hidden tab was not visible to recipients, employees' names, dates of birth and even salaries were exposed. The organisation worked swiftly to make things right, but it didn't change the fact that personal information was shared – a situation in clear violation of GDPR laws.

1%

of users are responsible for 88% of data loss events. The identity of this 1% is likely to change month to month.

Technical causes appear next, in the form of compromised (48%) and misconfigured (45%) systems, with lack of time and resources adding a significant human element to these issues.

Top Causes of Data Loss



The message from practitioners is clear: data loss is a problem caused by the interaction between people and machines. And where people are concerned, there are clear opportunities to limit future mishaps with contextual user prompts and targeted cybersecurity awareness training.

Twenty percent of respondents said a malicious employee or contractor was behind their incident. While this number is significantly lower than those who attributed data loss to a careless user, the consequences can be much greater. Malicious users are motivated by personal gain and are looking to do harm to an organisation's data, systems and networks. Examples could be application misuse, system sabotage and industrial espionage. Departing employees also fall into this category. Incidents with malicious insiders may also result in litigation, which can be costly.

Using data from the Proofpoint information protection platform, we took a closer look at the human factor of data loss. It turns out that only a very small number of users are responsible for DLP alerts. In fact, for most organisations, only 1% of users are responsible for 88% of alerts. While this might imply that the risk is contained, the reality isn't quite that simple. In a modern workplace, with employees regularly joining, leaving and changing jobs, and circumstances constantly shifting, the identity of this 1% is likely to change month to month. And the remaining 12% of alerts still carry a significant risk – especially as insiders may approach data theft slowly, exfiltrating important documents periodically to avoid detection. So, while the target is reassuringly small, security teams must stay alert to keep ahead of this cohort of risky users.

1/3 of users

sent one or two email to the wrong recipient.

84%

of misdirected emails contained attachments last year.

One of the most common manifestations of user carelessness is misdirected email. With most webmail and native email clients offering address autofill, it's easy for users in a hurry to make mistakes. According to 2023 data from Tessian, which Proofpoint acquired last fall, the problem is widespread. About a third of users sent about two emails per year to the wrong recipient. That means a business of 5,000 employees can expect to deal with around 3,400 misdirected emails per year.

The consequences of sending an email to the wrong recipient can be severe. A misdirected email containing sensitive information is one of the simplest forms of data loss; once sent, the organisation is relying on the goodwill of recipients to ensure that the breach doesn't get any worse.

And even if the recipient is cooperative (or pays attention to the ubiquitous email footer boilerplate), there may still be regulatory implications. A misdirected email containing employee, customer or patient data may still trigger a significant fine under GDPR and other legal frameworks. And of course, even if no sensitive data is involved, emailing the wrong person, replying all, or using CC instead of BCC can cause embarrassment and reputational damage.

Beyond directing email to the wrong recipient, a careless user will sometimes send the wrong information to the right person, either in the email body or as an attachment. Basic email security systems may alert users when a recipient's address belongs to a different domain. But only advanced solutions can detect and alert them to the presence of sensitive information in attached files or email body. Tessian data suggests that in 81% of organisations, at least one user sent the wrong attachment in an email last year.

Counting the Costs

The high incidence of data loss reported in our survey is mirrored by an almost equal incidence of negative consequences. More than 90% of those who experienced at least one incident reported a negative outcome. Over half said the result was business disruption and almost 40% said their organisations suffered reputational damage. It's important to note that these consequences are not mutually exclusive. For example, a data loss incident can result in reputational damage that leads to lost revenue.

