



TESSIAN

THE FUTURE OF HYBRID WORK

# Securing the Future of Hybrid Working

How can IT leaders create strategies that empower employees to work remotely and securely, reduce the risk of human error over time and avoid overwhelming their IT teams?



Share this report





75%

of IT decision makers believe the future of work will be “remote” or “hybrid”.

[Jump to Page 5 ↗](#)

## One-third of organizations

[Jump to Page 12 ↗](#)

saw an increase in ransomware delivered by phishing during the lockdown period.



78%

of IT decision makers believe their company is at greater risk of insider threats when employees work remotely.

[Jump to Page 17 ↗](#)



58%

of businesses intend to introduce more security training if their company adopts remote working permanently.

[Jump to Page 27 ↗](#)



85%

of IT leaders believe their teams will be under more pressure in a hybrid working structure.

[Jump to Page 10 ↗](#)



## Half of organizations

experienced a data breach between March – July 2020.

[Jump to Page 13 ↗](#)



## Phishing was the leading cause

[Jump to Page 13 ↗](#)

of security incidents when employees worked remotely.

## Email traffic increased by 129%

at the start of the lockdown period enforced by the COVID-19 pandemic.

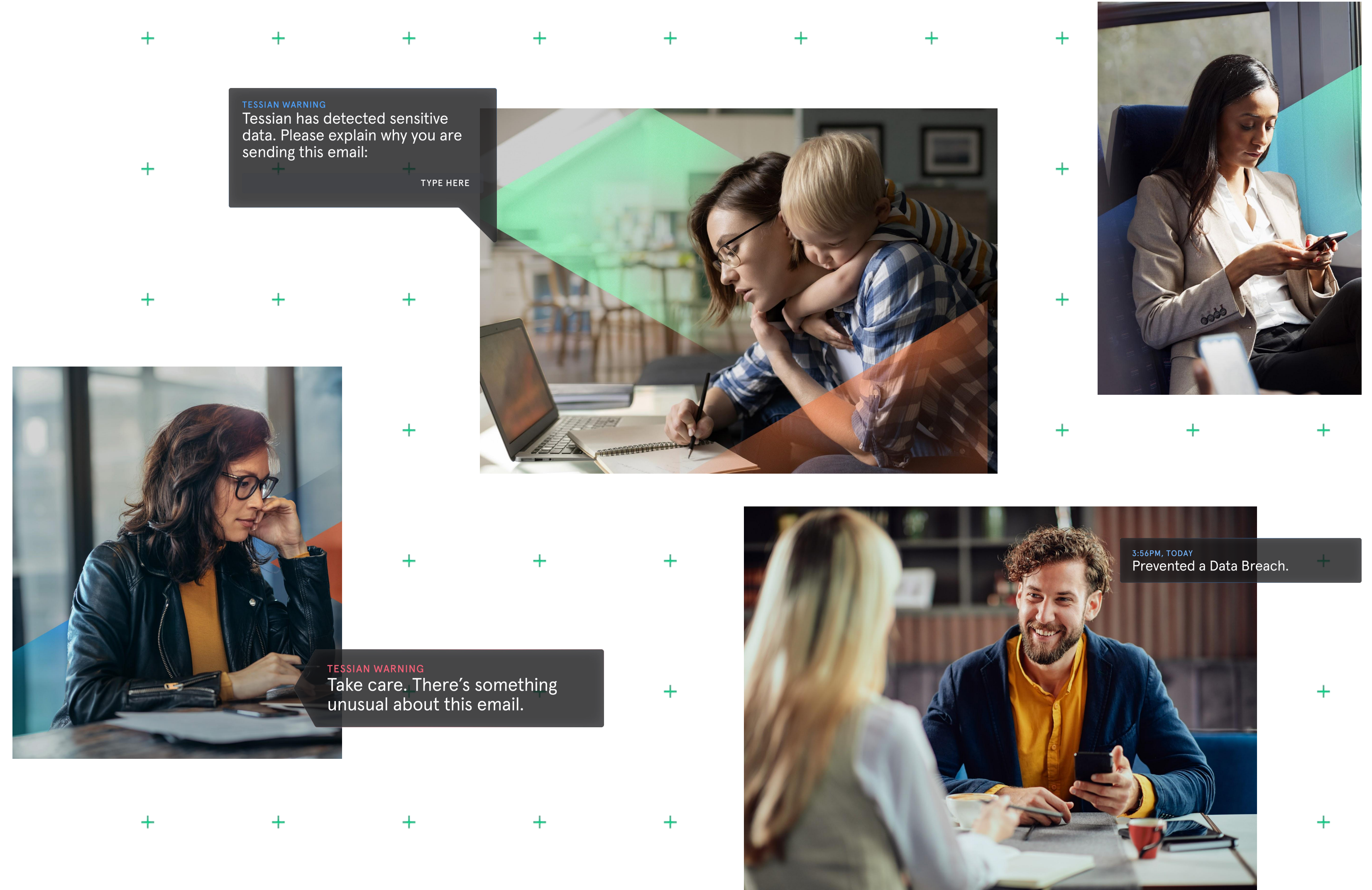
[Jump to Page 24 ↗](#)



# As the world went into lockdown, ways of working changed forever.

Now, after months of working from home, businesses are at a crossroads. They must plan for what happens post-pandemic and decide whether the long-term future of work for their employees is remote, office-based, or a combination of the two.

While there's no right or wrong answer, one thing is for certain: **employees will expect a level of flexibility from their employer.** They want to work however and wherever they want post-pandemic. They will also need to be able to work securely. This will require companies to make significant changes to how they operate – changes which will have huge implications for IT and security teams.



Chapter 1

# The Future of Work is Hybrid

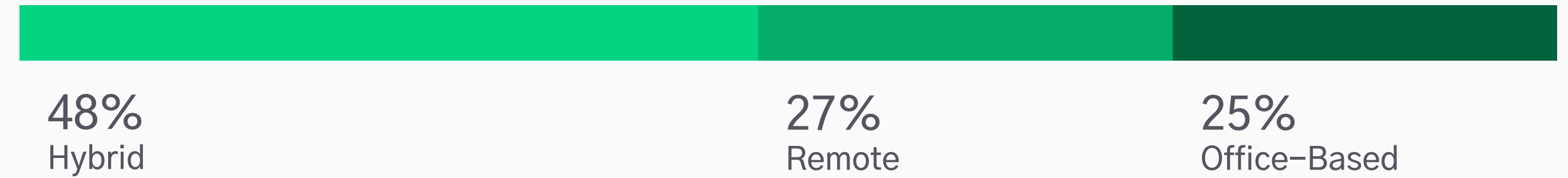
# The future of work will be hybrid.

Working in an office five days a week will be a thing of the past, according to the majority of IT leaders we surveyed.

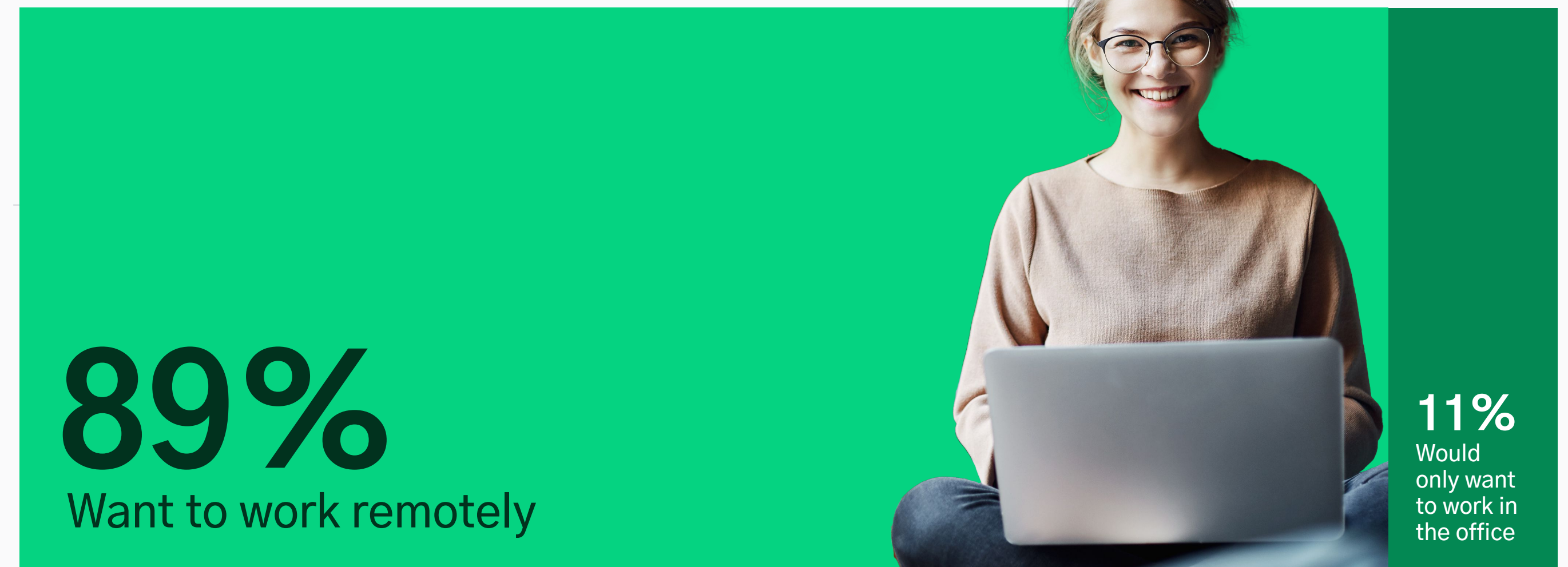
Three quarters of IT decision makers (75%) believe the future of work will be “remote” or “hybrid” — where employees choose to split their time between working in the office and anywhere else they’d like.

Employees agree. Just 11% of all employees said they want to work exclusively from the office post-pandemic. Instead, the average employee wants to be able to work remotely at least two days a week.

