



TESSIAN

THE STATE OF DLP 2021

Data Loss Prevention in Healthcare

Data loss prevention (DLP) is a top priority for security leaders across industries, especially in healthcare. But, most don't have clear visibility of data movement or employee behavior, which means preventing data loss and avoiding breaches can be an uphill battle. Our latest research can help.

Share this report





[Jump to Page 10 ↗](#)

57%

of employees working in healthcare say they'll find a workaround for security policies and technology.

800+

[Jump to Page 5 ↗](#)

misdirected emails are sent every year in firms with 1,000 employees



85%

of security leaders say rule-based DLP is admin-intensive.

[Jump to Page 10 ↗](#)



49%

of employees working in healthcare say security software impedes their productivity at work.

[Jump to Page 10 ↗](#)



Nearly half

of employees working in healthcare say they're less likely to follow safe data practices when working remotely .

[Jump to Page 7 ↗](#)



38x

more unauthorized emails are sent than security leaders estimate.

[Jump to Page 5 ↗](#)

35%

of employees working in healthcare admit to exfiltrating data before leaving a job.

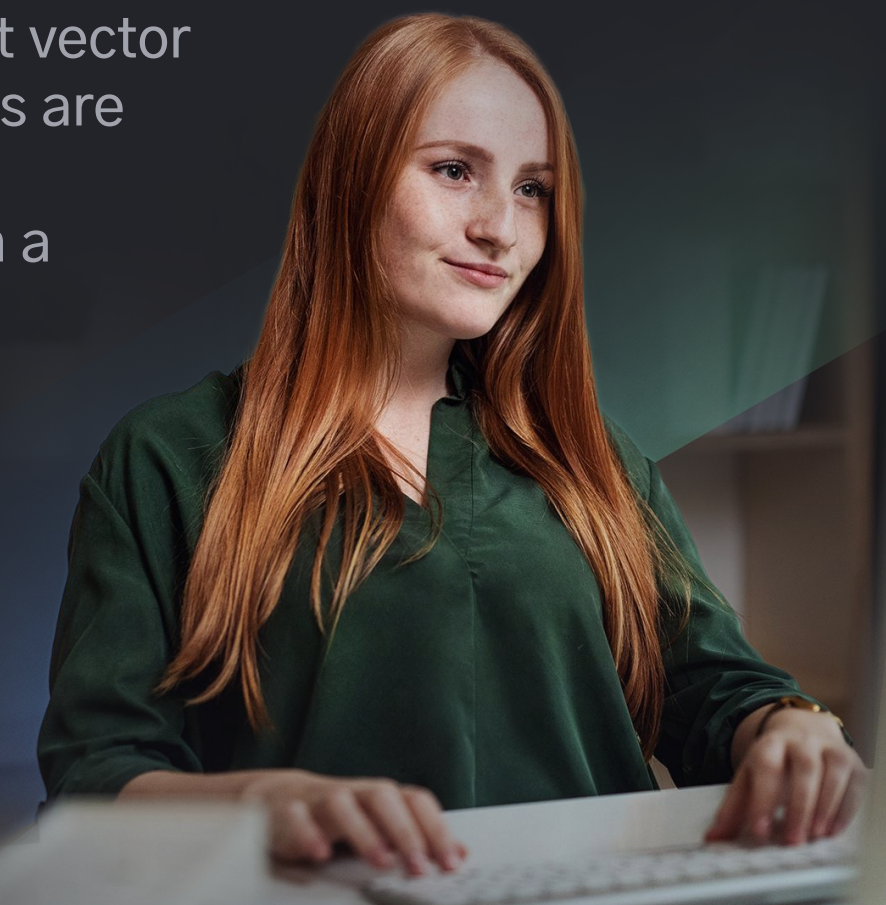
[Jump to Page 8 ↗](#)



Email

is the #1 threat vector security leaders are worried about protecting with a DLP solution.

[Jump to Page 4 ↗](#)