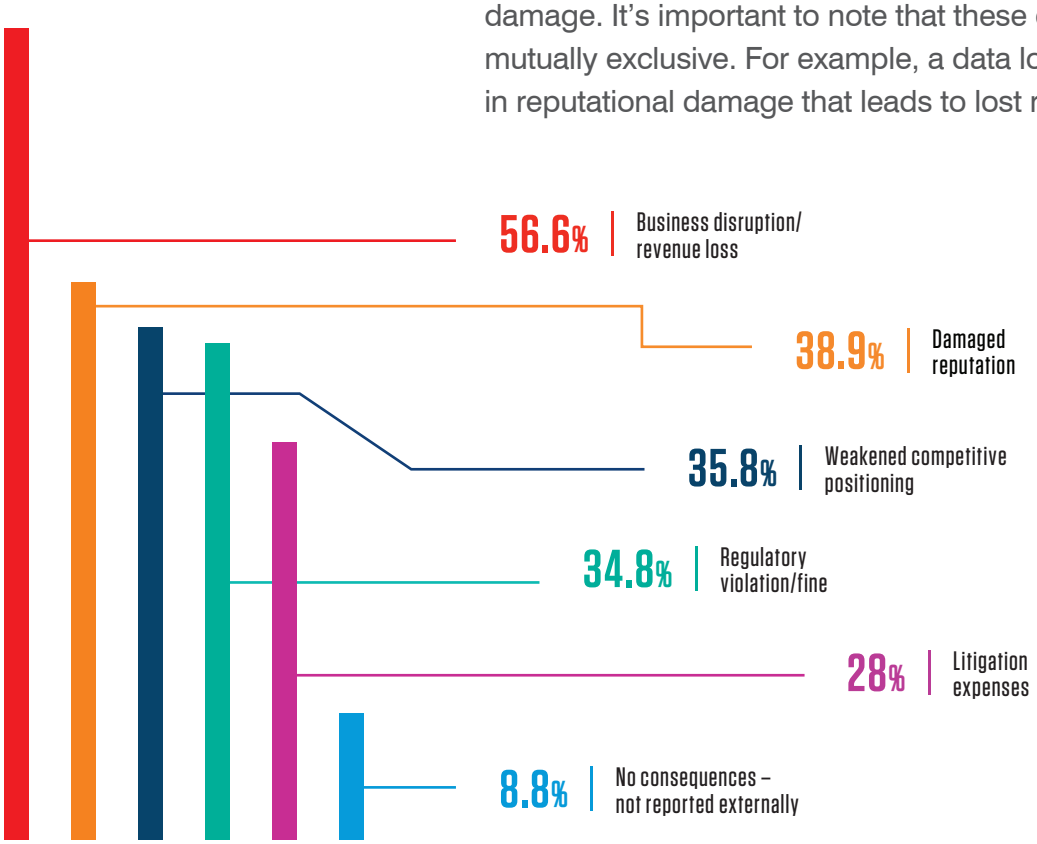


Figure 1. Consequences of data loss incidents

The likelihood of negative consequences was also shared evenly among both countries and industries. More than 97% of respondents from South Korea and Singapore said they suffered bad outcomes from data loss incidents. Ninety-six percent of retail business respondents said the same. But with more than 80% of all countries and industries reporting negative consequences, this is clearly a significant and universal challenge.

As for the 9% that said they suffered no consequences, as their incident was not reported, these respondents may be enjoying a false sense of security. Even if an incident is not reported in the moment, there is no guarantee that details will not eventually emerge. Additional reputational damage may accrue if it appears that an organisation has tried to cover up or evade responsibility. And as increasing amounts of regulation are imposed, organisations may soon have no choice in the matter.

80+%

More than 80% of all countries and industries reporting negative consequences.

Departing Users and Determined Attackers

The modern threat landscape presents security teams with challenges from all sides. Employee turnover, hybrid work, cloud adoption, generative AI and evolving attack techniques all threaten data security.

With resources spread thinly across all these surface areas, accurate risk assessment becomes a critical part of effective response. Our survey asked participants to weigh up which users present the greatest risk of data loss. Employees with access to sensitive data, such as HR professionals, finance teams and customer support personnel, were the most popular answer, cited by 63% of survey respondents globally. These employees often have access to valuable data such as PII and financial data, or in the case of HR employees, payroll, performance and medical leave records. An employee's role may also make them an attractive target to external threat actors, hoping to steal their credentials with a phishing email or bribe them into sharing intellectual property.

Only one country gave a different top answer – U.S. respondents named IT users with privileged access as the riskiest group. Respondents in manufacturing and technology industries also pointed to IT users as the top answer. This may reflect a greater awareness among these respondents of IT users' ability to manipulate or destroy data as well as steal it.

