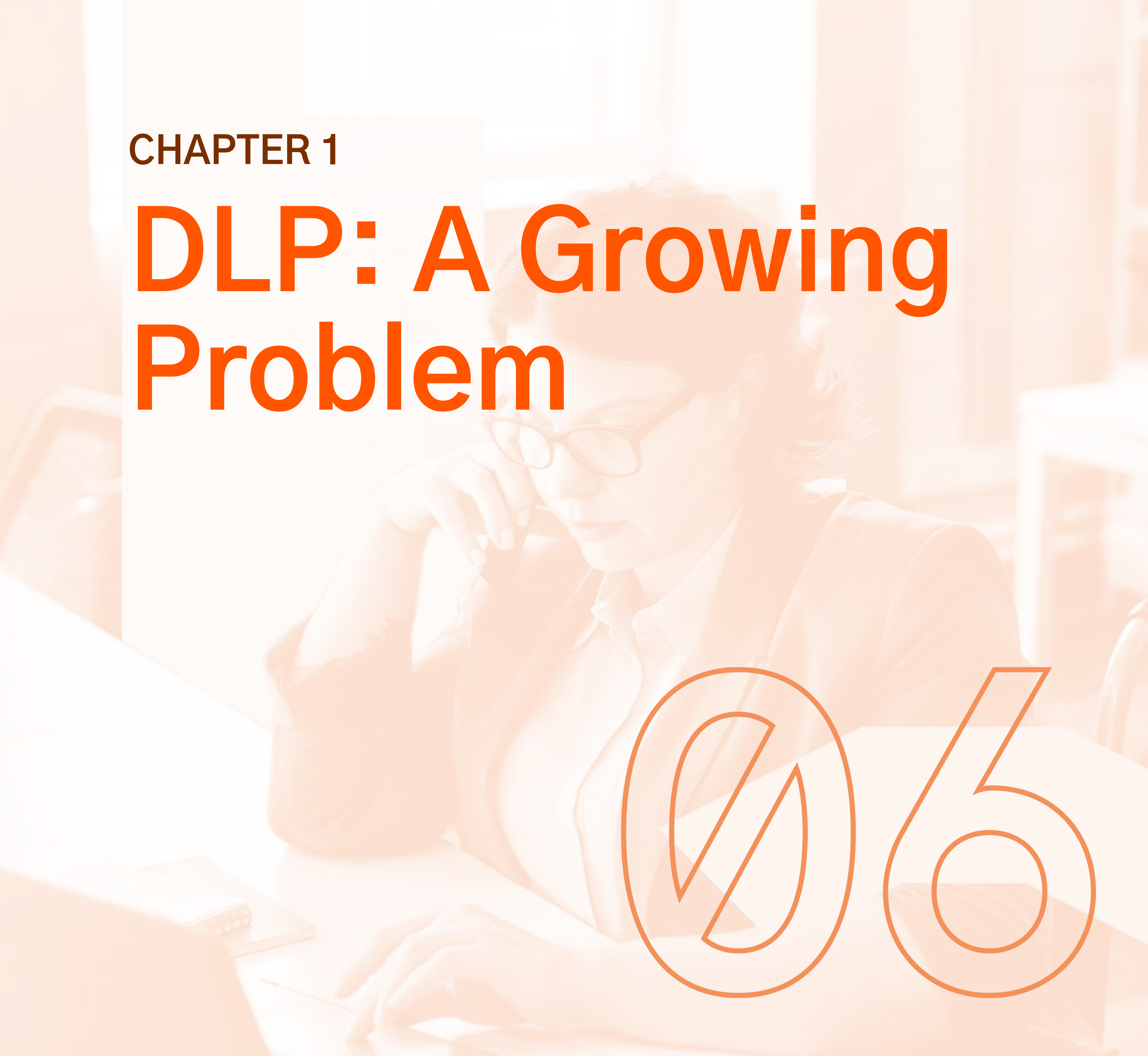
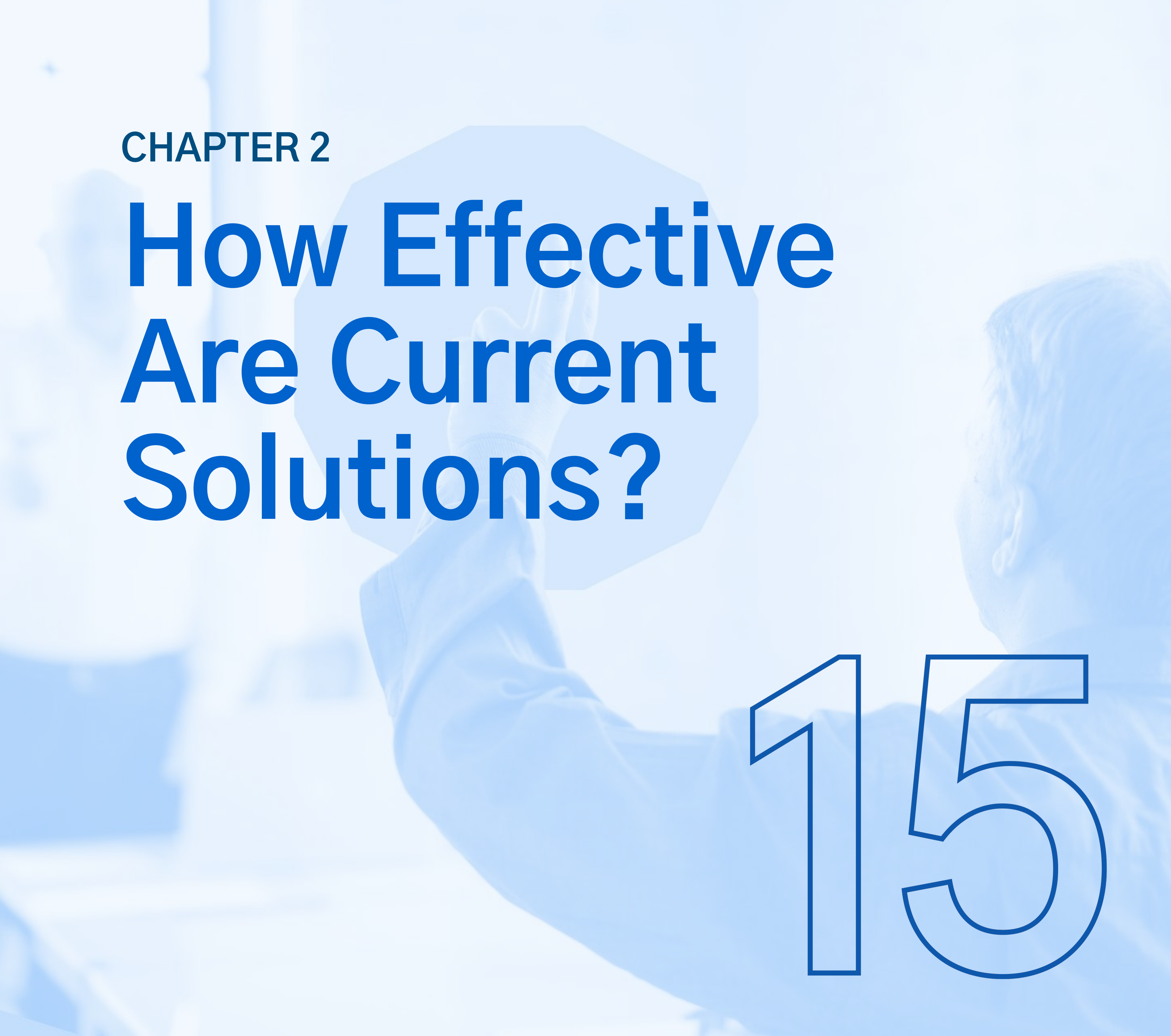
TESSIAN

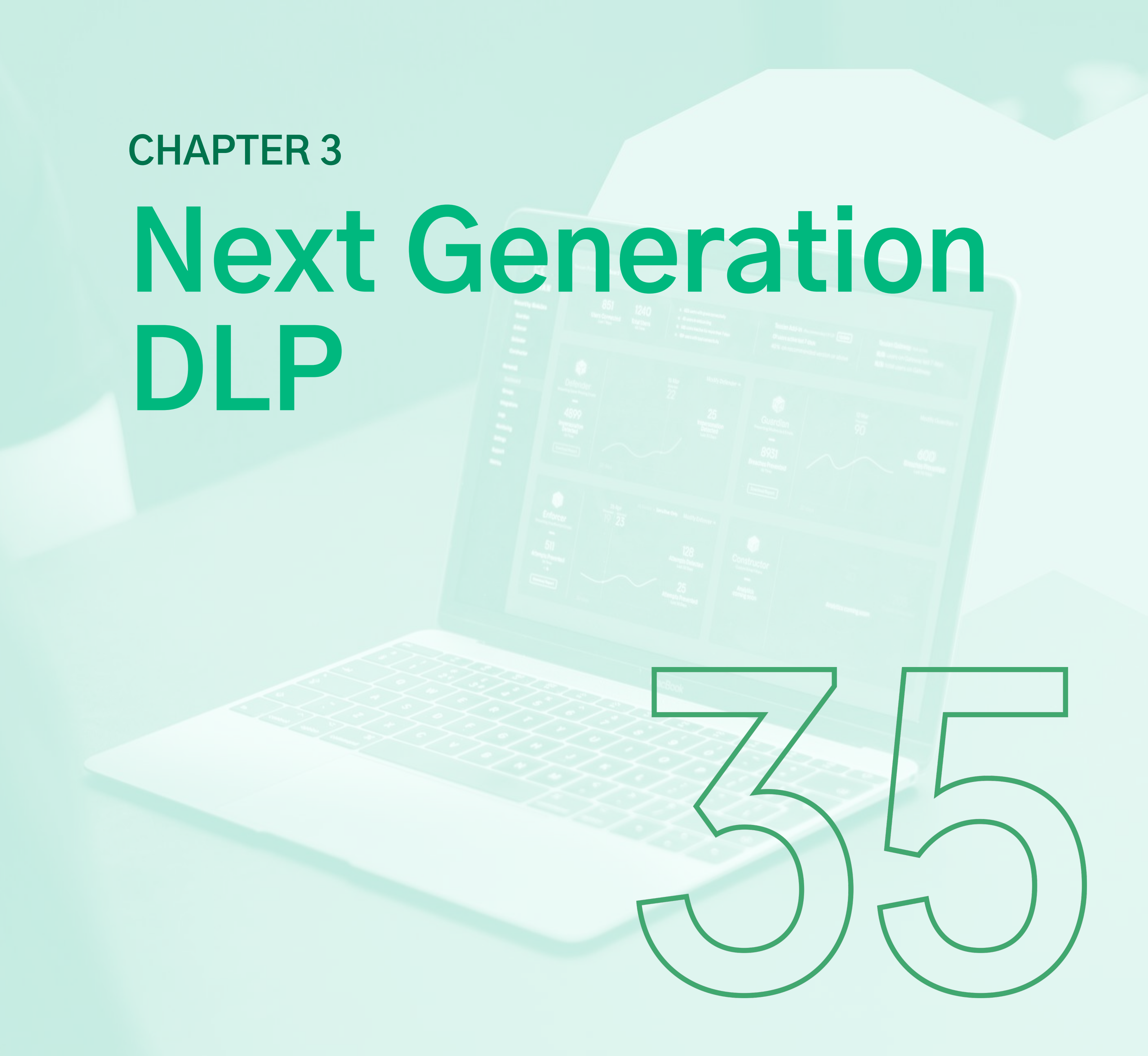
THE STATE OF DLP

Why DLP Has Failed and What the Future Looks Like

Data loss – whether accidental or intentional – is a big problem for organizations. Why? Because people control our data, and people break the rules and make mistakes. We're only human.







Further Reading — Industry Reports

Financial Services — Healthcare — Legal

Introduction

Data breaches are a bigger problem than ever, especially with distributed workforces.

While email threats from external bad actors like spear phishing and business email compromise dominate headlines, **email threats from insiders are steadily rising**. In fact, there's been a 47% increase in incidents[1] over the last two years; this includes accidental data loss and deliberate data exfiltration by negligent or disgruntled employees or contractors.

While every incident of data loss or leakage may not result in a breach, many do, and the cost can be tremendous.

And, with GDPR fines totaling nearly $200 million between January 26, 2020, and January 27, 2021[2] alone, data privacy regulations are going to drive the cost of resolution even higher.

That's one reason why data loss prevention (DLP) is one of the top spending priorities for IT leaders[3] and why email is the threat vector most IT leaders are concerned about protecting.

The question is: **Do security, IT, and compliance leaders have true visibility over how their employees are handling and mishandling data on email?**

According to our research, not yet. But, after reading this report, they should have enough information to better inform their view.

Executive Summary

The State of Data Loss Prevention explores new and perennial challenges around data loss and identifies the most (and least) effective DLP solutions.

To better understand the DLP landscape and why solutions, policies, and training programs seem to be failing, we analyzed Tessian platform data and commissioned OnePoll to survey 2,000 professionals (1,000 in the US and 1,000 in the UK) and 250 Information Technology (IT) leaders. We also interviewed IT, security, and compliance leaders about their own experiences with DLP.

Our findings reveal that data loss on email is a bigger problem than most realize, that remote-working brings new challenges around DLP, and that the solutions currently deemed most effective may actually be the least.

Readers will:

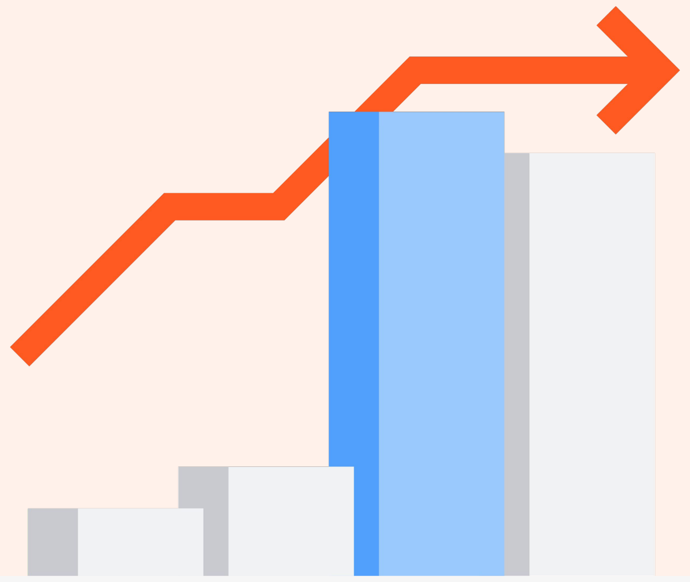
1. Gain visibility into the frequency of data loss incidents on email, which are happening as much as 38x more often than IT leaders currently estimate.
2. Learn why security awareness training, policies and procedures, and rule-based solutions alone aren't enough to prevent data loss, particularly when employees are working remotely.
3. Understand the impact compliance standards like GDPR have on how employees handle data.

THE STATE OF DLP

Key Findings

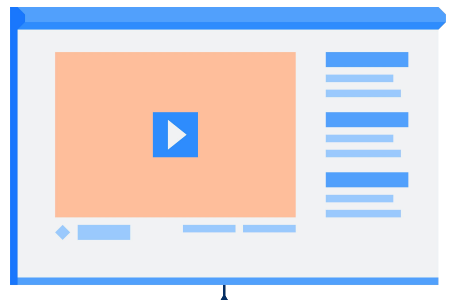
Data loss incidents on email happen **38x more often** than IT leaders think

Jump to Page 24 ↗



Employees who received training **once every 1–3 months are 2x as likely** to send company data to personal email accounts (unauthorized emails)

Jump to Page 19 ↗



48% of employees say they're less likely to follow safe data practices when working from home

Jump to Page 12 ↗

91% of IT leaders say they trust employees to follow security policies while working from home

Jump to Page 12 ↗

800 misdirected emails are sent every year (in organizations with 1,000+ people)

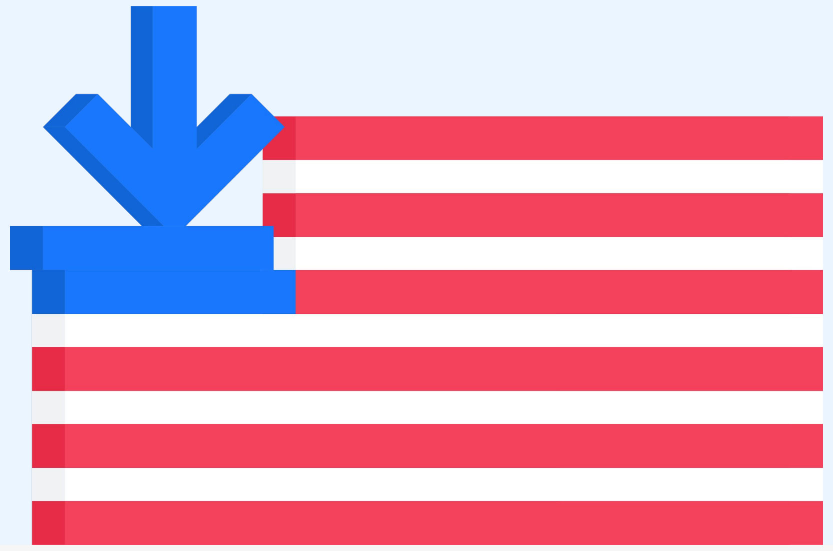
Jump to Page 23 ↗

27,500 emails containing company data are sent to personal accounts every year (in organizations with 1,000+ people)

Jump to Page 24 ↗

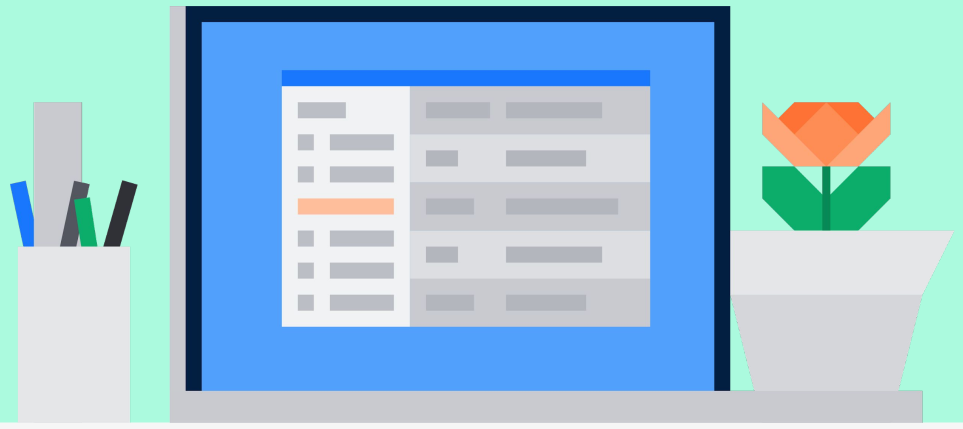
US employees are 2x more likely to download, save, or send work-related documents to their personal email accounts before leaving or being dismissed from a job compared to UK