The healthcare DLP landscape

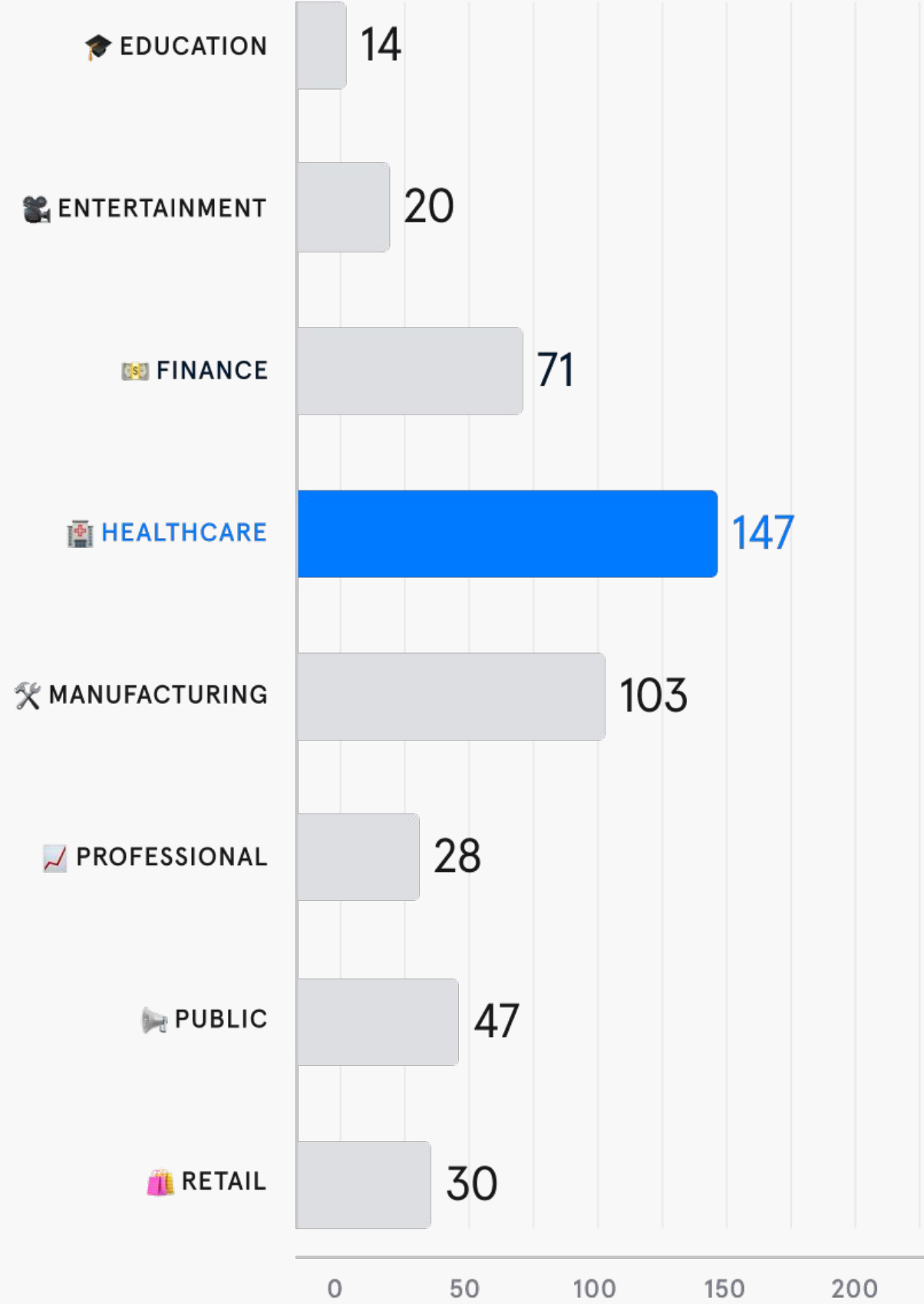
Across B2B and B2C, employees working in healthcare process and hold incredible amounts of personal and medical data, research and development (R&D), and Intellectual Property (IP).


Unfortunately, this makes the industry especially vulnerable and prone to breaches.

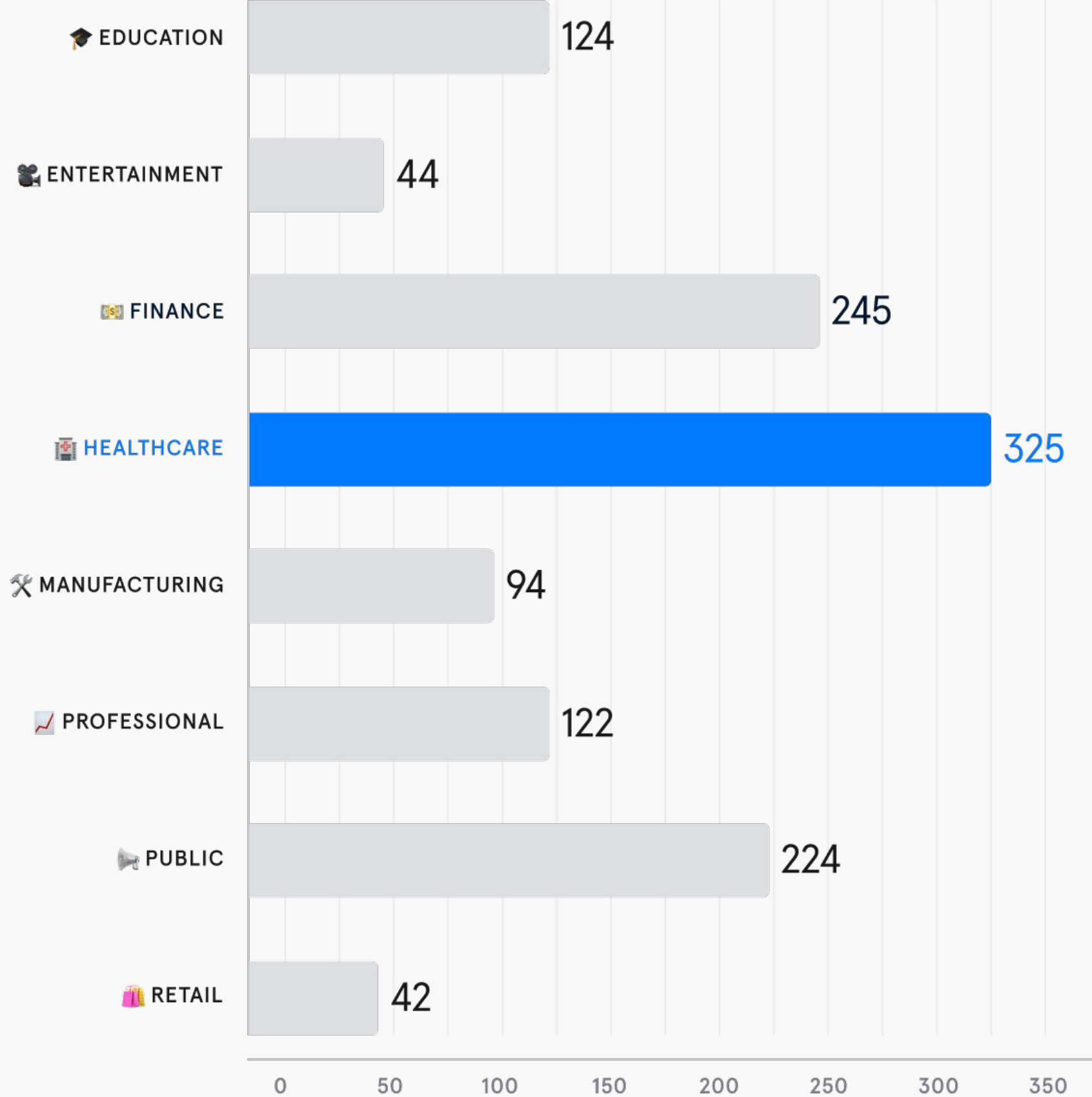
While – yes – ransomware is a growing problem, healthcare is *also among the most likely* to experience an incident involving employees misusing their access privileges; the most likely to have assets lost or stolen; *and* sees the most human errors (for example, an email being sent to the wrong person).