## The future of work will be...



## Employees do not want to work in the offices.






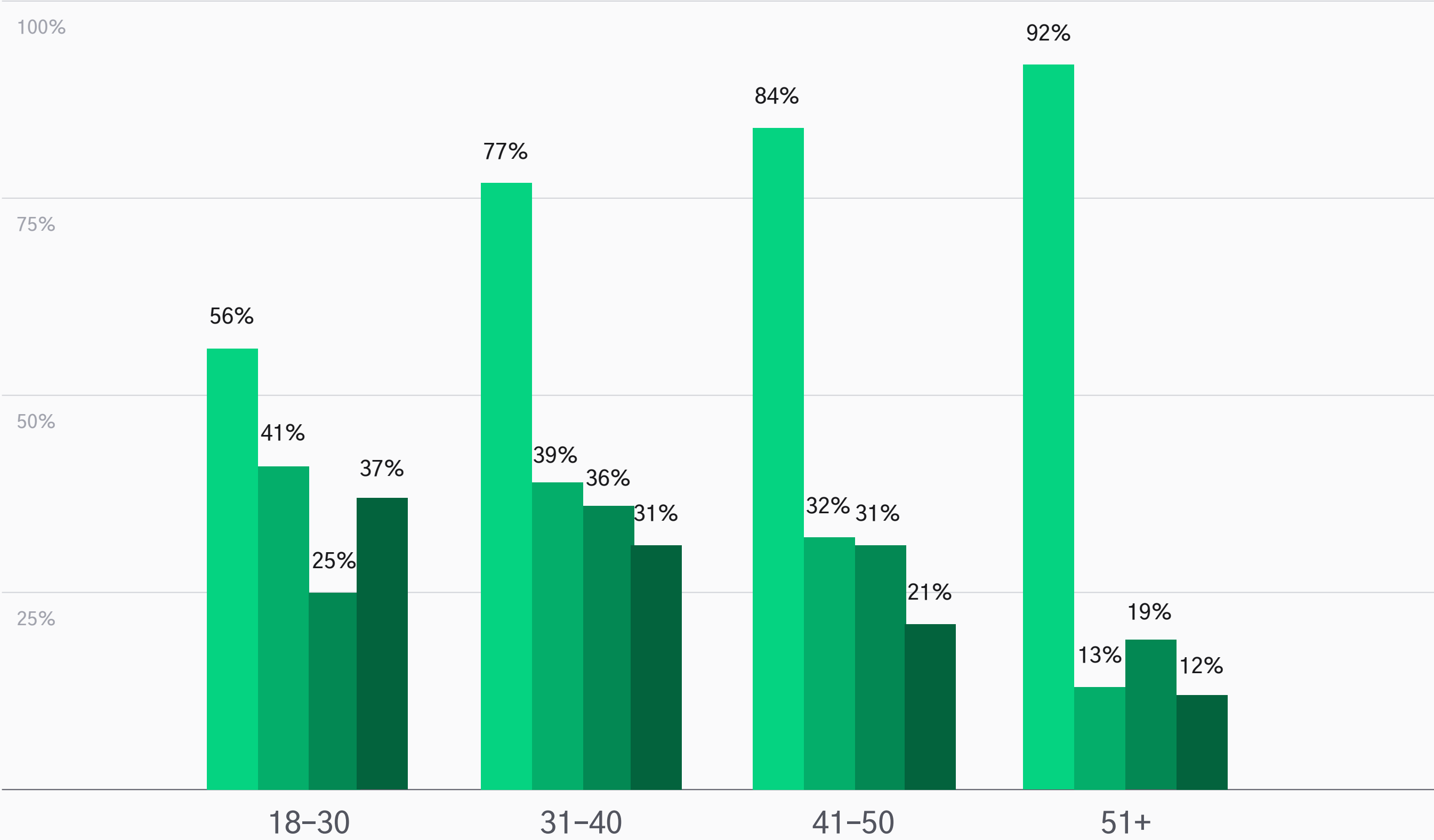
### Opinions vary based on department, gender, and age, though.

People working in accountancy and finance were twice as likely as people in sales and marketing to want to work exclusively in an office post-pandemic – 17% versus 9% respectively. Likewise, men are almost twice as likely as women to want to return to a full week in the office – 22% of men versus just 13% of women.





Older employees were much more likely to want to work from home, with 92% of respondents over 51 saying so versus 56% of 18–30 year olds. There are a number of reasons for why this could be, namely having a better work/life balance and spending more time with family. A [study](#) also found that older staff are actually most likely to have jobs that can be done remotely.

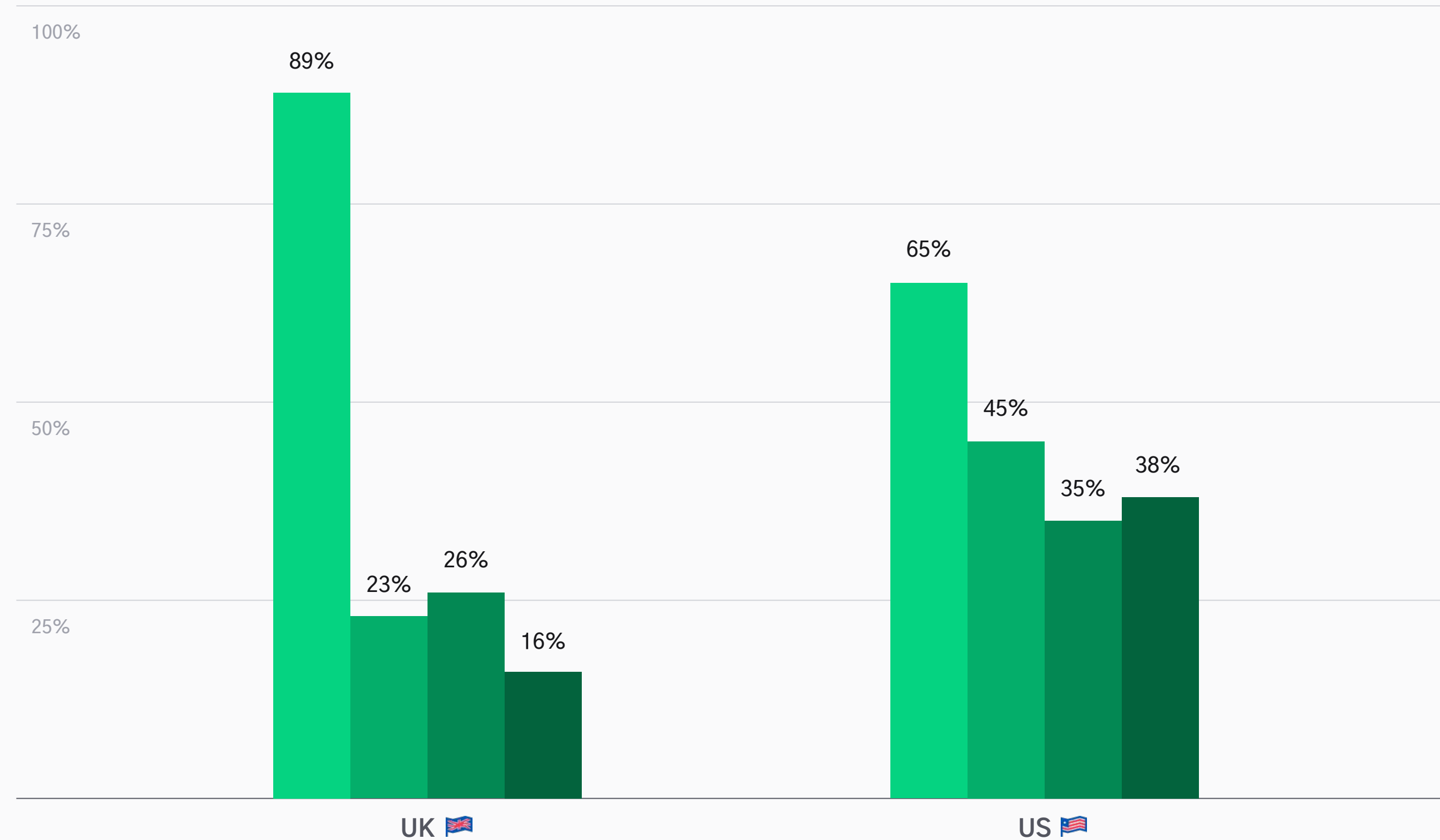
### The locations employees want to work, broken down by age:

-  My home
-  Abroad / in a holiday home
-  Co-working / hot desking spaces
-  A local cafe or restaurant



### Locations employees want to work in, broken down by geography:

 My home    Abroad / in a holiday home    Co-working / hot desking spaces    A local cafe or restaurant



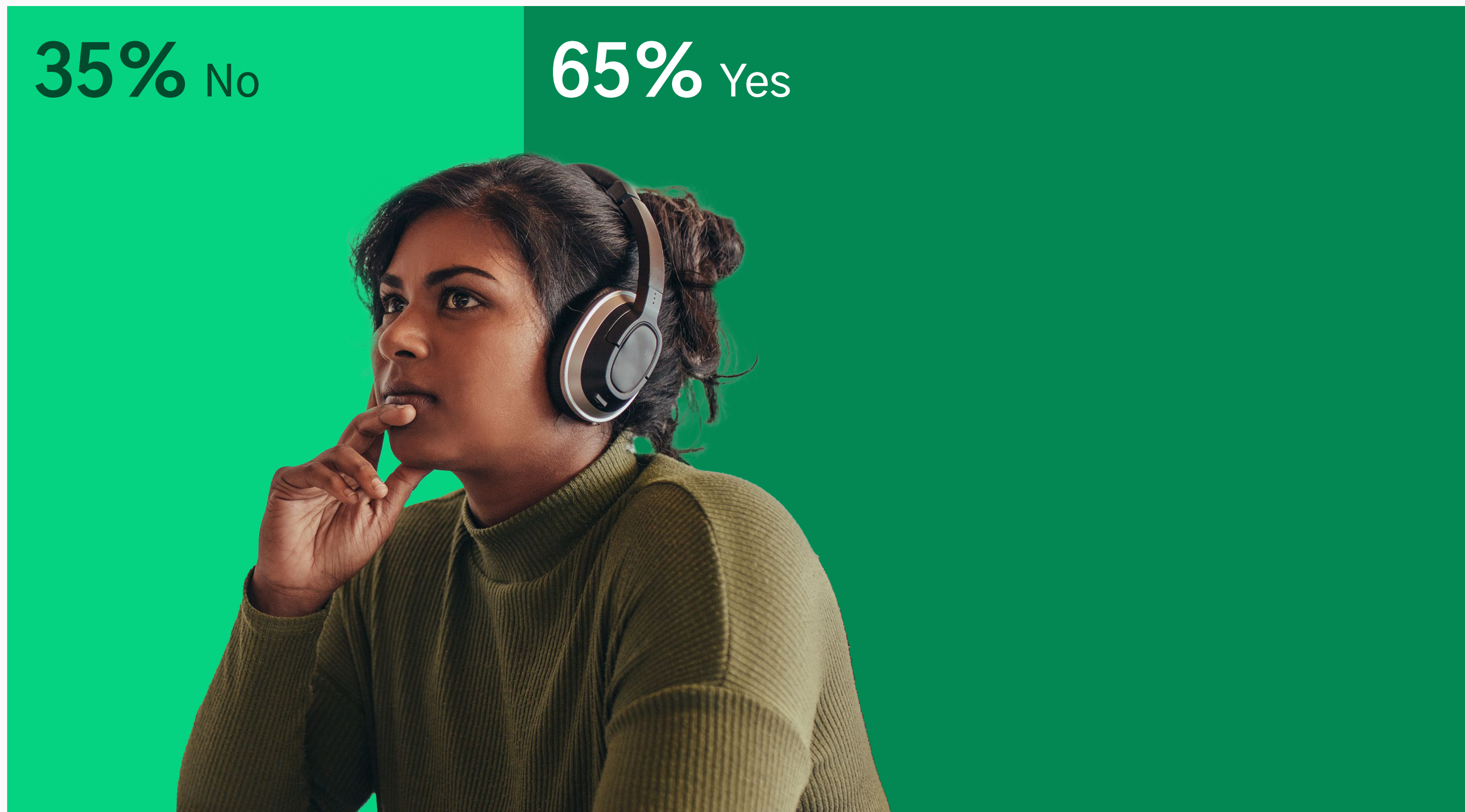
## People want to work from anywhere.