Jump to Page 26 ↗



84% of IT leaders say DLP is more challenging when their workforce is working remotely

Jump to Page 11 ↗



CHAPTER 1

DLP: A Growing Problem

06

CHAPTER 2

How I
Are C
Solut

15

CHAPTER 3

Next Ge
DLP

35

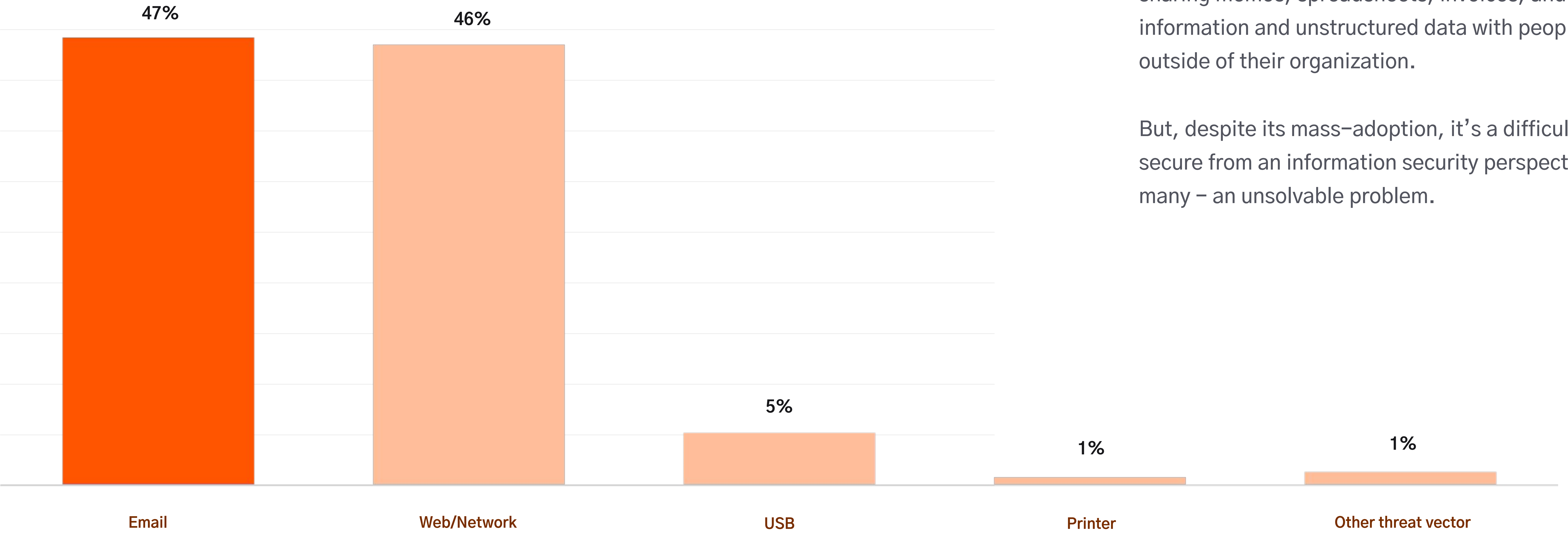
Email is The #1 Threat Vector

Over time, the causes of data loss have become increasingly diverse.

Before data was shared electronically, the biggest cause originated from the physical sharing of confidential documents, like unauthorized printing or unsecure document disposal. In these instances, lockable confidential waste bins and paper shredding services would have sufficed in securing sensitive data. Easy.

But, as technology has developed, new channels for data loss have emerged and now, email is the focus for DLP efforts for most IT leaders.

Which threat vector are you most concerned about protecting with a DLP solution?



Nearly half (47%) of the IT leaders surveyed say email is the threat vector they're most concerned about protecting. It makes sense.

Over 124 billion business emails are sent and received every day[4] and employees spend 40% of their time on email[5], sharing memos, spreadsheets, invoices, and other sensitive information and unstructured data with people both in and outside of their organization.

But, despite its mass-adoption, it's a difficult channel to secure from an information security perspective. It is – for many – an unsolvable problem.

> People understand phishing. It’s in the news, it’s mainstream. Data loss and the implications of human error aren’t. These things just don’t get as much attention, which naturally means they won’t be taken as seriously. But, that doesn’t mean phishing is a bigger threat than these outbound threats. Not at all.

Shanit Gupta
HEAD OF TECHOPS

Carbon

To start, the underlying technology behind email hasn’t evolved since its inception in the 1970s. While this makes it user–friendly and easy–to–implement, there are core security features missing that modern communication platforms have as a standard. This includes the ability to redact or recall and encryption–by–default.

When you combine this with ease–of–access (email accounts today are managed on laptops, smartphones, tablets, and even watches) and the fact that inboxes are treasure troves for sensitive data, it’s easy to see why 90% of data breaches start on email[6].

It only takes **one** rushed email to the wrong person or **one** disgruntled employee to expose sensitive data.

It’s important to remember, though, that data loss isn’t always the result of malicious activity, and employees shouldn’t be typecast as “bad guys” by default. We’re only human.

People Control Our Data

Employees control business' most sensitive systems and data. Whether it's someone in your finance department who oversees billing and banking platforms, someone in your HR department who controls employee social security numbers and compensation plans, or someone in a client facing role handling customer data — they are the first and last line of defense; the gatekeepers of digital systems and data.

But, it's unfair and unreasonable to expect people to do the right thing 100% of the time. As the proverbial phrase goes, "to err is human", which means people are bound to break the rules and make mistakes.

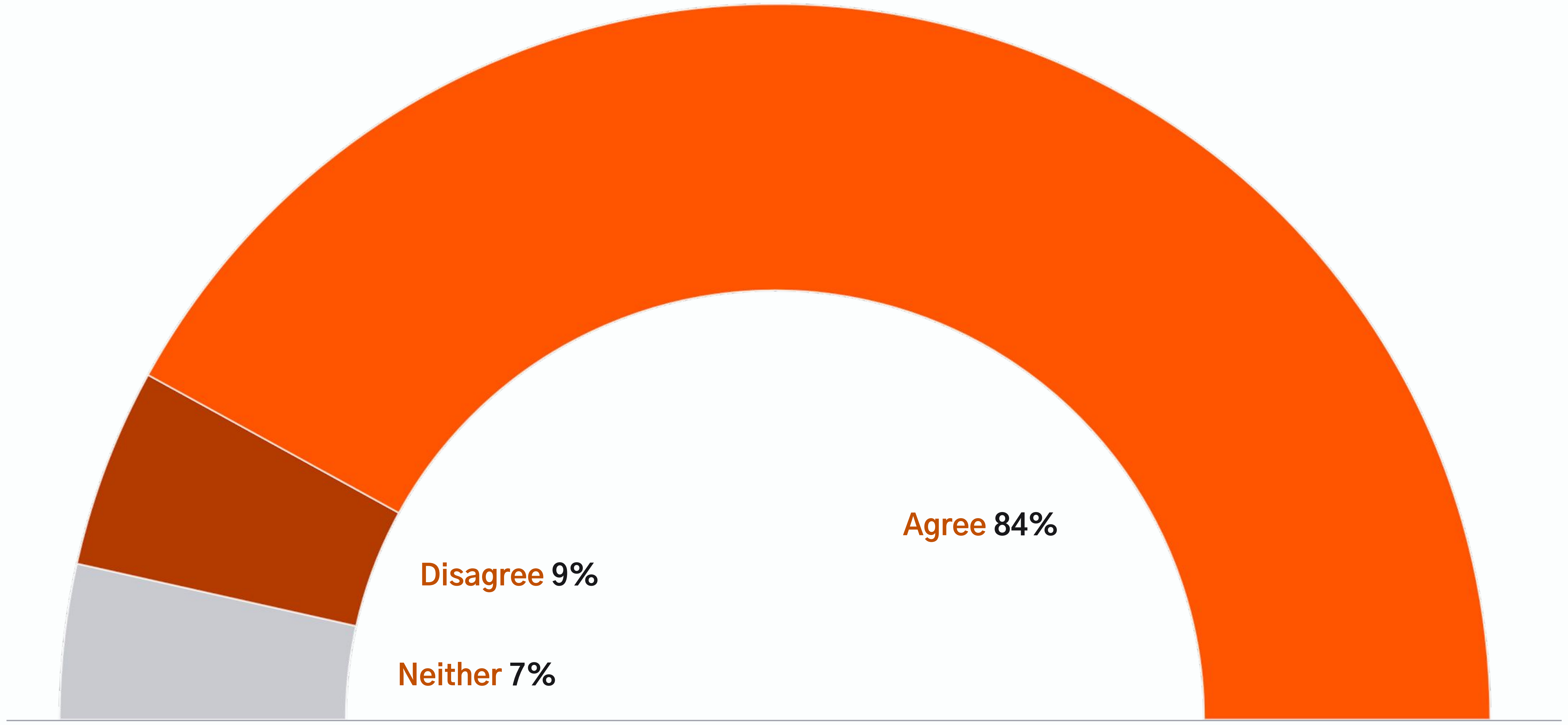
And, according to our research, they're even more likely to break the rules and make mistakes when working from home.

New Challenges Around Remote–Working

As workforces have transitioned from office–to–home, IT leaders are struggling to maintain visibility over data flow: 84% of IT leaders report DLP is more challenging when their workforce is working remotely.

And, why wouldn't it be more challenging? The perimeter has – quite literally – disappeared as organizations have made the sudden shift to one or two offices to potentially thousands, depending on how many staff they employ. The means past strategies have become obsolete.

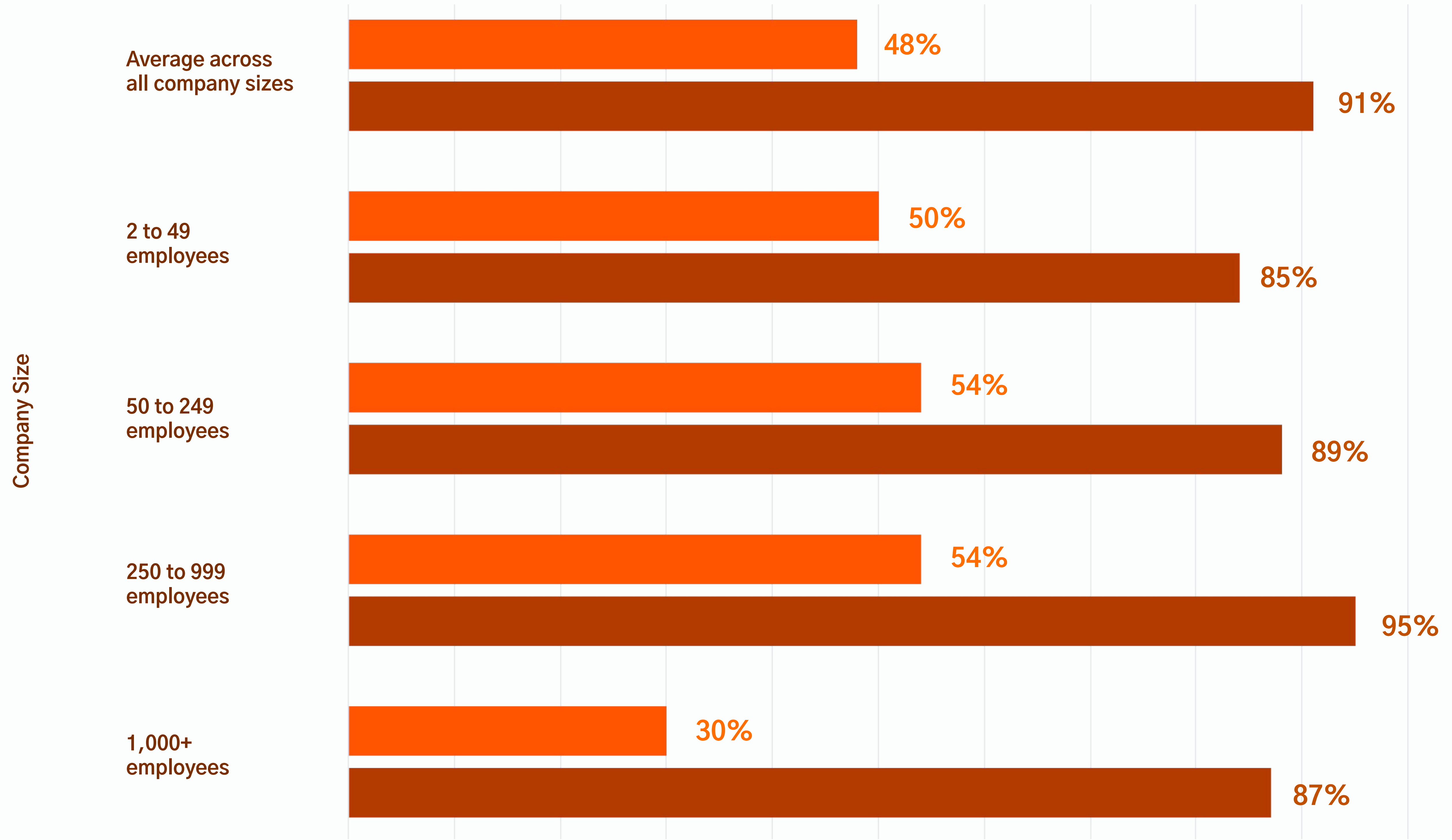
"Preventing data loss is more challenging when my workforce is working remotely."



Remote-Working & Security: Employees vs. IT Leaders

● Employees: "I'm less likely to follow safe security practices when working from home."

● IT Leaders: "I trust my employees to follow security policies when working from home."



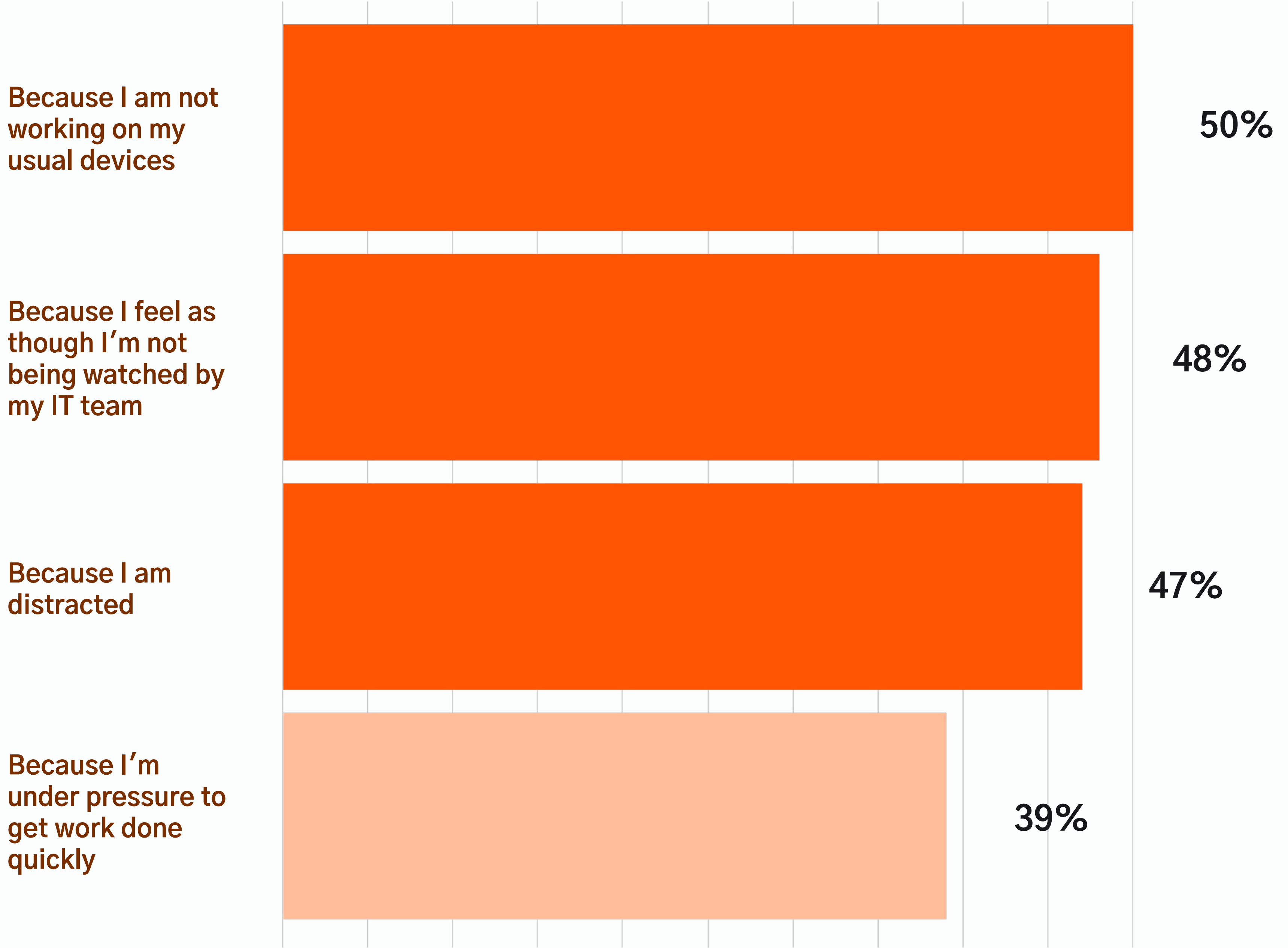
Nonetheless, IT leaders are hopeful, with 91% saying they trust their employees to follow security best practice while out of the office.

Unfortunately, this trust isn't necessarily deserved, with almost half (48%) of employees saying they're *less* likely to follow safe data practices when working from home.

Interestingly, though, these numbers vary based on company size. Trust from IT leaders is the highest in organizations with 250–999 employees and lowest in those with 2–49 employees.

But, when it comes to the behaviors of employees, those working in the largest organizations (1,000+) are the **most** likely to stay secure while working remotely, with just 30% saying they're less likely to follow safe data practices while working from home. That's 18% lower than the average across all organizations.

Why are you less likely to follow safe data practices when working from home?



When asked why they were less likely to follow safe data practices when working from home, employees cited not working on their usual devices (50%) and being distracted (47%) as two of the top three reasons.

Most of us can relate. When working remotely – especially from home – people have other responsibilities or distractions like childcare and roommates and, more often than not, they don't have dedicated workstations like they do in their normal office environment. This isn't trivial.

