TESSIAN

BACK TO WORK

Security Behaviors Report

As businesses transition back to the office, and the majority adopt a hybrid approach to work, what security pitfalls do IT teams need to address and how will employees' behaviors have changed?

Share this report

Jump to Page 8 ↗

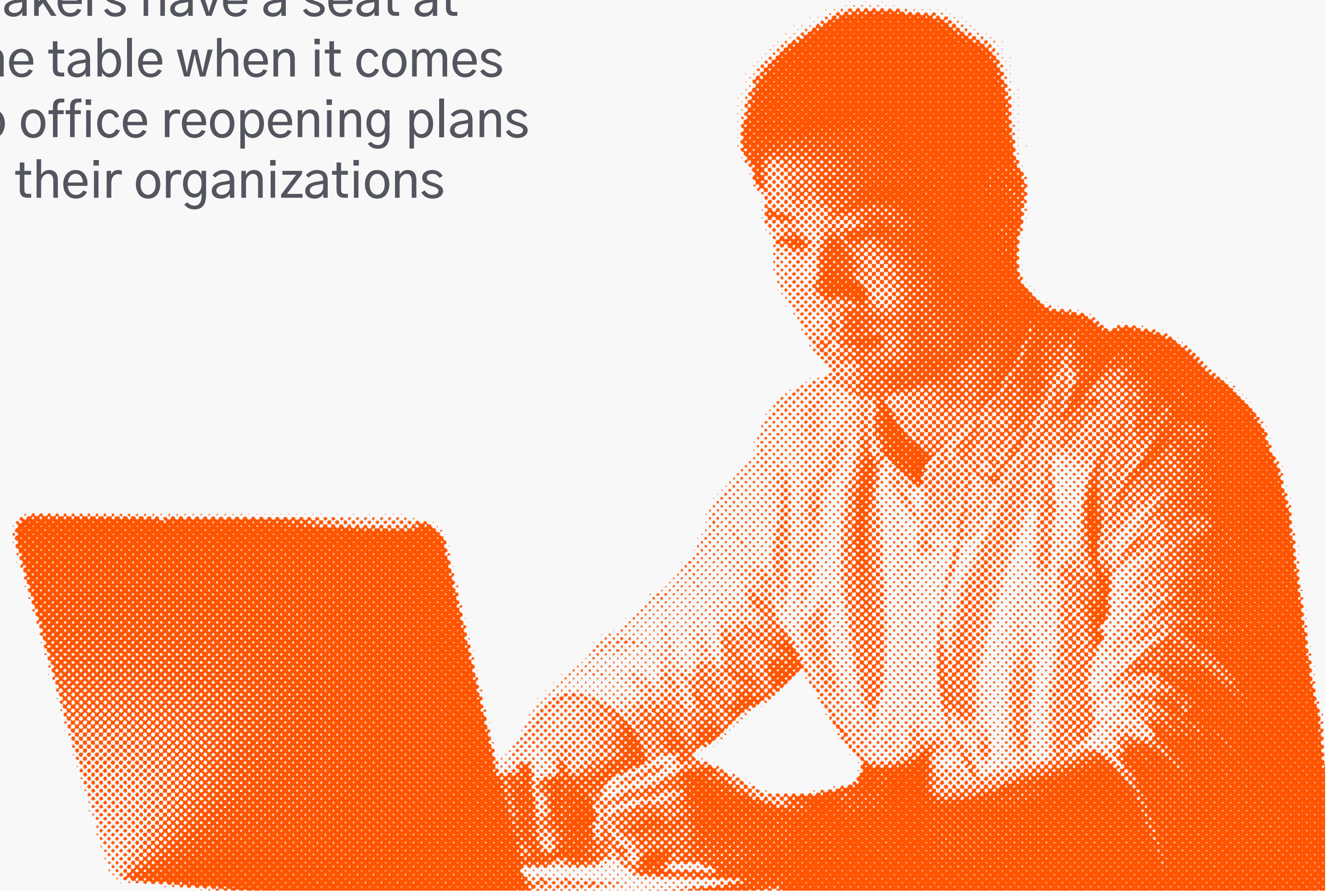
56%

of IT leaders believe employees have picked up bad cybersecurity behaviors since working from home

Jump to Page 5 ↗

Nearly 7 in 10

cybersecurity decision makers have a seat at the table when it comes to office reopening plans in their organizations



1 in 3

employees think they can get away with riskier security behaviors when working remotely

Jump to Page 10 ↗

40%

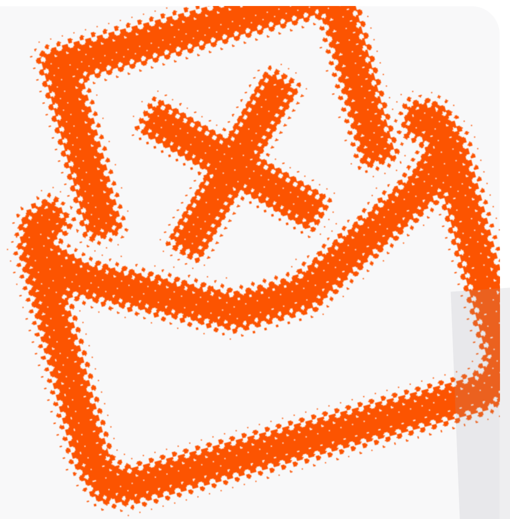
of employees plan to bring their personal device into the office to work on

Jump to Page 12 ↗

54%

of IT decision makers are worried remote workers will bring infected devices and malware into the office

Jump to Page 12 ↗

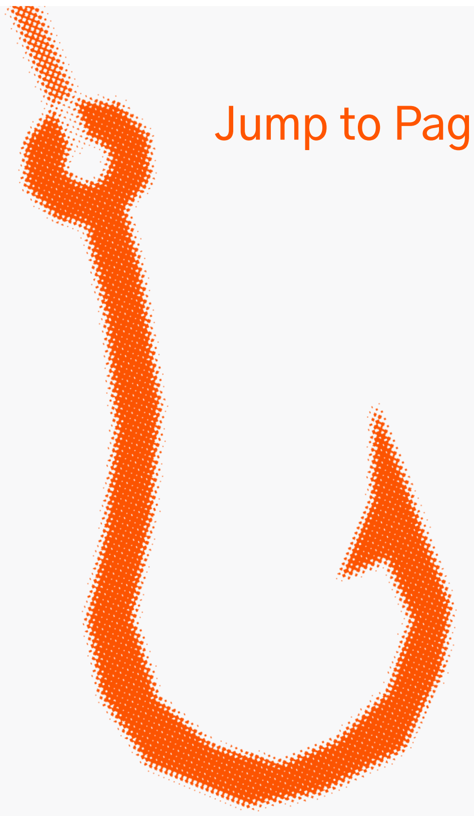


69%

of IT leaders think that ransomware attacks will be a greater concern in a hybrid workplace

Jump to Page 13 ↗

Jump to Page 15 ↗



67%

of IT professionals predict rise in ‘back to office’ phishing emails.

Jump to Page 17 ↗

42%

of younger employees have made cybersecurity mistakes while working from home that no one will ever know about

Jump to Page 17 ↗

27%

of workers are afraid to tell IT they’ve made a security mistake

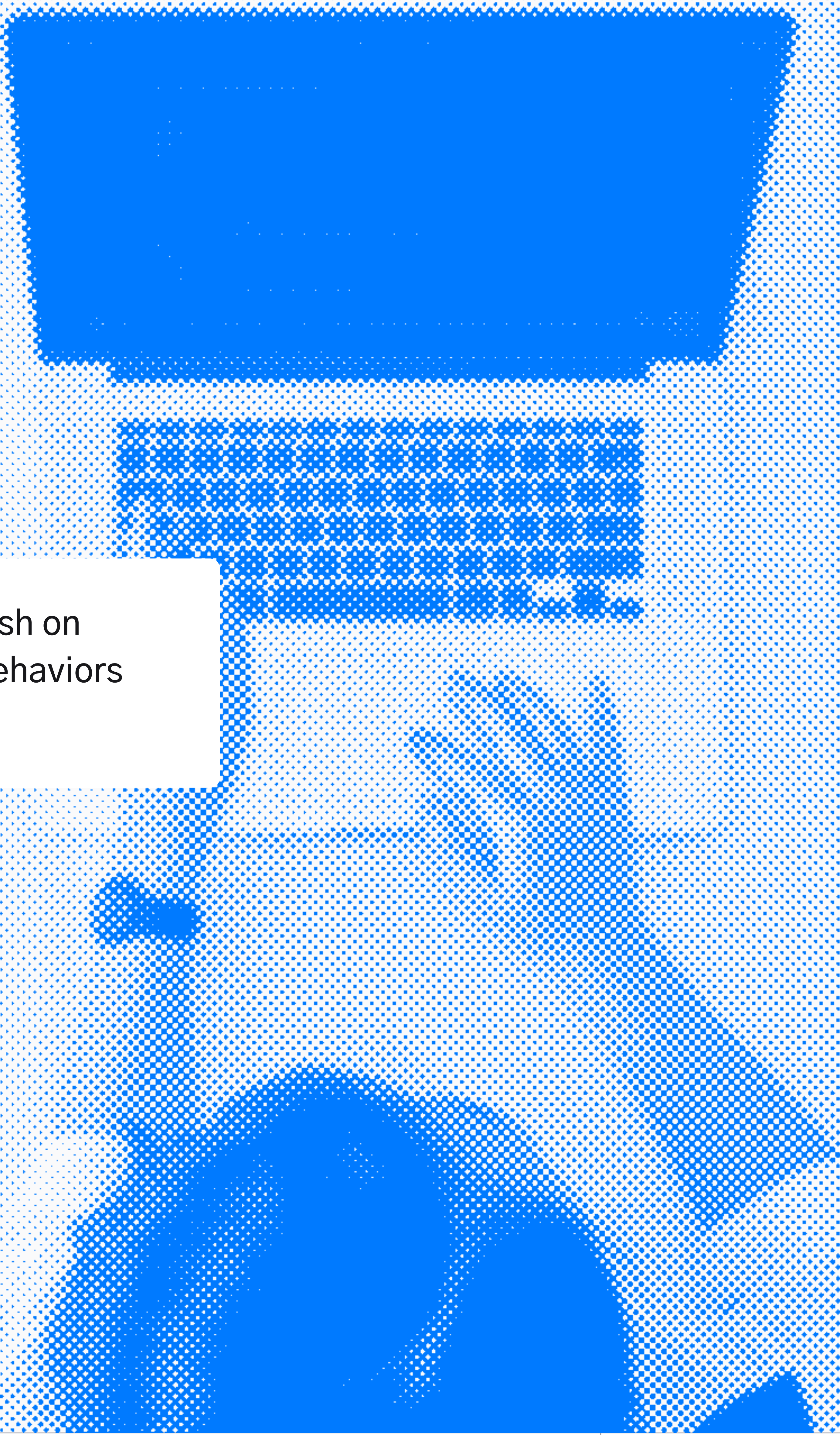
Hybrid is the way forward for post-pandemic workforces, say nine out of 10 organizations surveyed by McKinsey.

As employees have grown accustomed to a world without commutes and a better work/life balance, businesses will be missing a trick if they don’t allow their employees to choose where they want to work in the future. So, thankfully, most companies have, at the very least, a high level plan for how they will carry this out.

Part of that plan must factor in cybersecurity, though.

IT leaders have done an amazing job in responding to the shift to remote work. Now, another significant change in working behaviors equals a fundamental shift in security priorities. So, as businesses plan for the “great return”, certain questions need to be asked.

We answer these questions in this report.



① And what role does the CISO play in this new hybrid way of working?