While home is the preferred location for people to work remotely from, respondents revealed they want the flexibility to be able to work from “anywhere”.

Nearly a third of employees (30%) said they’d like to work abroad or in a holiday home, and just over a quarter said they’d like to work in coworking or hot desking spaces.

Preferences on where people would like to work also varied between UK and US respondents. Nearly nine in 10 UK office workers (89%) would like to work from home versus only 65% of American office workers, while employees in the US are more likely to want to work from a holiday home or abroad.

## Percentage of employees that would work for a company without flexible working



The bottom line: employees want the flexibility to be able to work in an environment that suits them best. People from different age groups, genders, geographies, and departments all have their own ideas of how and where they want to work. And, now that they've had a taste of flexible working, it'll be hard to go "back to normal."

Accommodating those preferences and expectations won't be easy though, especially from an IT and security standpoint.

Not only do IT teams have to secure their organization from remote-working risks – like phishing, BYOD, and employees' unsafe data practices – but they also have to consider security risks such as employees bringing infected devices or documents into the office, potentially compromising the company's entire network.

While the adjustment may be difficult, organizations have a lot to lose if they don't adapt. More than a third of survey respondents said they would not consider a job that didn't offer remote working.



# IT leaders are feeling the pressure.

IT decision makers are most concerned about people's wellbeing if their company were to adopt a permanent remote working structure.

This is important. A [previous Tessian study](#) highlighted how stress negatively impacts people's cybersecurity behaviors and, by putting people first, IT professionals recognize the correlation between employee wellbeing, their productivity, and security.

IT leaders also fear employees' unsafe data practices could compromise their company's security and lead to more data breaches and phishing attacks.

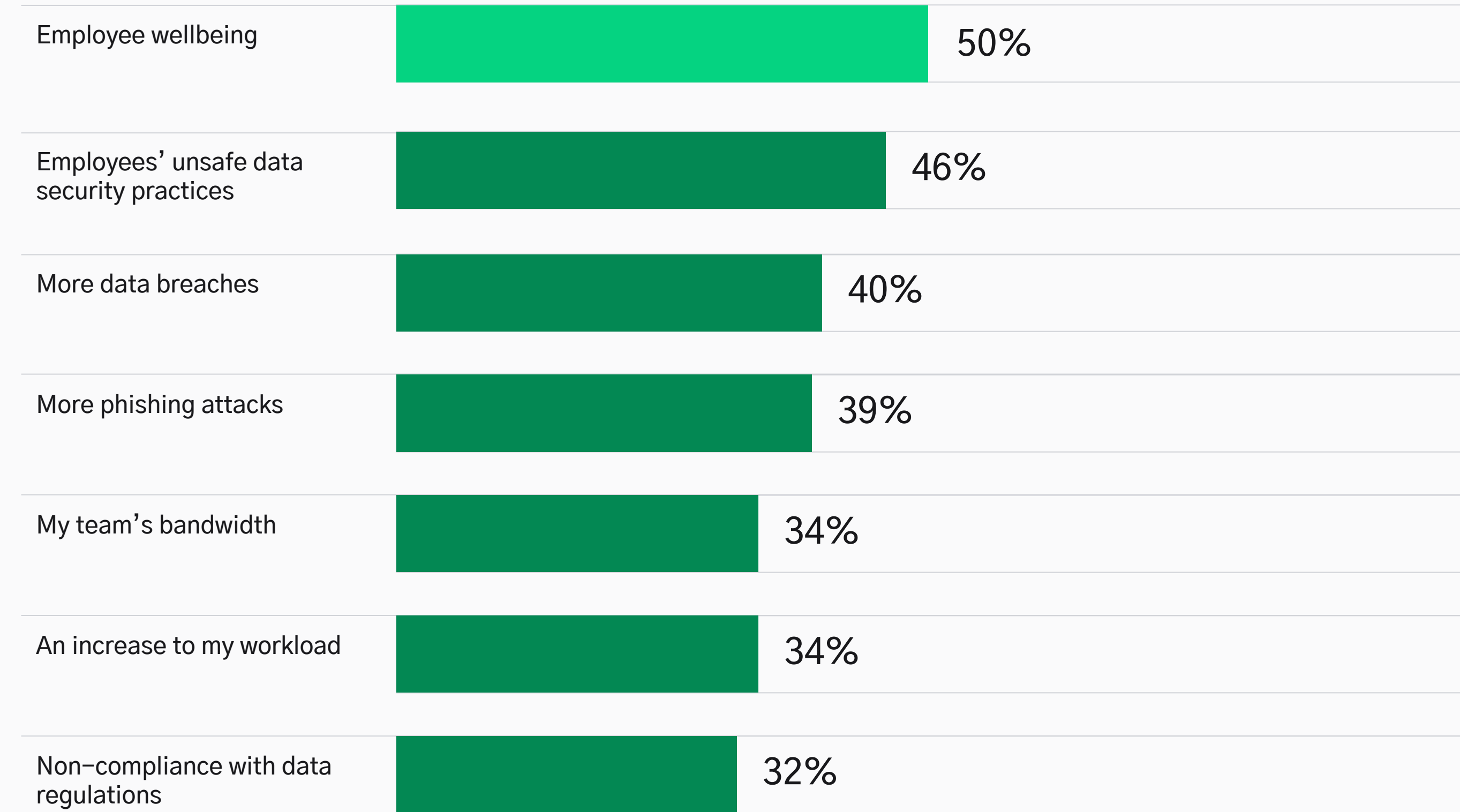
[SUBSCRIBE TO THE TESSIAN BLOG](#)

**Get more insights straight to your inbox.**

Helpful resources and shareable guides, tips for CISOs, and early access to our latest research.

[SIGN ME UP →](#)

## IT leaders' concerns if their company adopts a permanent remote working structure:



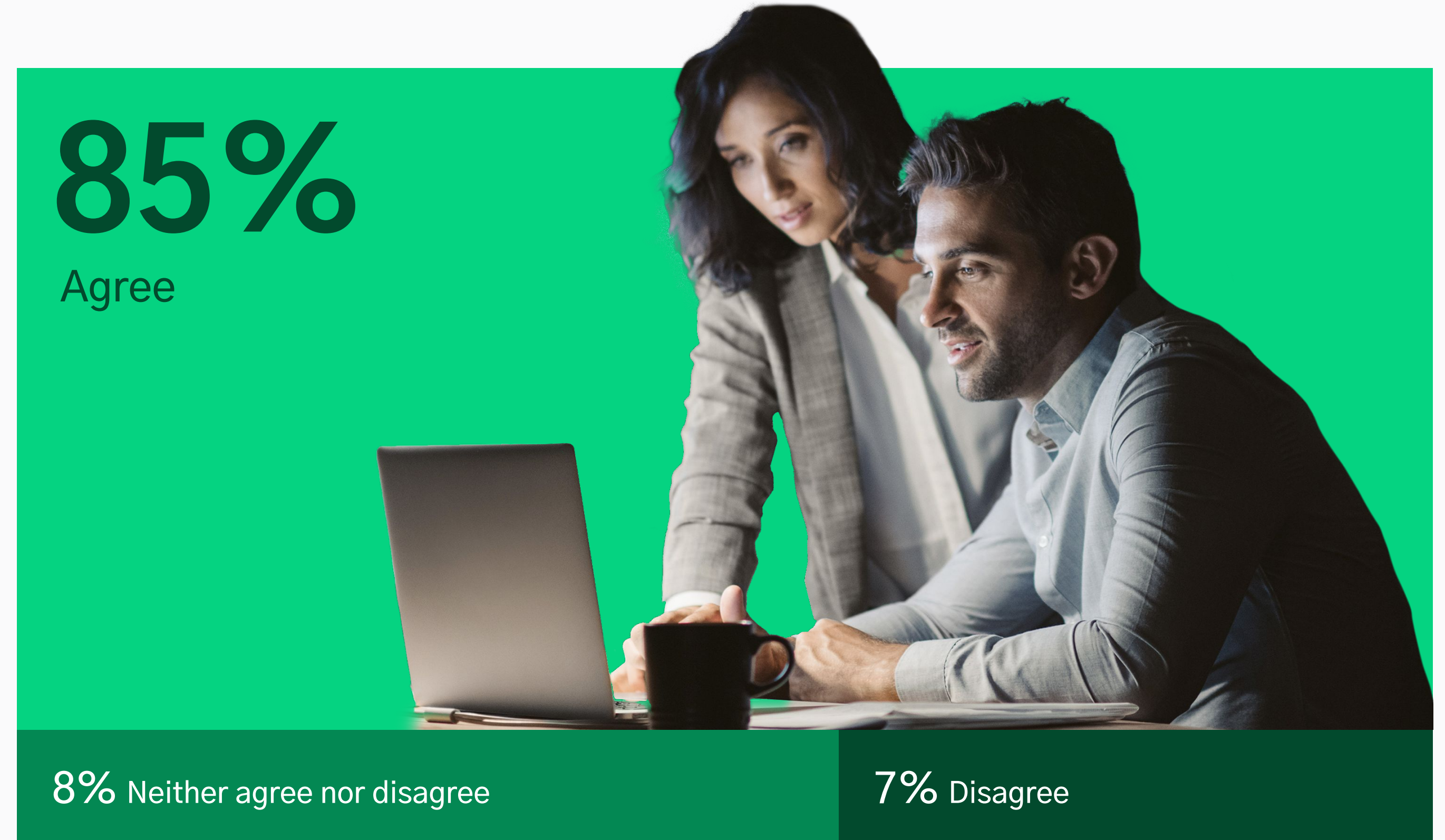
But that's not all. Over a third (34%) of IT leaders are worried about their teams being stretched too far in terms of time and resource.

They also have serious concerns about their own workload increasing, with 85% of IT leaders believing their teams will be under more pressure operating in a permanent remote working structure.

These insights are worrying, especially when you consider that earlier this year, over half of IT professionals have experienced burnout and feel overworked.