But, 48% of employees also count not being closely monitored by IT teams as a reason to ignore safe data practices.

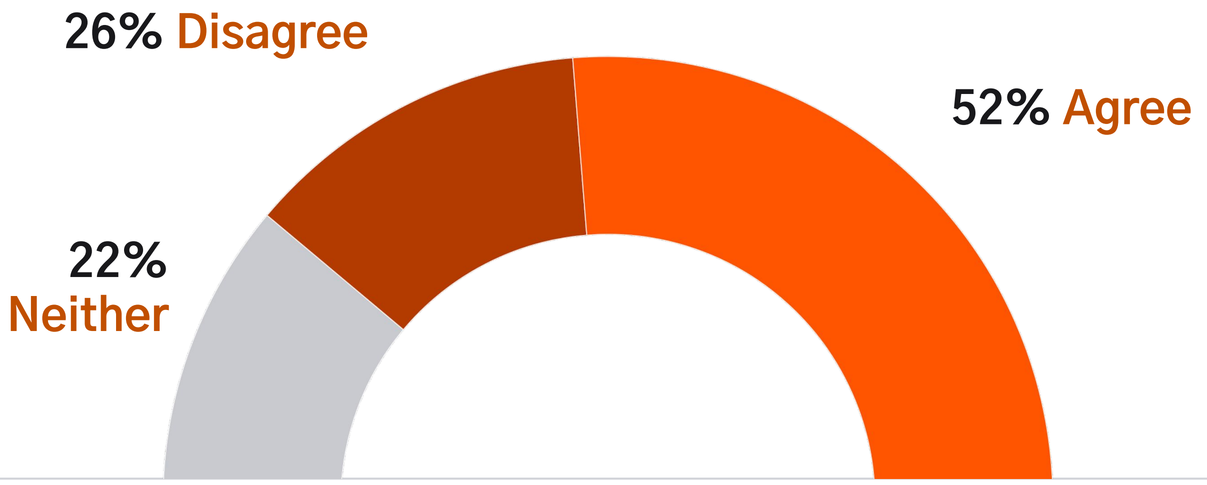
> Communication with the IT department is more important now than ever. We have to maintain a sense of community, trust, and visibility, even with everyone siloed in their own homes. We have to make sure they feel the presence of IT and security teams. They have to know that, even though they can't come tap us on the shoulder and ask us a question, that we're still here to help.

Jay Leaf-Clark
HEAD OF INFORMATION TECHNOLOGY
DASHLANE

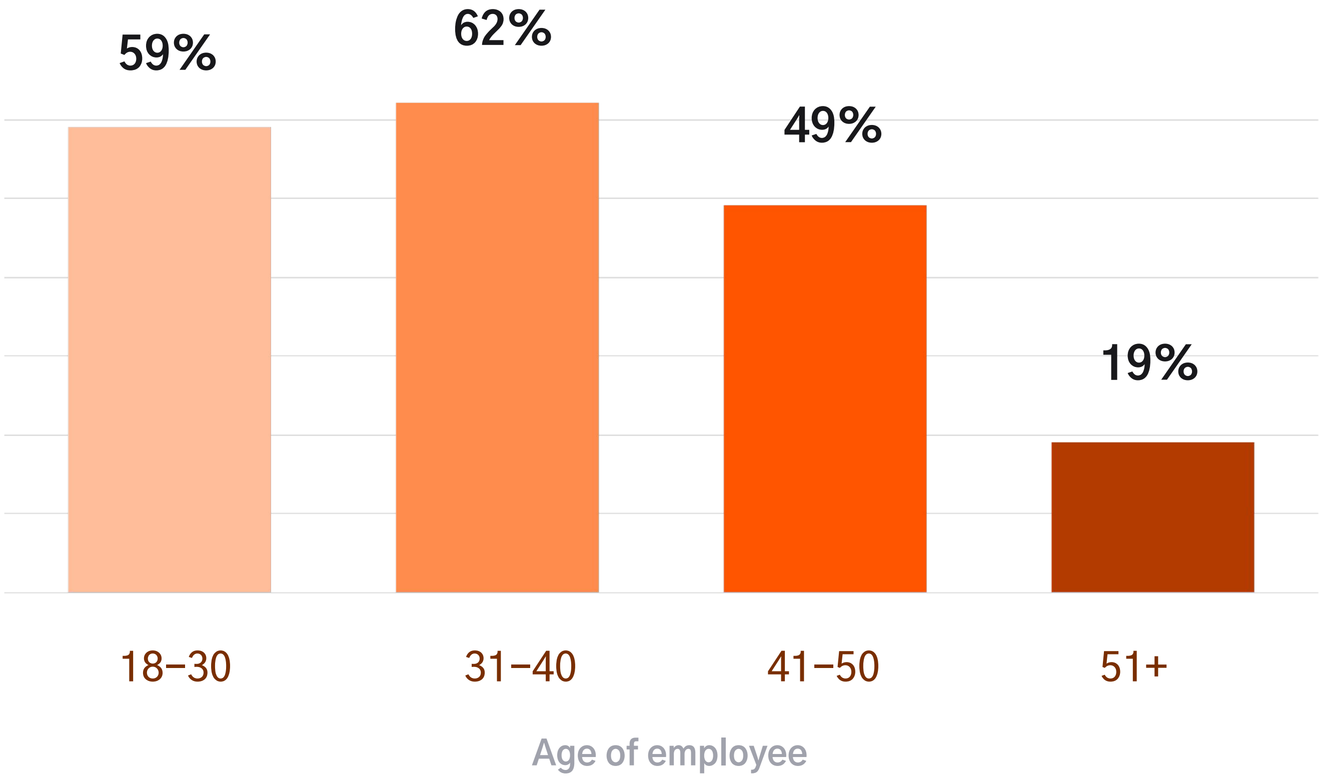
This is likely also why over half (52%) of employees feel they can get away with riskier behavior when working outside of the office. Again, opinions vary. This time, based on age and region.

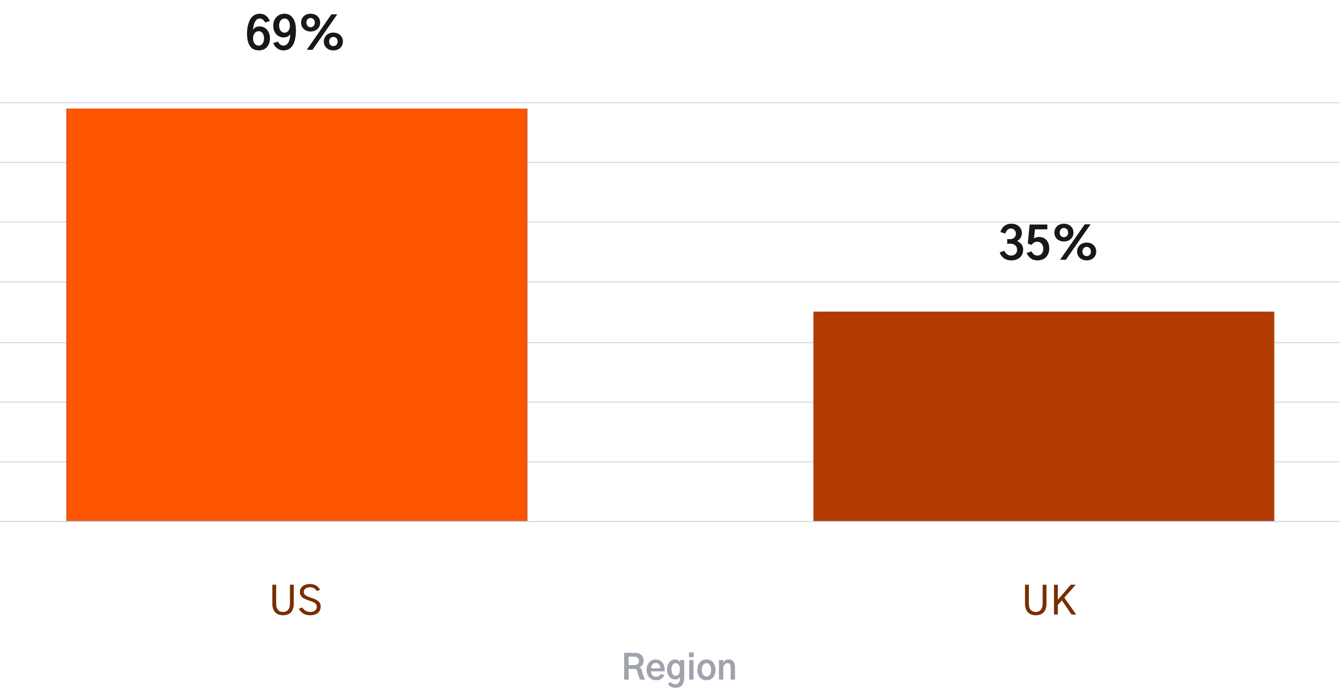
While just 19% of employees 51 and over feel they can get away with riskier behavior while working from home, 59% of employees aged 18–30 said the same. Likewise, US workers are almost twice as likely to agree they can get away with more while working outside of the office.

"I feel as though I can get away with riskier behavior when working from home."



"I feel as though I can get away with riskier behavior when working from home."





R 1

P: A
wing
blem

6

CHAPTER 2

How Effective Are Current Solutions?

15

CHAPTER 3

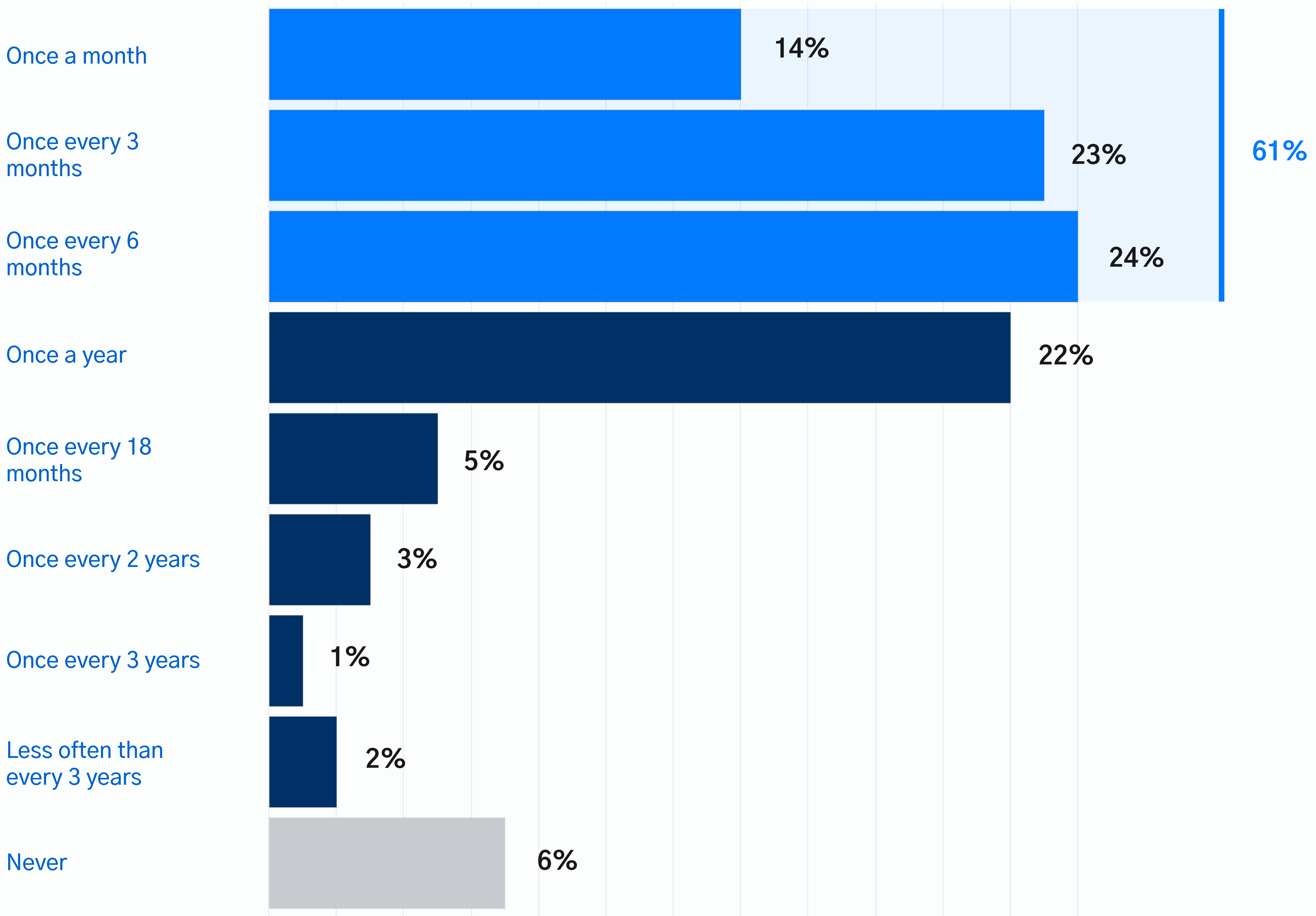
Next Ge
DLP

35

More Training Doesn’t Equate to Fewer Security Incidents

According to IT leaders, security awareness training and “following company policies and procedures” are the most effective ways to prevent data loss. Perhaps that’s why over half (61%) of employees have training every 6 months or more.

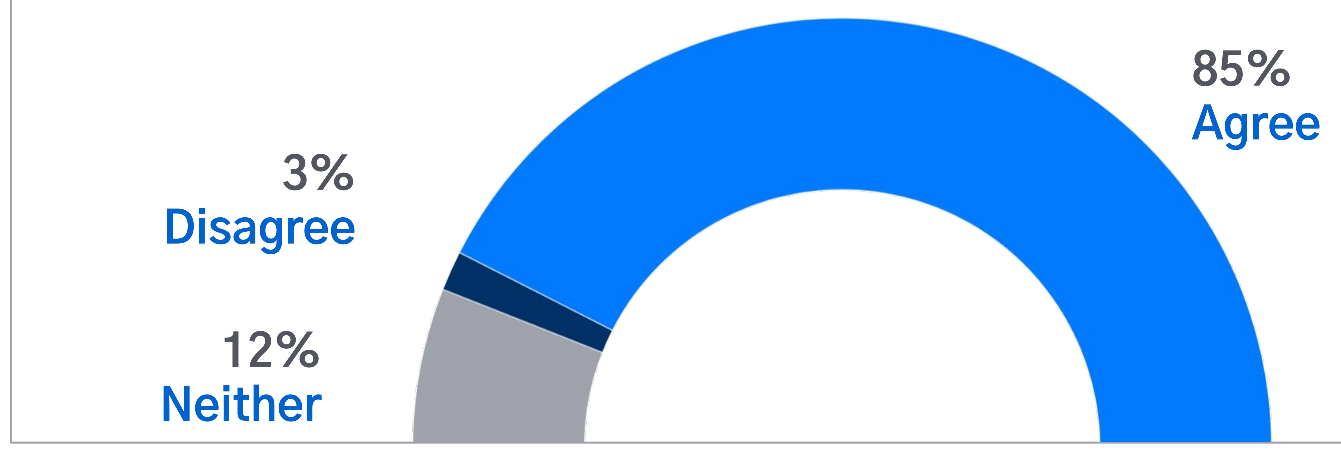
How frequently does your organization have security awareness training?



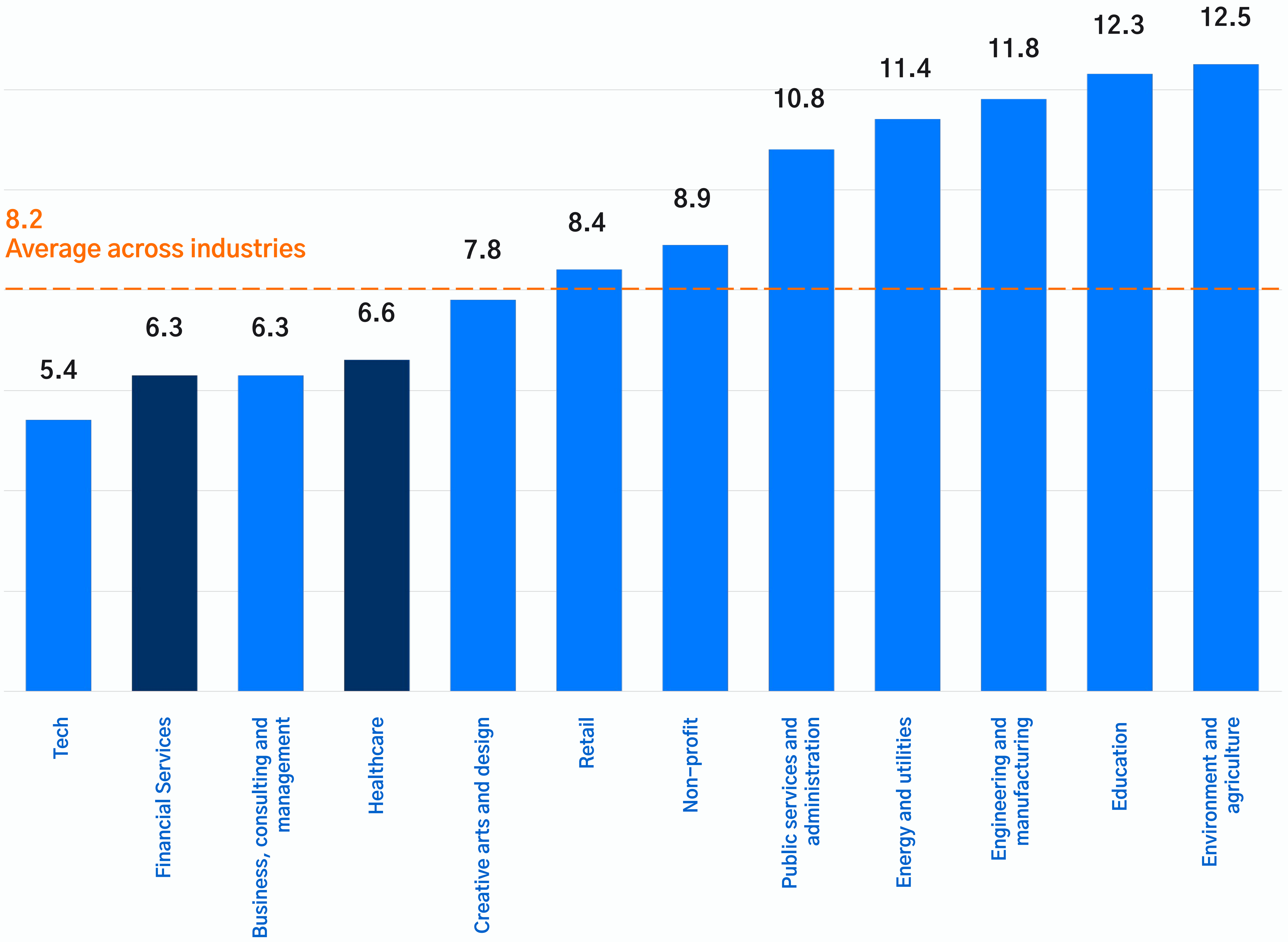
Unsurprisingly, training is even more frequent in highly regulated industries. While the average employee has security training every 8.2 months, employees working in Financial Services have training every 6.3 months and those working in Healthcare have training every 6.6 months.