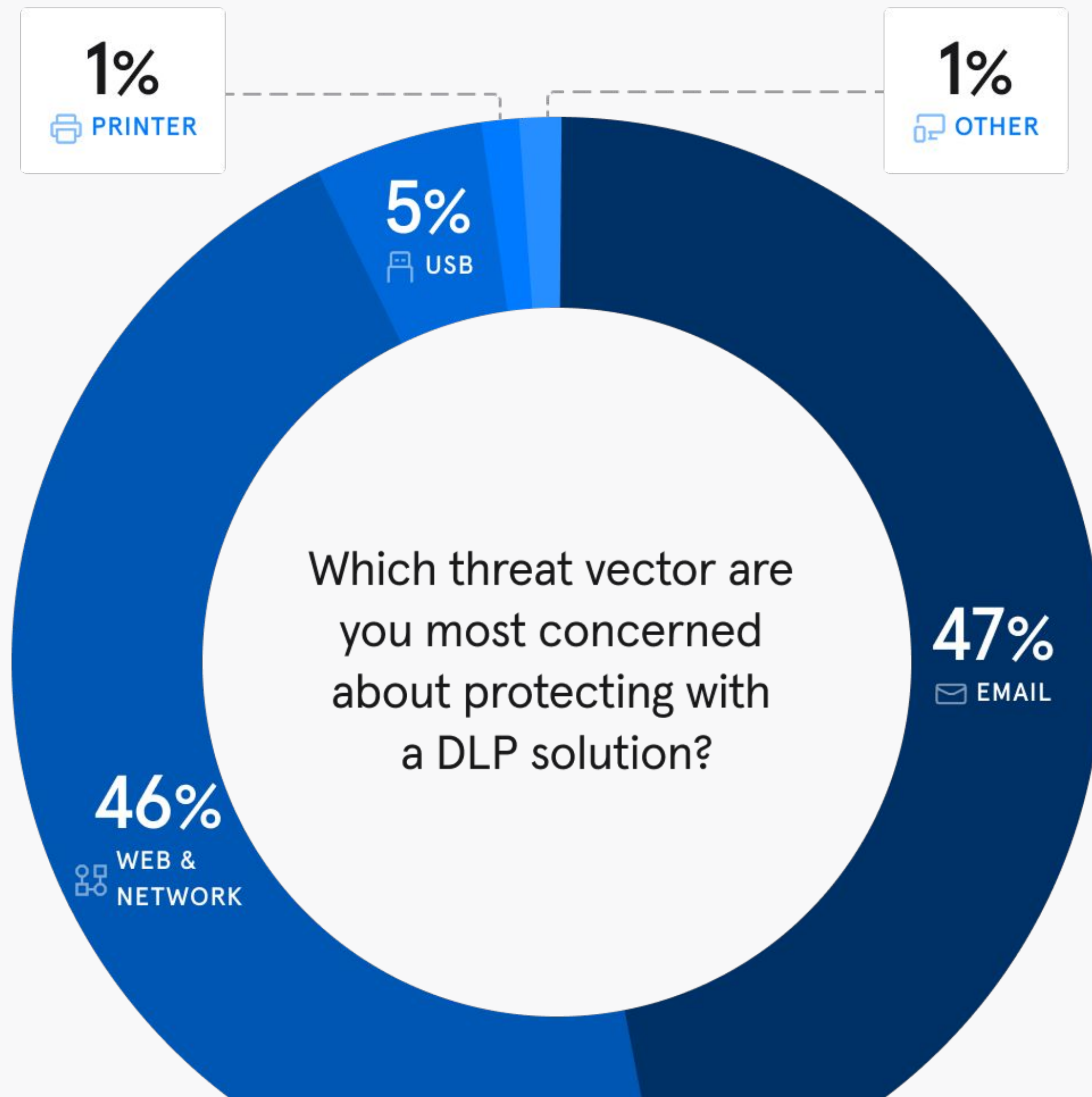
Source: Verizon 2020 Data Breach Investigations Report

 Number of incidents and breaches involving privilege misuse



 Number of incidents and breaches involving human error





Email: your organization's leaky pipeline

When it comes to DLP, security leaders have hundreds – if not thousands – of networks and endpoints to monitor and lock down.

But, when asked what threat vector they're most concerned about protecting, they said email. It makes sense.

Over [306.4 billion emails](#) were sent and received in 2020 and employees spend [40% of their time](#) on email. Accidents happen.

For example, in 2019 when an [employee at a gender identity clinic](#) in London exposed the details of close to 2,000 people on its email list after cc'ing recipients instead of bcc'ing them. A simple mistake can cause big problems, especially with strict data privacy laws like HIPAA and HITECH.

Unfortunately, accidents like this happen a *lot* more frequently than security leaders estimate.

For more examples of data breaches caused by misdirected emails, [click here](#).