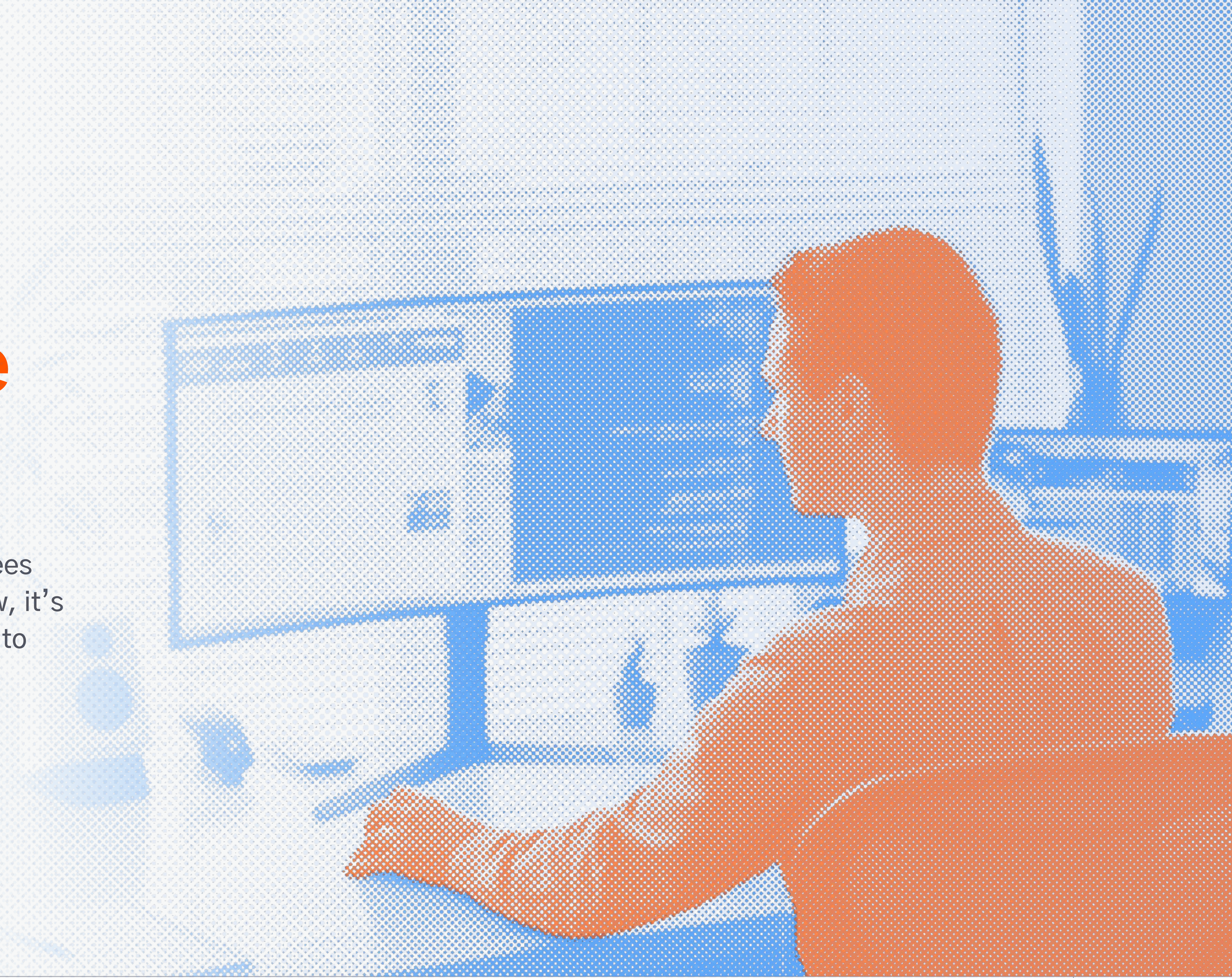
② Will employees need a refresh on acceptable cybersecurity behaviors in the workplace?

③ To what extent will the threat landscape change?

PART 1

Cybersecurity in the ‘New Normal’

IT leaders did an amazing job in making sure their employees could work remotely when lockdowns came into force. Now, it’s time to take those learnings, and prepare for new threats, to help businesses thrive in this hybrid model.

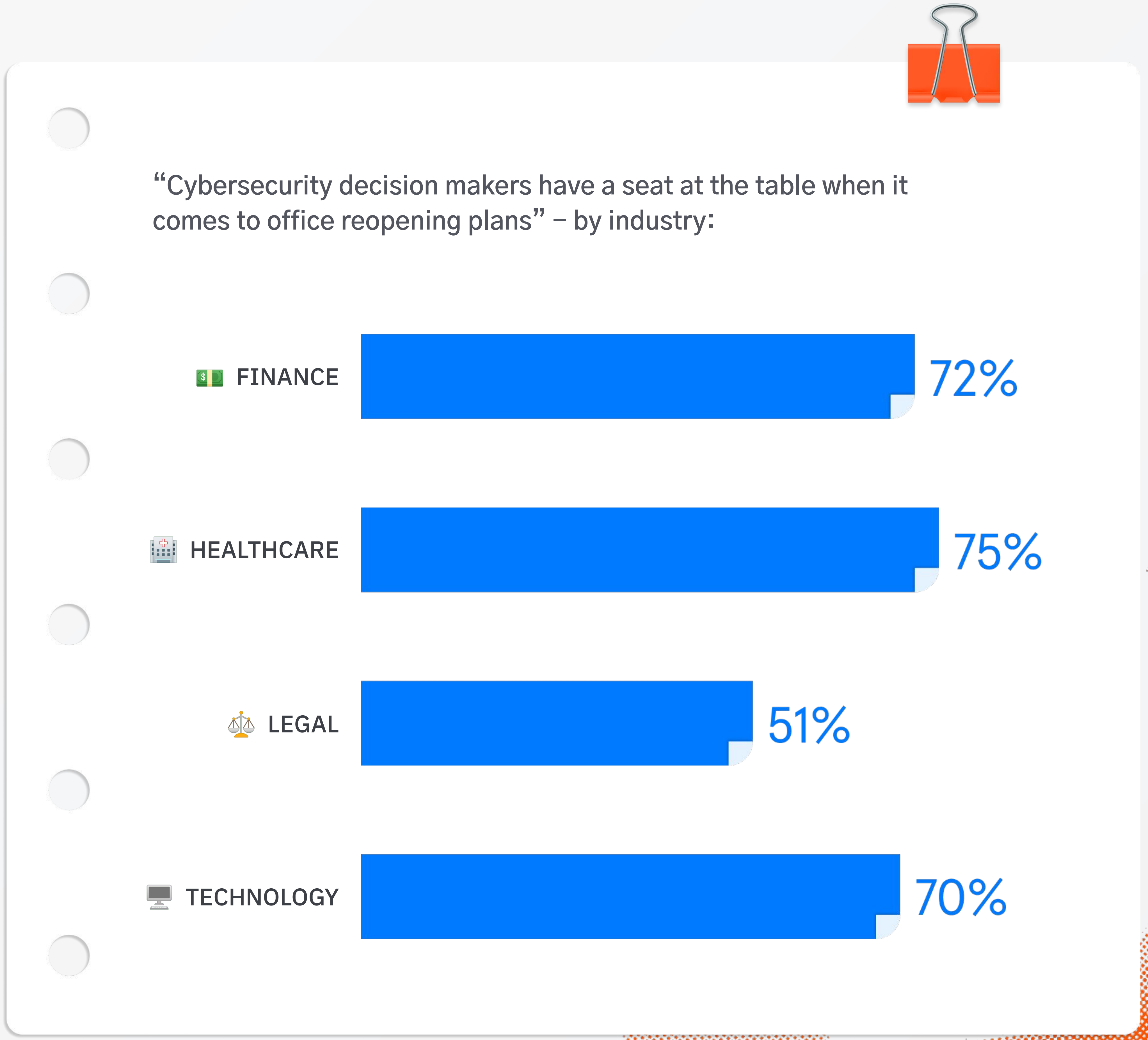


There’s no denying that cybersecurity is now business-critical – and the CISO has a huge role to play in a hybrid way of working.

So it’s encouraging to see that 67% of IT decision makers we surveyed say that they have had a seat at the table when it comes to office reopening plans in their organizations.

This was most likely the case in healthcare organizations, and least likely in legal firms.

> “To be successful in implementing security change, you have to bring the larger organization along on the journey. CISOs no longer live in the back office and address just tech aspects. It’s about being a leader and using security to drive value.”
>
> KEVIN STORLI
> Global CTO and UK CISO at PWC



“Cybersecurity decision makers have a seat at the table when it comes to office reopening plans” – by industry:

A seat at the table is likely backed by the incredible work CISOs have delivered during the pandemic and the mandatory remote work set-up.

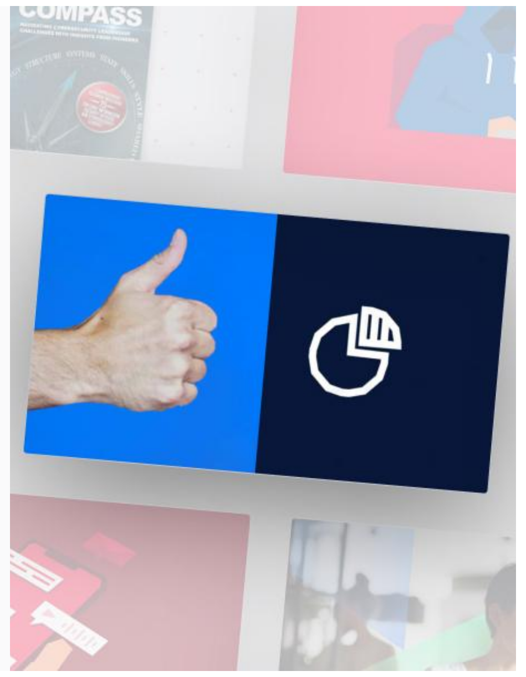
They have proven how critical their role is, with 59% of IT leaders voicing that their role and responsibilities have been recognized as more important by the senior leadership team over the past year. This sentiment was overwhelmingly shared by respondents in the healthcare and tech industries.

Interestingly, respondents in the legal industry were the most likely to disagree with the statement that IT and security leaders have been recognized as more important by leadership teams.

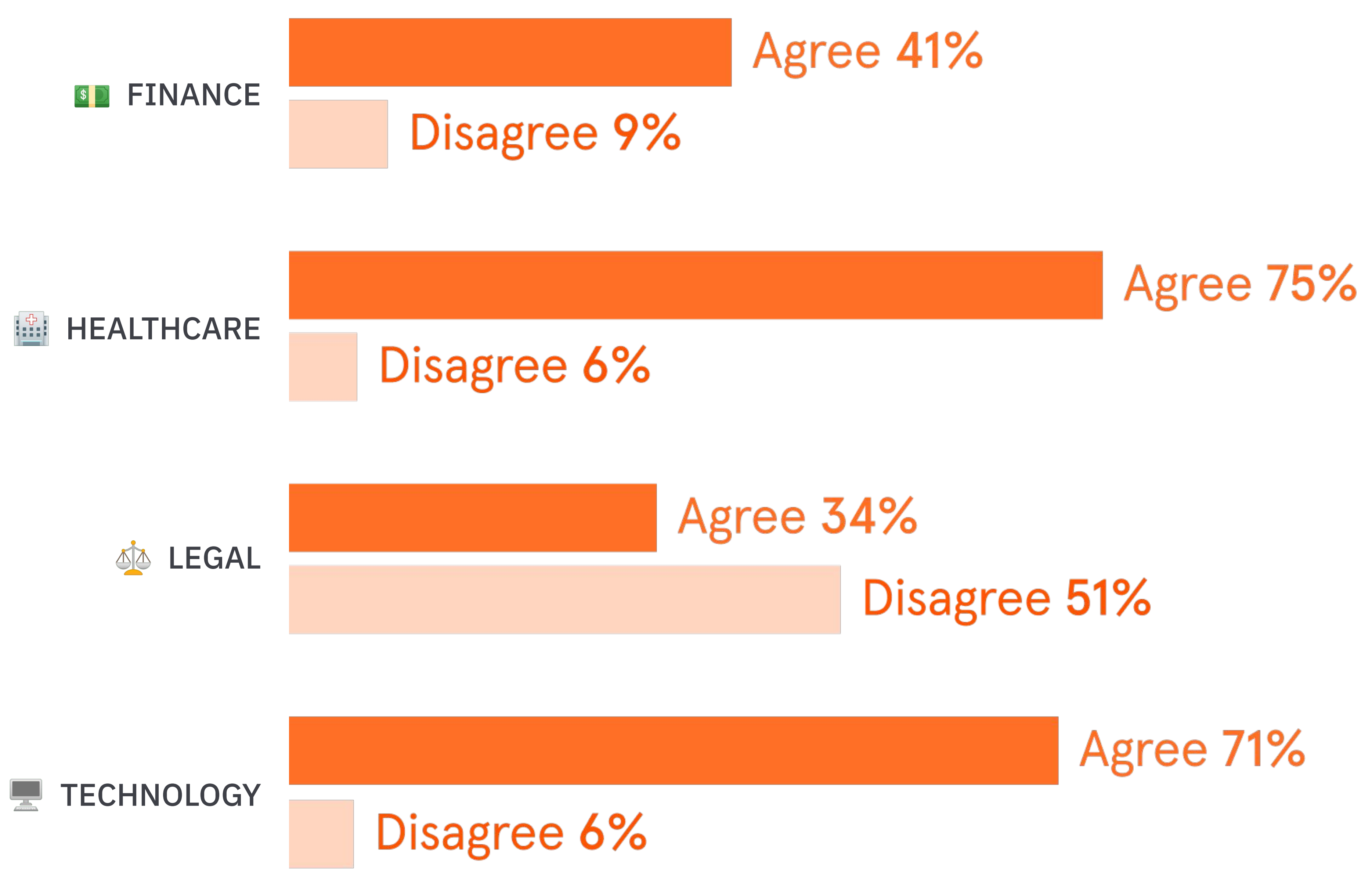
16 Tips to Prove the Value of Cybersecurity

We asked security leaders how they prove the value of cybersecurity and influence change in their organization. Check out 16 of their tips on our blog.

TAKE ME THERE →



"The role of the IT leader is considered more important today"– by industry:



PART 2

Office Etiquette: Back to Basics?