Security awareness training confronts the crux of the data loss problem by educating employees on security best practice and in-house policies and procedures. Employees seem to get it: 85% of office workers say they have a good understanding of their company's security policies and how to apply them in their day-to-day work.

"I have a good understanding my company's security policies and how to apply them in my day-to-day work."



Average frequency of security awareness training by industry



But – somehow – security awareness training doesn’t appear to be curbing the problem of data loss.

It could be because training is often more focussed on inbound threats like phishing than outbound threats like data exfiltration. It could be because employees don’t consider accidents like sending misdirected emails (emails accidentally sent to the wrong person) a data loss incident. Or, it could simply be because you can’t train away people’s propensity to make mistakes or break the rules.

> As with most things related to cybersecurity, user awareness is a big deal, and training programs are key. But, a lot of organizations don’t have a follow-up to training. They don’t have a system in place to measure user compliance, performance, and success around protecting sensitive information. So what happens if they repeatedly fail, do we only re-train them? There often aren’t clear consequences or avenues for remediation, which means nobody is actually held accountable when an incident occurs.

Allen Look
FORMER CHIEF INFORMATION SECURITY OFFICER

SI Group

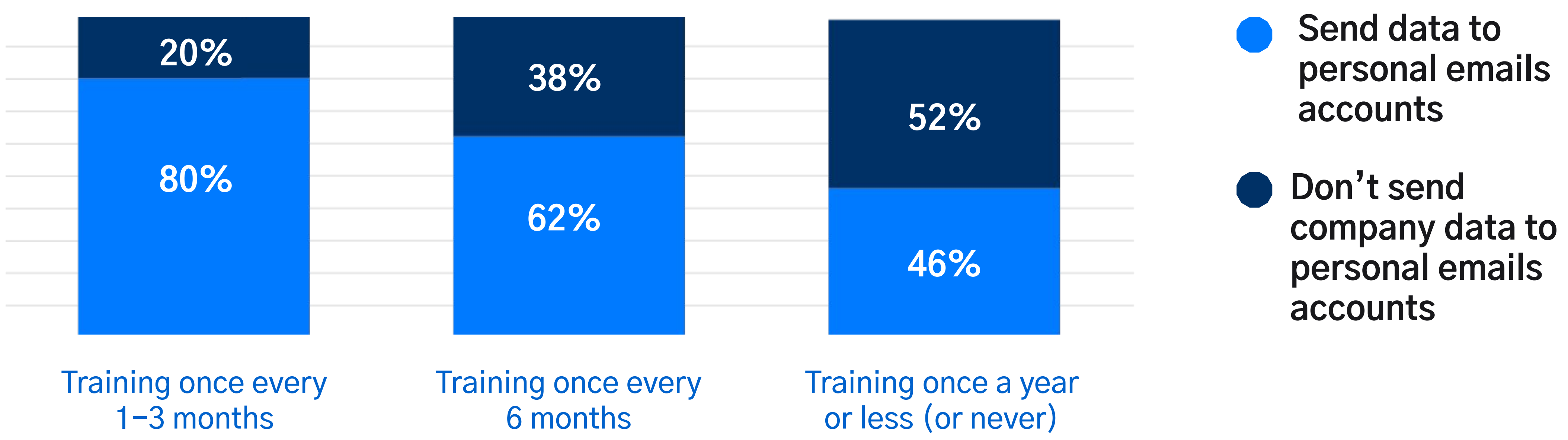
Whatever it is, more training isn't equating to fewer security incidents.

The percentage of employees who admit to sending misdirected emails is actually the highest in organizations that provide security awareness training the most frequently: 63% of employees who receive training every 1–3 months say they remember sending emails to the wrong person.

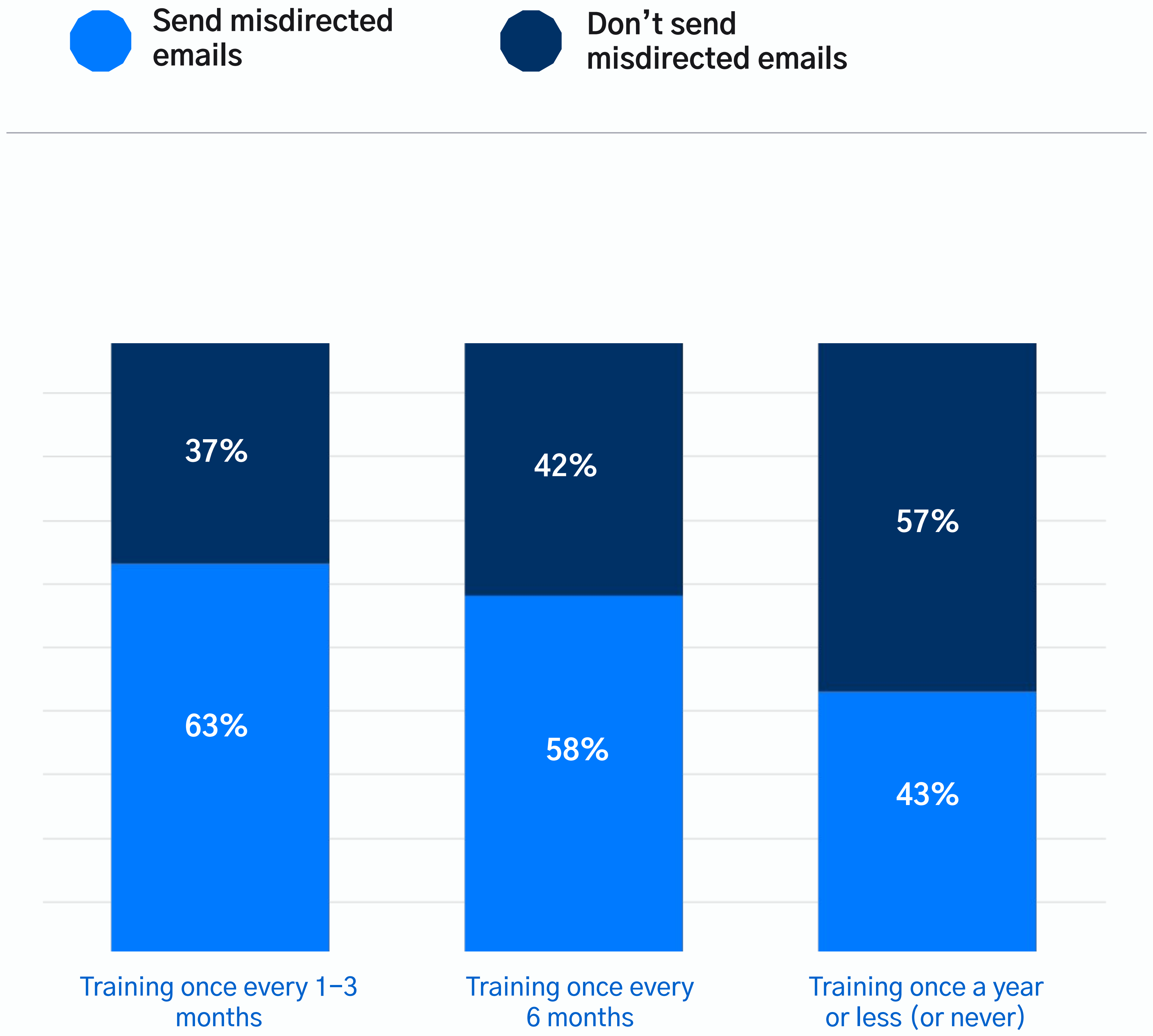
This number drops to 43% in organizations that conduct training once a year or less often.

Likewise, employees who receive training once every 1–3 months are almost twice as likely to send company data to personal email accounts as employees who receive training just once a year.

Percentage of survey respondents who send emails containing company data to personal email accounts vs. frequency of training



Percentage of survey respondents who send misdirected emails vs. frequency of training



As we've mentioned, training is more frequent in highly regulated industries like Financial Services and Healthcare.

But, is it working? Apparently not. These industries are among the most likely to download, save, or send work-related documents to their personal accounts before leaving a job or being dismissed.

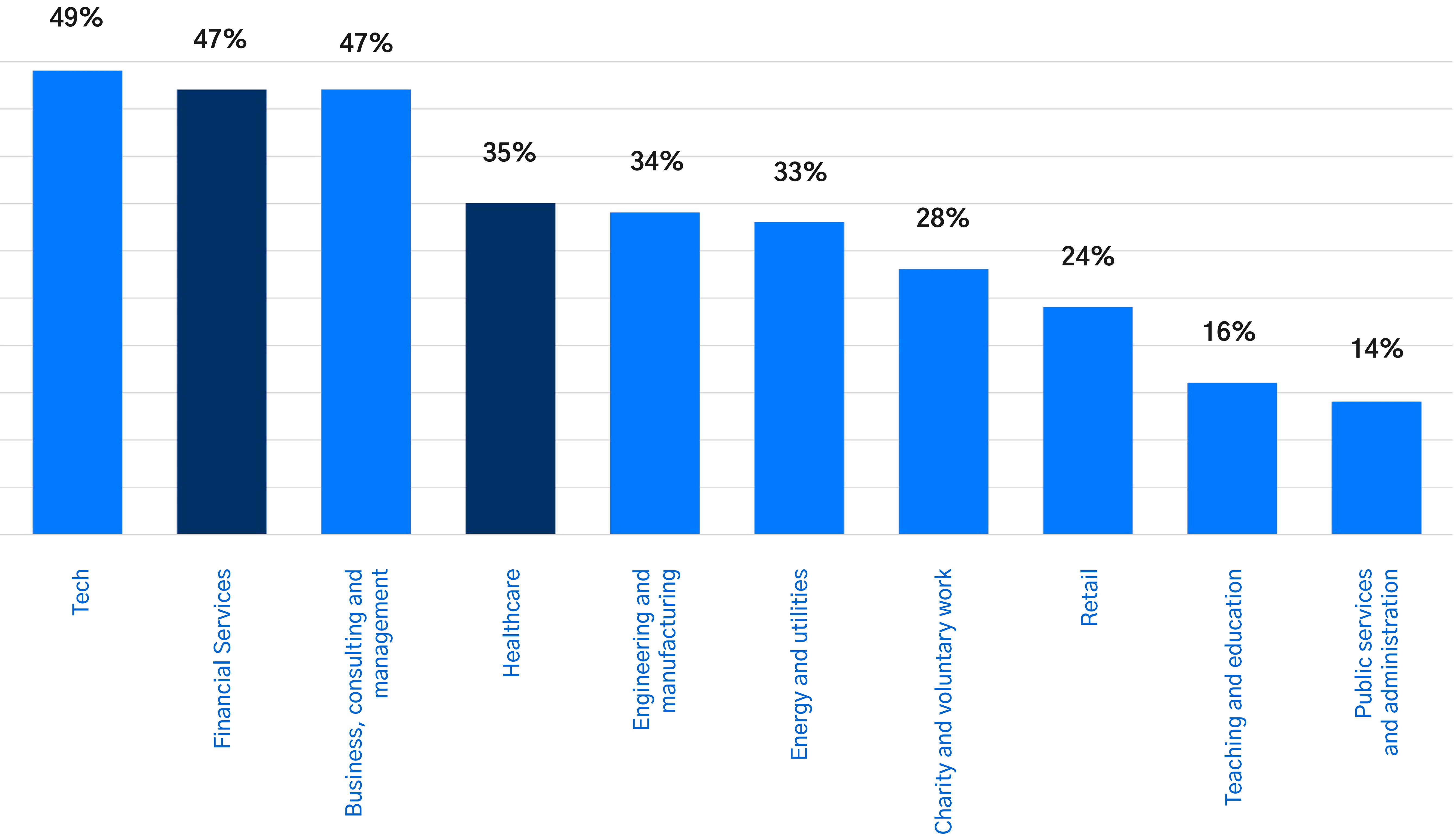
READ THE INDUSTRY REPORTS

State of Data Loss Prevention in Financial Services — DOWNLOAD NOW →

State of Data Loss Prevention in Healthcare — DOWNLOAD NOW →

State of Data Loss Prevention in Legal — DOWNLOAD NOW →

Percentage of employees who say they've downloaded, saved, or sent work-related documents to their personal accounts before leaving or after being dismissed from a job

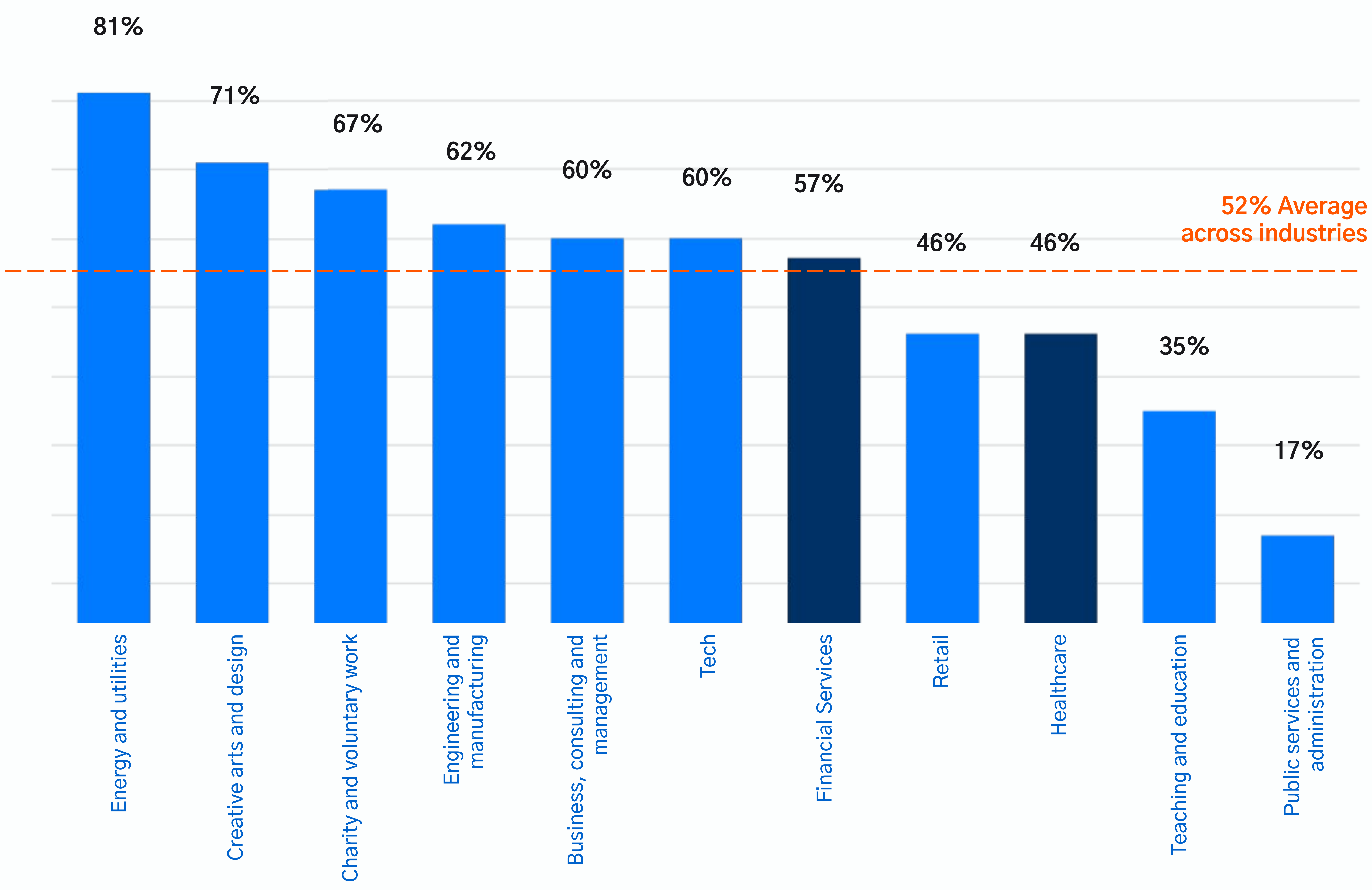


Additionally, over half (57%) of employees working in Financial Services admit to sending misdirected emails while 46% of employees working in Healthcare admit to the same.

While these two industries aren't amongst the biggest offenders, we can't overlook the *type* of data these employees handle.

Someone working in Financial Services might handle sensitive information like confidential M&A data or individual bank account details. Someone working in Healthcare might handle medical records and other Personally Identifiable Information (PII).