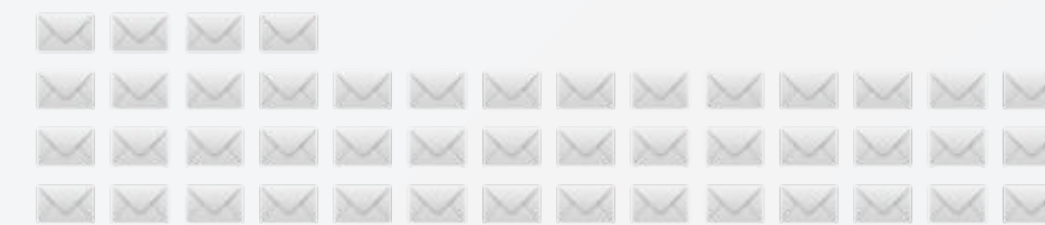
480

Number of misdirected emails security leaders think are sent every year.



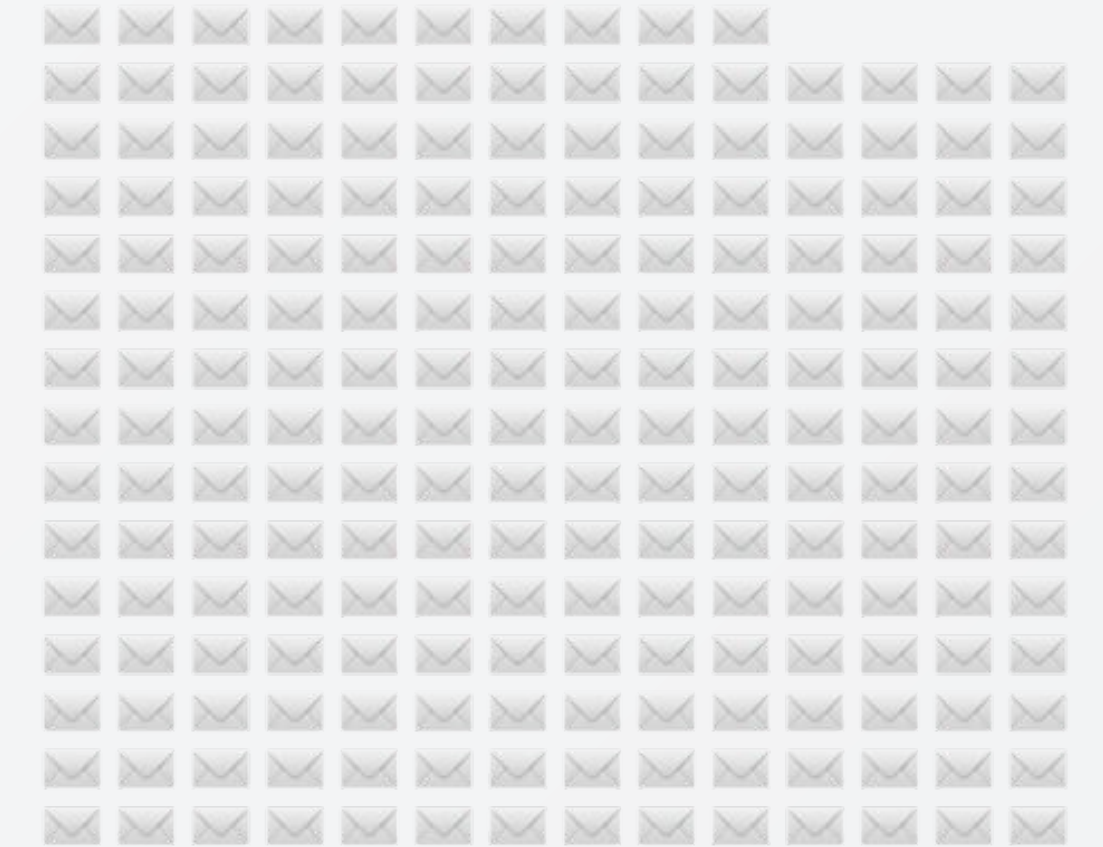
800

Number of misdirected emails actually sent in organizations with 1,000 employees every year.



720

Number of unauthorized emails security leaders think are sent every year.



27,500

Number of unauthorized emails actually sent in organizations with 1,000 employees every year.

Just the tip of the iceberg

According to Tessian platform data, at least 800 emails are sent to the wrong person in companies with 1,000 employees each year. **That's more than two every day.**

And, in healthcare specifically, 46% of employees admit to having sent an email to the wrong person before. Depending on the organization and the employee, these emails could contain social security numbers, medical records, invoices, R&D, IP, and more.

Meanwhile, security leaders estimate just 480 are sent every year. That means visibility is a big problem, that self-reporting mistakes isn't a viable solution, and that legacy DLP solutions aren't effectively stopping data loss.