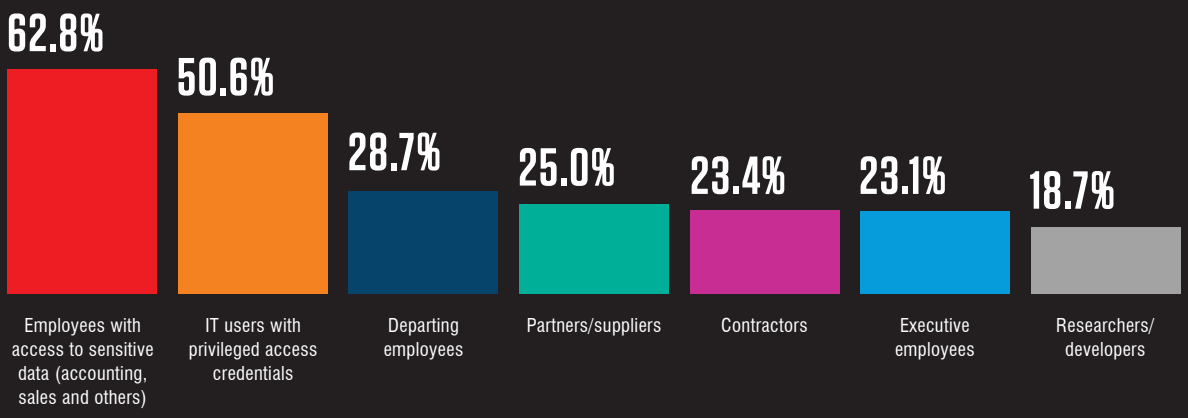
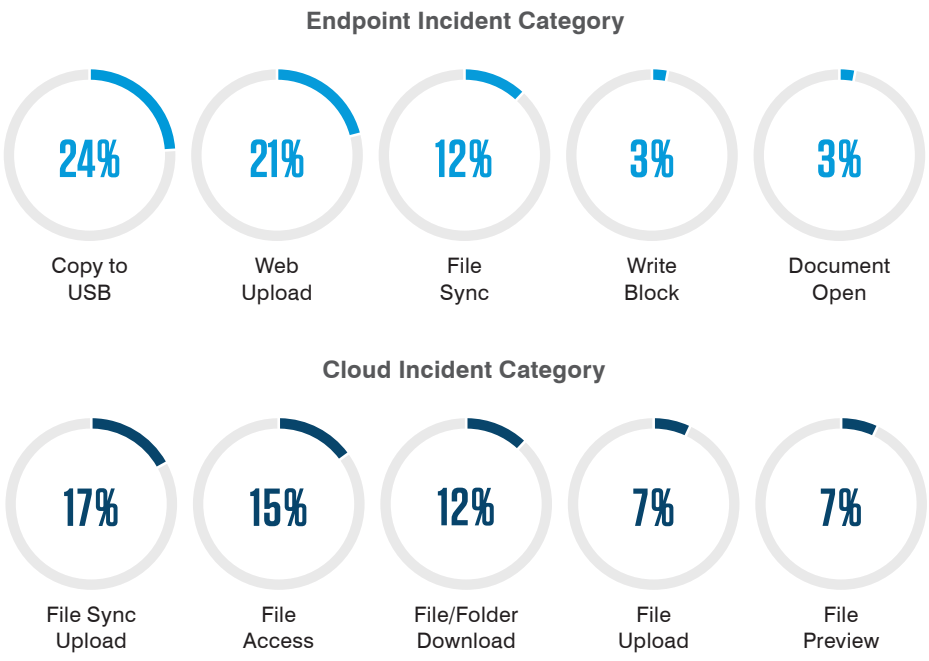


Figure 2. Users who pose the greatest risk for potential data loss incidents

Sounding the Alarm

The threat from careless, compromised or malicious users is reflected in the kinds of data alerts triggered on the Proofpoint information protection platform. Among endpoints, almost half of all alerts were caused by either copying files to USB or uploading them to the web. The top cloud incidents are more evenly spread, with various file upload and access operations featuring in the top five.



WHAT IS A MALICIOUS USER?

While it might be comforting to think of cyber criminals as distant figures in far-off places, sometimes the threat comes from in-house. In fact, insider threats can be even more dangerous than external attacks. Malicious insiders are able to bide their time, using privileged access to find valuable data and weak spots in security.

In December 2020, **Ubiquiti employee Nickolas Sharp** stole gigabytes of the company's confidential data. Sharp used the Surfshark VPN service to cover his tracks and to keep his identity hidden. He also used his administrative credentials to erase signs of intrusion on the company's server logs. Soon after, in January 2021, Ubiquiti publicly disclosed the breach. Luckily for Sharp, he was on the investigating team. Meanwhile, behind the scenes, he continued with his plot. Posing as an anonymous hacker, Sharp demanded that Ubiquiti pay 50 bitcoins (approximately $1.9 million at the time) in return for the files he'd stolen and details about the vulnerability he'd exploited. Ubiquiti refused to pay the ransom. In response, Sharp leaked a portion of the files on a public platform.