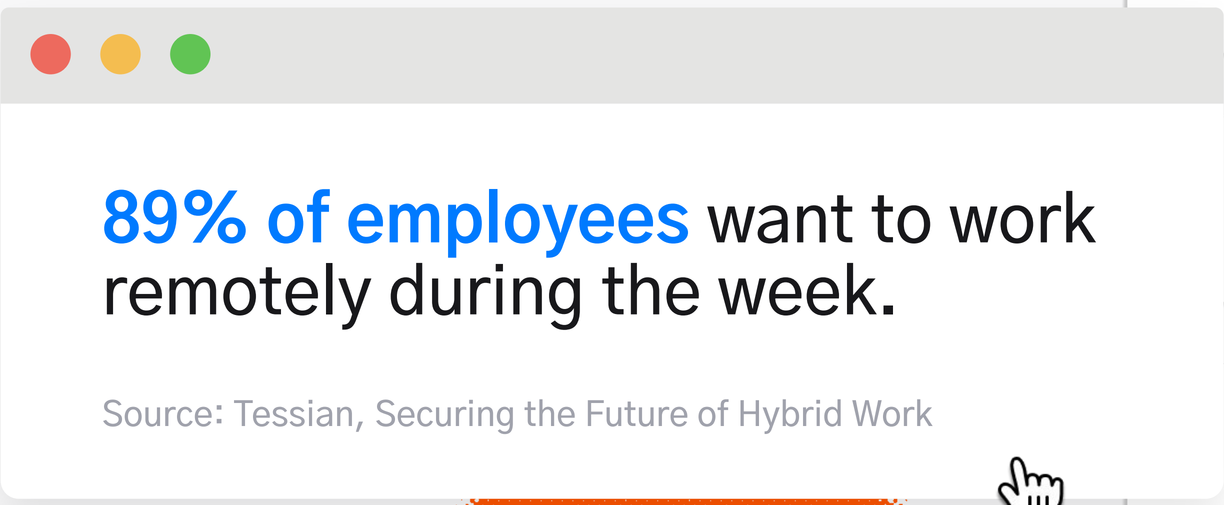
But as employees go back to the office, IT leaders now need to address changes to employees' security behaviors since they have been working remotely.

The majority of IT leaders (56%) believe their employees have picked up bad cybersecurity behaviors since working from home.

Are they right to worry? To some degree.

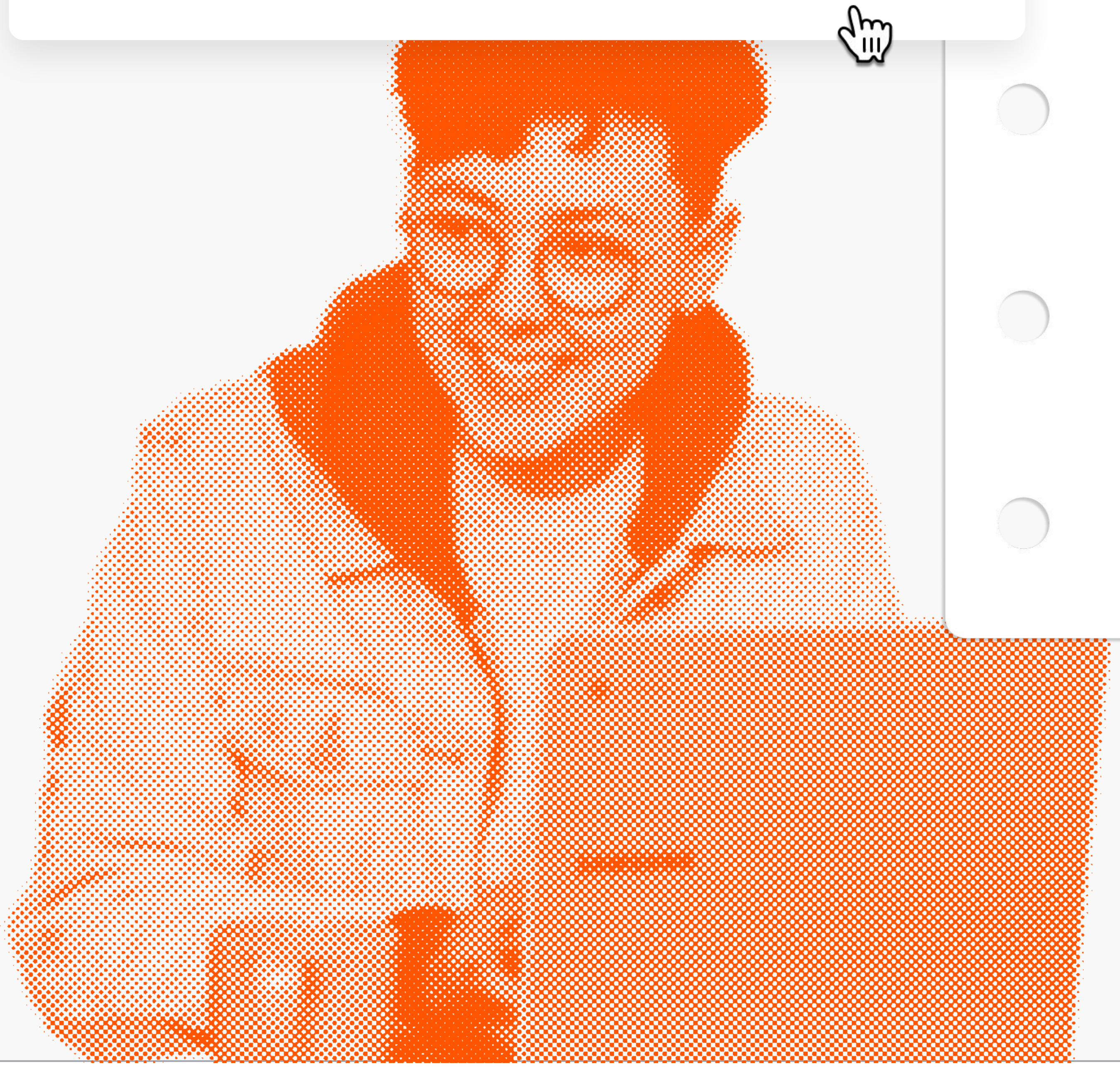
Over a third (36%) of employees say they have picked up bad cybersecurity behaviors and found security ‘workarounds’ since working remotely.

> “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 that employees won’t try to bypass the system. Still, I wish there was a better way.”
>
> CHRIS FREEMAN
> Information Security Lead at EY

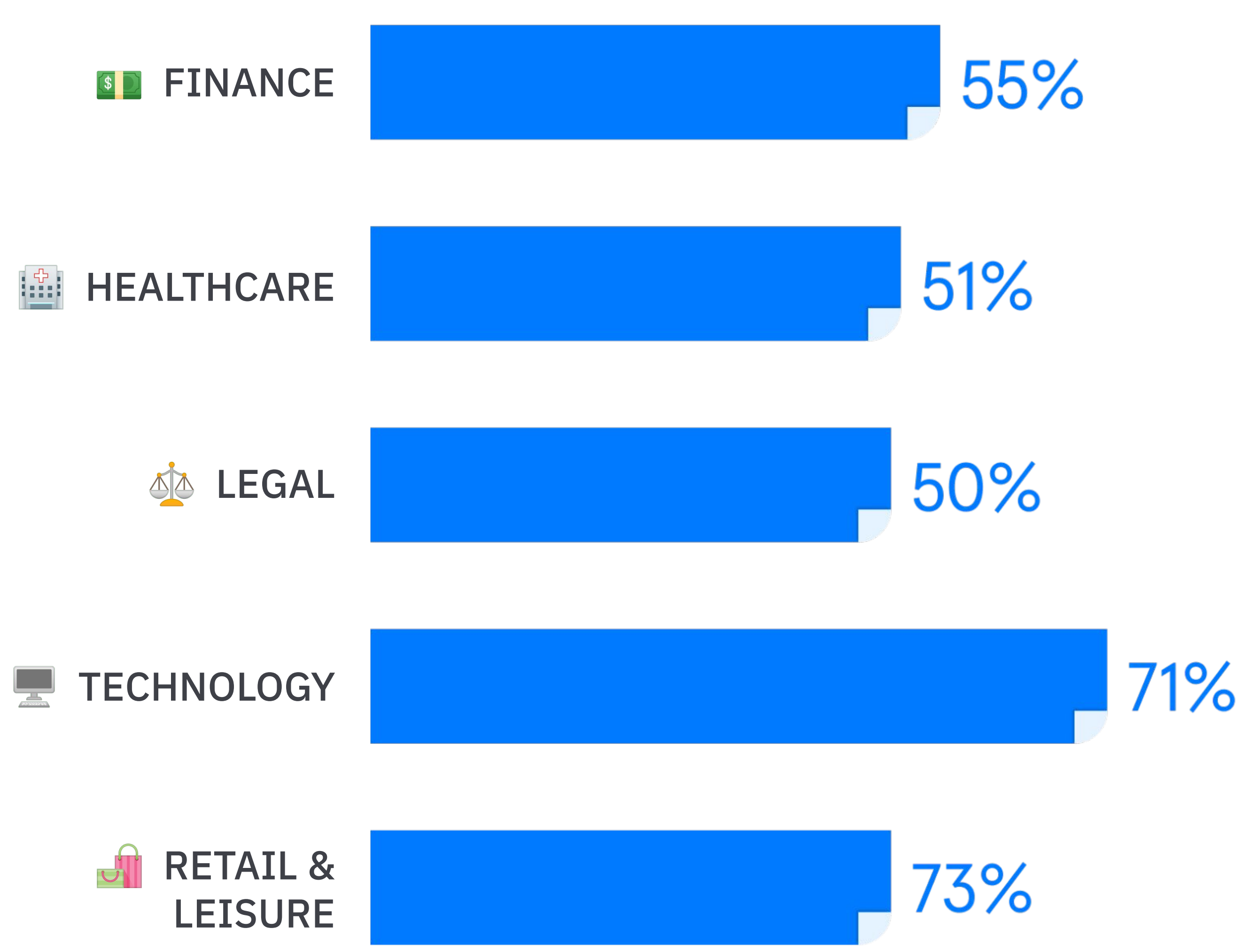


89% of employees want to work remotely during the week.

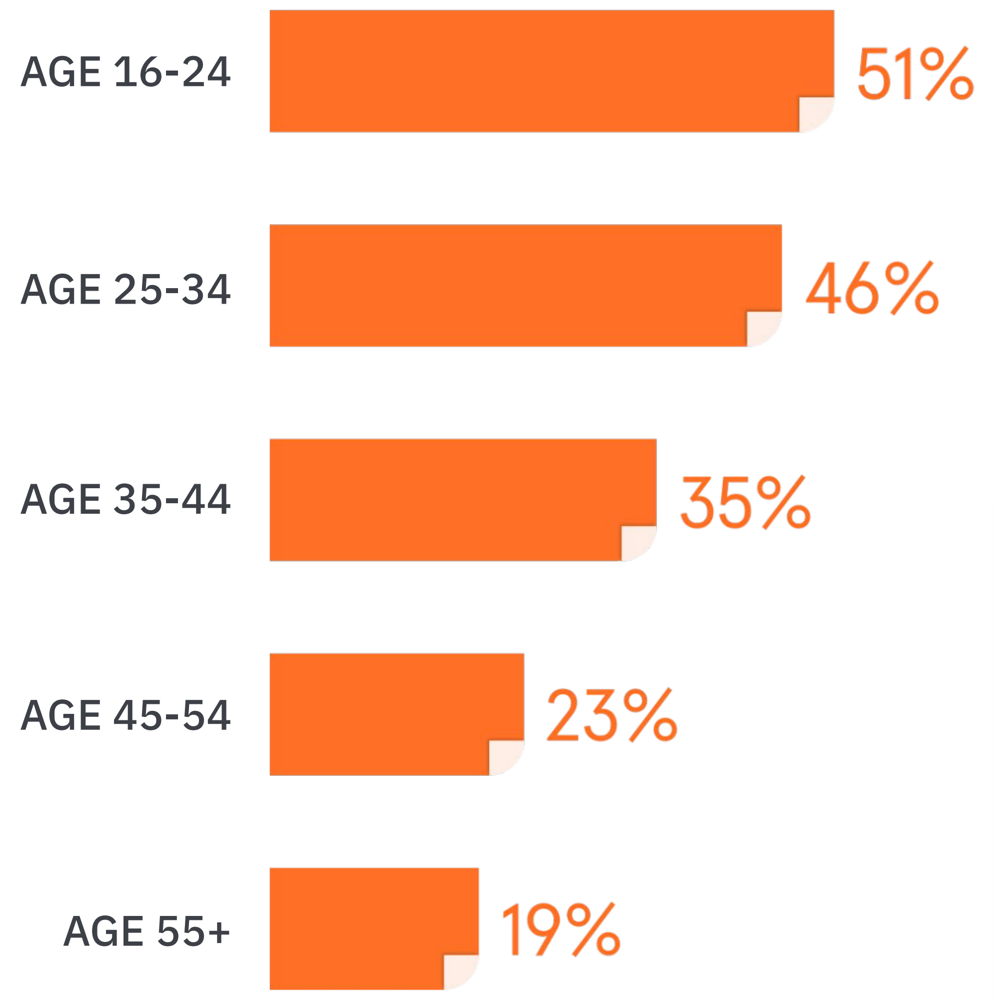
Source: Tessian, Securing the Future of Hybrid Work