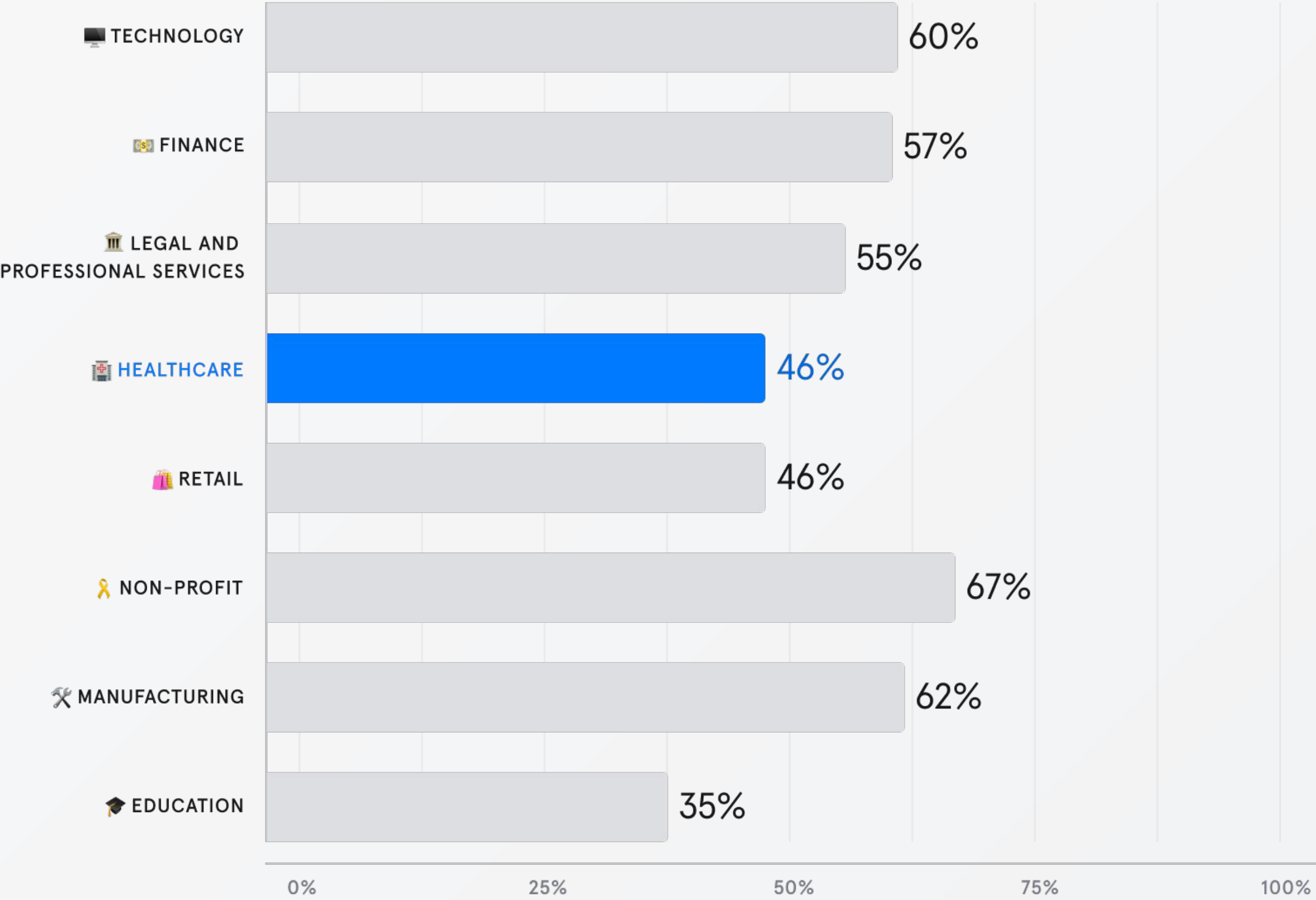
[SUBSCRIBE TO THE TESSIAN BLOG](#)

Get more insights straight to your inbox.

[SIGN ME UP →](#)



"Yes, I have sent an email to the wrong person before"



Driven to distraction at work *and* at home

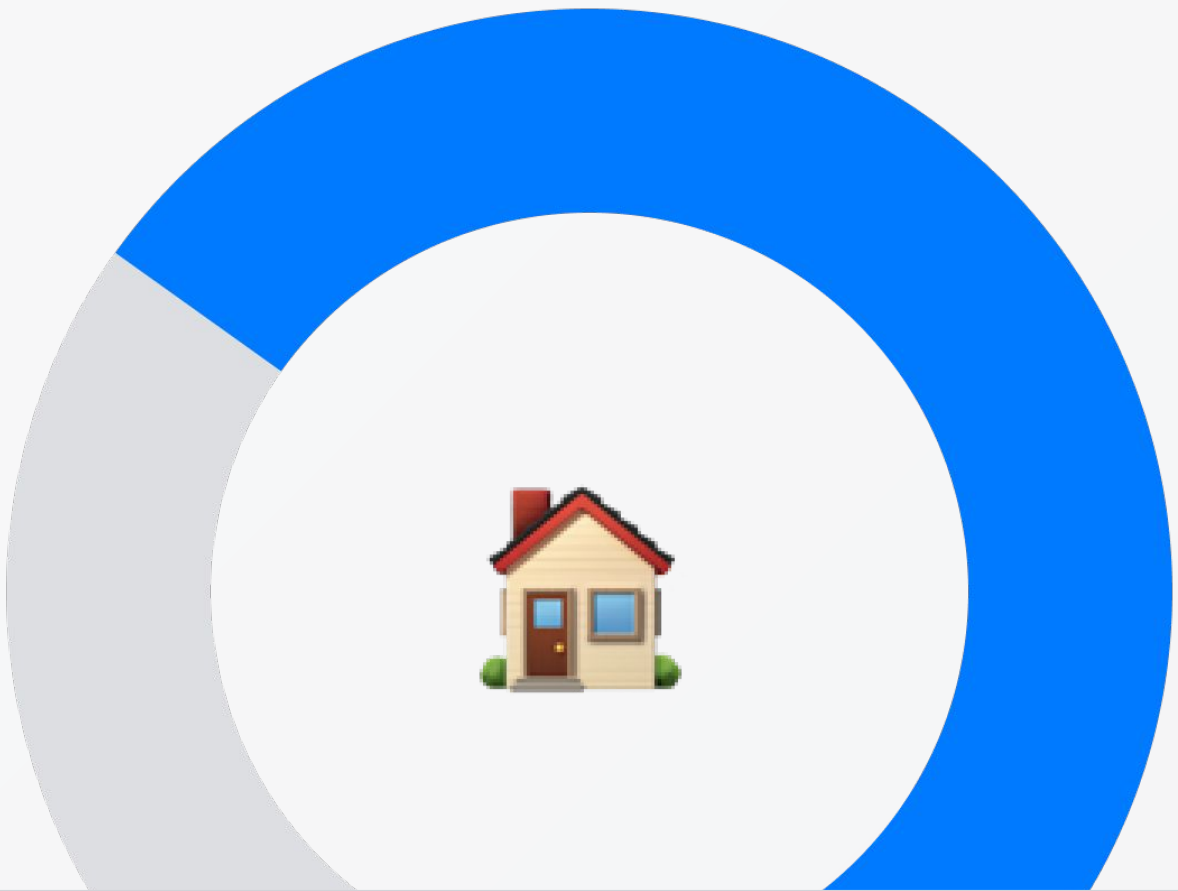
So, why do employees make mistakes at work that compromise security?