Two months later, the FBI executed a search warrant on Sharp's home and seized some of his electronic devices. Unfazed, Sharp approached the media pretending to be a whistleblower. He claimed the company was downplaying the breach. When the false story broke, Ubiquiti's stock tumbled 20% in a single day. No matter the setback, Sharp didn't give up his get-rich-quick scheme. Eventually, however, a technical glitch was his downfall. It turned out that during the original data theft, his VPN experienced a temporary outage, exposing his home IP address. In May 2023, Sharp was sentenced to six years in prison.

The prevalence of USB notifications on the endpoint list is perhaps unsurprising, as these are the most common category of alerts configured by administrators using our products. Beyond file activities, Active Directory changes in fourth place attest to the significant risk to networks from internal and external threats. In fifth place comes use of generative AI sites. While this alert wasn't triggered often enough to feature among the top notifications, its presence on the list of configured alerts shows how seriously security professionals are taking this new risk to data security.

Most Configured DLP and Insider Threat Alert Rules

- Copy to USB
- Exfiltration by web upload
- Exfiltration to cloud synch folder
- Changes to Active Directory
- Browsing generative AI sites

The presence of generative AI is particularly noteworthy as a rule for this action has only been available starting this year. The risk of users inputting sensitive data into systems such as Grammarly, ChatGPT, Bing Chat and Google Bard is growing daily as these tools increase in power and utility. But with little transparency about how the data submitted is stored and used, and even less clarity about how it can be removed or deleted if sent in error, these systems clearly represent a risky new channel through which data can leak. While some companies have banned the use of generative AI sites altogether, others recognise the productivity benefits they can provide and have instead opted to monitor use.

Departing Dearly

Security professionals consider departing employees the third riskiest category of user – a risk no doubt enhanced when leavers have had access to privileged or sensitive data during their employment. Departing employees often feel a sense of entitlement to information when leaving, given the time and effort they put into an initiative, product or project. This information may also give them a head start for their next opportunity.

Data from our platform backs up this concern. Over a nine-month period, 87% of anomalous file exfiltration among cloud tenants using Proofpoint was caused by departing employees. This unusually high volume may signal that an employee is hoarding files and data before they leave. Allowing data access and storage on employees' personal devices can offer companies a productivity gain, but it's easy to see how quickly this policy can turn into a potential data loss risk.

Dark Cloud Overhead

Nearly 38% of respondents said that the proliferation of cloud/SaaS applications is a challenge for their DLP programmes. With many businesses now fully embracing cloud solutions due to the shift to hybrid work and digital transformation, these data stores are a rich target for attackers.