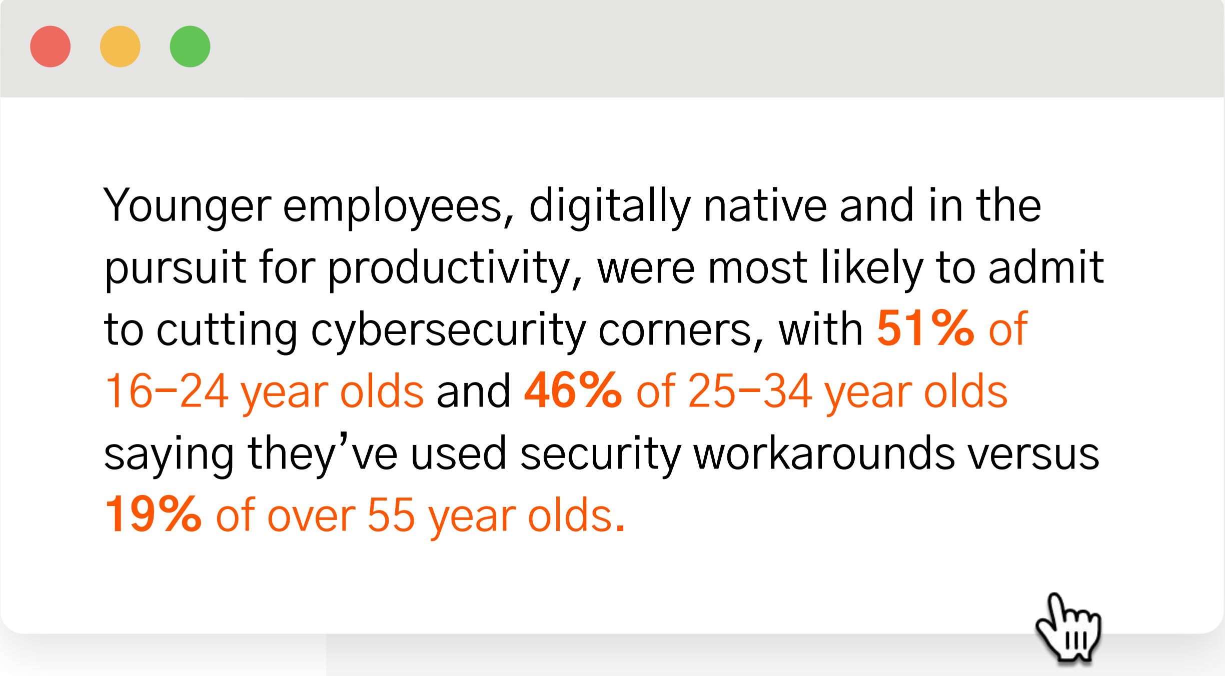


IT leaders believe employees have picked up bad cybersecurity behaviors since working remotely, by industry:



Employees have found security 'workarounds' while working remotely. By age:



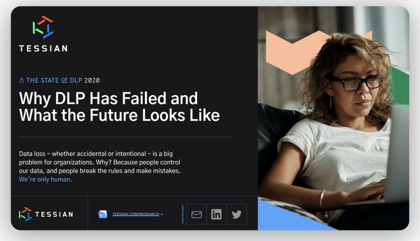


Younger employees, digitally native and in the pursuit for productivity, were most likely to admit to cutting cybersecurity corners, with **51%** of 16–24 year olds and **46%** of 25–34 year olds saying they've used security workarounds versus **19%** of over 55 year olds.

This discrepancy in behavior by generation is reinforced by a previous Tessian report, which showed younger employees were more than twice as likely to think that security tools and software impede on their productivity at work – 56% versus 23% of 55+ year olds.

It's little wonder then that they've tried to find ways around security blockers.

> "People just need to get their jobs done. If you can allow people to do their jobs securely without seeing security at all, that's a fantastic outcome."
>
> SIMON HODGKINSON
> Former CISO at BP



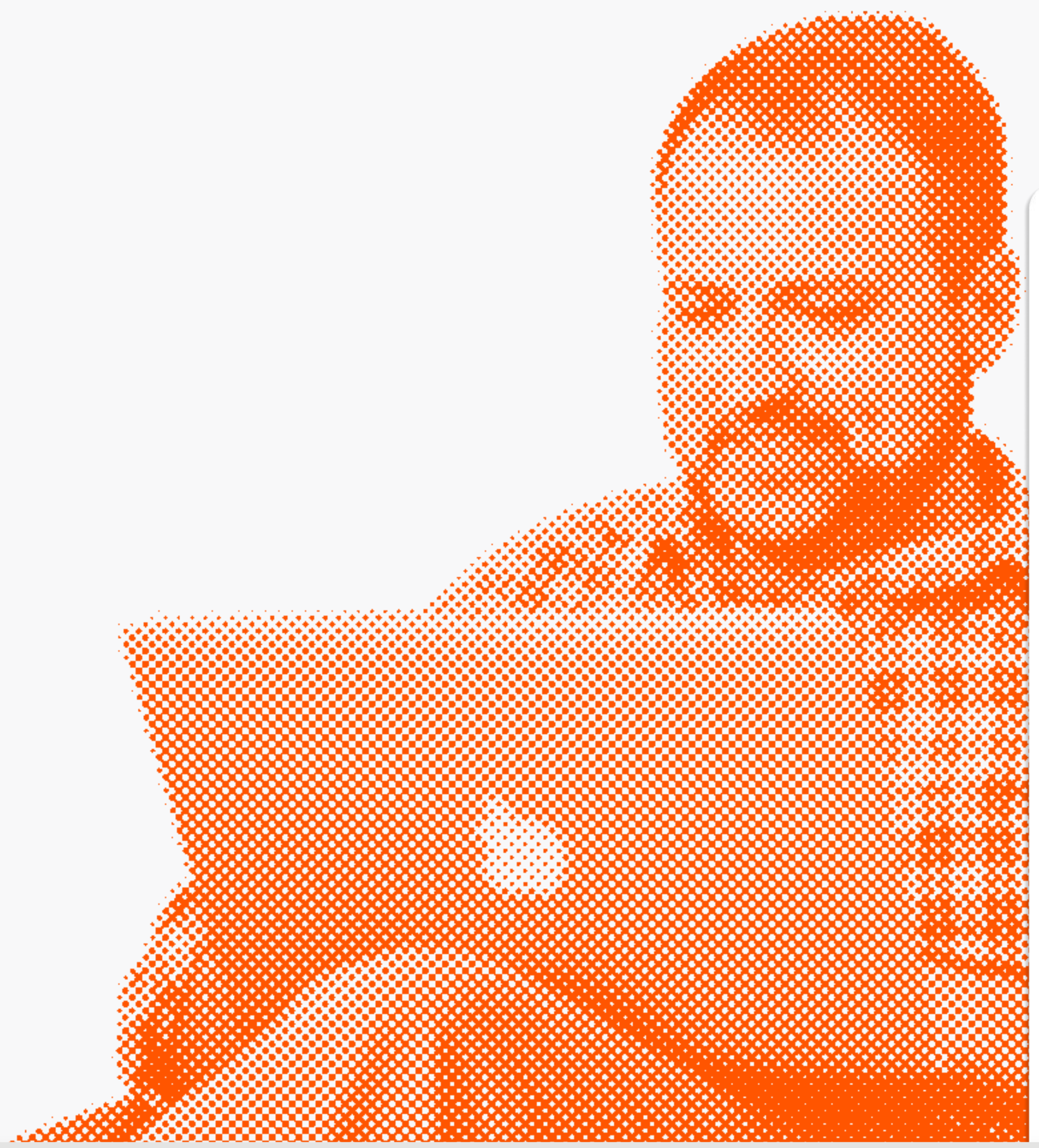
You can read more about the **State of DLP** in this research report →

Nearly a third of employees (30%) also believe they can get away with riskier security behaviors when working remotely, with two in five (39%) admitting the cybersecurity behaviors they practice while working from home are different to the behaviors practiced in the office.

The reason? Nearly half (49%) say it's because they feel they **aren't** being watched by IT. 👀

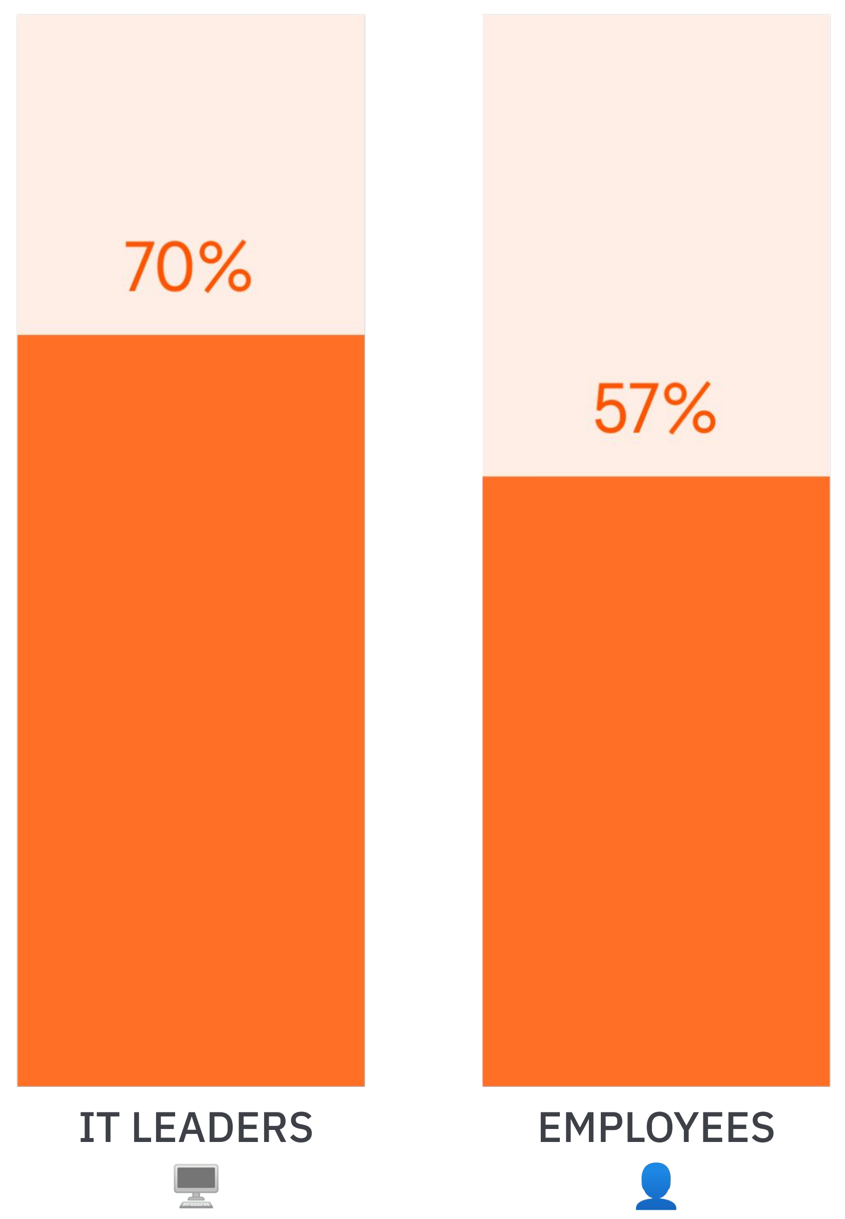
So will the shift back into an office environment result in safer security practices? 70% of IT leaders seem to think so, believing that staff will be more likely to follow company security policies around data protection and data privacy while working in the office.

Yet, they could be overly optimistic; 57% of employees think the same. Is this because they've simply forgotten company security policies and protocols and need a refresh? Or did they never really know them in the first place?



1 in 3 employees think they can get away with riskier security behaviors when working remotely.

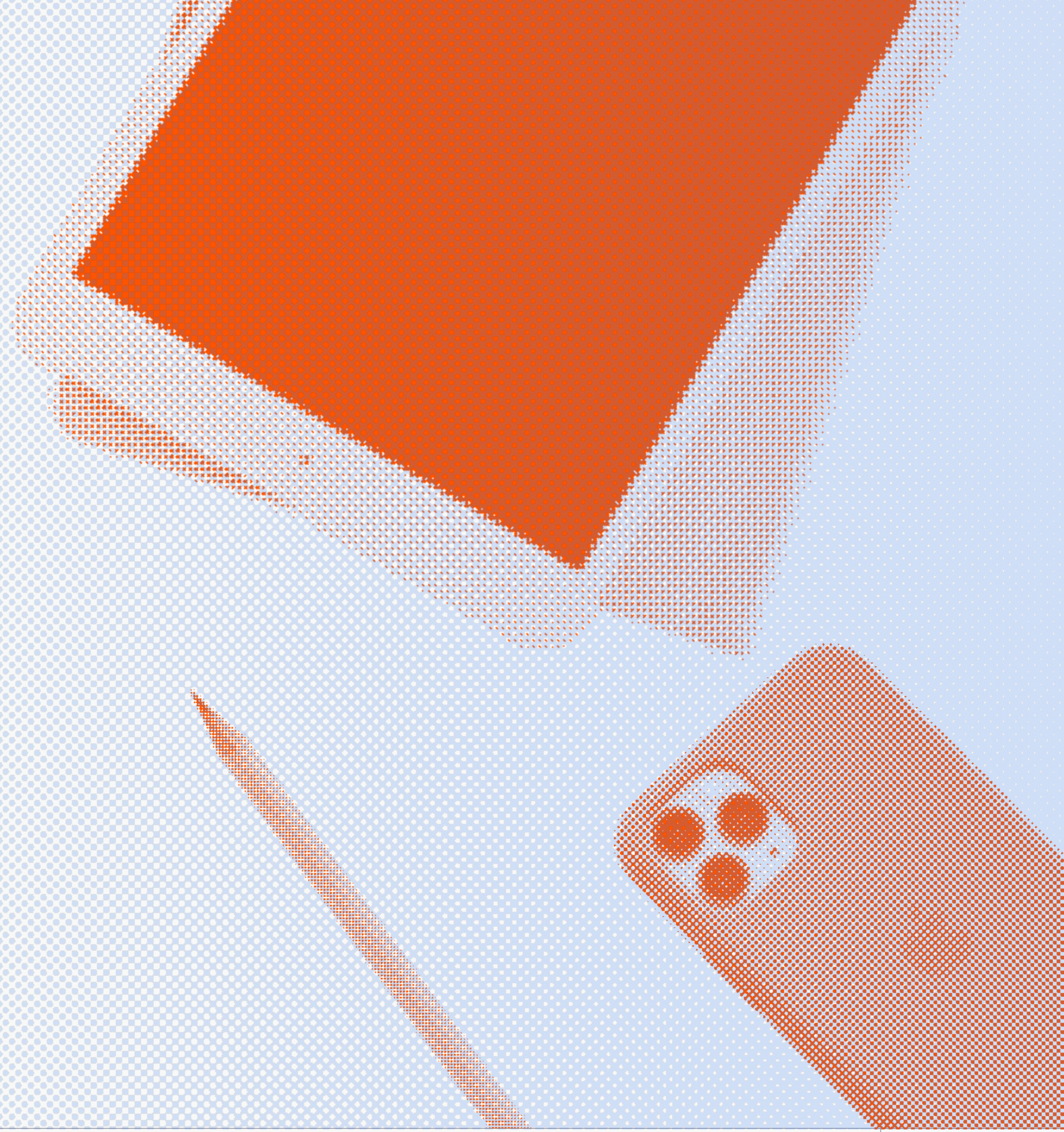
70% of IT leaders think employees will follow safe data practices in the office vs. 57% of employees who say they will



PART 3

Security Pitfalls in a Hybrid Workforce

In addition to addressing employees' remote work security behaviors, IT leaders could face further challenges with security threats in a hybrid workforce.