Percentage of employees who say they've sent misdirected emails



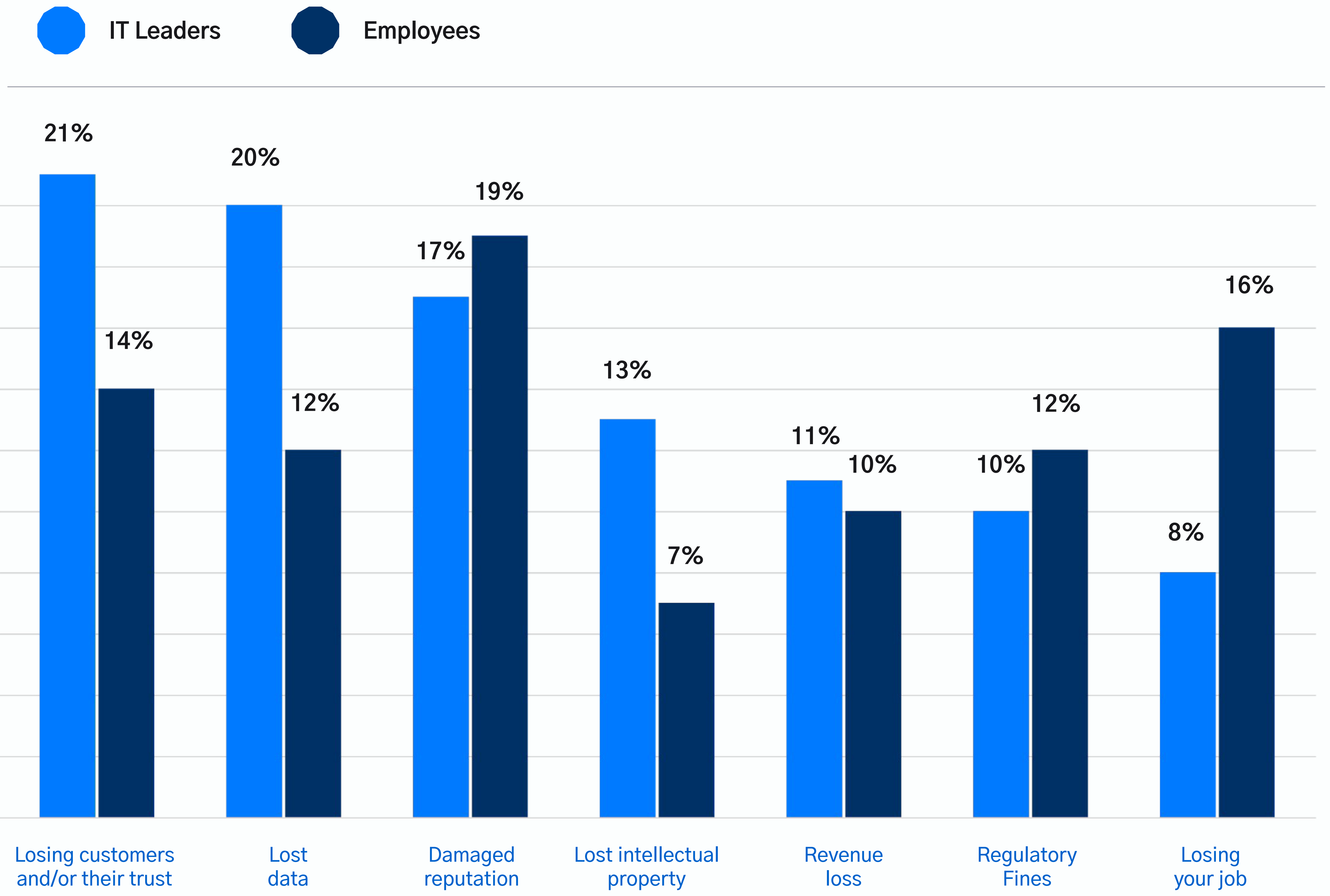
So, what are the consequences of leaked PII and other sensitive information like customer data?

A breach is bad news for everyone involved, including employees, the organization, and any third parties like customers, suppliers, or patients.

But, employees and IT leaders aren’t aligned on what they consider the biggest consequences to be.

Employees count “damaged reputation” and “losing their job” as the top consequences while IT leaders maintain that “losing customers and/or their trust” and “lost data” are the biggest implications. That may explain why most employees may never report mistakes related to data mishandling.

In your opinion, what is the biggest consequence of a data breach to an organization?



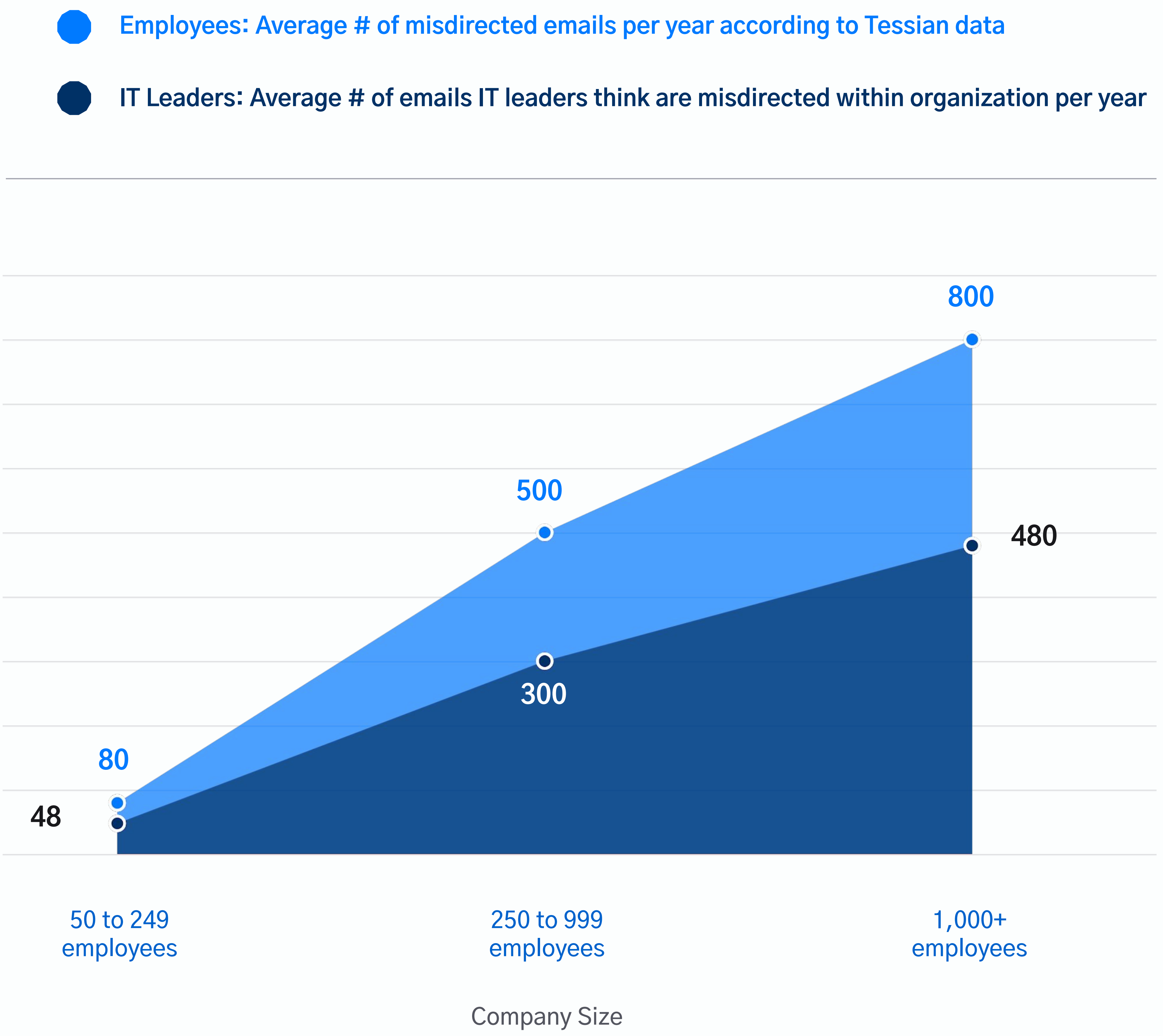
Employees Aren’t Reporting Their Mistakes

IT leaders working at organizations with 1,000+ people in the US estimate **480** emails are sent to the wrong person every year.

On the other hand, according to Tessian data, an average of 800 emails are misdirected in organizations with 1,000 employees during a single year.

That means at least 1.6x more misdirected emails are sent than IT leaders expect, many of which will contain structured and unstructured data in either the body copy, as attachments, or both. Depending on the industry and department of the sender, the consequences of this data falling into the wrong hands could be far-reaching.

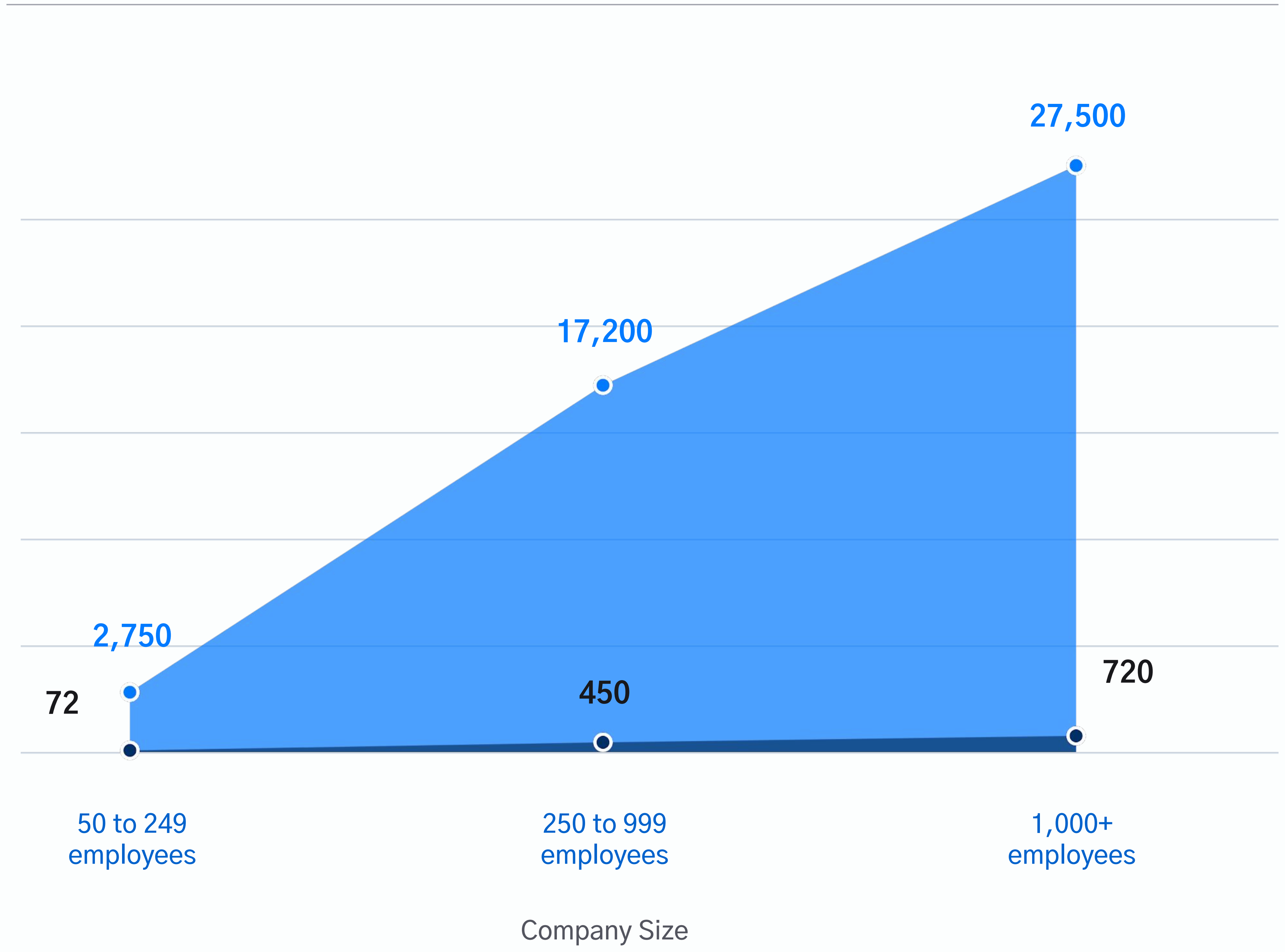
Average number of misdirected emails sent vs. estimated by IT leaders



Average number of emails sent to personal accounts vs. estimated by IT leaders

● Employees: Average # of unauthorized emails per year according to Tessian data

● IT Leaders: Average # of unauthorized emails IT leaders think are sent within organization per year



Non–compliant and unauthorized emails (emails sent to personal email accounts) are a bigger problem than most realize, too.

While they estimate just **720 unauthorized** emails are sent each year in organizations with 1,000+ employees, according to Tessian data, an average of 27,500 unauthorized emails are sent a year in an organization with 1,000 employees.

That’s 38x more than estimated.

NOTE

While sending company data to personal email accounts isn’t always malicious, it is often against security policies. Sending company data to a personal email account can also be a sign of intentional data exfiltration by, for example, a disgruntled employee on their way out or an insider threat.

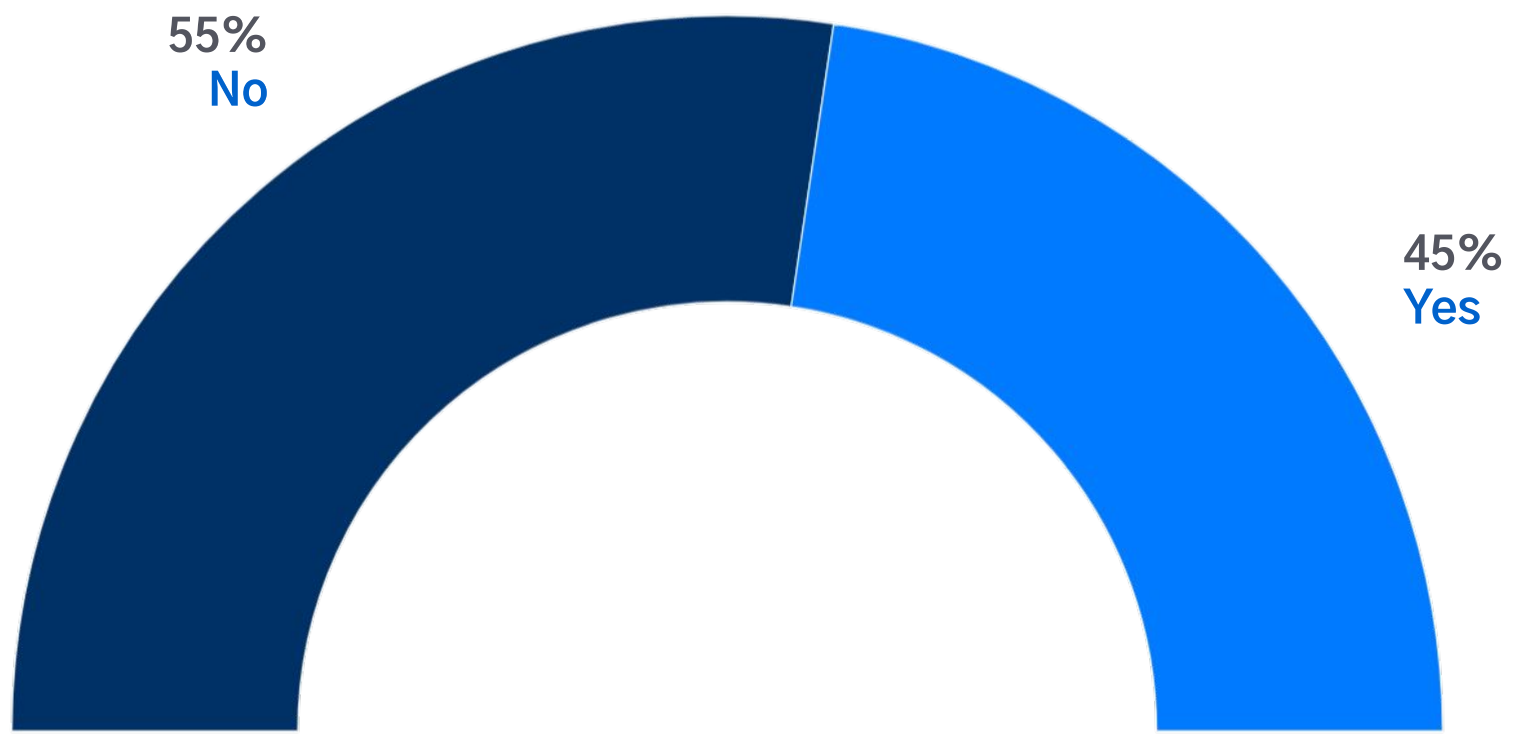
> I'm an optimist, so I genuinely believe that the average employee is trustworthy. I think if you give people the opportunity to make a good decision and make the easiest path to get their job done, the secure path, then they will take it. That is our job as security professionals.

Tim Fitzgerald
CHIEF INFORMATION SECURITY OFFICER
arm

And this doesn't even account for the 45% of US employees who admit to downloading, saving, or sending work-related documents to their personal accounts before leaving or after being dismissed from a job.

Does this mean that employees simply don't care about security best practice? Not necessarily. More often than not, they're just trying to do their jobs and are prioritizing efficiency over security. (Jump to page 29 for more insights around how security policies impede employee productivity.)

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



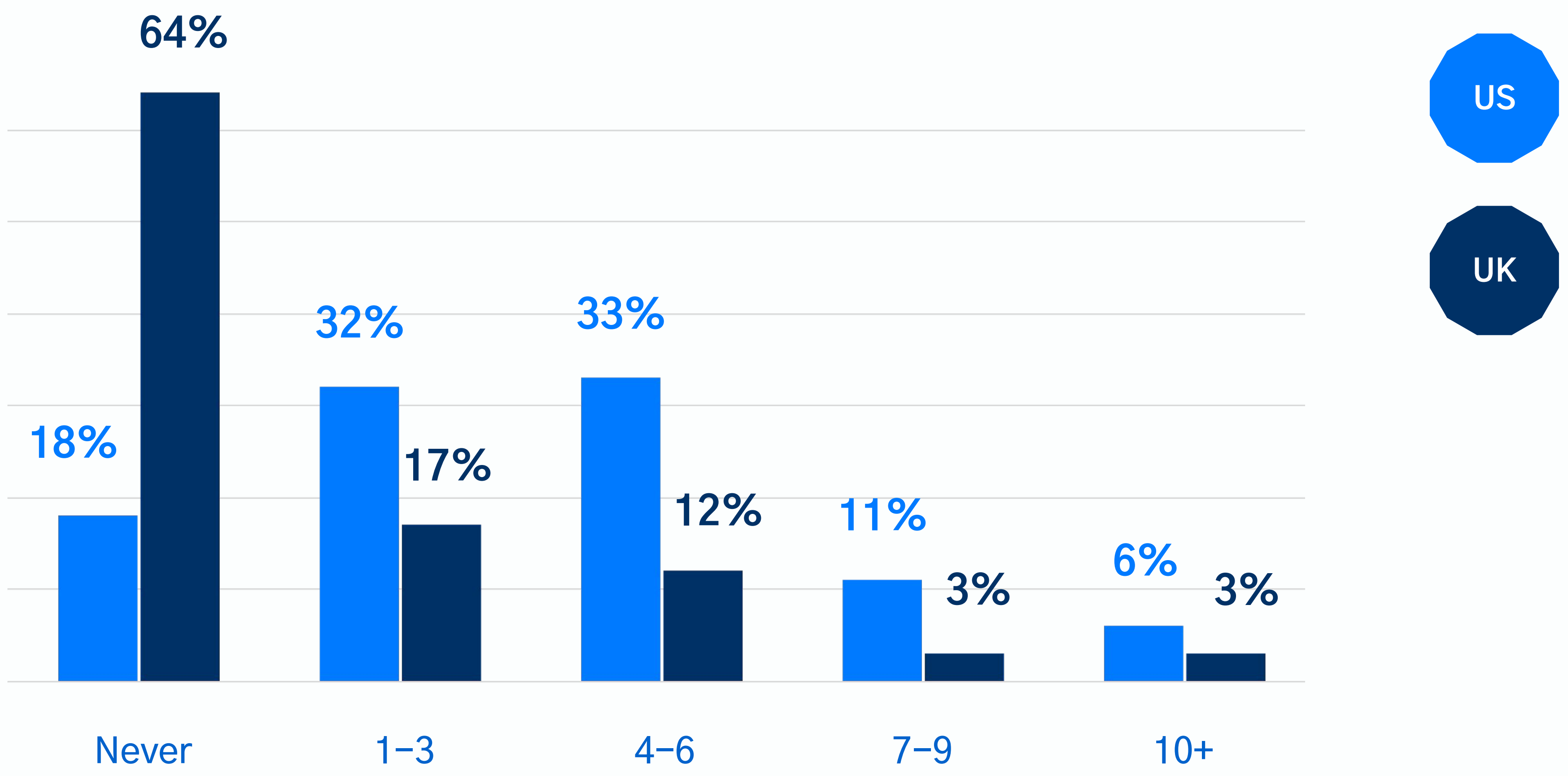
US Employees and Young, Digital Natives are the Least Careful and Compliant

The repercussions associated with data breaches in the UK and Europe grew immensely when the General Data Protection Regulation (GDPR) was introduced. And, while regulatory fines aren't top of mind as a consequence of a breach for either IT leaders or employees, it looks like data privacy regulations could actually influence how people handle data.