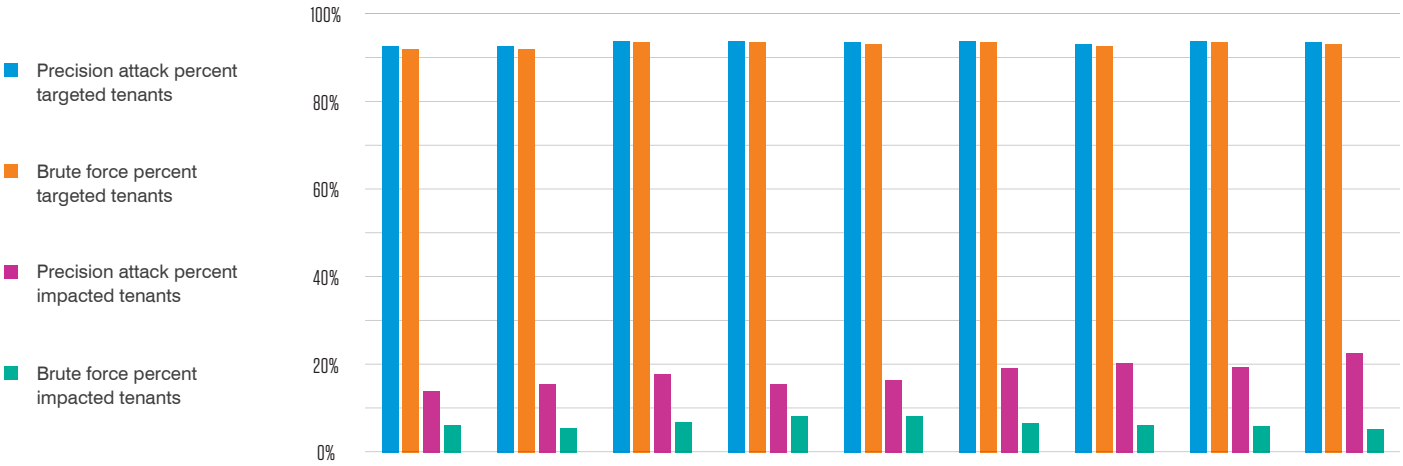


Figure 3. Attack vectors over time

The risk to cloud tenants is borne out by threat data from our platform. Between January–September 2023, 96% of monitored cloud tenants were targeted by brute-force attacks. In a brute-force attack, threat actors try to gain access by password guessing or other automated means. More worryingly, over the same period, 96% of tenants were subject to precision attacks, such as targeted phishing attempts. And many of these more sophisticated attacks were successful, with 54% of tenants breached at least once, compared to just 20% being successfully breached by brute force methods.

This huge difference in efficacy can be explained by the use of social engineering and sophisticated toolkits that allow attackers to bypass advanced security mechanisms such as multi-factor authentication (MFA). But across all attack types, external threat actors had a 58% overall success rate when trying to infiltrate cloud tenants, showing that they recognise data loss is people-centric and are looking to exploit users' vulnerabilities.

WHAT IS A COMPROMISED USER?

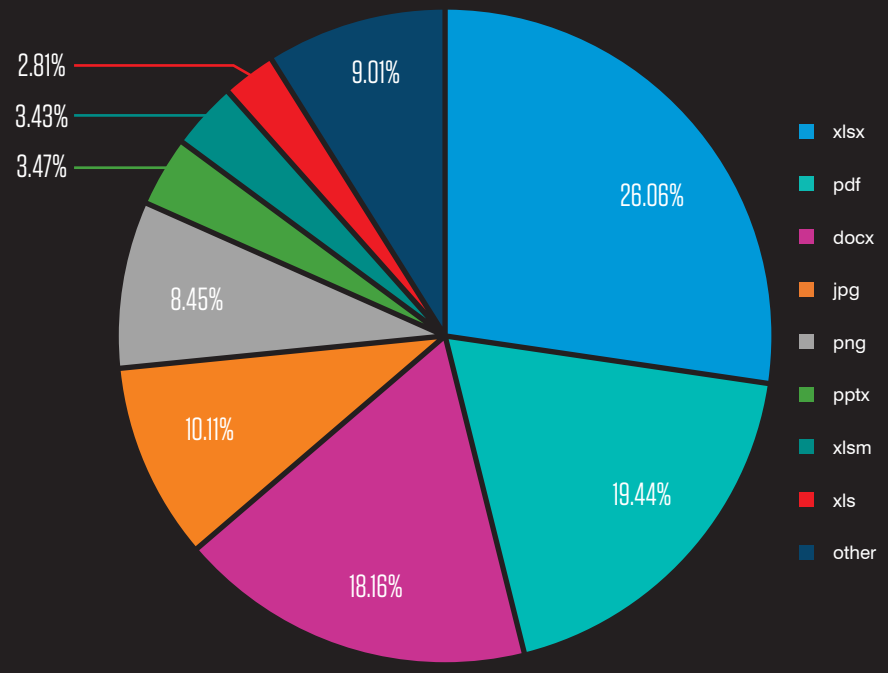
Zero-day vulnerabilities might make a lot of headlines, but there's a reason most large-scale cyber attackers focus on bypassing people rather than systems. Employees in finance, human resources, customer support and IT can have access to troves of valuable data. Compromising the identity of an employee with high privileges can open an entire network to lateral movement, data theft and ransomware infection – with the latter now often including both data encryption and data exfiltration as attackers engage in double extortion.

In 2022, one of the world's most popular password managers, LastPass, suffered a major data breach that resulted from a single compromised user. The trouble started in August 2022, when LastPass revealed that an unauthorised person had gained access to its development environment through a compromised engineer's home computer. During the attack, a keylogger was installed and source code was stolen. And the attack was just getting started. Over the next two months, the attacker accessed more information, including employee credentials and decryption keys. With valid credentials, the attacker was able to work undetected for several months. Later, the stolen keys came in handy for decrypting storage volumes within the company's Amazon S3 buckets. Once inside, the attacker exported a wide range of data, including customer password vaults. From a single compromised user, an attack unfolded that eventually undermined confidence in password management as a security best practice.