Dodgy Devices

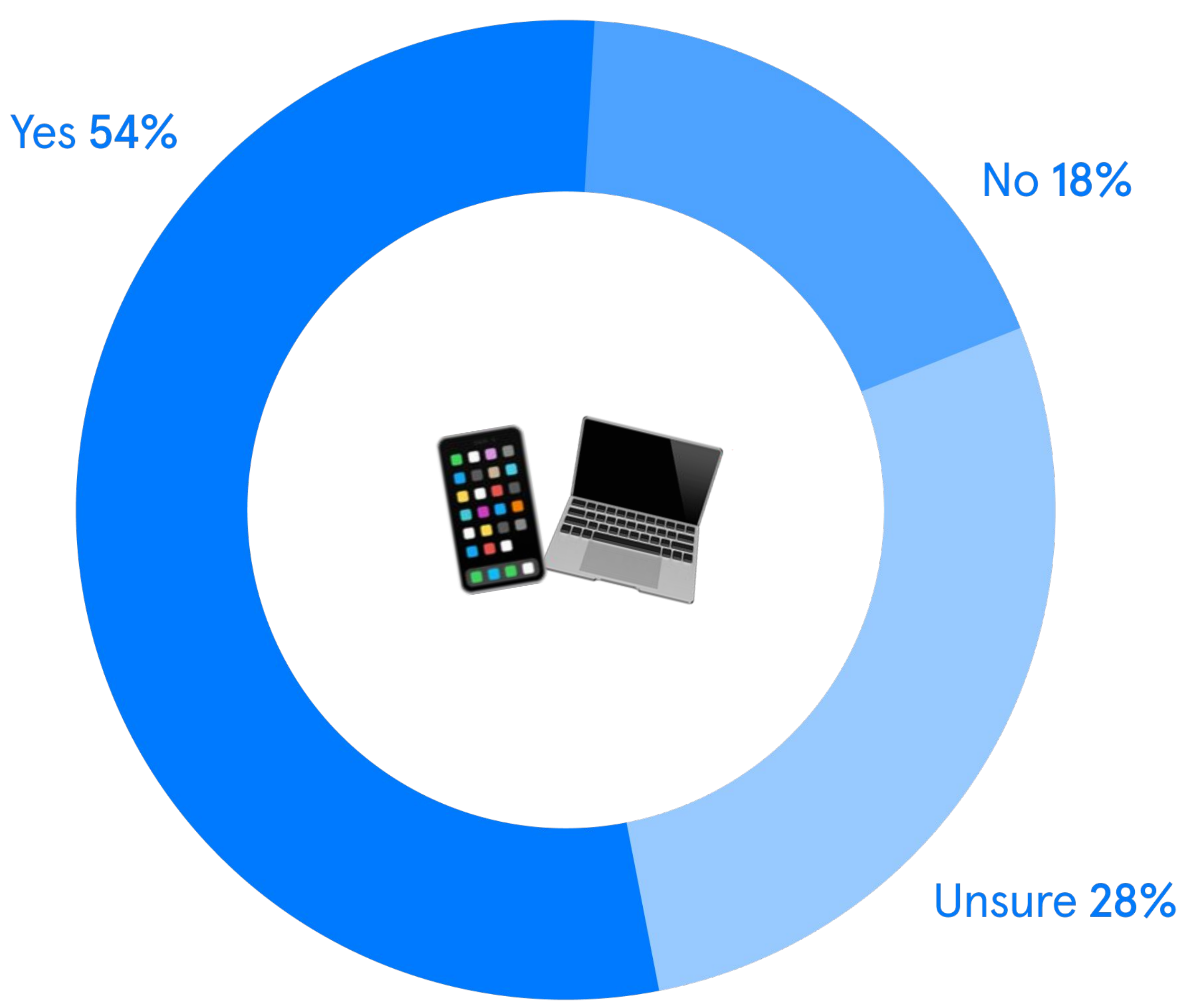
Over half of IT leaders we surveyed (54%) are concerned that staff will bring **infected devices and malware** into the workplace when businesses transition back to the office.

It's hardly surprising when you consider that 40% of employees said they plan to bring personal devices into the office to work from when they transition to a hybrid way of working.

The perimeter has been coming down for a long time, but with employees now working fluidly across corporate and home networks, and accessing business critical applications on personal, untrusted devices, it has truly crumbled.

IT and security leaders now have to shift to a new security architecture for good – one that involves **zero-trust network access, endpoint security,** and **multi-factor authentication.**

IT leaders are concerned about employees bringing infected devices into the office



Ransomware Rising

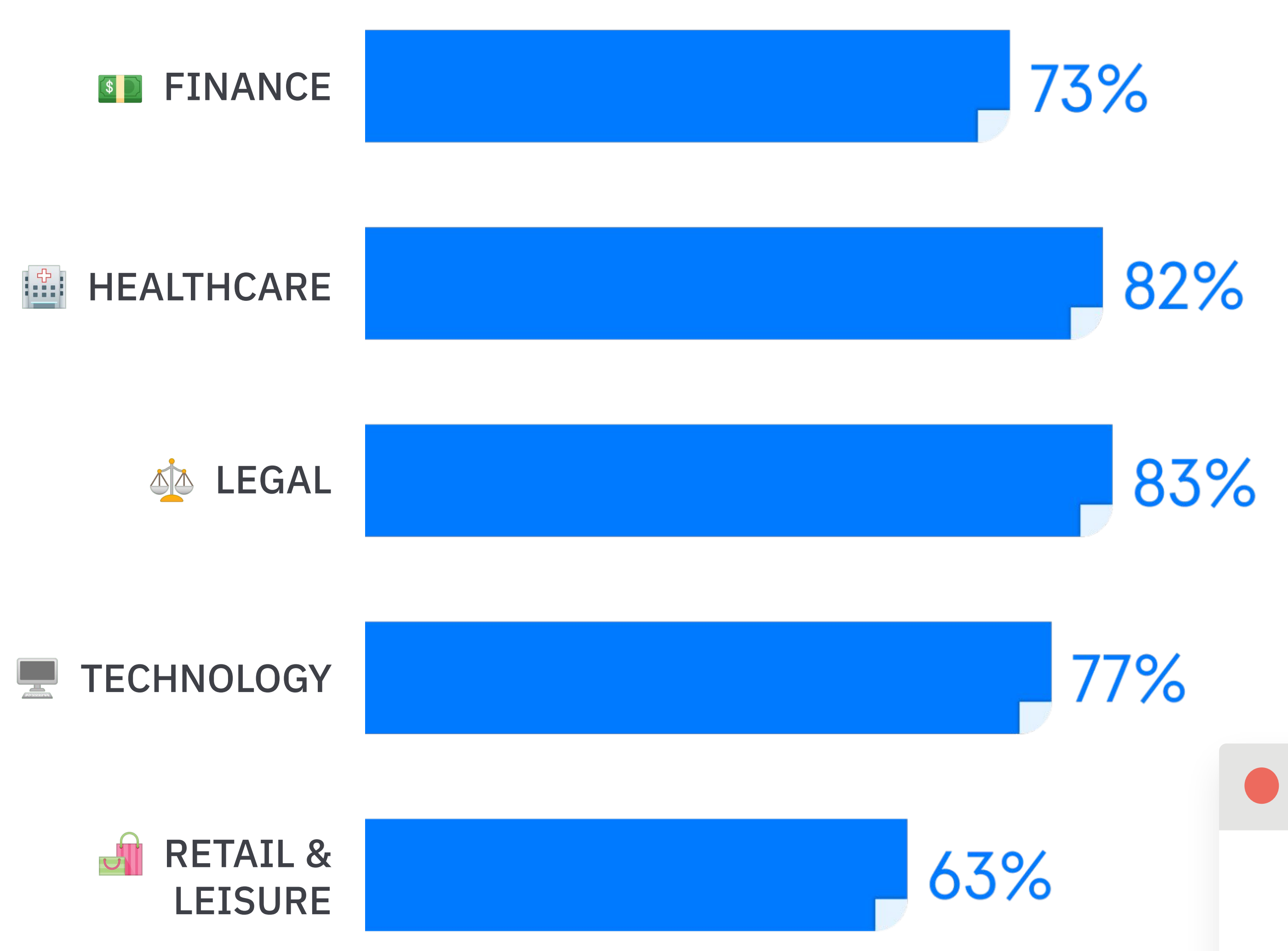
The majority of IT leaders (69%) believe that ransomware attacks will be a greater concern in a hybrid workplace, with one in four (25%) strongly agreeing.

Legal firms and healthcare organizations are most likely to believe that ransomware would increase in a hybrid way of working.

We understand their concerns. Major ransomware attacks have dominated security headlines in 2021, with Ireland's public healthcare systems being targeted by a ransomware attack that reportedly cost the organization tens of millions of euros to repair, and hacker group Darkside successfully shutting down a critical gasoline pipeline to the U.S. East Coast.

According to Verizon's [2021 Data Breach Investigations Report](), too, ransomware attacks doubled in frequency in 2020.

IT leaders believe ransomware is a greater concern, by industry:



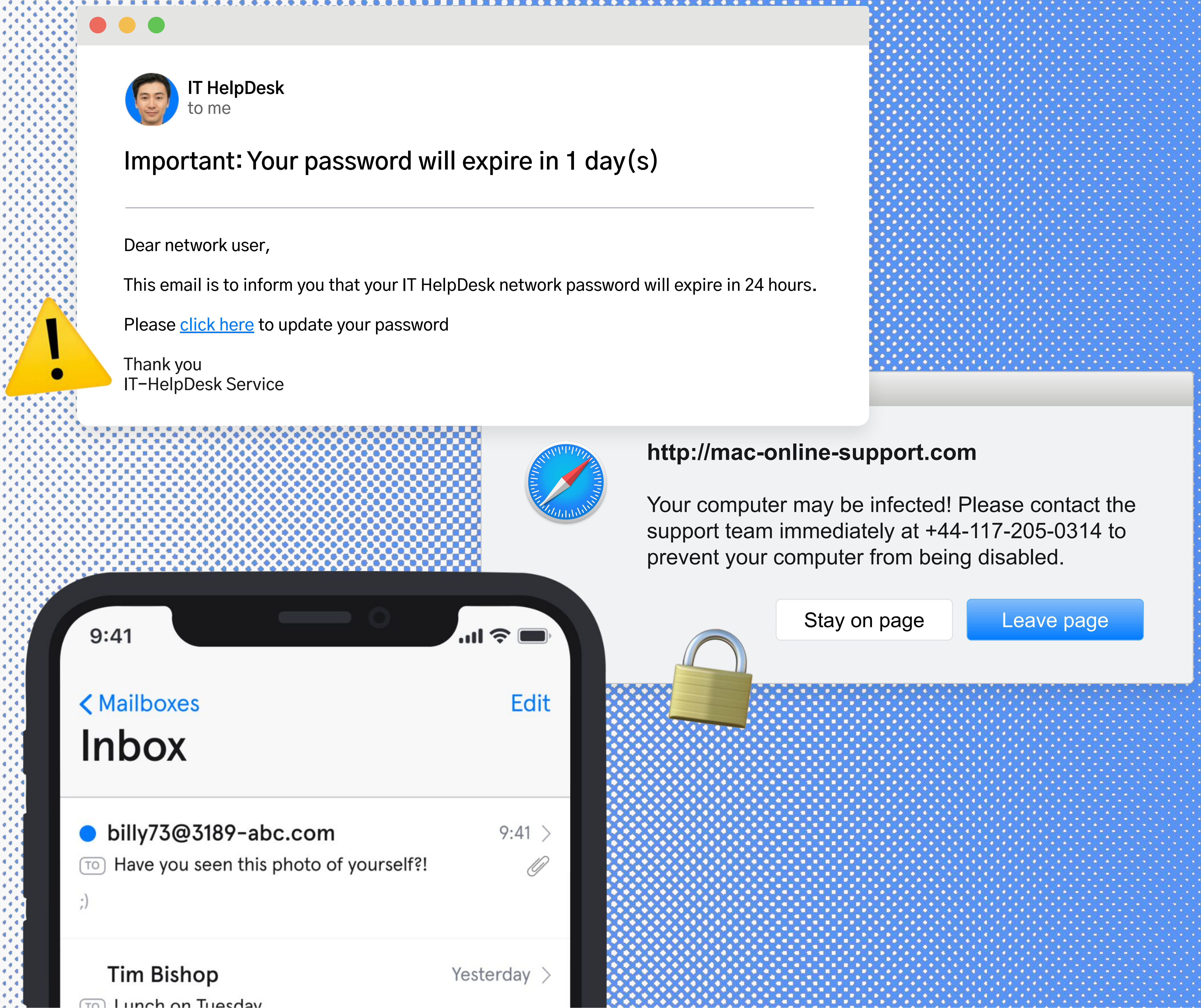
69% of IT leaders believe that ransomware attacks will be a great concern in a hybrid workplace.