[According to employees](#), the top three reasons are: stress, fatigue, and distraction.

And, while many organizations are slowly transitioning back to the office, the rise of virtual health and telemedicine have enabled some to adopt permanent remote or hybrid working structures.

The problem is, over half ([59%](#)) of security leaders in [healthcare](#) say they're concerned about employees' unsafe data security practices in a hybrid-remote environment. And they have every right to be concerned.

42% of employees working in healthcare say they're *less* likely to follow safe data practices when working remotely.

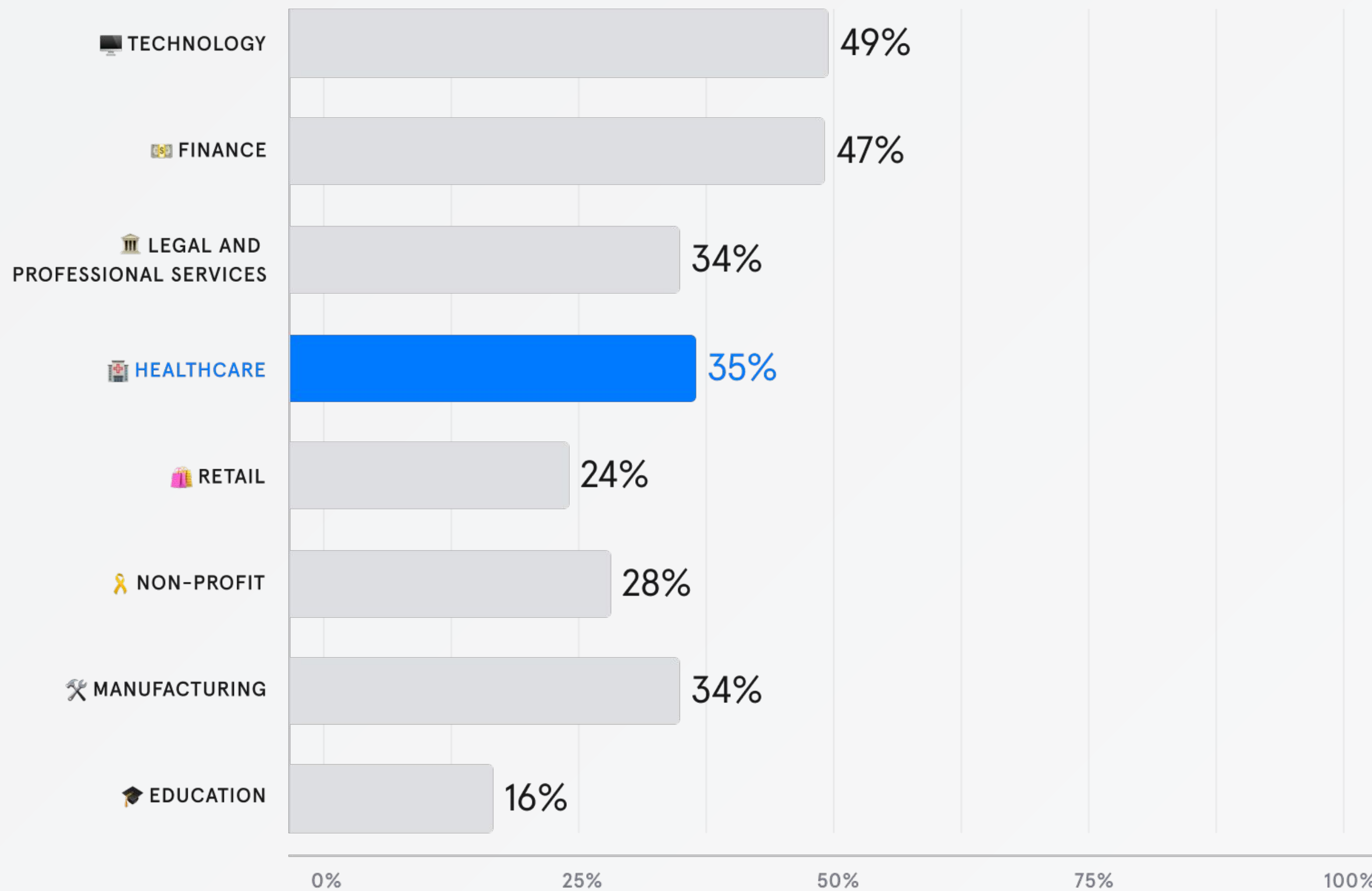


59%
of security leaders in healthcare say they're concerned about employees' unsafe data security practices in a hybrid-remote environment.

42%
of employees working in healthcare industries say they're less likely to follow safe data practices when working remotely.



🔍 "Yes, I have downloaded, saved, or sent work-related documents to personal accounts before leaving or after being dismissed from a job."



It's not always "just an accident"

Security leaders know that the vast majority of employees are well-intentioned and want to build a security culture based on trust.