When a cloud tenant is compromised, attackers will often begin exploring stored files and other data. Thirty percent of breached tenants were observed to have experienced post-compromise data exfiltration or file manipulation, with Office documents such as .docx, .xlsx and .pdf having the highest levels of suspicious activity. The .docx file type being the most prevalent may reflect an evolution beyond the highly structured, regulated data often found in .xlsx. Attackers know that valuable corporate data is now being captured in less structured documents, so this is where they are looking.

For instance, in a recent incident investigated by Proofpoint, attackers accessed several sign-in apps, including Azure Portal and Office 365 SharePoint Online to compromise the account. They either uploaded, modified, previewed or downloaded 45 sensitive files. In a similar case, an attacker exfiltrated four Excel files that included the word "Payroll' in the file name.

Breakdown of File Types in Suspicious File Activities



Cloud workspaces are also increasingly under threat from malicious or abused OAuth applications. Like traditional malware, a malicious OAuth app can give threat actors the freedom to do as they please on an infected tenant. In our data, we found 11% of cloud tenants were impacted by persistent malicious OAuth apps. But the threat isn't limited to specific malicious applications. Legitimate cloud applications are now commonly abused by attackers to give them persistent access to a tenant after compromise. This is because an OAuth application remains authorised until its access is revoked. We found that more than 15% of compromised organisations experienced this kind of authorised app abuse after an initial breach.

Maturing Beyond Compliance

Many DLP programmes were first spun up in response to legal regulations. But according to respondents, regulation and compliance are no longer the main drivers. It appears that as these initiatives mature, focus is shifting to protecting customer and employee privacy, with over 50% of respondents citing these as a primary driver for their DLP programme. While some of this is doubtless linked to new privacy regulations being introduced at local and international levels, there appears to be a real desire to do more than simply comply with the legal minimum.

Figure 4. Primary motivational drivers for DLP programmes

However, there are outliers, particularly in Europe, where strict data protection laws exist such as the General Data Protection Regulation (GDPR). Respondents from France and the U.K. both said conforming with external regulations was their chief DLP motivator. On the other hand, respondents in Spain and Brazil were the least likely to give regulation as a key reason, at around 18% each. Respondents in Germany also cited minimising costs associated with data loss and protecting intellectual property as their second and third drivers after privacy. In South Korea, internal compliance was the top factor, with external compliance the second most cited response.

At an industry level, regulation was the key driver among finance respondents – unsurprising, given the typical degree of oversight those organisations face. Healthcare and government respondents also gave it as their second most common response.

However, the picture becomes a little more complex when we look at the categories of data respondents said were most important to protect. Here, valuable corporate data was the most common answer, with customer information close behind. Healthcare is an understandable outlier at an industry level, with protected health information being cited by 60% of those respondents.