Today, the leading point of entry for ransomware attacks is phishing.

Threat actors are manipulating human behavior to successfully hack an organization.

Ransomware campaigns such as Avaddon, for example, prey on people's insecurities and vanity, using convincing email subject lines to trick people into opening a message that claims to contain a photo of themselves. Once an attachment is opened, ransomware is downloaded and infected devices display a ransom demand that must be paid in order to gain the software needed to retrieve their files.

Stop phishing, business email compromise, account takeover attacks and social engineering scams, and you significantly reduce the risk of ransomware.



IT HelpDesk
to me

Important: Your password will expire in 1 day(s)

Dear network user,

This email is to inform you that your IT HelpDesk network password will expire in 24 hours.

Please click here to update your password

Thank you
IT–HelpDesk Service

http://mac-online-support.com

Your computer may be infected! Please contact the support team immediately at +44-117-205-0314 to prevent your computer from being disabled.

Inbox

billy73@3189-abc.com 9:41
TO Have you seen this photo of yourself?!
;)

Tim Bishop Yesterday
TO Lunch on Tuesday

Phishing attacks scale

You don't need us to tell you that phishing attacks went up in 2020; they went up by a lot.

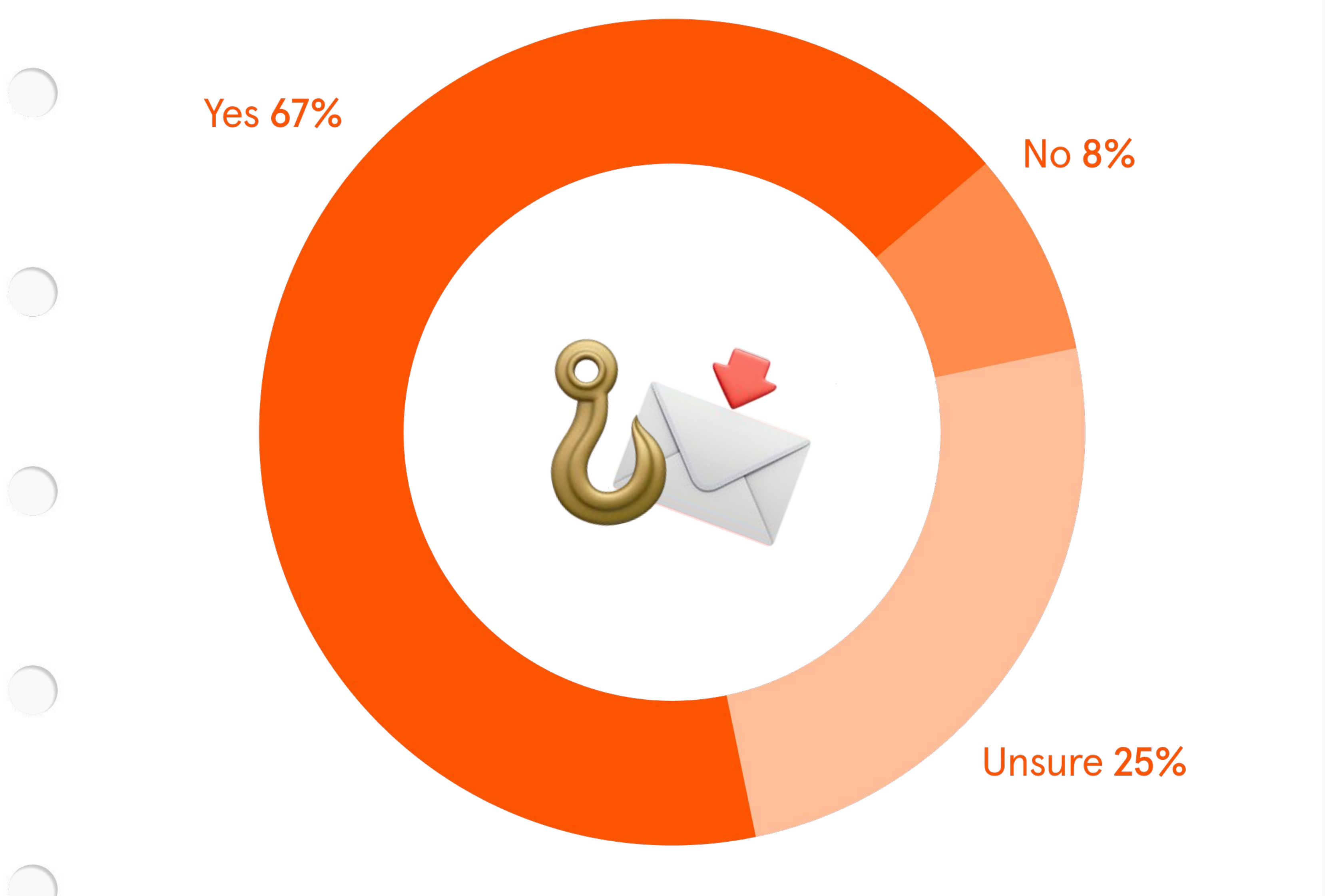
FBI statistics reveal that phishing attacks doubled in frequency last year, and our own data showed a 15% increase in social engineering incidents in the last six months of 2020.

Cybercriminals were quick to take advantage of the global pandemic, using COVID-19 phishing lures to trick people into sharing data and those all-important account credentials when the world went into lockdown. The ultimate goal of these phishing attacks? To influence human behaviors.

According to Verizon, **"altering behavior'' was the top integrity violation in phishing attacks and pretexting** – a type of social engineering attack that involves a situation or pretext created by the attacker – last year.

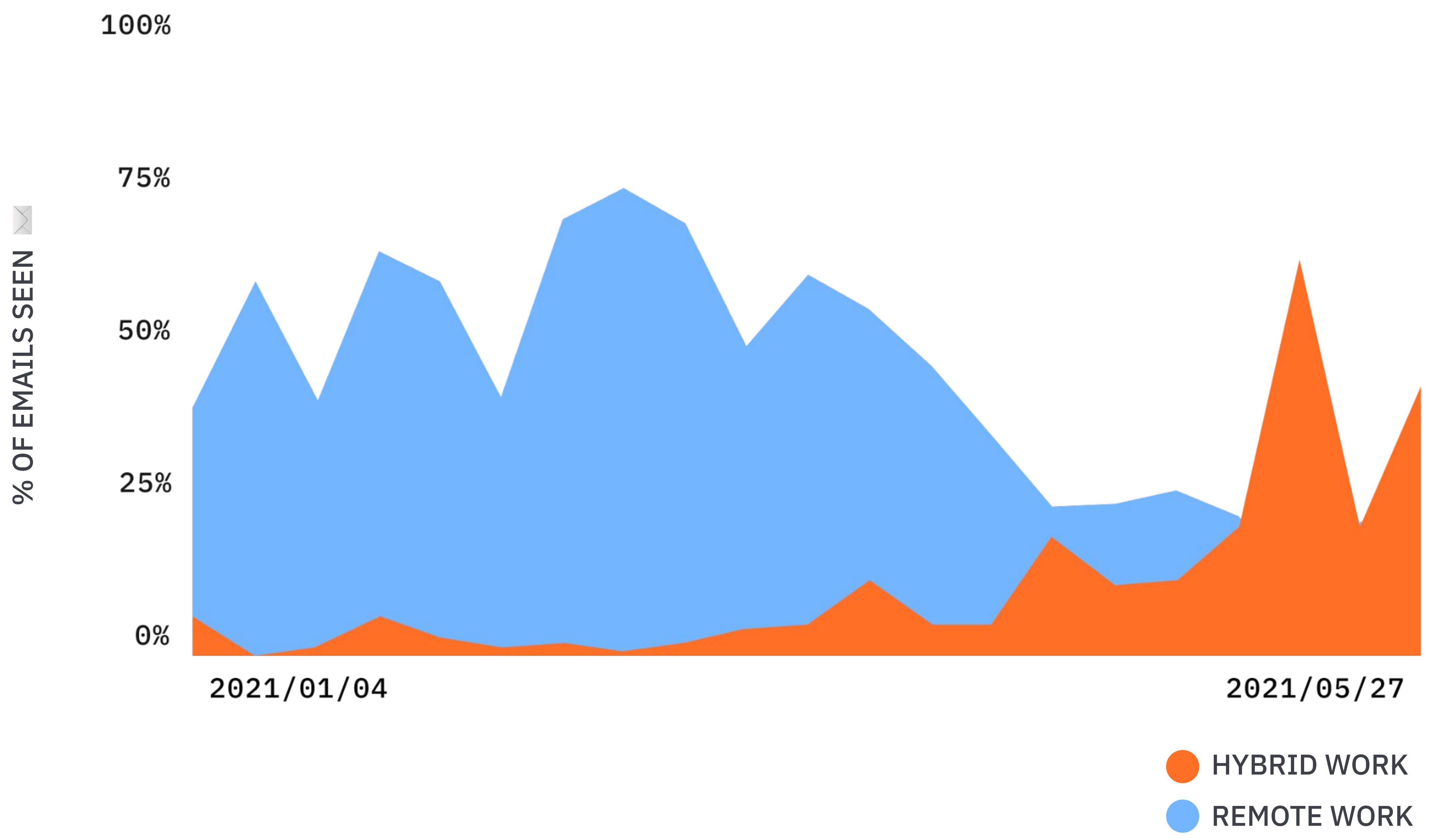
And it seems there's no rest for the wicked. As the world starts to open up, and ways of working change once again, more than two-thirds of IT decision makers (67%) predict an increase in targeted phishing emails in which cybercriminals take advantage of the transition back to working in the office.

Read more about how **hackers exploited the COVID-19 vaccine rollout** →



IT leaders think employees will receive a surge in phishing emails related to 'back to work'

Trend: ‘remote work’ vs. ‘hybrid work’ in suspicious emails related to office reopening



In fact, when lockdown restrictions eased in the UK during the week of May 10 2021, Tessian platform data found that the number of suspicious emails related to “hybrid work” was 39% higher than the overall weekly average of “back to office” themed emails flagged by Tessian Defender since the start of 2021.

This graph shows the number of suspicious emails related to “remote work” and “hybrid work” themes, flagged by Tessian Defender. You can see that cybercriminals were consistently capitalizing on the remote work trend throughout 2021 – but as soon as ‘hybrid’ hit the headlines, they quickly changed tact.

One particularly convincing ‘back to work’ campaign, observed by Cofense, targeted employees with emails purporting to come from their CIO, welcoming staff back into office and asking them to provide their login credentials. WIth hackers looking for every opportunity to trick people into falling for their scams, investment in security solutions that can protect employees against the most sophisticated impersonation attacks or social engineering campaigns will be critical to company security in the “back to work” transition.

TESSIAN DEFENDER

Learn how Tessian Defender can identify the advanced phishing attacks, business email compromise and external account takeover that legacy secure email gateways can’t.

Employees' fear of being found out

Creating a strong security culture is going to be even more important in a hybrid model.