As the pressure increases, businesses must find ways to alleviate stress, unburden teams of labor-intensive and manual tasks, and empower IT professionals to work effectively and efficiently in order to protect their company and employees.

IT security teams will be under more pressure if their company adopts a permanent remote working structure:





Chapter 2

# Hybrid Working Risks

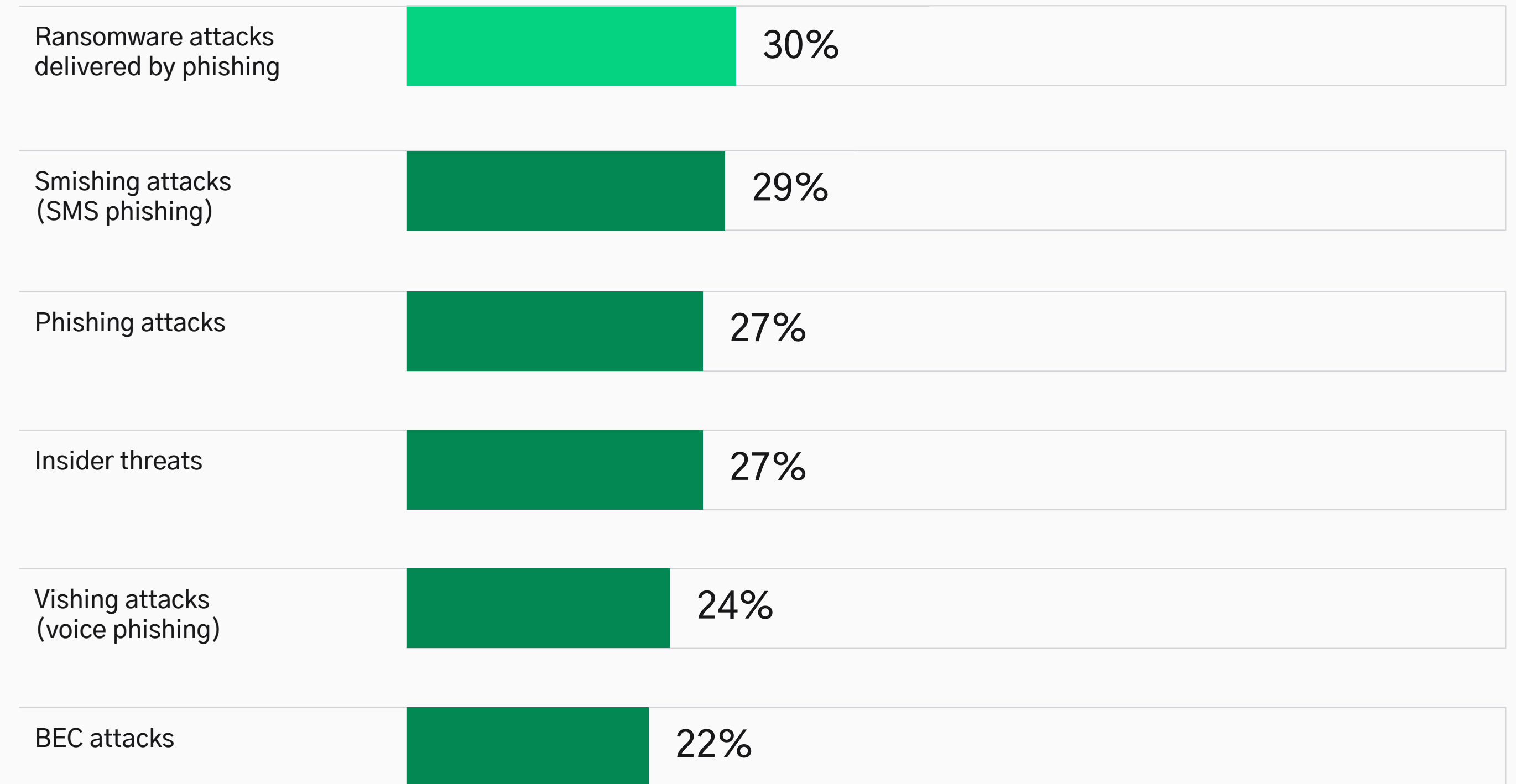
# The risks that threaten safe hybrid working.

The concerns identified by IT leaders in this report are valid. How do we know? During the remote working period enforced by the global COVID-19 pandemic, organizations reported spikes in both phishing attacks and security incidents caused by insider threats.

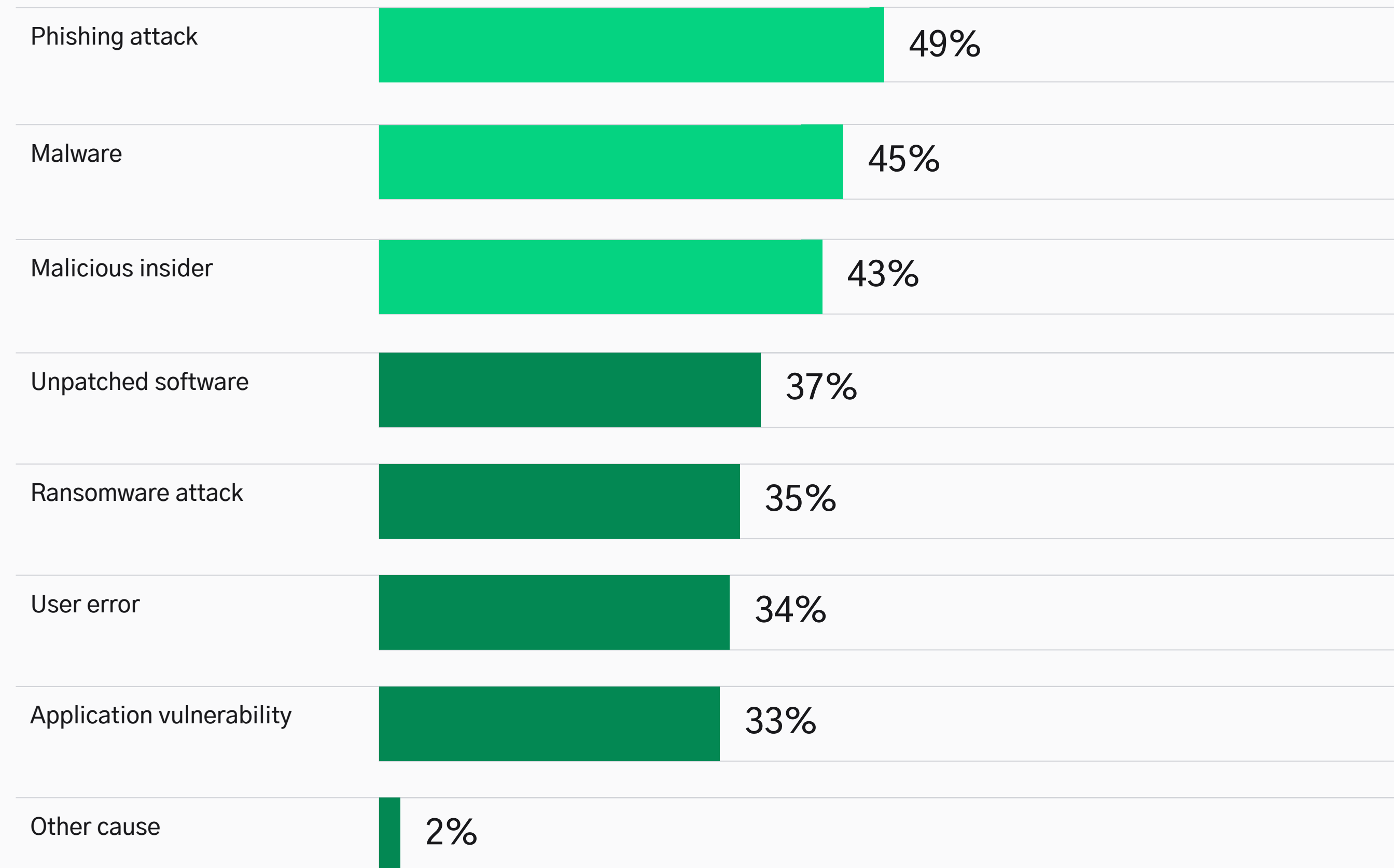
Between March and July 2020, one in three organizations saw an increase in ransomware delivered by phishing compared to the five months prior. In addition, around a quarter of IT decision makers reported that their company had received more impersonation scams like phishing, smishing, and vishing—a technique reportedly used by cybercriminals to trick employees at Twitter into sharing account information in July 2020.

In July 2020, Twitter experienced a major data breach, which led to the hacking of accounts belonging to celebrities and politicians like Joe Biden and Kim Kardashian-West. Attackers used a “vishing” attack to target a small group of Twitter employees, tricking them into sharing network credentials. The scammers reportedly made more than \$100,000 from the attack and exposed how easily attackers can dupe people into sharing highly sensitive information.

Percentage of IT decision makers that experienced more of the following threats between March — July 2020 compared to five months prior:



### Causes of data breaches that occurred between March - July 2020:

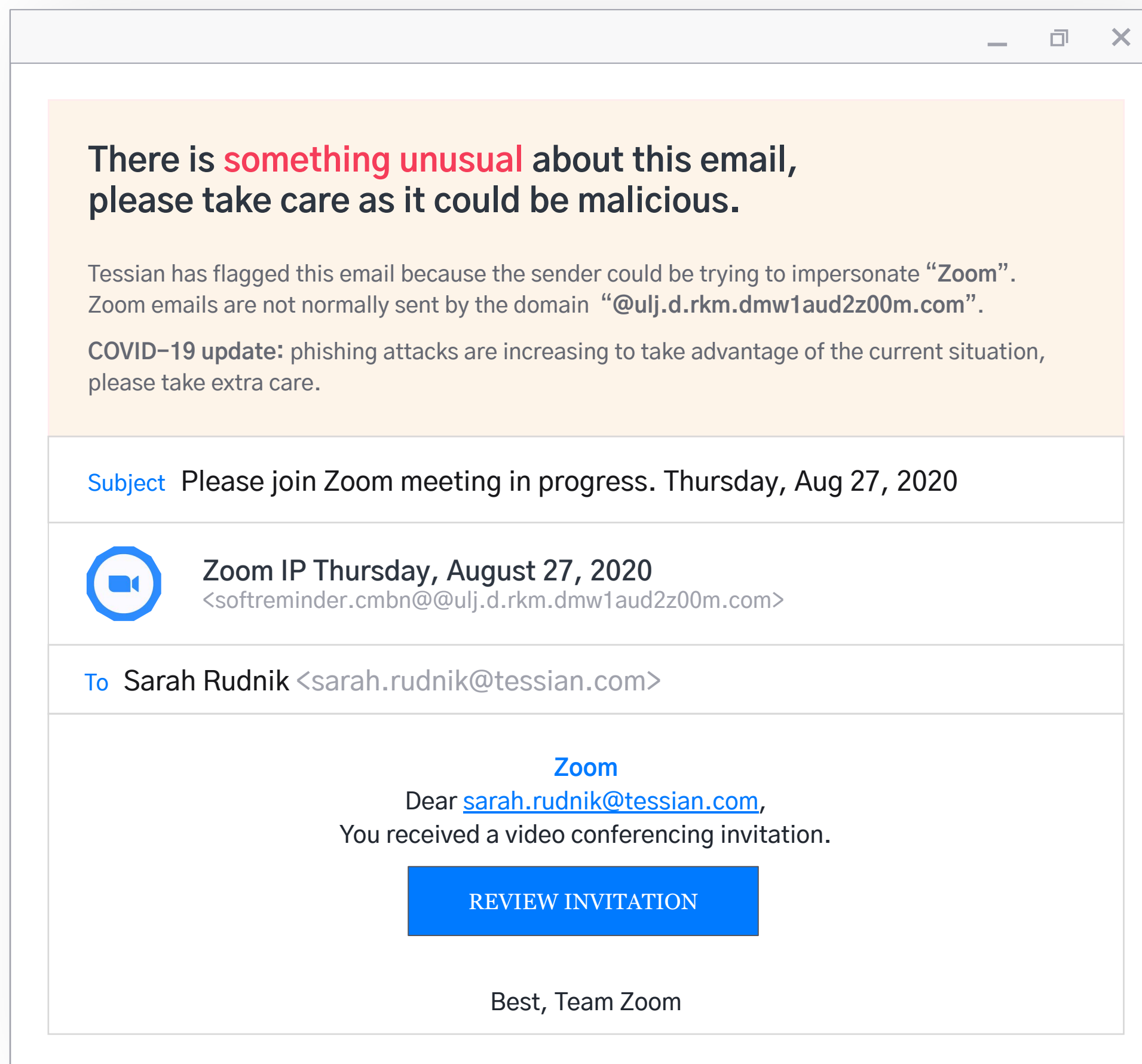


## Phishing was the top attack vector during the pandemic.

In fact, between March and July 2020, nearly half of companies experienced a data breach or security incident; half of these attacks were caused by phishing.

What's more, nearly two-thirds of US and UK employees (65%) said they received a phishing email during the remote working period that was enforced by the global COVID-19 pandemic.

[Tessian Defender](#) saw a spike in phishing attacks during this period too. It detected and prevented over 128,000 malicious attacks during the time of lockdown (March-July 2020). In contrast, during the previous five-month period, it had flagged just over 44,000.



Given the increase in phishing attacks, it's perhaps no surprise that 82% of IT leaders think their company is at greater risk of phishing attacks when employees are working away from the office.

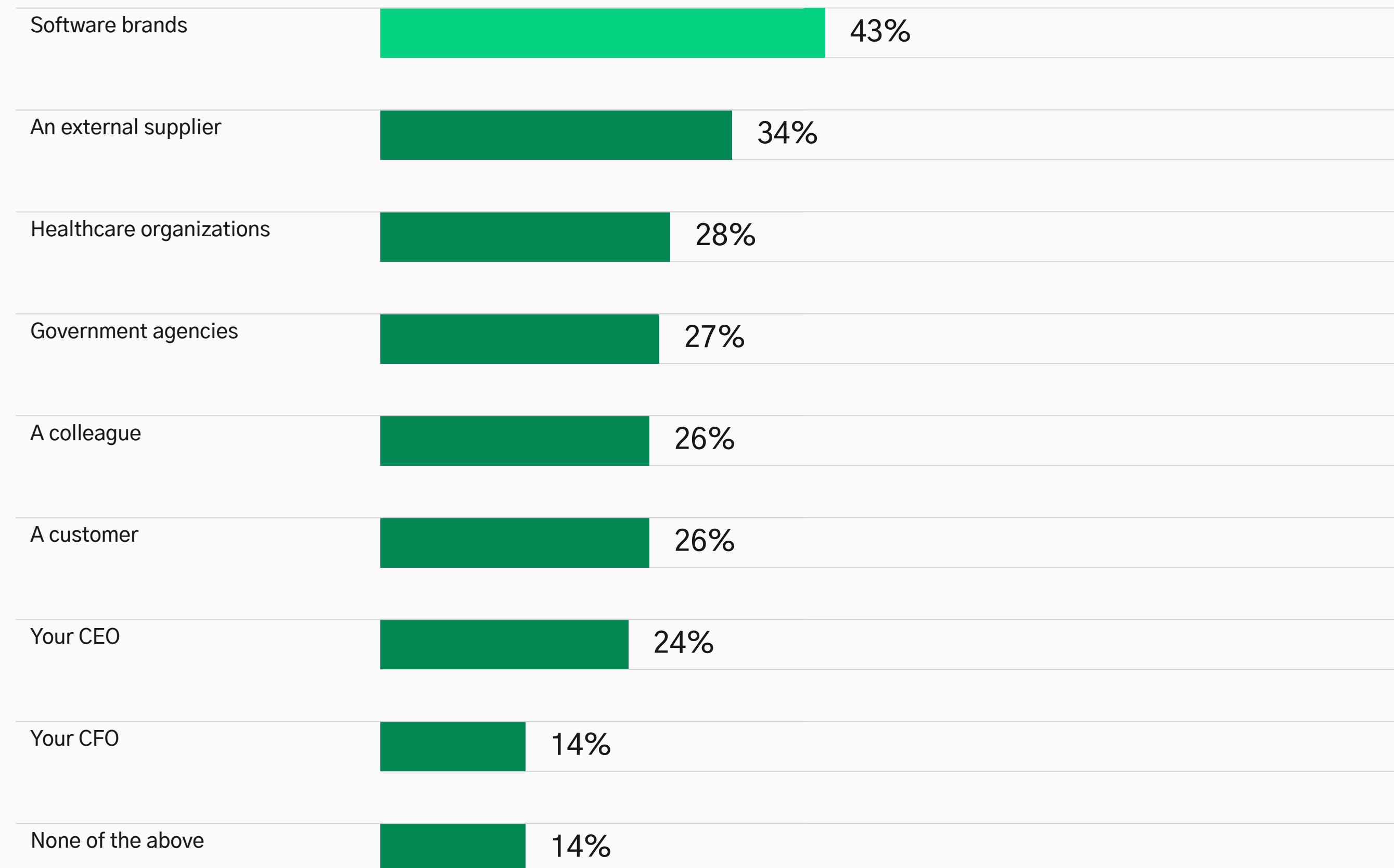
But why is phishing a greater risk for remote workers?

Because it is not uncommon for an employee to receive information about a new software update for a video conferencing app, or an email from a healthcare organization providing tips on how to stay safe, or a request from a senior executive asking them to send customer information for an important matter.

To the left is an example of such a phishing attack that Tessian Defender detected and flagged. The hacker has impersonated Zoom to trick an employee into clicking a "meeting" link.

If the sender's email domain looks legitimate and if hackers have used the correct logos in the body of the email, there's very little reason why an employee would suspect they were the target of a scam. And, when working remotely, employees can't easily verify the email with a colleague. As a result, they may click the link to "join the meeting", download the "new update" or share account credentials.

## Most impersonated brands in phishing attacks



While impersonation scams aren't new — we've seen these types of attacks grow in frequency and severity even before the pandemic — trends related to "who" the hackers were impersonating during lockdown is something we've been paying close attention to.

For example, rather than just impersonating the senior executives in an organization, we saw hackers were actually more likely to impersonate healthcare organizations like the WHO and government agencies at the start of the pandemic, as people looked for information about the COVID-19 virus.

They, then, quickly pivoted to impersonating software brands in response to the sudden shift to remote working. In fact, the majority of IT leaders said that employees received emails from software brands — like Zoom and other video conferencing services or collaboration platforms — between March and July 2020.

## It isn't just attacks from the outside that keep IT leaders awake at night while people work remotely.

43% of security incidents that occurred between March and July 2020 were caused by malicious insiders and over a quarter of businesses (27%) experienced more security breaches caused by insider threats during this period, compared to the five months before the pandemic.

Data from [Tessian Enforcer](#) also reveals a 25% increase in the number of employee attempts to exfiltrate data to unauthorized email accounts between March to July 2020, compared to the five months prior.

Of course, not all these attempts were malicious and, in many cases, people may not have realized they were doing anything wrong.





A number of our customers found that employees were sending documents to personal email accounts so that they could print from their home devices.

Others told us that company information was being shared over personal emails as employees needed updates from furloughed staff on specific projects or cases they were previously working on.

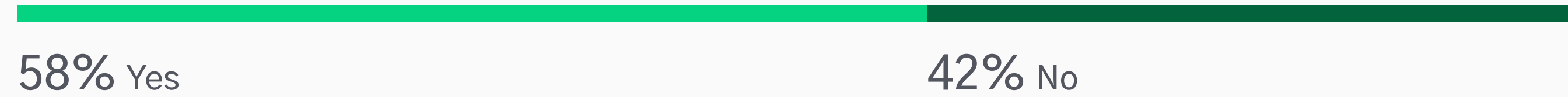
Even though the employees had good intentions, sensitive information was leaving the organization, putting it in danger and putting the company at risk of non-compliance.

Consequently, 78% of IT decision makers believe their company is at greater risk of insider threats when employees are working remotely.