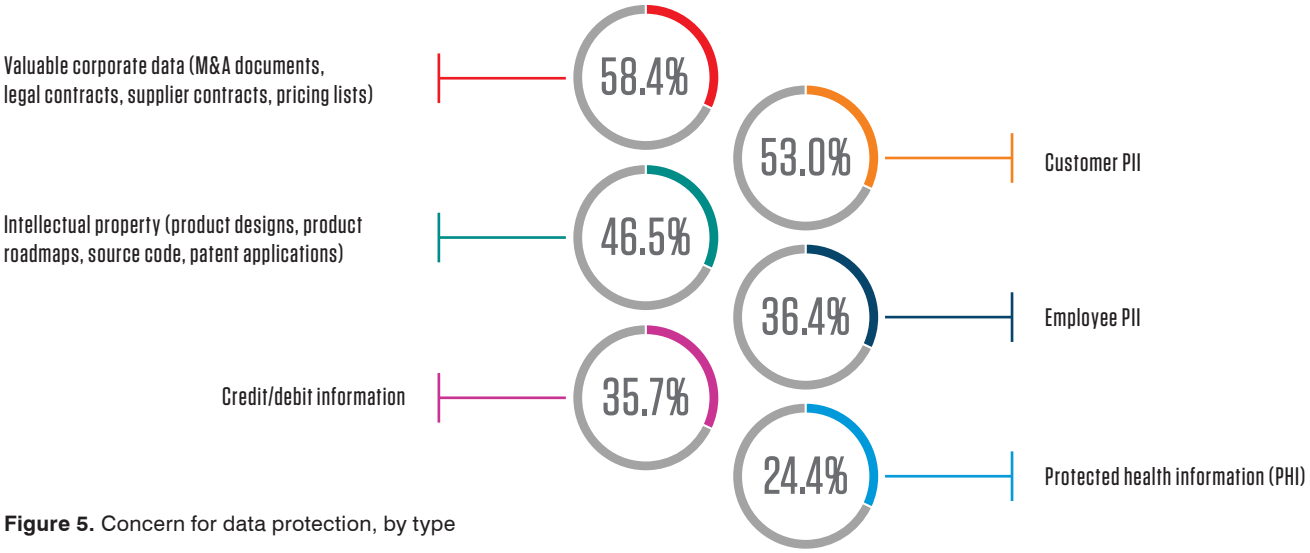


Figure 5. Concern for data protection, by type

DLP MATURITY LEVELS

Emerging: Organisations with a limited or no formal DLP programme. They may leverage point solutions that have some DLP capabilities (CASB, IPS, SWG, SEG).

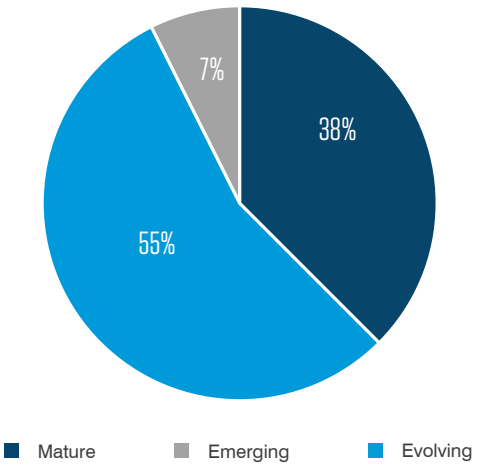
Evolving: Organisations with a formal DLP programme across some DLP channels. Used primarily for auditing and reporting purposes.

Mature: Organisations with a formal DLP programme across key DLP channels with classification and automated prevention and remediation.

This focus on "valuable corporate data" – a nebulous category that includes contracts, price lists and M&A documents – possibly reflects the growing maturity of DLP platforms as much as it does a change in priorities. DLP systems were initially designed to protect highly structured data, such as payment information, citizen ID numbers and user accounts. But many are now flexible enough to monitor and protect data in non-static domains, where information flows in and out in the daily course of business. Innovative DLP solutions have adjusted to recognise the growth in the diversity and volume of data driven by digital transformation. For example, non-traditional categories such as source code and CAD designs could now represent an organisation's most valuable intellectual property.

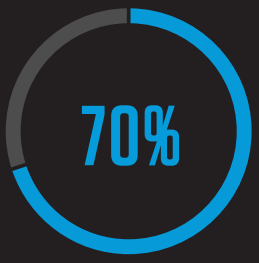
But while DLP programmes and technology are undoubtedly maturing, only a little over a third of respondents rated their programme as fully "mature." The majority rated themselves as "evolving" – so we can expect the balance of drivers and data prioritisation to keep shifting as overall levels of maturity increase.

Status of DLP Programme Maturity, Globally



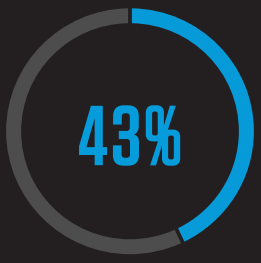
Looking Ahead: Better Visibility, More Expertise

As DLP programmes mature, respondents largely agree about the most significant ongoing challenges. Almost 70% cite visibility into sensitive data, user behaviour and external threats as the most important capability for their DLP programme. But 43% say that this is an area where improvements are still needed. Given a distributed modern workforce, (increasing access to data across email, endpoint, web and cloud) and the sophistication of threat actors, it is not surprising that visibility is seen as the most important DLP capability. Visibility across multiple channels is what gives security teams the context they need to respond appropriately to a careless, malicious or compromised user.



cite visibility into sensitive data, user behaviour and external threats as the most important capability for their DLP programme

but



say that this is an area where improvements are still needed.

In terms of resourcing, most respondents said they were happy with the level of investment and executive support for their DLP programme. This might seem surprising considering the never-ending arms race between malicious actors and defenders. But it does at least validate the idea that data security has become a C-level issue and that senior leaders appreciate the need to protect their organisation's "crown jewels." With no shortage of high-profile incidents making global headlines, many executives and boards will be conscious of avoiding the fate of others in their industry.