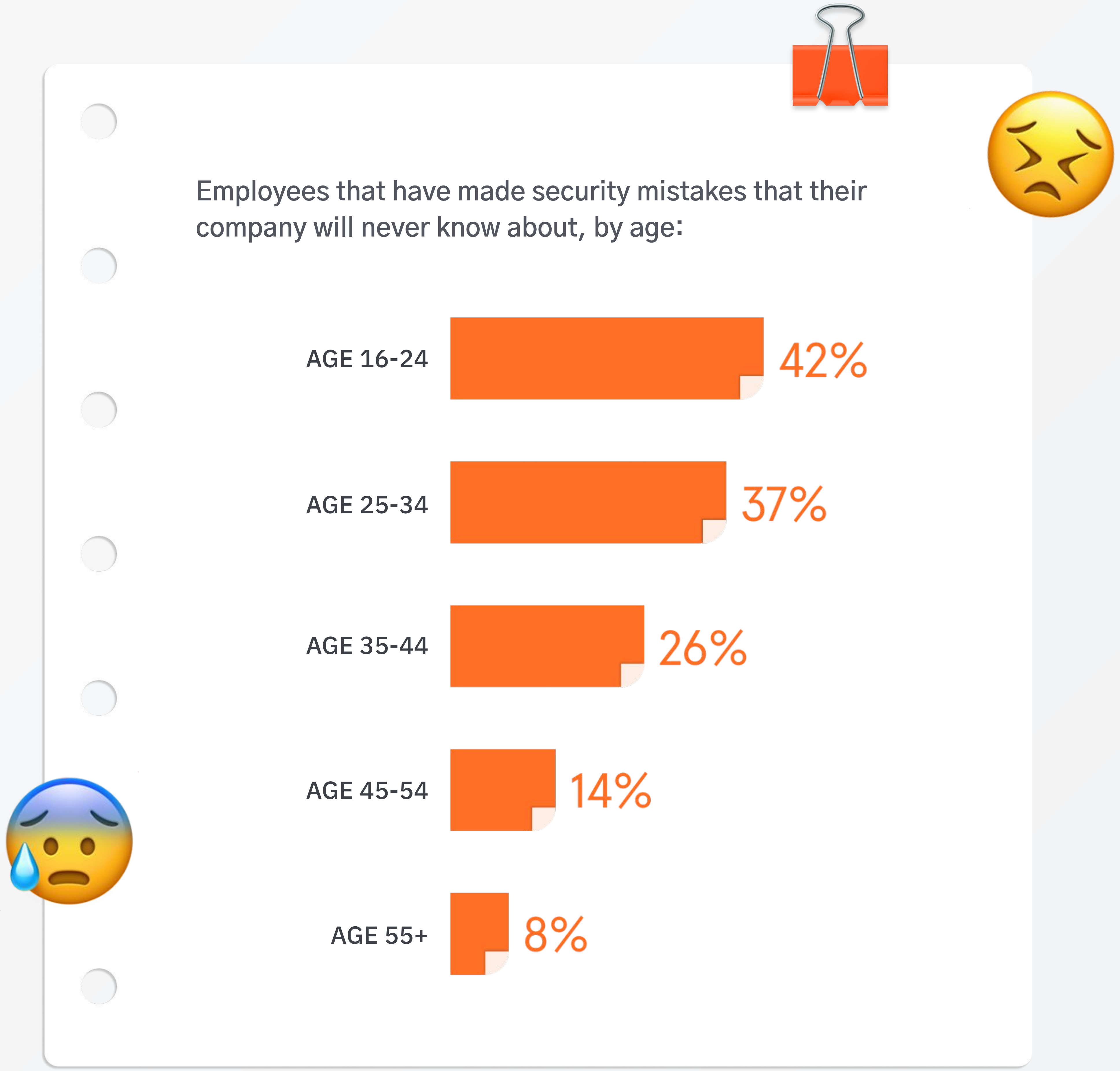
Why? Because an effective security culture equals an engaged workforce that takes responsibility for security issues.

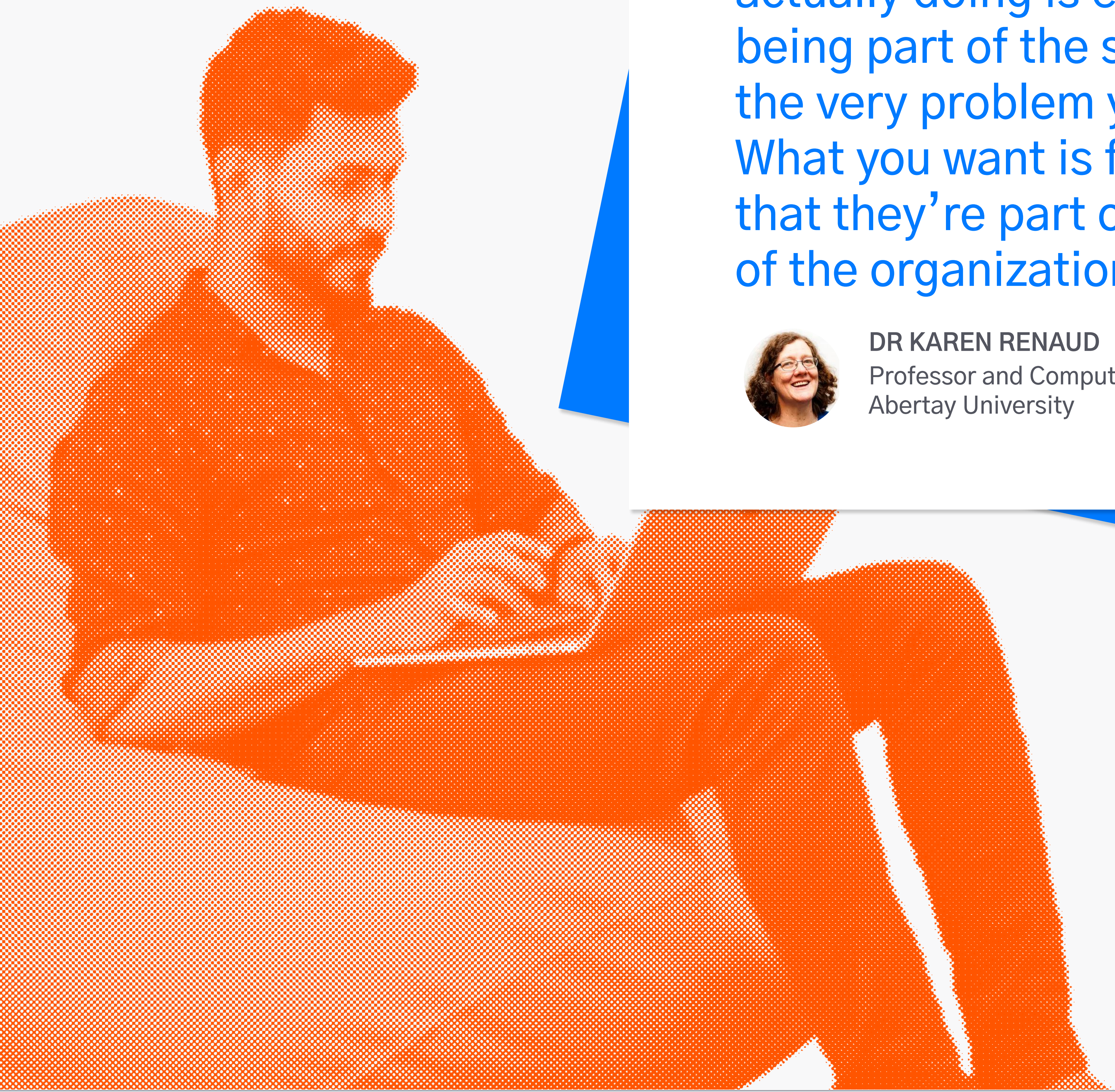
It reduces insider threats, builds self-efficacy and employee confidence, and leads to better security compliance – regardless of location.
It's not always easy, though, and there is certainly work to be done.

Over a quarter of employees admit to making cybersecurity mistakes – or mistakes that have compromised company security – while working from home that, they say, no one will ever know about.

What's more, just 51% of respondents always report when they receive a phishing email or click on a phishing email.

The main reason why employees aren't reporting security mistakes to IT teams – such as clicking on a phishing link or sending an email with sensitive information to the wrong person – is because they are scared of the repercussions. 27% of respondents said they feared facing disciplinary action or being required to take more security training.


Employees that have made security mistakes that their company will never know about, by age:



> A lot of organizations see their employees' behaviors as a problem. They'll train them, they'll constrain them, and then they'll blame them when things go wrong. But what you're actually doing is excluding them from being part of the solution. So, it creates the very problem you're trying to solve. What you want is for everyone to feel that they're part of the security defense of the organization.

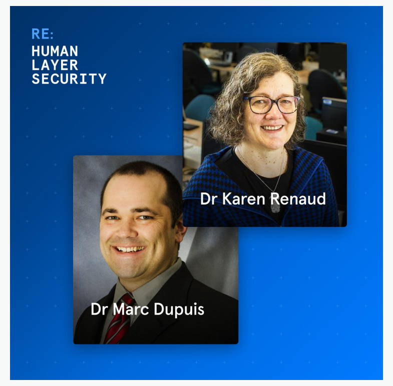
DR KAREN RENAUD
Professor and Computer Scientist,
Abertay University

27% of employees fear owning up to security mistakes because of punitive repercussions

So, create a security culture that encourages people to come forward about their mistakes, and support them when they do.

Not every employee is a security expert, and scaring them into compliance isn't working.

To improve security behaviors, help your employees build a level of self-efficacy – a belief in themselves that they are equipped with awareness of threats and the knowledge of what to do if something goes wrong. When employees are empowered, through knowledge and self-efficacy, they're more likely to be part of the solution.



Listen to Tessian's podcast interview with academics Dr Karen Renaud and Dr Marc Dupuis to learn why FUD in cybersecurity doesn't work.

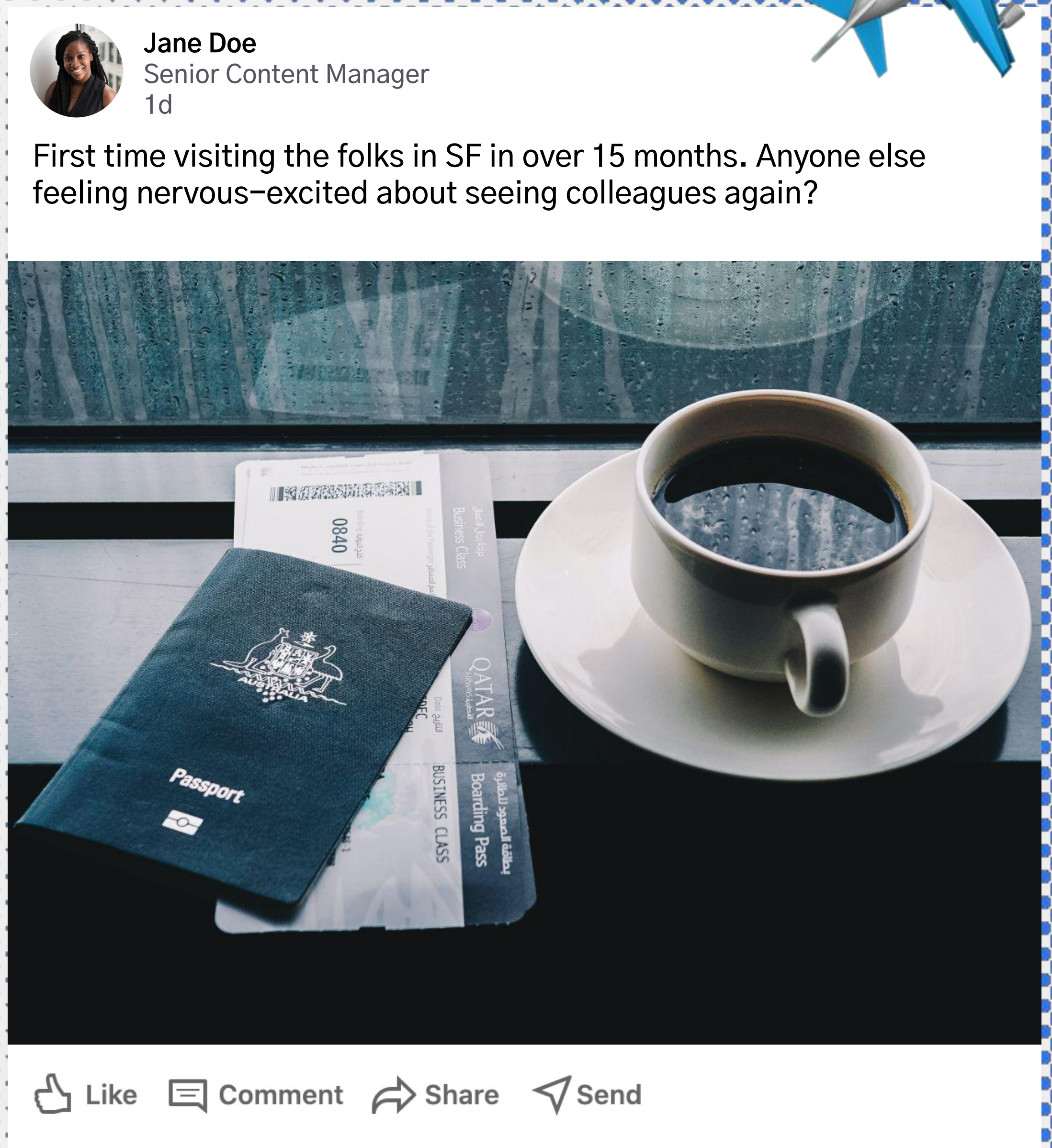
RE: Human Layer Security Podcast

Business Travel

As lockdown restrictions are lifted, 6 in 10 IT leaders (60%) think the return to business travel will open up greater cybersecurity challenges and risks for their company, too.