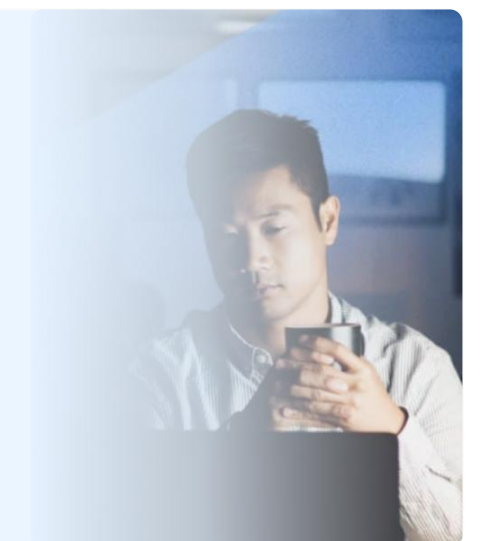
But, that doesn't mean there aren't some people who knowingly exfiltrate data. 35% employees working in healthcare admit to downloading, saving, or sending work-related documents to personal accounts before leaving or after being dismissed from a job.

And according to Tessian platform data, at least 27,500 non-compliant, unauthorized emails are sent every year in organizations with 1,000 employees. Security leaders estimated just 720.

WHAT IS AN UNAUTHORIZED EMAIL?

An unauthorized email is an email sent to a personal email account or a third-party that contains sensitive information. While this isn't always malicious, it is generally against security policies and could be a sign of intentional data exfiltration.

[Read the blog to find out more.](#)



The biggest concern? Job security.

While healthcare has the highest costs associated with data breaches – [60% higher than the average across all industries](#) – and has for ten years running, the cost of a breach isn't security leaders' biggest concern.

Instead, our research shows that across industries, they're most worried about losing customers' trust and data in the aftermath of a breach.

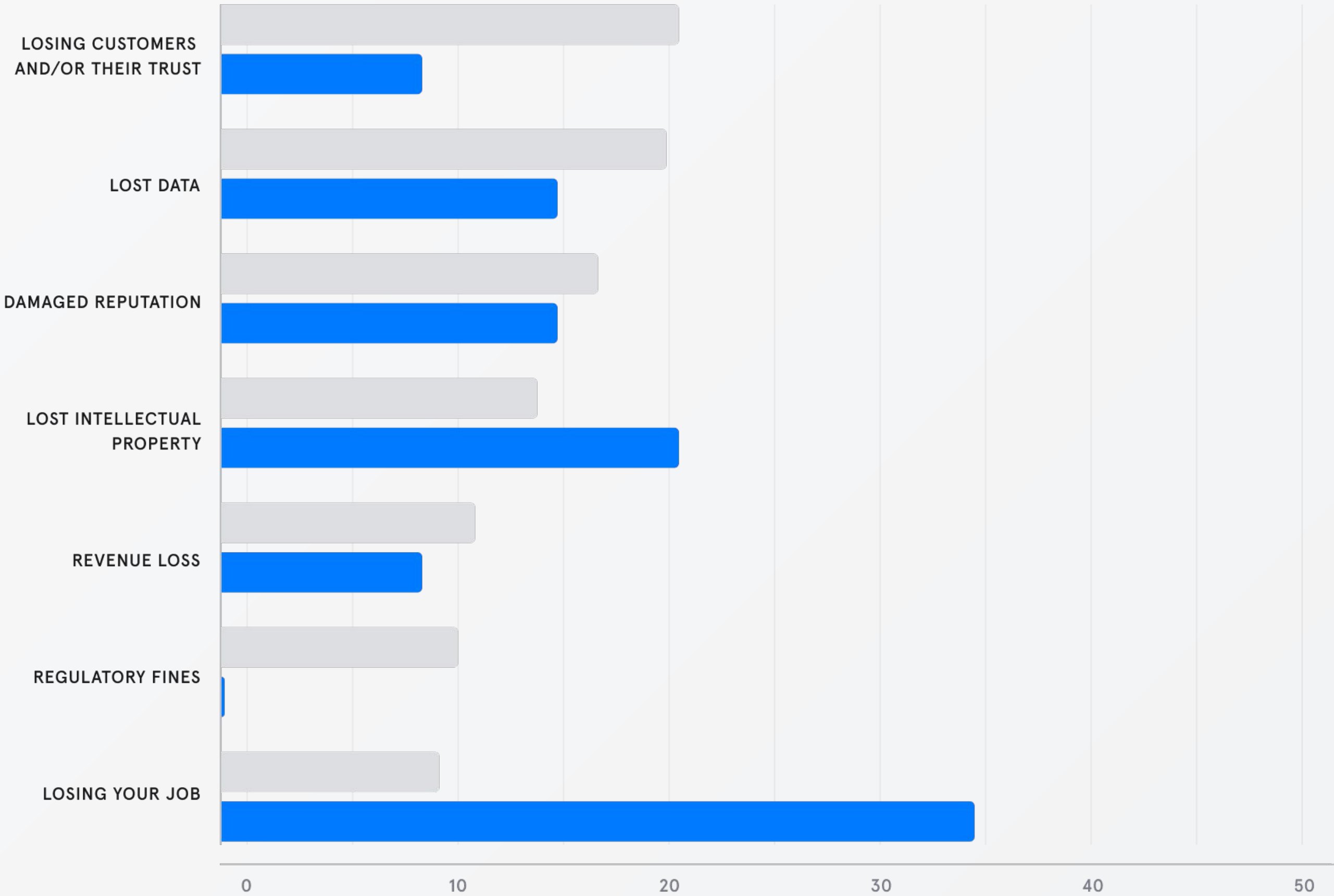
But, when you isolate security leaders working in healthcare specifically, you can see a stark difference. Instead of losing customer trust and a damaged reputation, their top concerns are losing their jobs and lost IP.