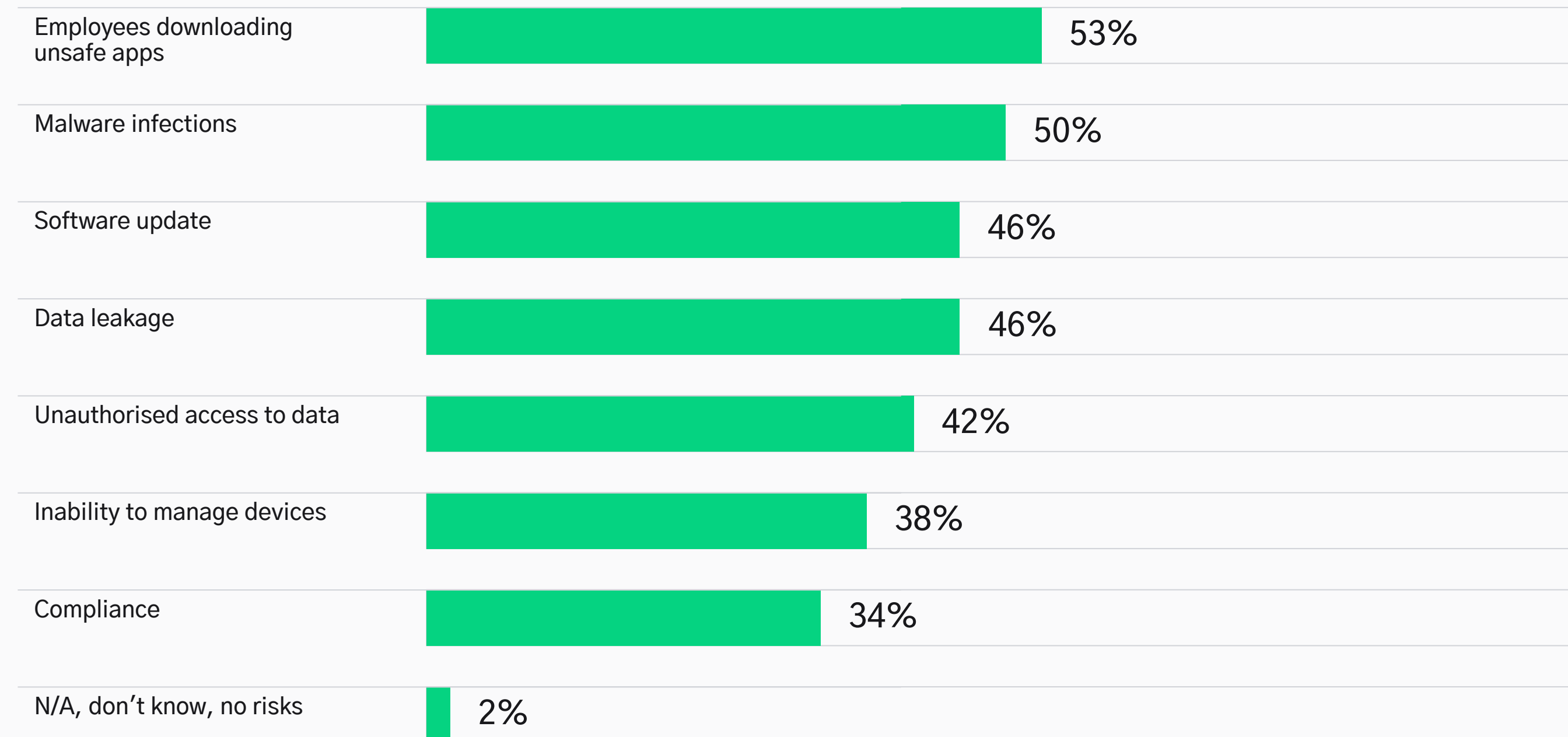
My company is at greater risk of insider threats.



### Percentage of employees that worked on a personal device during the lockdown period:



### Biggest security risks caused by BYOD:



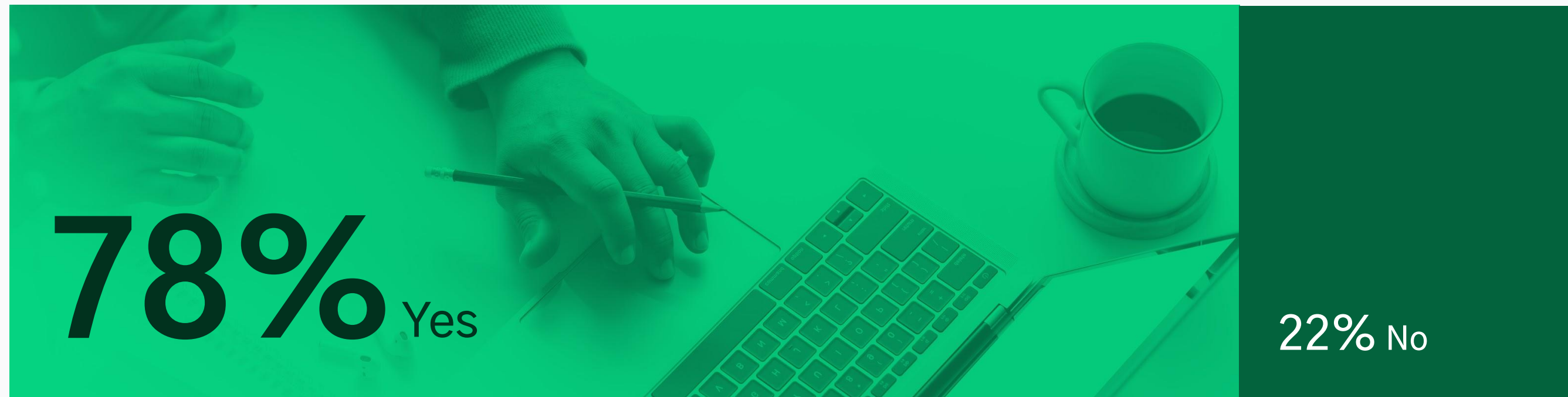
Bring Your Own Device (BYOD) also posed more security risks for organizations during the period of remote working.

Over half of employees (58%) reportedly worked on their personal devices to get their jobs done when the world went into lockdown.

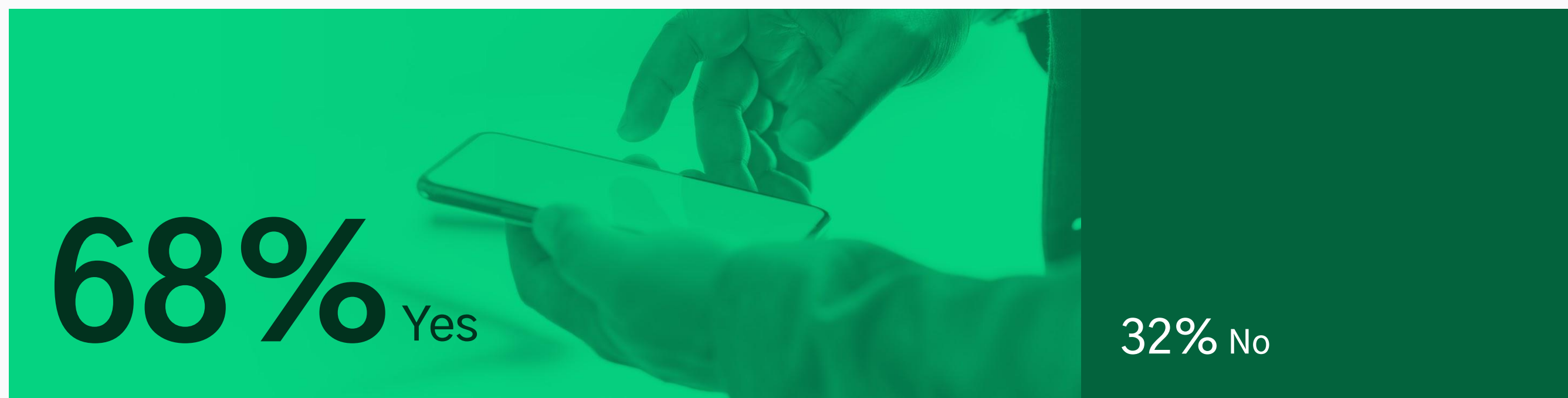
The top BYOD security risks cited by IT professionals included the downloading of unsafe apps, malware infections, and software updates.

As the lines between people's personal and professional lives continue to blur, IT teams are having to manage and mitigate threats that feel out of our their control.

Percentage of employees that received a phishing email while working on their personal device:



Percentage of employees that clicked on a phishing email while working on their personal device:



## Phishing was another security concern for employees working on their own devices.

Over three quarters (78%) of remote workers who used their personal devices for work said they received phishing emails, either in their work or personal inbox.

But perhaps more shockingly, over two thirds of these employees (68%) clicked a link or downloaded an attachment from the phishing emails they received on their own devices.

With this in mind, 43% of IT leaders said they are now looking to upgrade or implement new BYOD policies in order to better secure their organization for a future of hybrid working.

Chapter 3

# Balancing Flexibility and Security

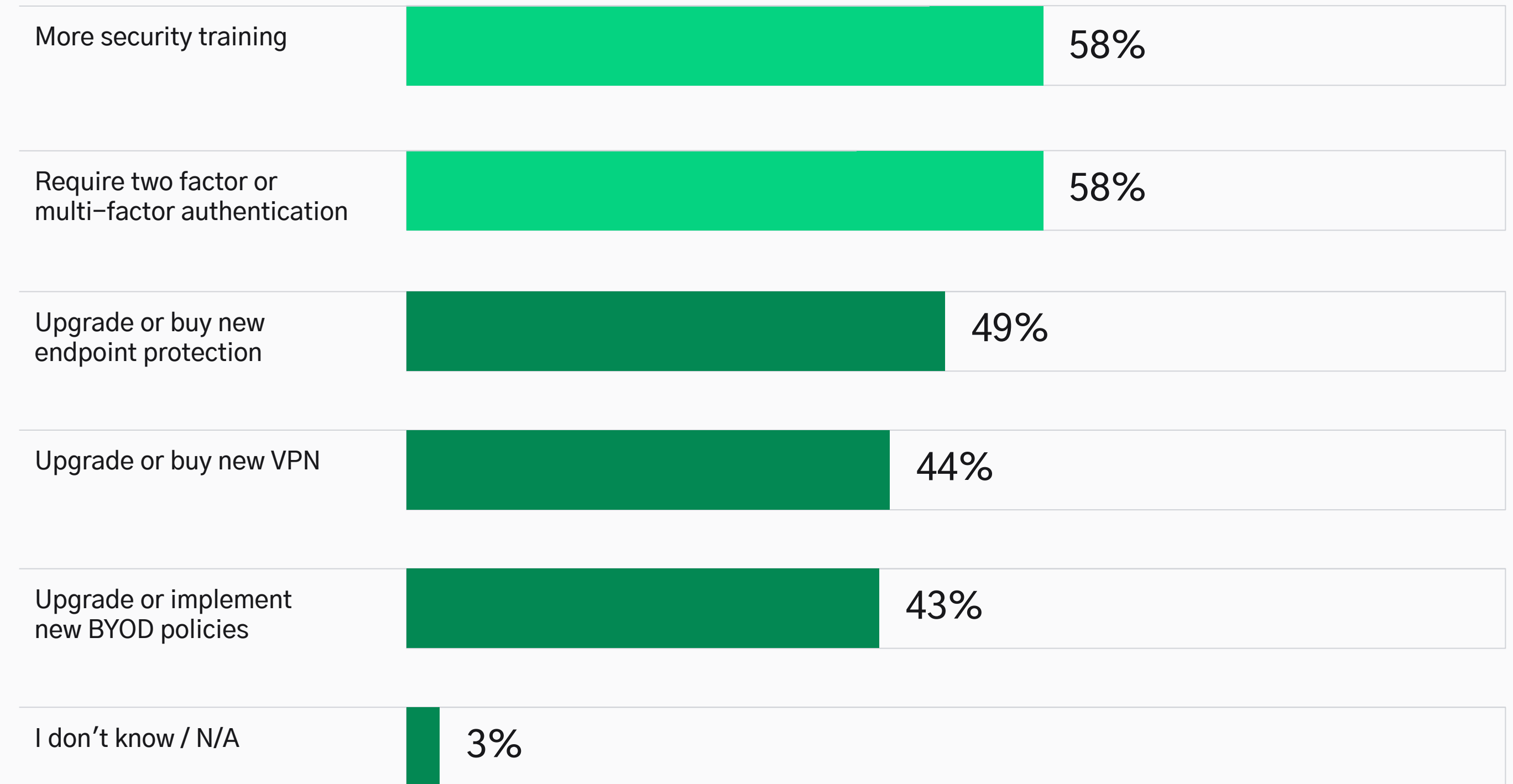


# Finding ways to balance flexibility and security.

Businesses are already thinking about the long-term future of hybrid working and are looking at a number of solutions to update their security measures, policies, and procedures.