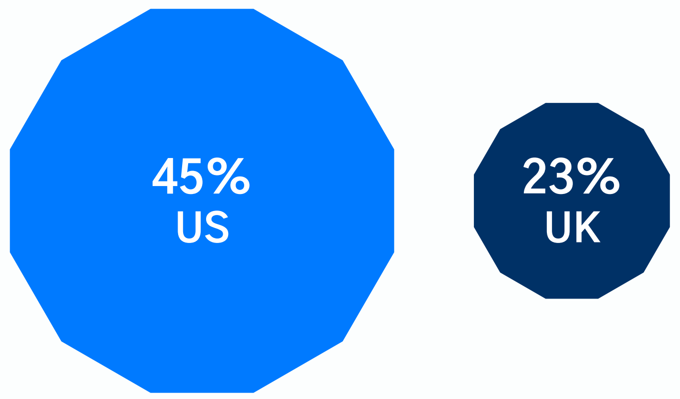
Case in point: Employees in the US break the rules more often than those in the UK.

Based on the survey results, employees in the US break the rules more often than those in the UK. Not only are they twice as likely to send unauthorized emails, they're also almost twice as likely to download, save, or otherwise exfiltrate work-related documents before leaving or after being dismissed from a job.

During the average month, how many times do you send company data to personal email accounts?



Have you ever downloaded, saved, or sent work-related documents to your personal accounts before leaving a job?

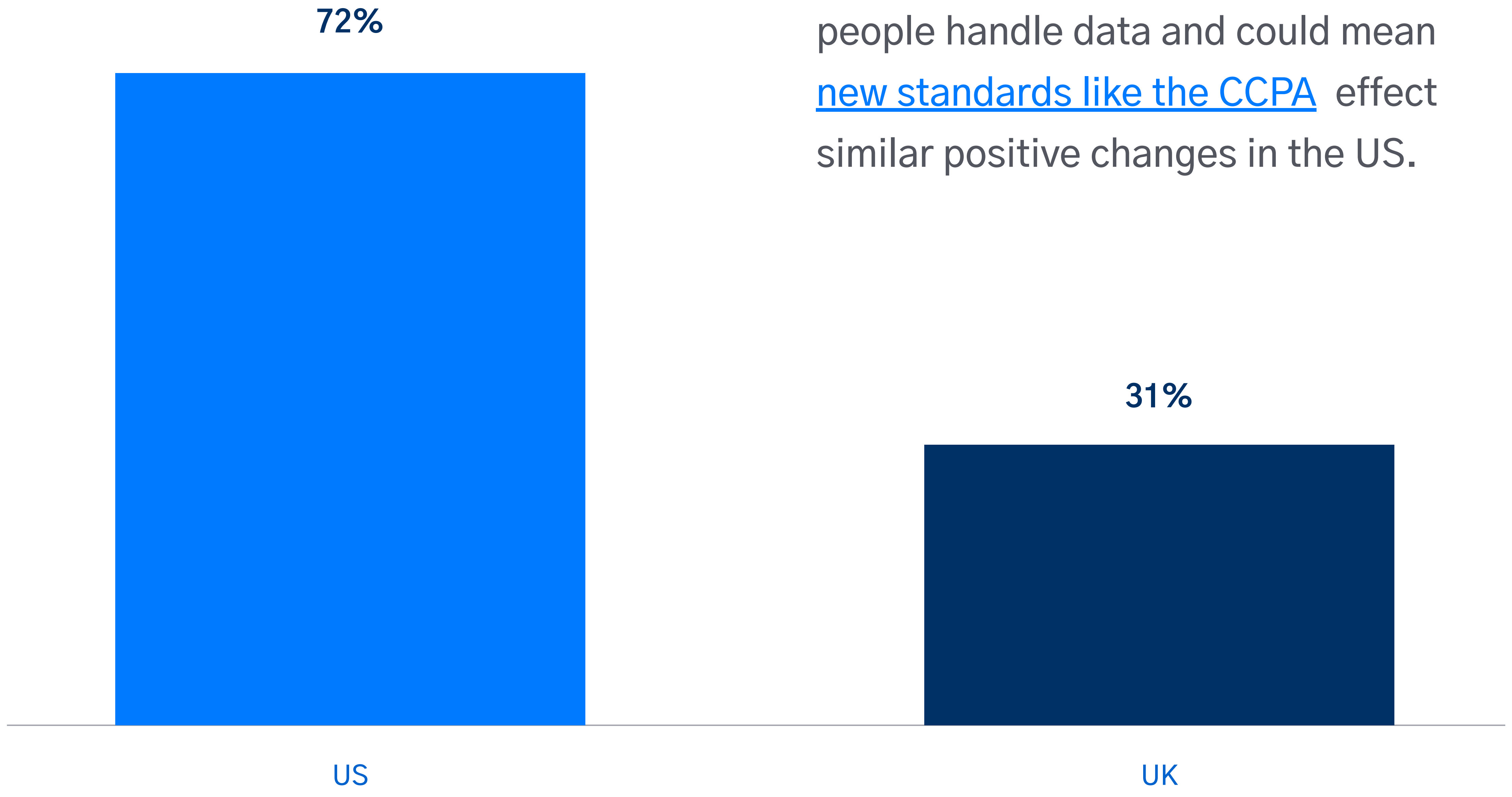


> The only action type that is consistently increasing year–on–year is frequency in Error. That isn't really a comforting thought, is it? Nevertheless, there is no getting away from the fact that people can, and frequently do, make mistakes and many of them probably work for you.
>
> Verizon 2020 Data Breach Investigations Report

verizon✓

They also seem to make more mistakes.

Percentage of employees who send at least one email to the wrong person each month



The likelihood of misdirecting an email doubles in the US, with 72% of US employees admitting to sending at least 1 email to the wrong person compared to just 31% in the UK.

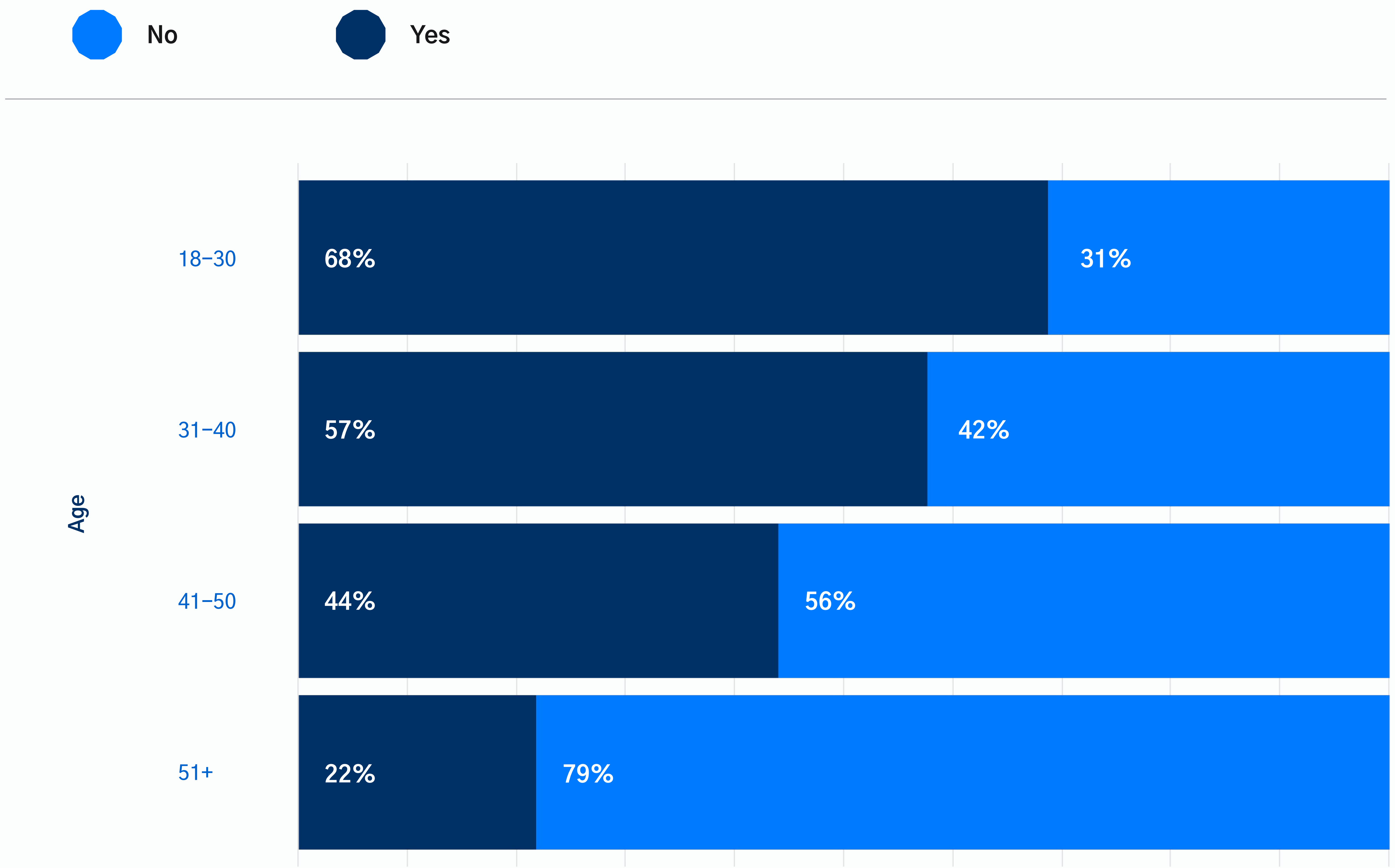
This suggests data privacy regulations like GDPR – which sparked a 44% increase in cybersecurity investment in the UK[7] – could be influencing how people handle data and could mean new standards like the CCPA effect similar positive changes in the US.

But, it's not just regional differences that are stark. There are trends in generational behavior, too.

For example, according to the survey respondents, 18–30–year–olds – who have grown up in an "always–on" culture – are 3x more likely to send misdirected emails than workers who are 51+. And, while 31–40 year olds are more careful on email, over half (57%) admit to firing off an email to the wrong person.

This is especially concerning because millennials (aged 22–38) represent the largest labor market share of any single generation.

Percentage of survey respondents who send misdirected emails

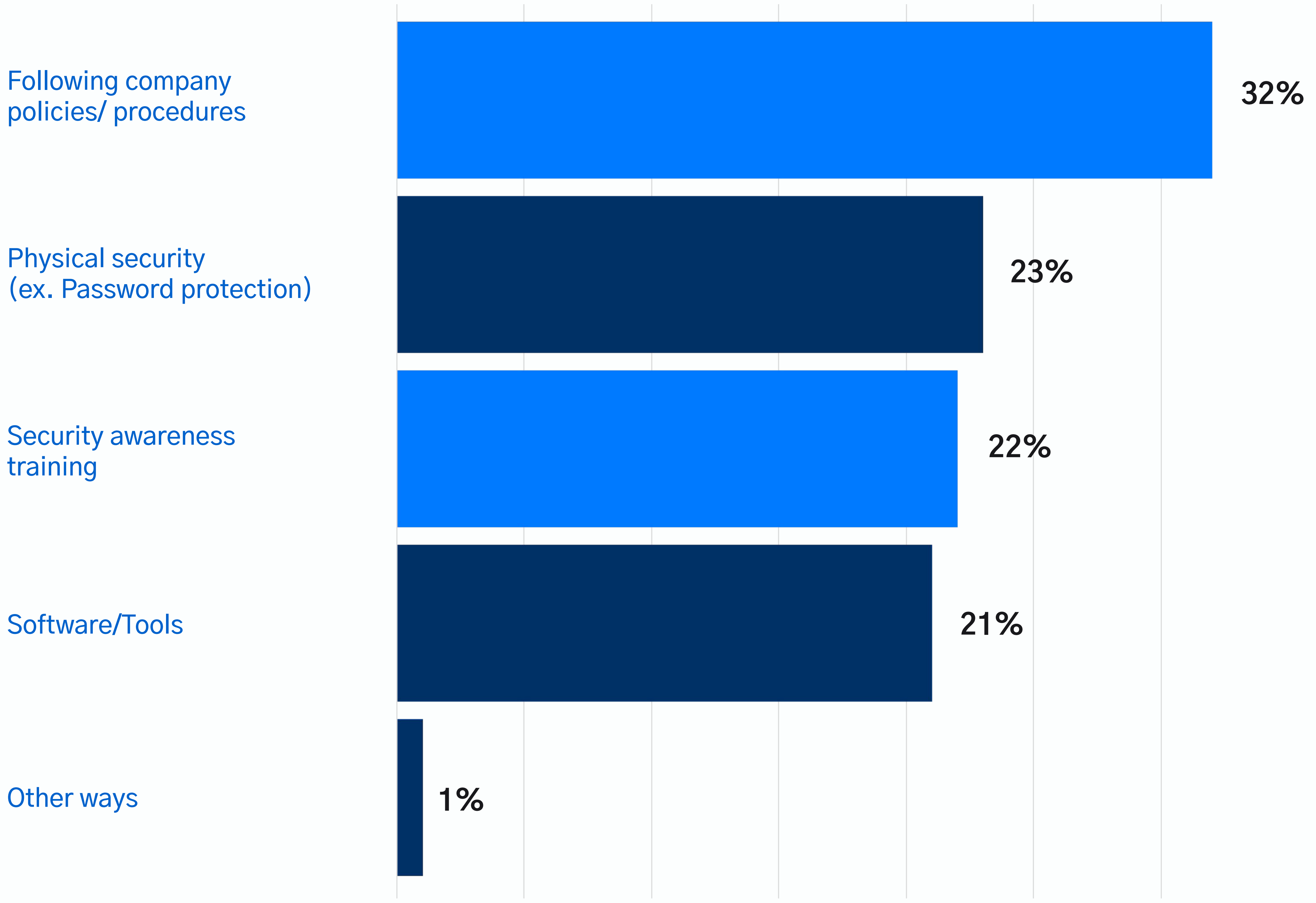


Security policies impede employee productivity

While IT leaders may be surprised that security awareness training isn't curbing non-compliant email activity, employees likely won't be. Only a fifth (22%) of employees said that security awareness training was the most effective way to keep the data they manage secure. Why? It could be because it's often unengaging, may seem irrelevant to their day-to-day-work, and doesn't impact behavior in the long-term.

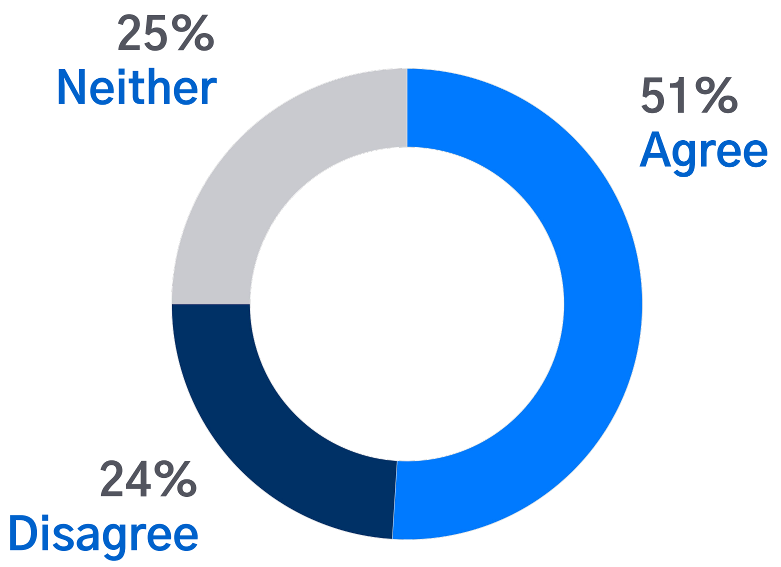
Instead, they count "following company policies and procedures" as the most effective way to keep data secure.

What is the most effective way for you to keep the data you manage for your company secure?



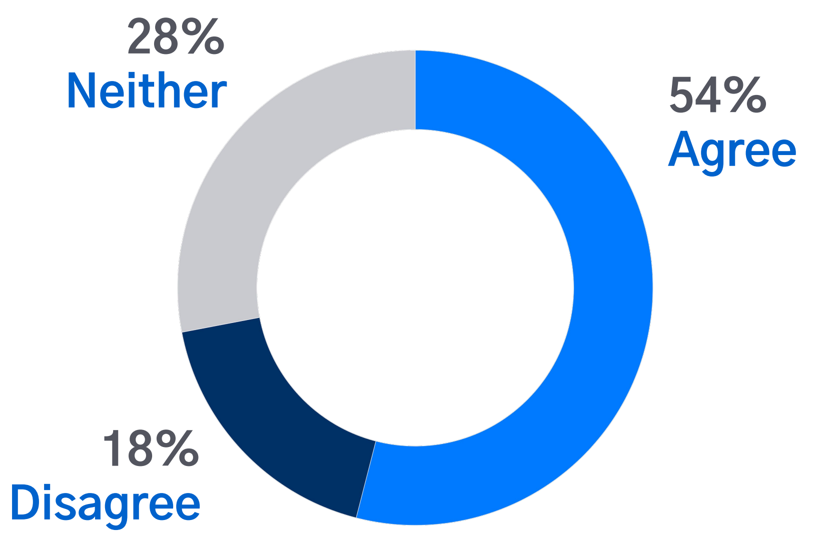
Interestingly, though, over half (51%) of employees also say that security tools and software impede their productivity at work.