70%

of respondents said that visibility into sensitive data, user behaviour and external threats were the most important DLP capabilities for defending their organisations against data loss.

However, the picture is a little different among those who rate their DLP programme as "emerging." Here, respondents are more likely to cite an ongoing need for bigger budgets and tools that improve visibility across all channels. It may be the case that these respondents are still using tools restricted to a single channel, unable to provide a holistic picture of potential data loss and insider threats.

Beyond better visibility, the other agreed-upon areas for future improvement are closer integration with the IT/security ecosystem and the need for more qualified personnel. The security industry is highly fragmented with many niche solutions addressing specific pain points. While the development of new solutions means new capabilities, it also puts a burden on security teams to ensure that everything works together seamlessly. If not, they run the risk of losing valuable time switching from tool to tool.

Respondents who rated their programmes as "mature" also expressed a growing desire for AI-powered tooling. With the ongoing shortfall in qualified security practitioners, AI has the potential to amplify analyst output and efficiency while reducing risk of burnout.

Conclusion

Over 90% of respondents in our survey said that their organisations are currently investing in DLP solutions – good news for consumers, employees and shareholders. However, only 41% strongly agreed that their investments were adequate.

Only 41%

of respondents strongly agree that their current level of investment in DLP tools and expertise is adequate.

As more organisations embrace the cloud, hybrid work and workflow innovations like generative AI, DLP solutions must do the same. Every insider threat and data loss incident is unique and has the potential to cause significant consequences. That's why detecting, investigating and responding to each one requires an approach that recognises data loss as a people problem, and that includes visibility into user behaviour, content and threats. And it needs to do so across multiple channels – cloud, endpoint, email and web. Whether DLP is mature, evolving or emerging, security teams should have processes in place to ensure the following as a minimum:

- Monitor people with access to sensitive data or have admin privileges.
- Establish a security review process for departing employees.
- Implement DLP policy rules for common data exfiltration methods such as email, copy to USB, web upload, file sync to cloud and broad sharing of files in the cloud.
- Identify and protect your "crown-jewels" and business-critical data by using data classification.
- Regularly review your DLP programme, keeping in mind that adoption of generative AI and other developments are likely to change user behaviour.

Beyond this checklist, moving past "emerging" means investing in a purpose-built DLP platform with a cloud-first, modern architecture. By providing user and data visibility into every incident, a robust DLP platform gives vital context so that security teams know how to respond. That way, you can tackle the full spectrum of people-centric data loss scenarios, from thwarting external threats to preventing malicious, careless and compromised users within your ranks.

Methodology

Proofpoint Internal Data

Data was sourced from our Proofpoint information protection platform between January–September 2023 and from randomly selected Tessian deployments between January and December 2023.

Survey Data

Proofpoint partnered with cybersecurity market research firm, CyberEdge Group, to develop the 15-question survey instrument, to localise the survey instrument into non-English languages, to host the survey, to facilitate survey completions by qualified research participants and to analyse survey results. Respondents are IT security professionals employed by a commercial, non-profit or government organisation with 1,000 or more employees.

Research participants were drawn from 12 countries and 17 industries. With a sample size of 600 participants, the global survey margin of error (at a standard 95% confidence level) is 4%. All results pertaining to individual countries and industries should be viewed as anecdotal, as their sample sizes are much smaller. Proofpoint recommends making actionable decisions based on global data only.

About CyberEdge Group

Founded in 2012, CyberEdge is the largest research, marketing and publishing firm to serve the cybersecurity vendor community, working with approximately one in every six established security vendors.

CyberEdge's highly acclaimed Cyberthreat Defense Report (CDR) and other single- and multi-sponsor survey reports have garnered numerous awards and have been featured by both business and technology publications alike, including The Wall Street Journal, Forbes, Fortune, USA Today, NBC News, ABC News, SC Magazine, DarkReading, CISO Magazine and others.

CyberEdge has cultivated a reputation for delivering the highest-quality market research data, survey reports, analyst reports, white papers and custom books and eBooks in the cybersecurity industry. The depth of its cybersecurity subject matter expertise and the breadth of its services are second to none.

To learn more about CyberEdge, connect to **www.cyber-edge.com**.

proofpoint.

About Proofpoint, Inc.

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organisations of all sizes, including 85 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at www.proofpoint.com.

0407-001-02-01 01/24