One of the top priorities for IT leaders is to **introduce more security training**, something 58% said they intend to do should their company adopt a permanent remote working structure.

## New measures, policies and procedures that IT leaders plan to put in place to secure hybrid working:



But, the problem is, security leaders cannot guarantee employees are actually tuning in to training outside of the office.

In fact, despite 57% of IT departments implementing more education and security training for their employees during the pandemic, nearly 1 in 5 workers said they didn't take part.

What's more, over a third of companies didn't actually provide any additional training to educate their staff on the security risks of remote working.

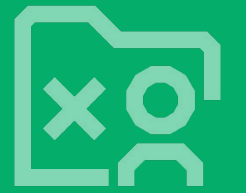
This isn't trivial. Businesses need to make their people aware of the ways attackers could target them when they are working away from the office, and educate them on the ways their remote working behaviors could compromise company security.

Percentage of employees that took part in security training during March — July 2020:

**39%** My company implemented training and I took part in it.



**18%** My company implemented training but I didn't take part.



**34%** My company didn't implement training.



**9%** I don't know

Security training also needs to be tailored if it's going to truly resonate and stick. When it comes to training, one-size certainly doesn't fit all.

But, by using machine learning, organizations can automatically alert employees to the specific threats they face. Providing employees with educational and contextual alerts not only stops a person from making a mistake they'll later regret, but it also helps reinforce safe cybersecurity behaviors over time.

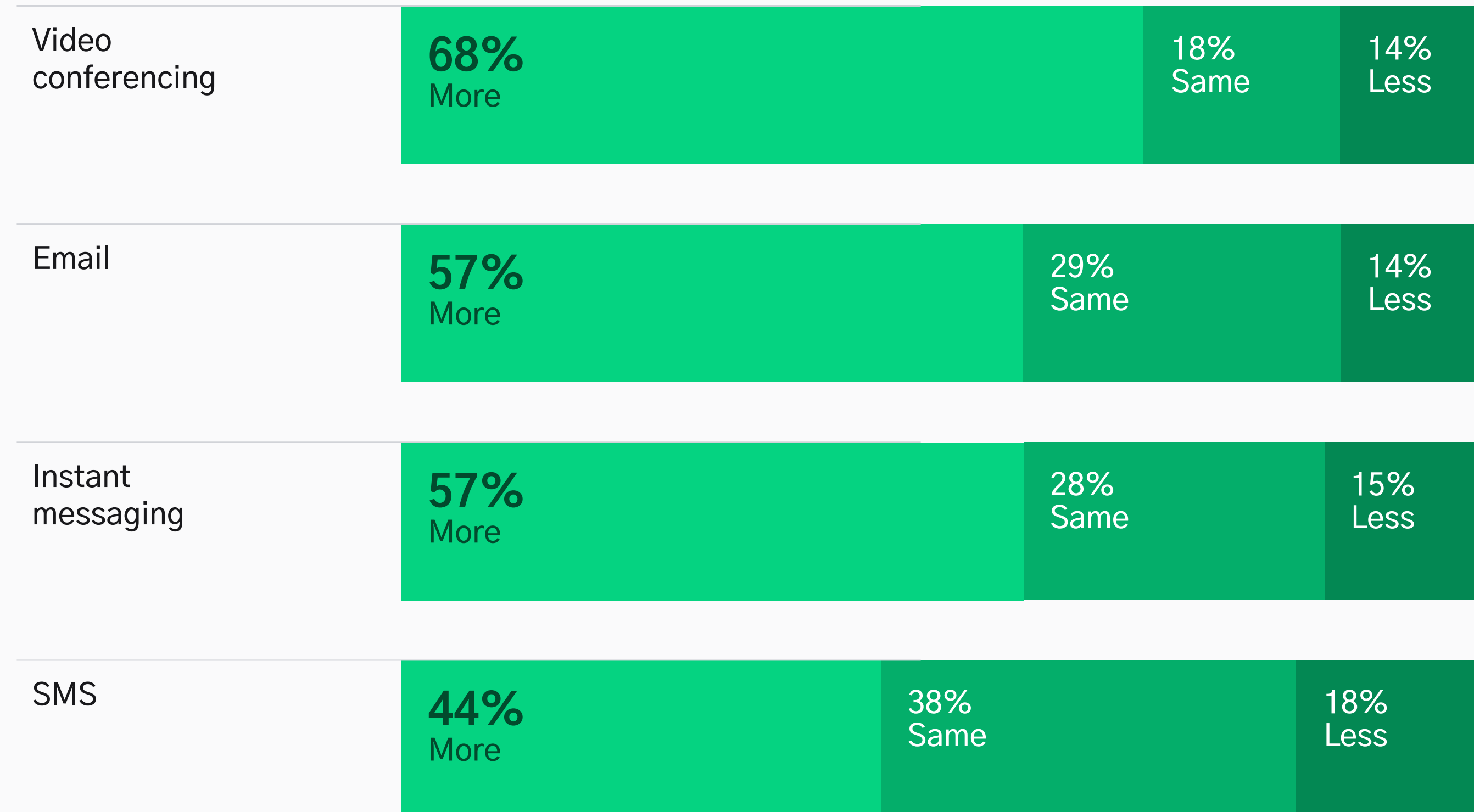
#### Did you know?

Tessian alerts people, in real-time, when something on email doesn't look right. That way, we can prevent security incidents from happening. By using explainable machine learning, we educate people on why the email they're about to send or have received is a potential threat and provide advice on what they should do next.

Targeted 14 times in the past 30 days.



The channels employees are more or less reliant on to stay connected when working remotely:



## Business must also protect people on email.

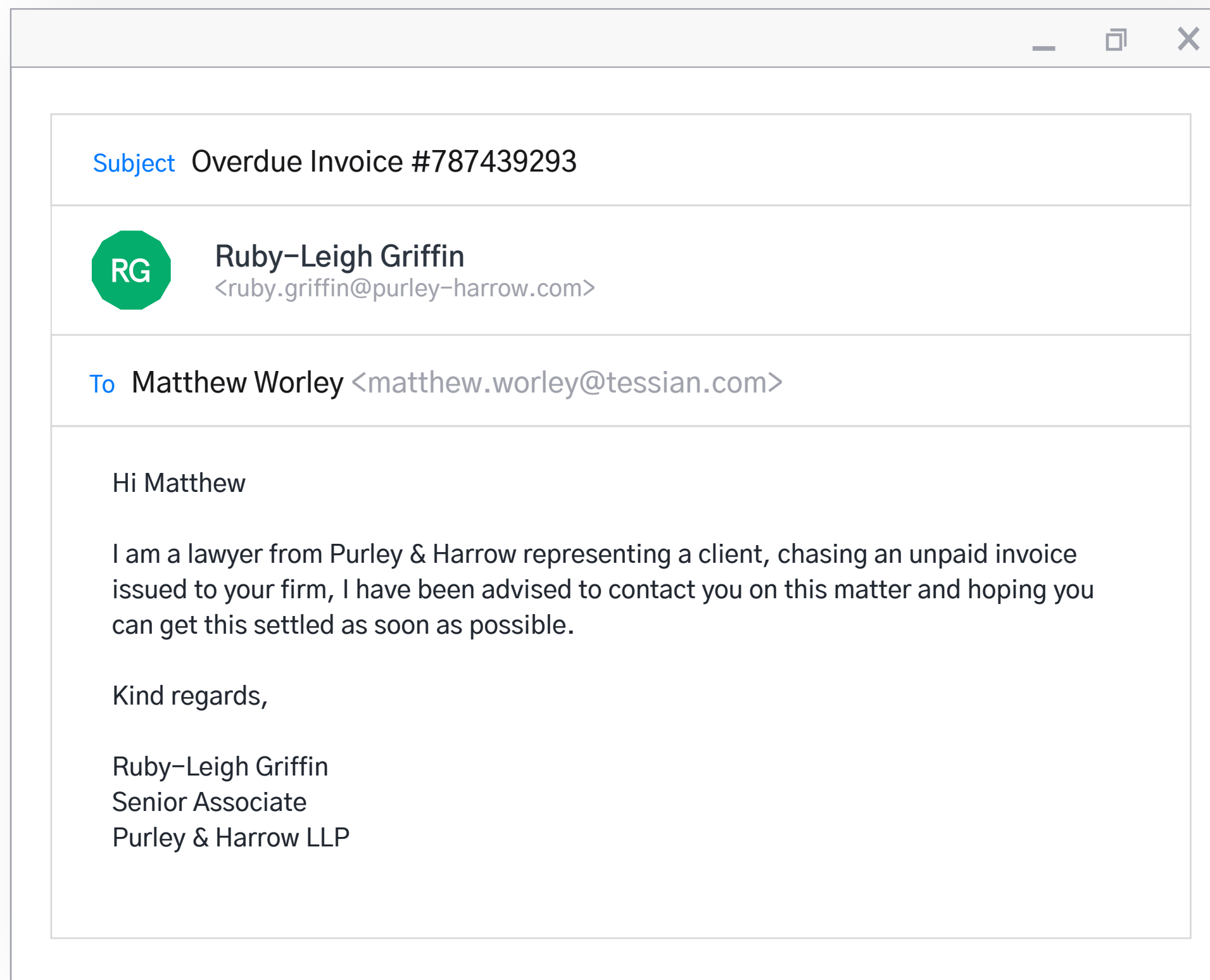
Securing channels like email is critical as workforces transition to permanent remote and hybrid working structures.

Why? 57% of employees were more reliant on email as a channel to stay connected with colleagues when they were working remotely.

This is supported by Tessian data, which shows that email traffic increased by 129% at the start of the remote working period (March – April 2020), compared to January – February 2020.

Within this period, people sent and received more emails to and from their colleagues, their customers, their suppliers, and software providers.





## A more crowded inbox opens up more opportunities for opportunistic cybercriminals.

With more emails and with more distractions around them when working from home, people could easily miss the cues that signal a threat.