So, how do you prevent a breach and avoid all of these consequences? Level-up your data protection strategy.

Note: The survey sample size of security leaders working in healthcare is not statistically significant.

What is the biggest consequence of a breach?

● ALL SECURITY LEADERS ● SECURITY LEADERS IN HEALTHCARE



Weighing the pros and cons

So, why do employees make mistakes at work that compromise security?

When asked about the most effective way to keep data secure, 32% of security leaders said following company policies/procedures. 23% said physical security. 22% said security awareness training. And 21% said software/tools.

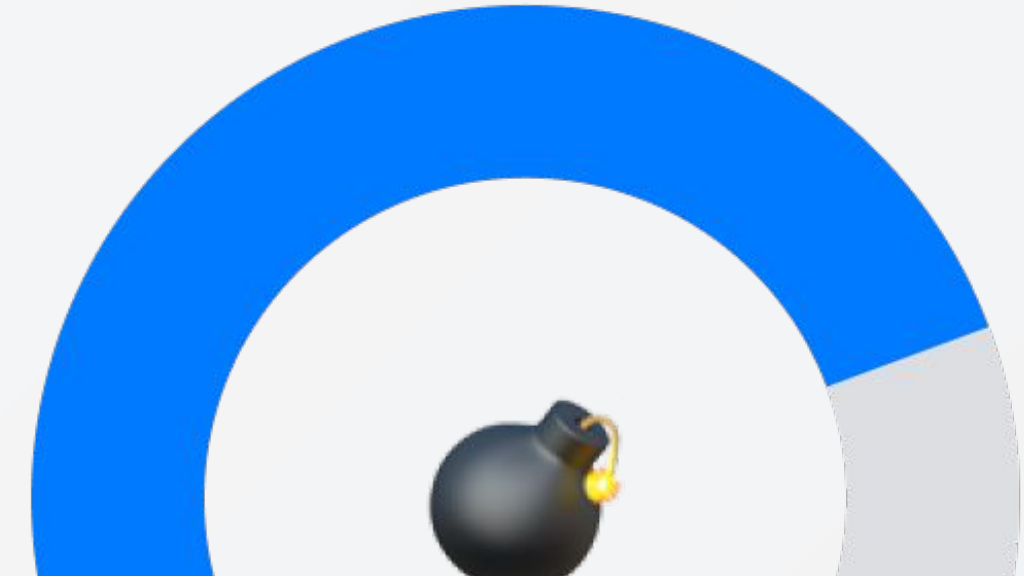
But, we all know one single solution isn't enough. Why? Because employees don't always follow policies and procedures, security awareness training alone can't change behavior long-term, and rule-based DLP is a blunt instrument that impedes employee productivity *and* creates too much noise for thinly-stretched security teams.

The bottom line is: It takes a village to prevent data loss and the best data protection programs take a nuanced and holistic approach by combining all of the above.



49%
of employees in healthcare say software impedes their productivity.

57%
of employees in healthcare say they'll find workarounds.



85%
of security leaders say rule based DLP is admin-intensive.

A different approach to DLP

Healthcare customers like [Cordaan](#) and British Medical Association trust Tessian to keep their critical client, patient, and employee data safe. Across two solutions, Tessian automatically detects and prevents [misdirected emails](#), [mistattached files](#), and [unauthorized emails](#). No rules required.

Better still, Tessian helps improve employees' security reflexes long-term with in-the-moment warnings that reinforce security policies while nudging them towards safer behavior over time. And, with [employee risk scores](#) that update automatically, security leaders get a bird's eye view of their most risky and at-risk employees.

It's the **only** solution that offers protection, training, and risk analytics *all in one platform*, giving security leaders a clear picture of their organization's risk **and** the tools needed to reduce that risk.



TRUSTED BY:



What we saw after our Proof of Value with Tessian was exciting, but also quite scary. We saw things that we didn't actually know were happening. Suddenly we had transparency and could see the true scope of the issues we had on email. But, we also saw how employee behavior changes with Tessian.



Cas de Bie

CHIEF INFORMATION SECURITY OFFICER, CORDAAN



Tessian is a leading cloud email security platform that intelligently protects organizations against advanced threats and data loss on email, while coaching people about security threats in-the-moment. Using machine learning and behavioral data science, Tessian automatically stops threats that evade legacy Secure Email Gateways, including advanced phishing attacks, business email compromise, accidental data loss and insider threats. Tessian’s intelligent approach not only strengthens email security but also builds smarter security cultures in the modern enterprise.

[TESSIAN.COM](https://tessian.com)



Level-up Your Data Protection Strategy

Want to learn more about Tessian’s DLP solutions? Talk to one of our experts.

[REQUEST A DEMO →](#)



More Insights, Every Week.

Subscribe to the Tessian blog to get more insights straight to your inbox.

- Helpful resources and shareable guides
- Tips for CISOs
- Early access to our latest research

[SIGN ME UP →](#)

Methodology

In addition to using Tessian platform data, we commissioned OnePoll to survey 2,000 working professionals: 1,000 in the US and 1,000 in the UK; additionally OnePoll surveyed 250 IT leaders in the US.

Survey respondents varied in age from 18–51+, occupied various roles across departments and industries, and worked within organizations ranging in size from 2–1,000+.

We also interviewed several IT, security, and compliance professionals with diverse backgrounds, all of whom provided insights that helped frame this report.

Publicly available third-party research was also used, with all sources listed in the downloadable PDF.

Midpoints and averages were used when calculating some figures and percentages may not always add up to 100% due to rounding.

Share this report



[TESSIAN.COM/RESEARCH →](https://tessian.com/research)