"Security tools and software impede on my productivity at work."



While IT leaders create and implement security policies and procedures with the best intentions, they aren't always well-received, especially when many workers are under constant pressure to perform. 54% of employees say they'll find a workaround if security software or policies make it difficult or prevent them from doing their job.

"If security software or policies make it difficult or prevent me from doing my job, I will find a workaround"



> When you implement a DLP solution, workarounds are almost inevitable. Oftentimes, you have to build them in for your employees with specific policies. At least that way you know with some level of certainty that employees won't try to bypass the system, which means the data movement is still being monitored. Still, I wish there was a better way.

Chris Freeman
INFORMATION SECURITY PROGRAM LEAD

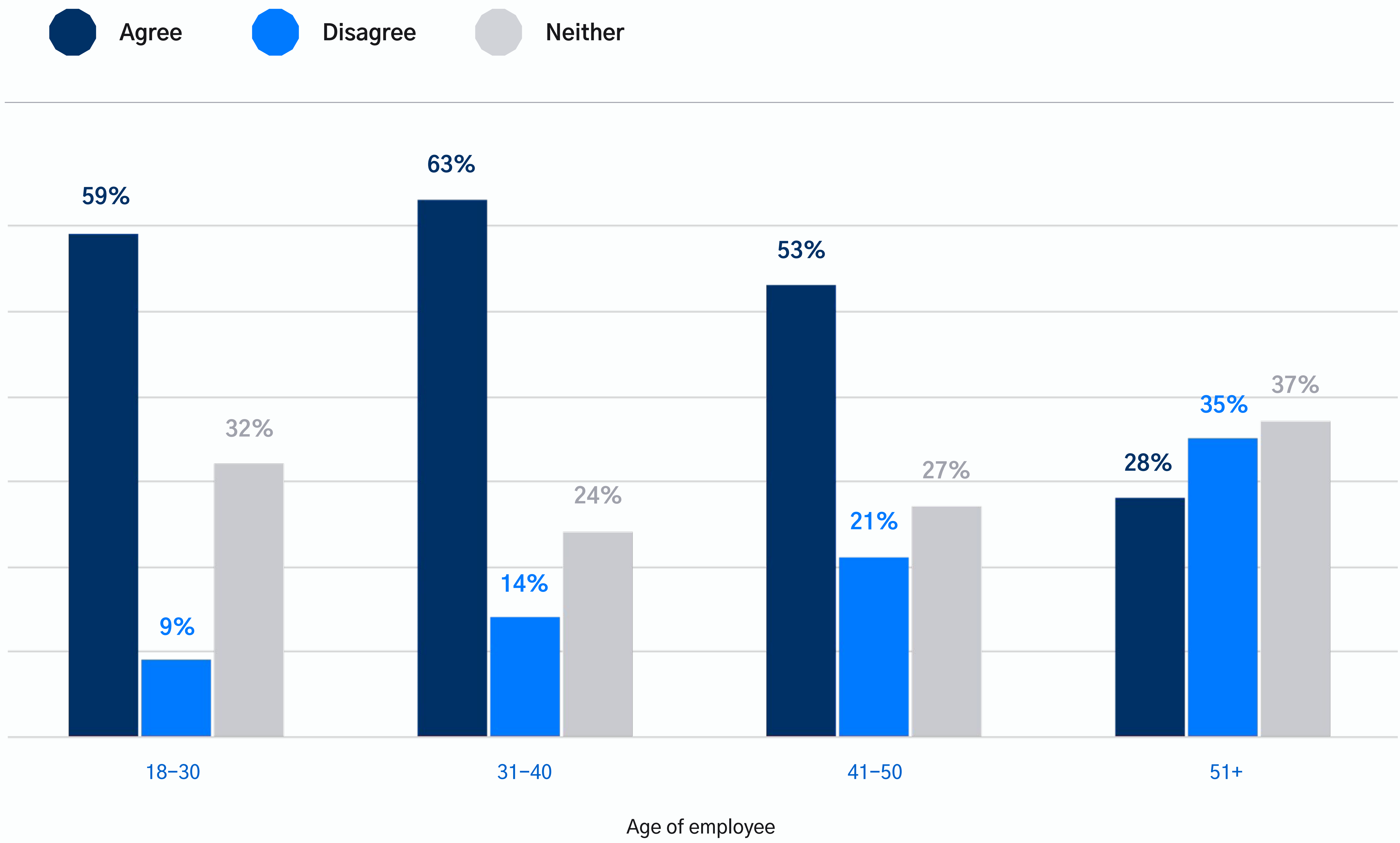
EY

It's only natural; employees are inclined to seek out the easiest or most convenient path to getting their jobs done.

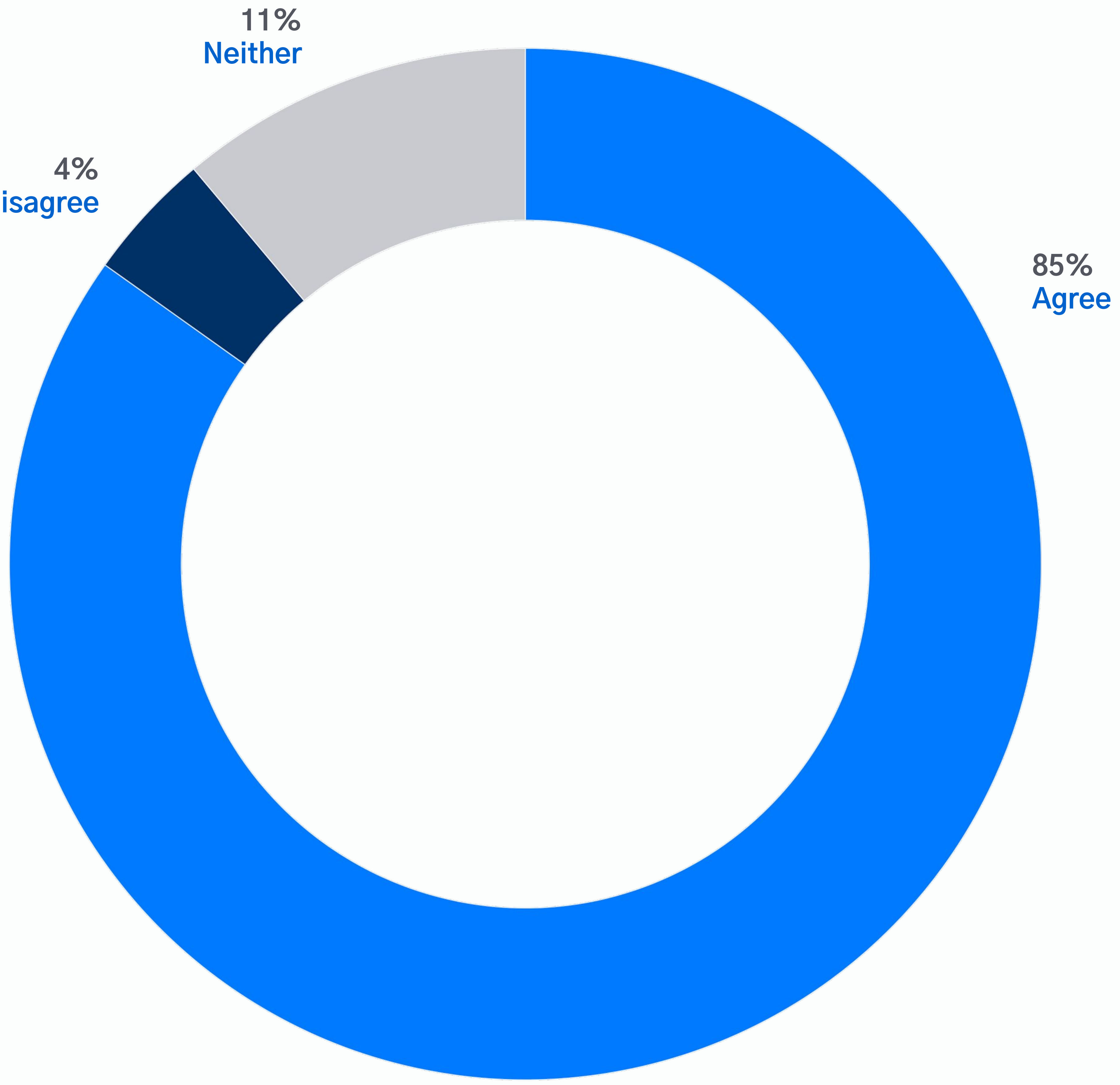
For many – especially younger workers – the easiest or most convenient path often involves skirting around security rules.

Conversely, survey respondents over 51+ are the only group of employees who are more likely to avoid workarounds than they are to find them. Why? While they could be more concerned about compliance, there's also the possibility that they simply aren't aware of shortcuts or alternatives.

"If security software or policies make it difficult or prevent me from doing my job, I will find a workaround."



"Rule-based DLP is admin-intensive."



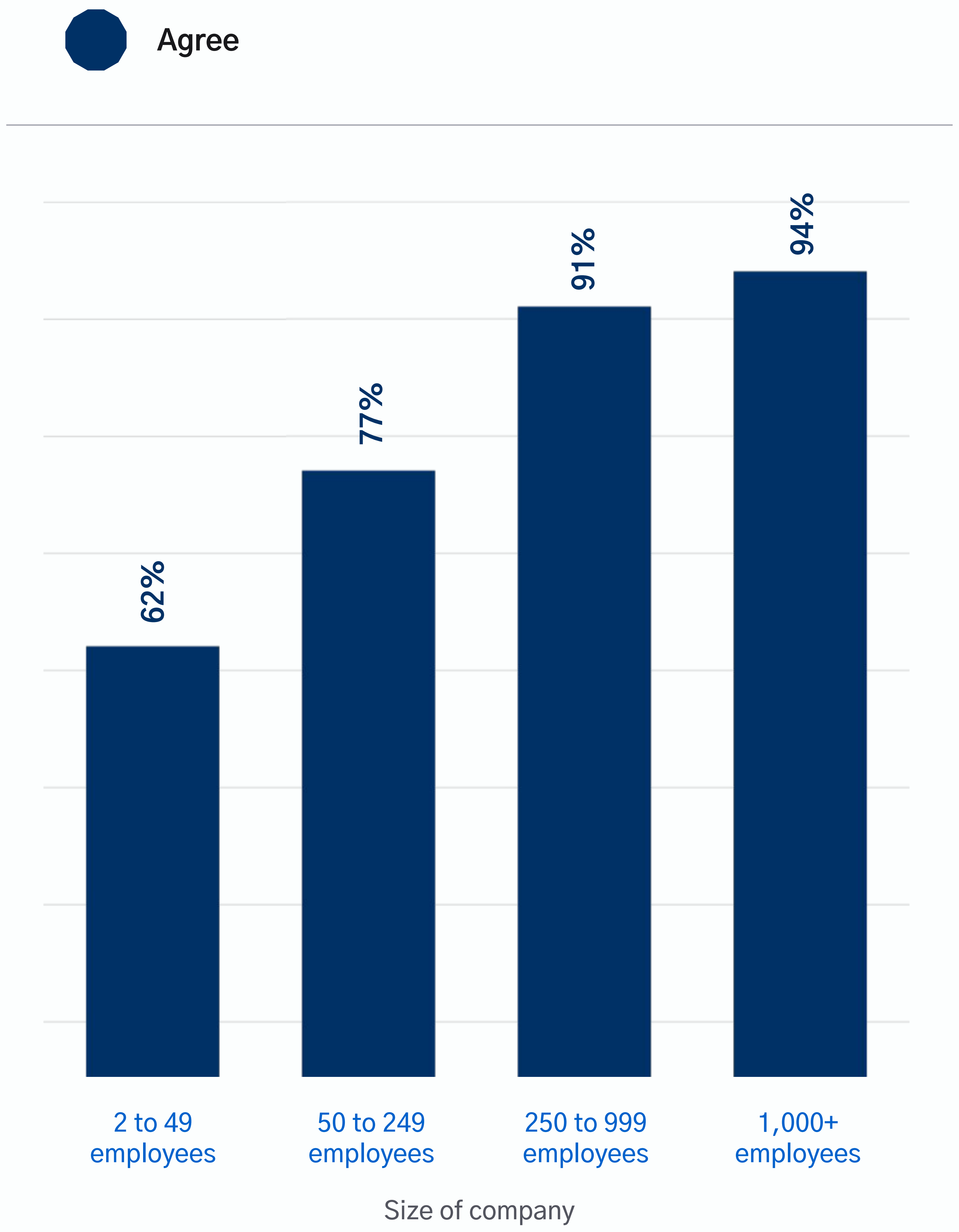
Rule-based Solutions Fall Short

IT leaders must identify a solution beyond training, policies, and procedures that provides insights into, and control over, how users handle sensitive information. That's where technology comes in.

The problem is, most of the DLP solutions available – whether Integrated DLP or Enterprise DLP – are rule-based. And you can't define and predict human behavior with rules.

Even if you *could*, the time and resources required to create rules, update rules, and analyze data captured by those rules would be more than any IT team could manage. This was echoed by our survey respondents, with 85% of IT leaders agreeing that rule-based DLP is admin-intensive.

"Rule-based DLP is admin-intensive."



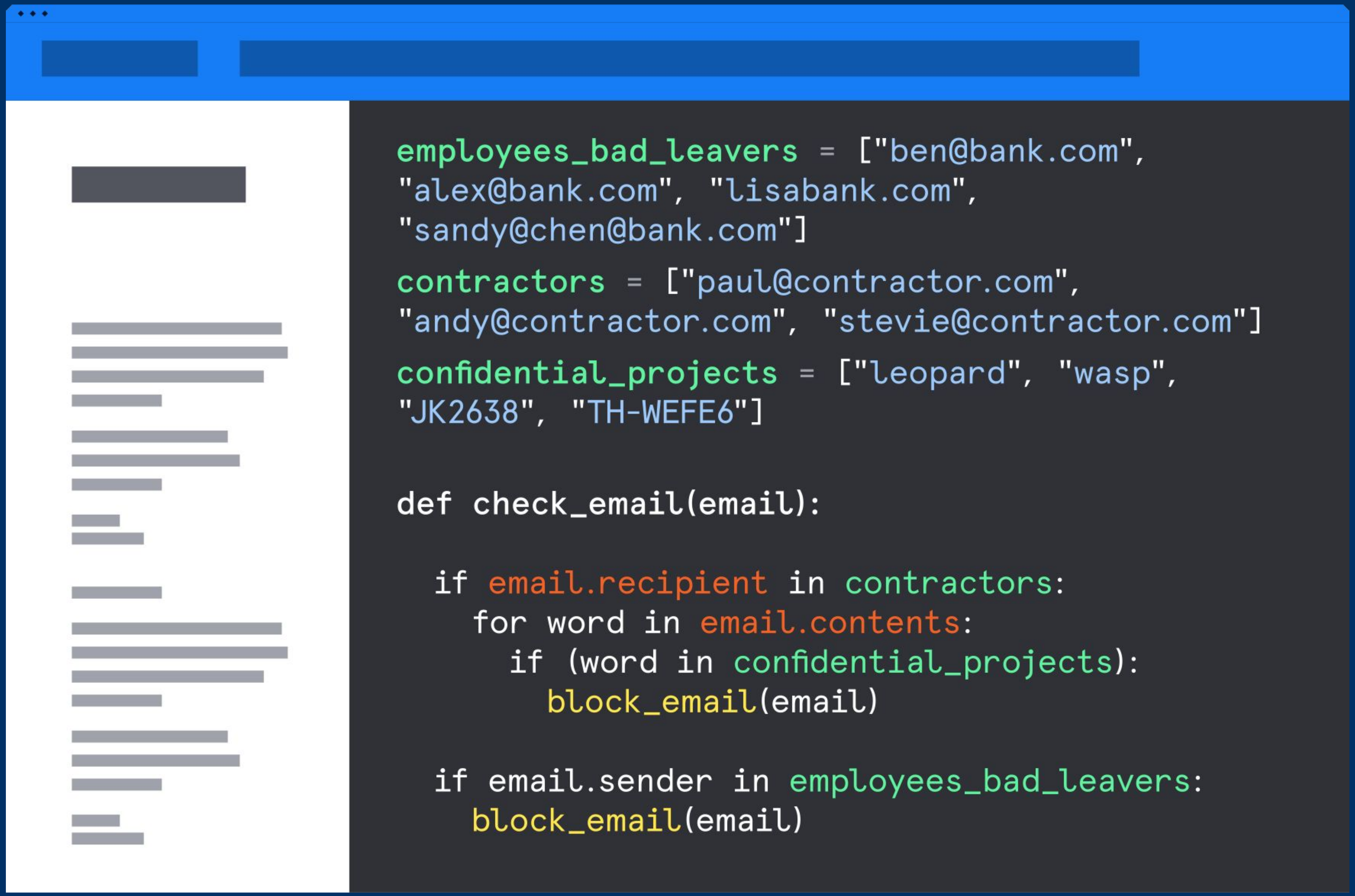
To really understand how heavy a burden rule-based systems place on IT teams, you have to consider what goes into configuring them. First, IT administrators have to have visibility on the problems they're trying to solve. *What* data is being handled? *Who* is handling that data? *How* could this data be mishandled? Those problems then have to be translated into "if-then" statements.

For example, if an organization wanted to prevent employees from sending emails to their personal email accounts, they could create the following rule: "If the recipient @gmail.com domain, then block the email."

The problem is, this rule would block an unnecessary amount of benign communications with @gmail accounts that aren't personal, for example freelancers, applicants, or employees at small firms. And, when you consider all the other possible examples of data loss – from bad leavers purposefully exfiltrating data to distracted employees misdirecting an email – you'd have to create custom policies for every single user in order to genuinely prevent data loss.

That's unfeasible.