But, that's not the only problem employees face. The inherently open nature of emails means that **hackers can email anyone** and they can easily impersonate any one of the people or brands your employees communicate with via email. In doing so, they can trick people into believing they are receiving an email from someone in their network and convince them into clicking a link, sharing credentials or downloading malware.

With remote work here to stay, **hackers will continue to find ways to take advantage of the channels people rely on most** to advance their malicious campaigns. We've seen this time and time again throughout the global pandemic.

Businesses must find ways to protect people from scams that exploit the channels they use the most frequently, like email and video conferencing services.

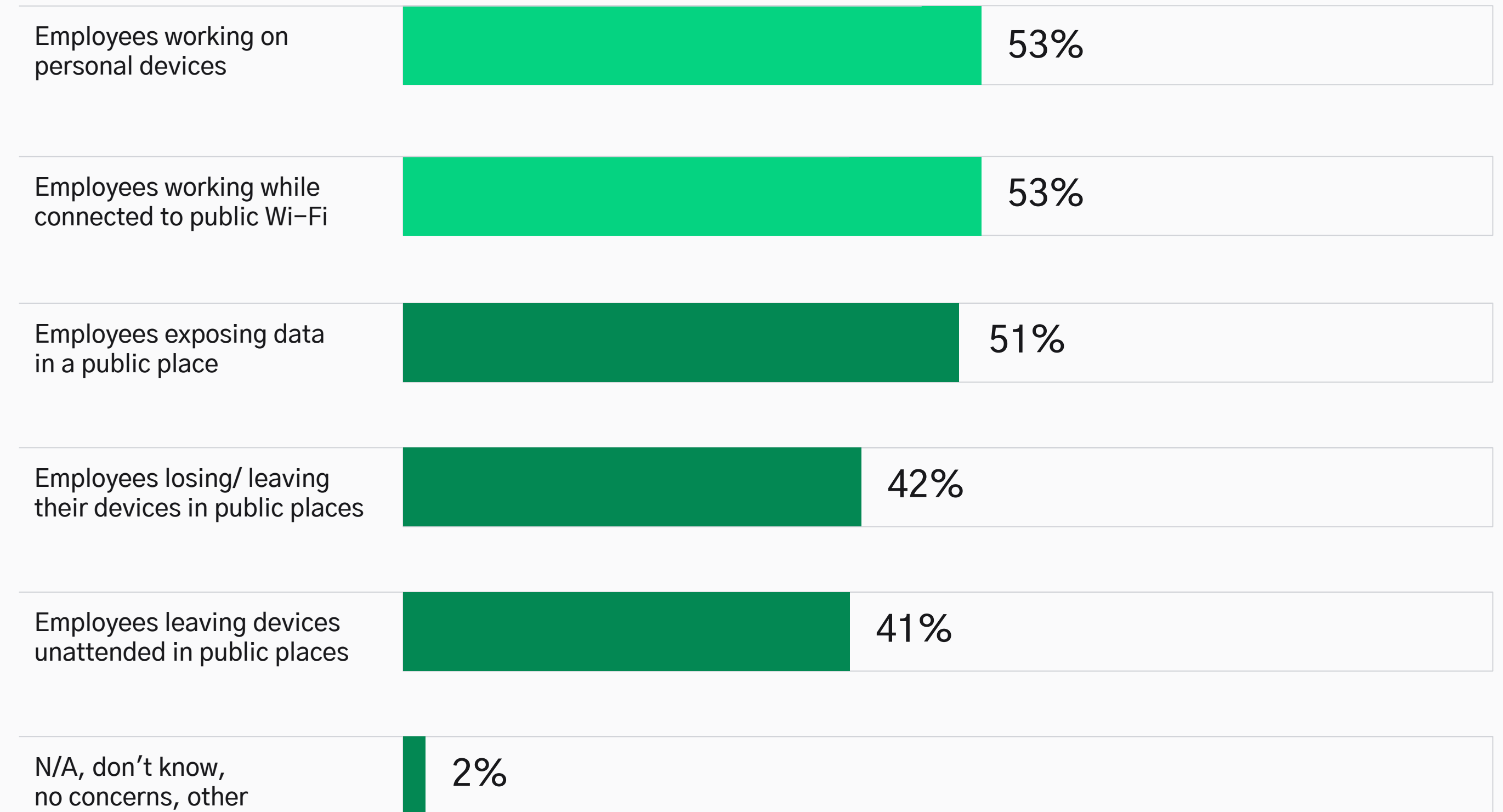
# Companies need to educate people on safe cybersecurity practices.

IT leaders also have concerns over security incidents that could result from carelessness or limited access to a secure internet.

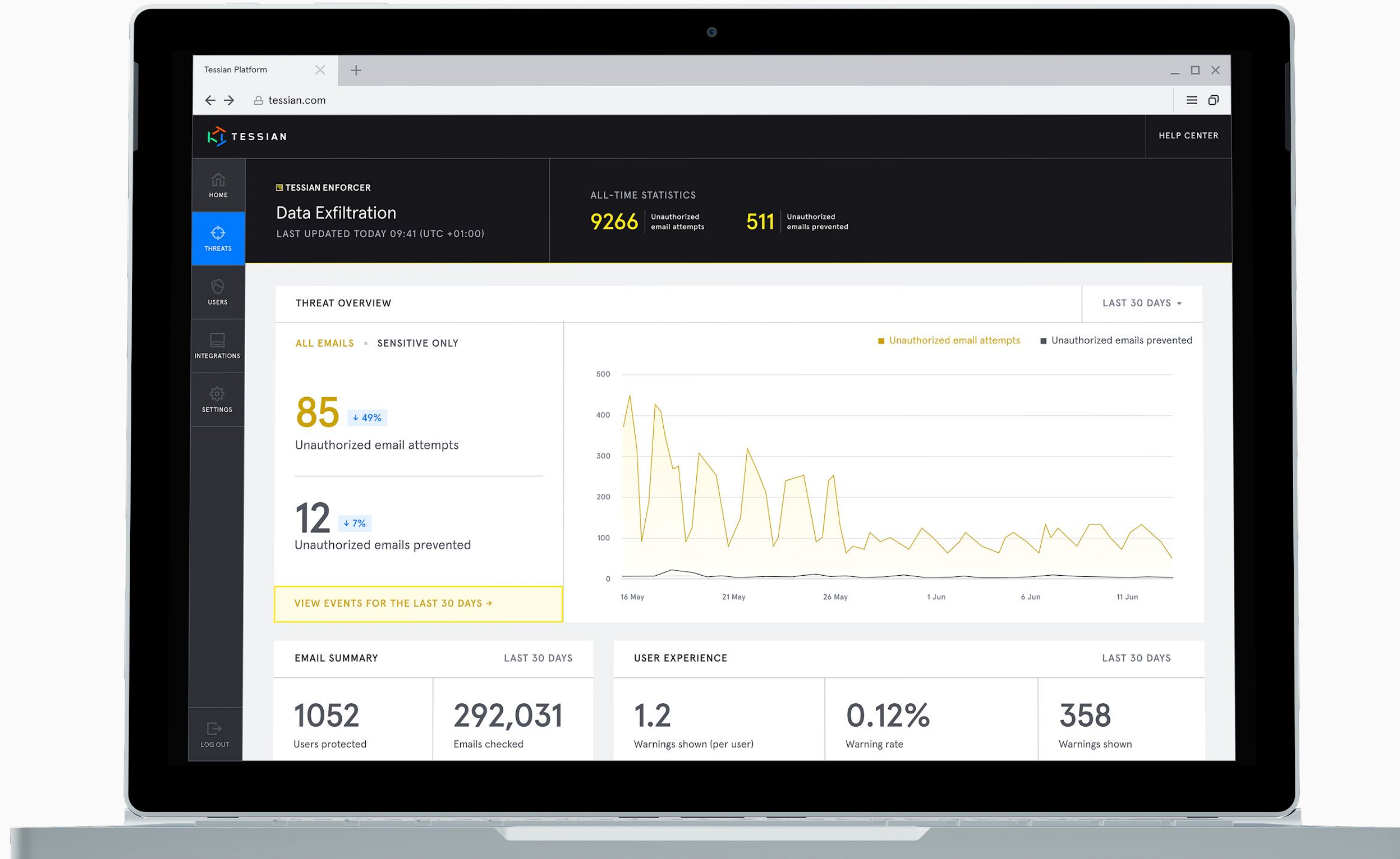
Over half (53%) are worried that employees will connect to public WiFi when working remotely, and it seems they're justified in their concerns as 58% of employees admit they've either considered connecting to public WiFi or – worse – already had done so.

They are also worried about employees exposing data in a public place and leaving devices unattended. Educating people on the risks – and the consequences – these behaviors could have to their company and also their own security has to be a priority if businesses want to keep data and employees safe.

## IT leaders' concerns about people working away from the office:



## TESSIAN HLS INTELLIGENCE



## Make security as flexible as your employees.

Putting in place a strategy that can successfully enable employees to work however and wherever they want is not going to be without its security challenges. Businesses must reinvent, redesign and transform everything they've previously done. IT teams will be under pressure to ensure people can work remotely, but safely.

To set yourself up for success, visibility is key. IT teams need visibility into their riskiest and most at-risk employees, no matter where they're working, in order to tailor training and policies and improve cybersecurity behaviors over time. Getting this level of visibility shouldn't be a burden to the IT team, though. IT teams will have enough on their plates which means finding solutions that leverage machine learning to take away labor-intensive tasks will be critical in freeing up IT professionals' time.

### Tessian HLS Intelligence in action

Here you can see how Tessian HLS Intelligence downtrends risk and improves people's cybersecurity behaviors over time. This Tessian customer significantly reduced employee attempts to send data to unauthorized email accounts by warning its staff about how data exfiltration breaks company policies and puts data at risk.

It's also important that security solutions don't hinder people's productivity, and that companies have a people-first approach to security.

It's obvious that people want to be able to work flexibly, so tools need to be flexible, too. Tessian is invisible to employees until threats are detected, meaning our solution has minimal disruption to people's workflow. Our warnings are helpful, not annoying. We give people the information they need to make safer cybersecurity decisions and improve their behaviors over time.

The way people work is quickly changing. But one thing will stay the same; people being your organization's most important asset. Protect them and empower them to do great work, without security getting in their way. Invest in security solutions that make your IT teams' lives easier and give them greater visibility into people's behaviors no matter where they decide to work.

The future of work is hybrid. Businesses that secure it will be better positioned to achieve their mission and thrive in this new world of work. We can help make that happen.





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)

## Methodology

During August 2020, Tessian commissioned OnePoll to survey 2,000 working professionals: 1,000 in the US and 1,000 in the UK. 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+.



## 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

[SIGN ME UP →](#)

Share this report



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