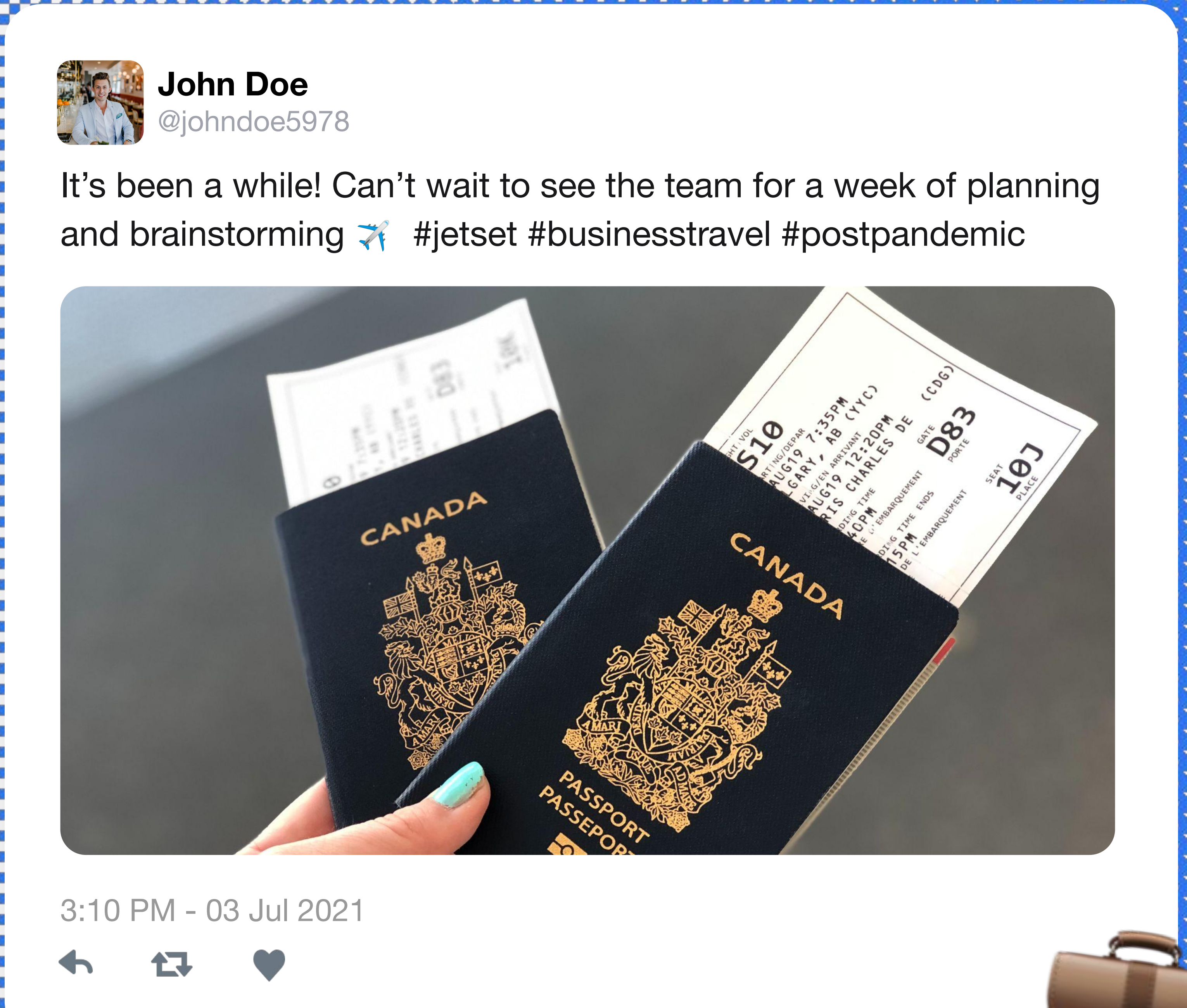
These risks could include a rise in phishing attacks whereby threat actors target individuals and impersonate airlines, booking operators, hotels, or impersonate senior executives supposedly on a business trip. There is also the risk that employees accidentally leave devices on public transport or expose company data in public places.

Once again, it's about securing companies against threats executed by risky human behaviors. The organizations that do this, will thrive in a hybrid environment.



Jane Doe
Senior Content Manager
1d

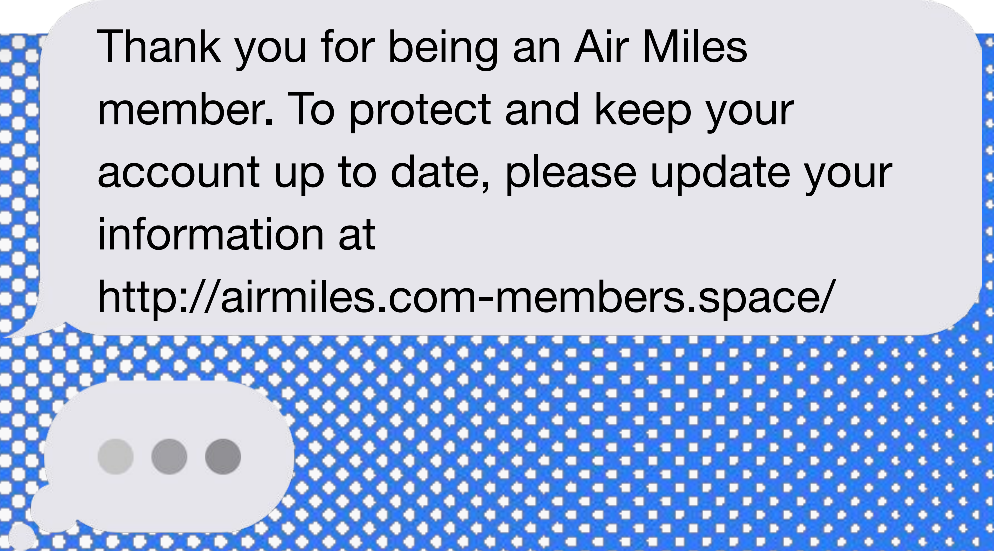
First time visiting the folks in SF in over 15 months. Anyone else feeling nervous–excited about seeing colleagues again?



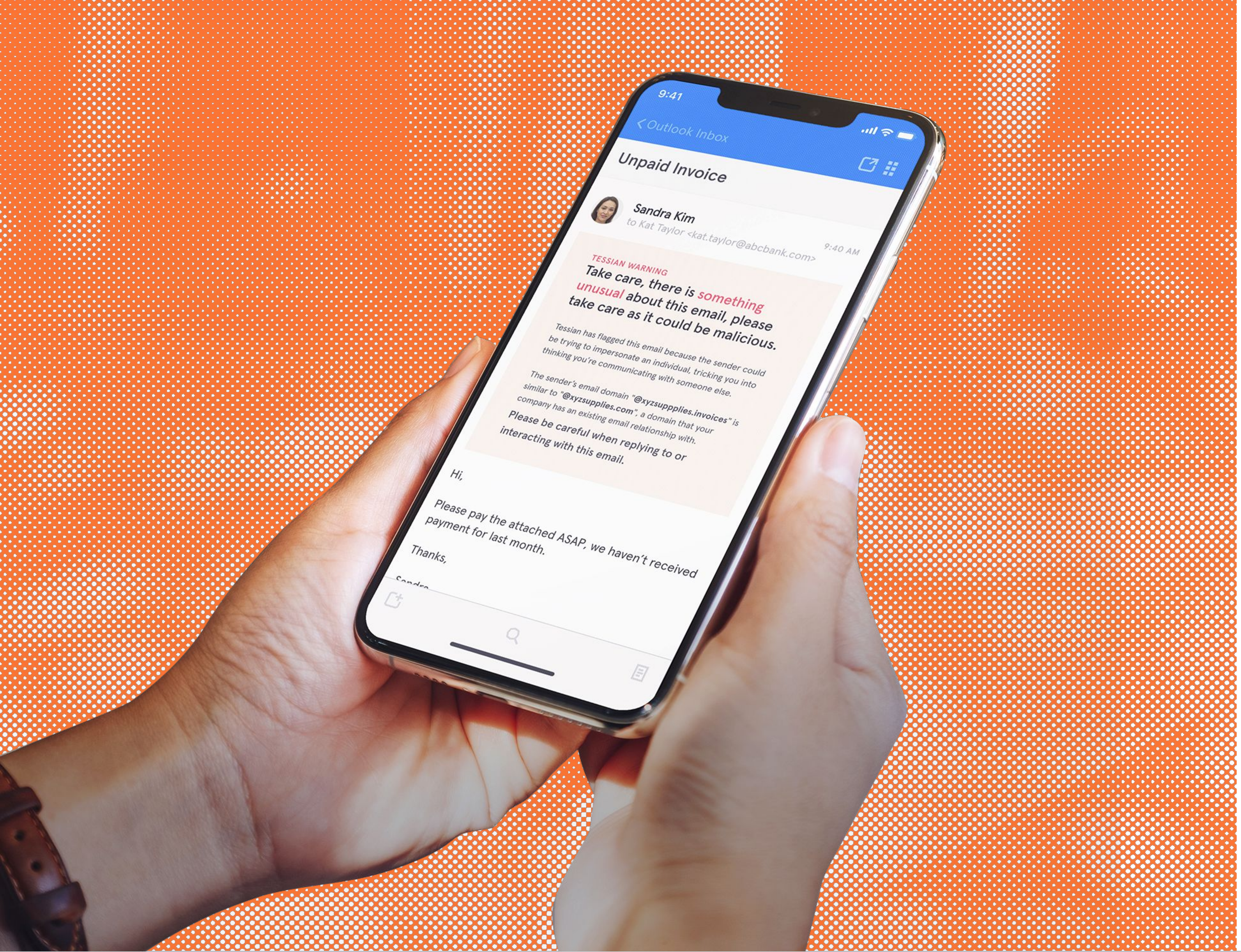
John Doe
@johndoe5978

It's been a while! Can't wait to see the team for a week of planning and brainstorming ✈️ #jetset #businesstravel #postpandemic

3:10 PM - 03 Jul 2021



Thank you for being an Air Miles member. To protect and keep your account up to date, please update your information at http://airmiles.com-members.space/



Unpaid Invoice

Sandra Kim
to Kat Taylor <kat.taylor@abcbank.com>
9:40 AM

TESSIAN WARNING
Take care, there is something unusual about this email, please take care as it could be malicious.

Tessian has flagged this email because the sender could be trying to impersonate an individual, tricking you into thinking you're communicating with someone else.

The sender's email domain "**@xyzsuppplies.invoices**" is similar to "**@xyzsupplies.com**", a domain that your company has an existing email relationship with.

Please be careful when replying to or interacting with this email.

Hi,

Please pay the attached ASAP, we haven't received payment for last month.

Thanks,

Sandra

Secure "Back to Work" Behaviors

While ways of working change once again, one thing remains the same: people are the gatekeepers to every organization's data and systems.

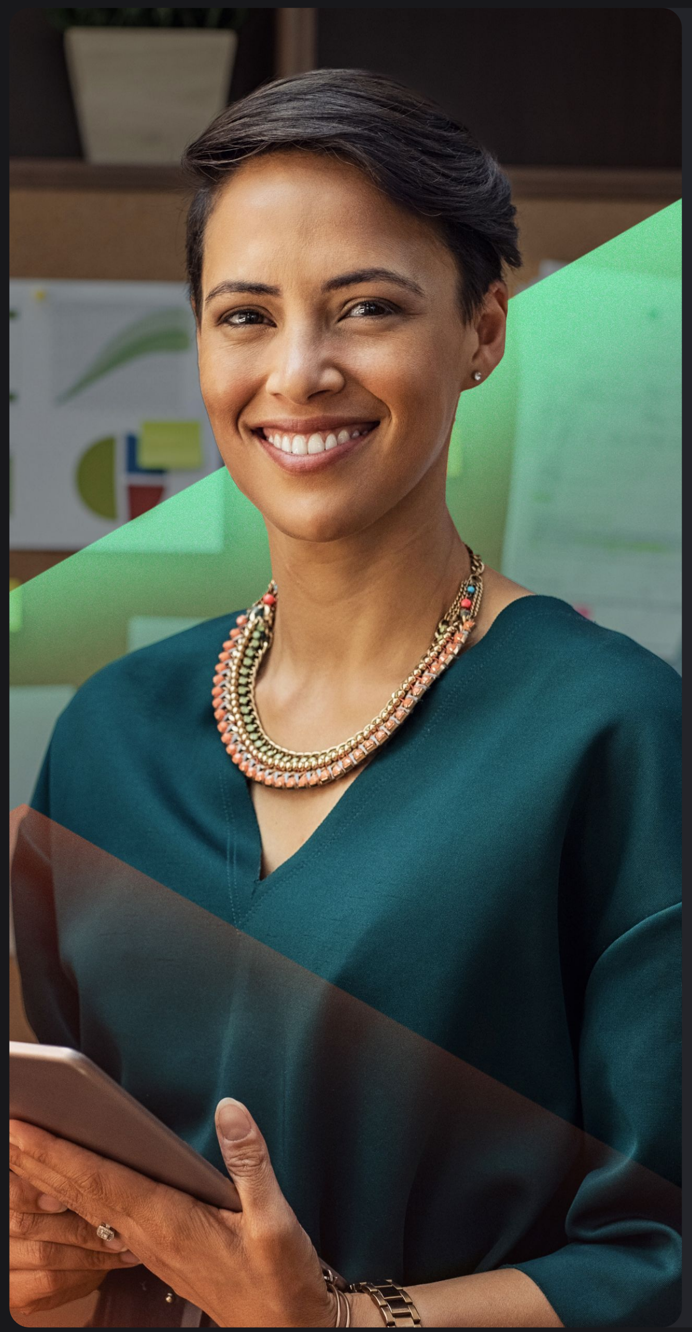
Their behaviors will make or break company security and they need to be part of the solution. Businesses need to put Human Layer Security at the heart of the hybrid work model if they are going to survive and thrive.

This means investing in technology that can detect and prevent threats caused by human error or social engineering, building a security culture that empowers people to work securely and productively, and understanding how to encourage long-lasting behavioral change overtime.

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 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 and threat intelligence

SIGN ME UP →

Methodology

In addition to using Tessian platform data, we commissioned Censuswide to survey 4,000 working professionals – 2,000 in the US and 2,000 in the UK – and 200 IT decision makers in the US and the UK.

Survey respondents varied in age from 16–51+, occupied various roles across departments and industries, and worked within organizations ranging in size from 2–1,000+.

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 →