Even in companies with fewer than 100 employees, the time and resources required to configure and consistently update rules are immense. It's no wonder, then, that the larger the company size, the more likely IT leaders are to agree that rule-based DLP is a burden on their team.



```
employees_bad_leavers = ["ben@bank.com",
"alex@bank.com", "lisabank.com",
"sandy@chen@bank.com"]
contractors = ["paul@contractor.com",
"andy@contractor.com", "stevie@contractor.com"]
confidential_projects = ["leopard", "wasp",
"JK2638", "TH-WEFE6"]

def check_email(email):

  if email.recipient in contractors:
    for word in email.contents:
      if (word in confidential_projects):
        block_email(email)

  if email.sender in employees_bad_leavers:
    block_email(email)
```

Rules need to be updated based on evolving relationships with other employees and third-parties. That means an update is necessary when new customers are onboarded, when there are any changes to the organizational structure of the business, and when access to systems or networks changes. And this doesn’t even scratch the surface for rules created around compliance and data privacy standards.

It simply isn’t sustainable and means that – inevitably – incidents will evade detection and turn into breaches.

R 1

P: A
owing
blem

ffective
urrent
ons?

15

CHAPTER 3

Next Generation DLP

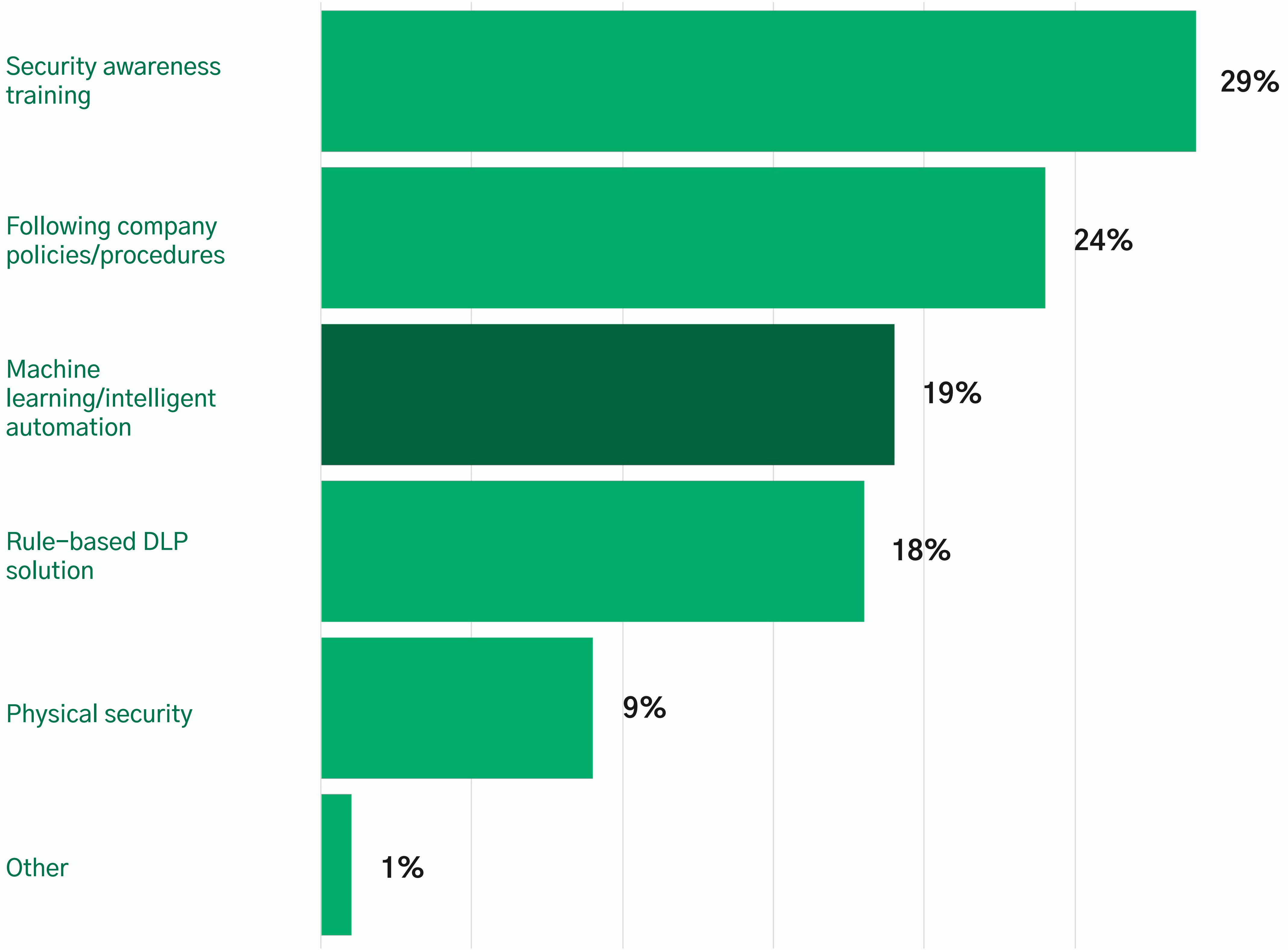
35

Security Leaders Trust Machine Learning

It takes a village to prevent data loss and, while security awareness training, up–to–date policies and procedures, and some rule–based configurations may have a place in security frameworks, they alone aren't the answer to DLP.

Machine learning based protections are a step in the right direction towards true DLP, though. In fact, one in five (19%) security leaders deem machine learning and intelligent automation the most effective way to prevent data loss.

What is the most effective way to prevent data loss?



Tessian's own DLP solutions are powered by machine learning technology and are deployed to customers across industries from SMBs to multinational enterprises and are detecting and preventing millions of inbound (and outbound) threats on email.

But, it's not just our customers who are talking about the power of machine learning. According to a new report from 451 Research, "the DLP market is ripe for change" and Tessian could be the next-generation solution organizations need to secure their data.

TRUSTED BY:

gubra
CHOATE
affirm
BRACEWELL

大成 DENTONS
CVC
Shearman SHEARMAN & STERLING
Schroders

JTC
rightmove
arm
Greenhill

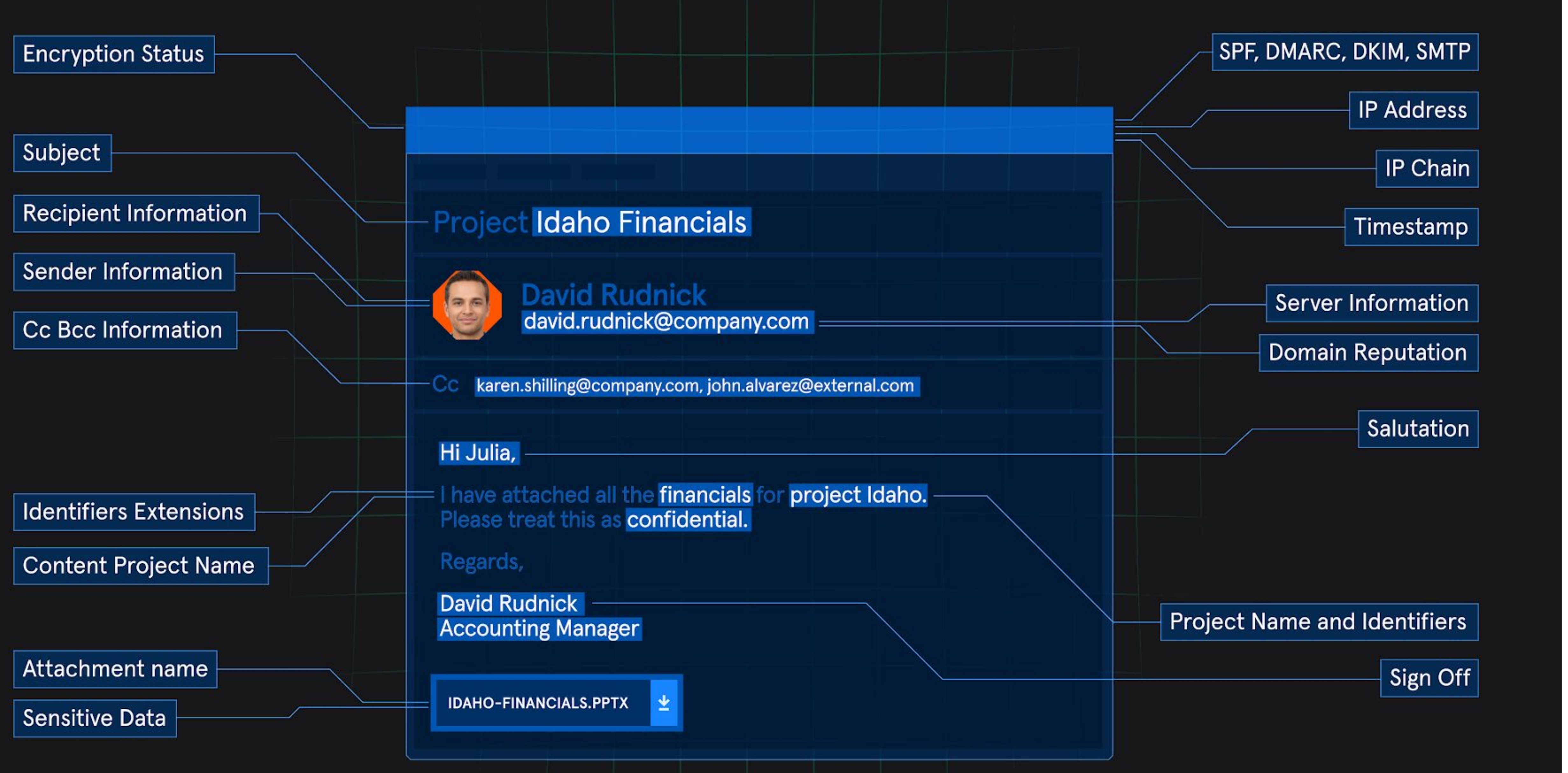
ITHACA ENERGY
HILL DICKINSON
Investec
GRAPHCORE

K&L GATES
ManGroup plc
clearwater
fieldfisher

> The speed and ease of deployment of Tessian has been unparalleled by any other solution we've dealt with, and has been our quickest GDPR win to-date. Misaddressed emails are a major cybersecurity problem that all organizations have to deal with, but trying to train human error out of employees is near impossible. Tessian's machine intelligence plays a vital role in helping mitigate these kinds of errors and ensure that customer data remains secure and private.

Chris White
FORMER GLOBAL CHIEF INFORMATION OFFICER
CLYDE&CO

How Does Tessian Prevent Data Loss?



Project Idaho Financials

David Rudnick
david.rudnick@company.com

Cc karen.shilling@company.com, john.alvarez@external.com

Hi Julia,

I have attached all the financials for project Idaho.
Please treat this as confidential.

Regards,

David Rudnick
Accounting Manager

IDAHO-FINANCIALS.PPTX

Your email data is an invaluable source of threat intelligence. Tessian turns that data into your best defense against inbound and outbound email security threats.

There's a wealth of information behind each and every email communication employees send and receive. By harnessing the power of this data through machine learning, our Human Layer Security technology understands human behavior and relationships, enabling Tessian Enforcer to automatically detect and prevent data exfiltration attempts and Tessian Guardian to automatically detect and prevent misdirected emails. Importantly, Tessian's technology automatically updates its understanding of human behavior and evolving relationships by continuous analysis and learning of the organization's email network.

No rules needed.

Tessian: The Most Effective DLP Solution

> Tessian gives us an opportunity to take a proactive step to prevent the bad things happening in the first place. I think that’s important, because historically the approach has been how do you detect it after it has happened.

Rob Hyde
CHIEF INFORMATION SECURITY OFFICER
Schroders

Instead of expecting people to do the right thing 100% of the time, we think it’s better to preempt these errors by detecting and preventing them from happening in the first place.

That way, IT leaders can proactively stop sensitive information from leaving their environment, company IP stays secure, compliance standards are met, and customer trust is maintained.

But, we also think it’s important to enable and empower employees to do their best work and reduce the investigative burden on IT teams.
Tessian does all of the above.

Without inhibiting employee productivity or putting extra pressure on IT teams, machine learning algorithms trained on millions of **your own historical email data points** can understand normal patterns of employee behavior and accurately and automatically predict when they’re making a mistake or breaking the rules.

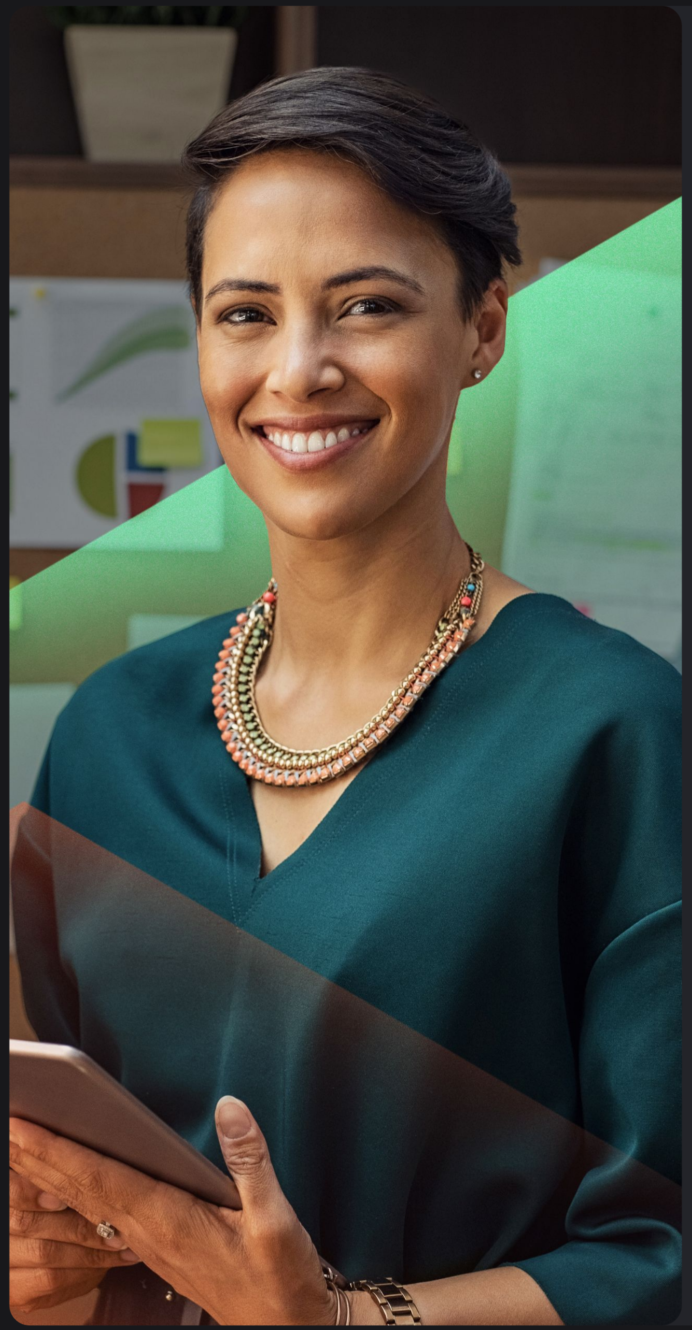
What’s more, Tessian offers protection on both desktop and mobile, meaning your employees are protected wherever – and however – they work.

But, detection is the first step in prevention. Unlock the value in cybersecurity a demo of Tessian’s Intelligent Cloud Email Security platform. Click here to see how many misdirected and unauthorized emails have been sent within your organization in the past year.

TESSIAN

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.

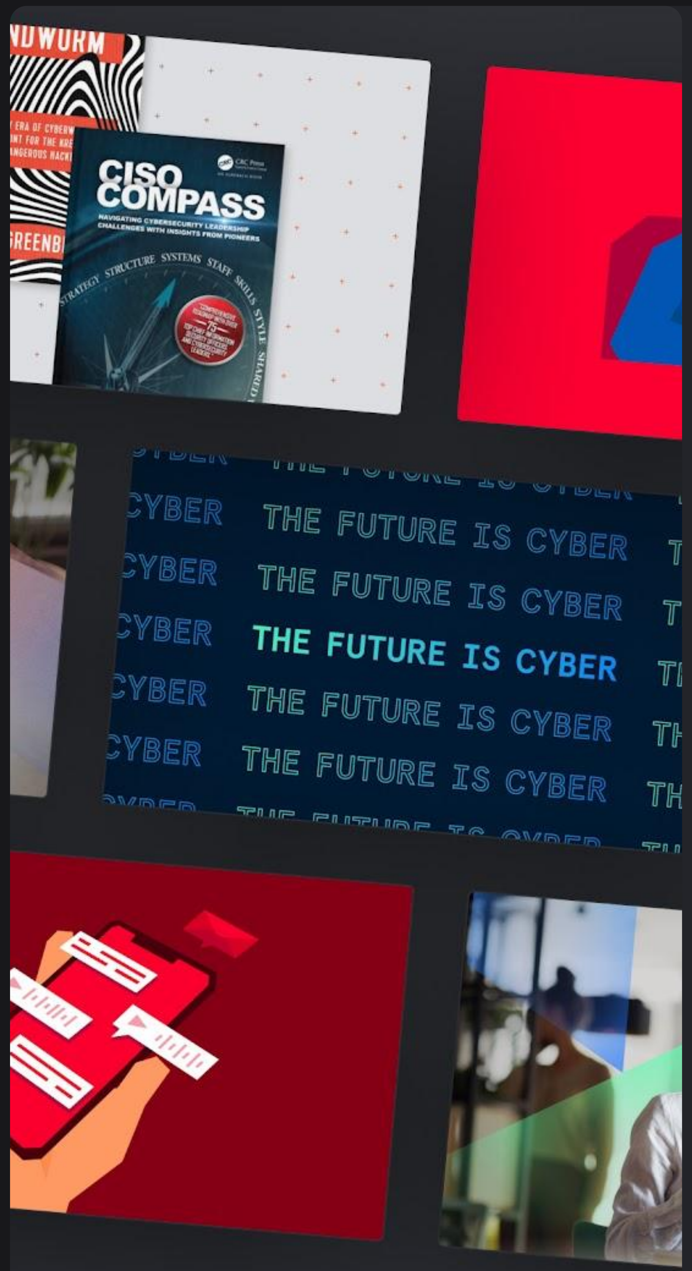
TESSIAN.COM



Learn More About Tessian.

Want to learn more about how Tessian prevents spear phishing, business email compromise, account takeover, and other targeted email attacks?

REQUEST A DEMO →



More Insights, Every Week.

Subscribe to our newsletter 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 →

Appendix

[1] 2020 Cost of Insider Threats Global Report

[2] DLA Piper's GDPR Data Breach Survey 2020

[3] eSecurity Planet's Ultimate Guide to IT Security Vendors

[4] Raticati's Email Statistics Report 2015–2019

[5] 2019 Adobe Email Usage Study

[6] Verizon's 2019 Data Breach Investigations Report

[7] Department for Digital, Culture, Media & Sport

About the Report

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.

Publically available third-party research was also used, with all sources listed on this page.

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 →