



↳ SECURITY CULTURES REPORT **2022**

How Security Cultures Impact Employee Behavior

Based on responses from security leaders and employees across industries and geos, as well as input from security awareness advocates, communications academics, and CISOs, we explore how to combine training, technology, and employee engagement to build a strong security culture at your organization.



↳ Executive Summary

Security leaders unanimously agree that a strong security culture is important in maintaining a strong security posture.

And, when we asked how they'd rate their company's security culture, they gave themselves high marks, with 8.4/10 being the average across the US and the UK. But something doesn't add up.

According to our survey, 75% of organizations suffered a breach in the last 12 months, and employees aren't just disengaged; many have even had negative experiences with security awareness training

programs. Based on responses from security leaders and employees across industries and geos, as well as input from security awareness advocates, communications academics, and CISOs, we explore how to combine training, technology, and employee engagement to build a strong security culture at your organization.





99%

99% of security leaders say a strong security culture is important in maintaining a strong security posture

→ PAGE 8



3 in 4

3 out of 4 organizations say they experienced a security incident in the last 12 months

→ PAGE 10



1 in 3

Only 1 in 3 employees are satisfied with their IT/security department's communication

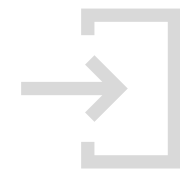
→ PAGE 27



45%

Nearly half (45%) of employees don't even know who to report security incidents to

→ PAGE 14



39%

Just 39% of security leaders say security teams play an important role in onboarding

→ PAGE 23



30%

30% of employees don't think they personally play a role in maintaining their company's cybersecurity

→ PAGE 13



Half

Half of employees say they've had a negative experience with a phishing simulation

→ PAGE 16



8.4

On average, organizations rate their security culture 8.4 out of 10

→ PAGE 2



CONTENTS

PART ONE What is a **Security Culture**, and Why Does it Matter?

PART TWO **Technology & Training**, Without Employee Engagement

PART THREE How Can You Make **Employees** Care?

PART ONE

What is a ■ Security Culture, and Why Does it Matter?

People often discuss the importance of a

**“STRONG SECURITY
CULTURE”**

...but what does that actually mean?

According to security leaders, it's:



"Knowing that data is safe, employees understand the importance of data protection and customers have confidence you take care of their sensitive information"



"How people communicate and adhere to policies"



"A feeling of security and safety that enables staff to work and gain trust from our customers"



"Awareness of security risks and techniques that may be used to jeopardize our company"



"Clear policy. Prompt timeline in responding. Risk reduction"



"Good employee understanding of threats and safeguarding of information"



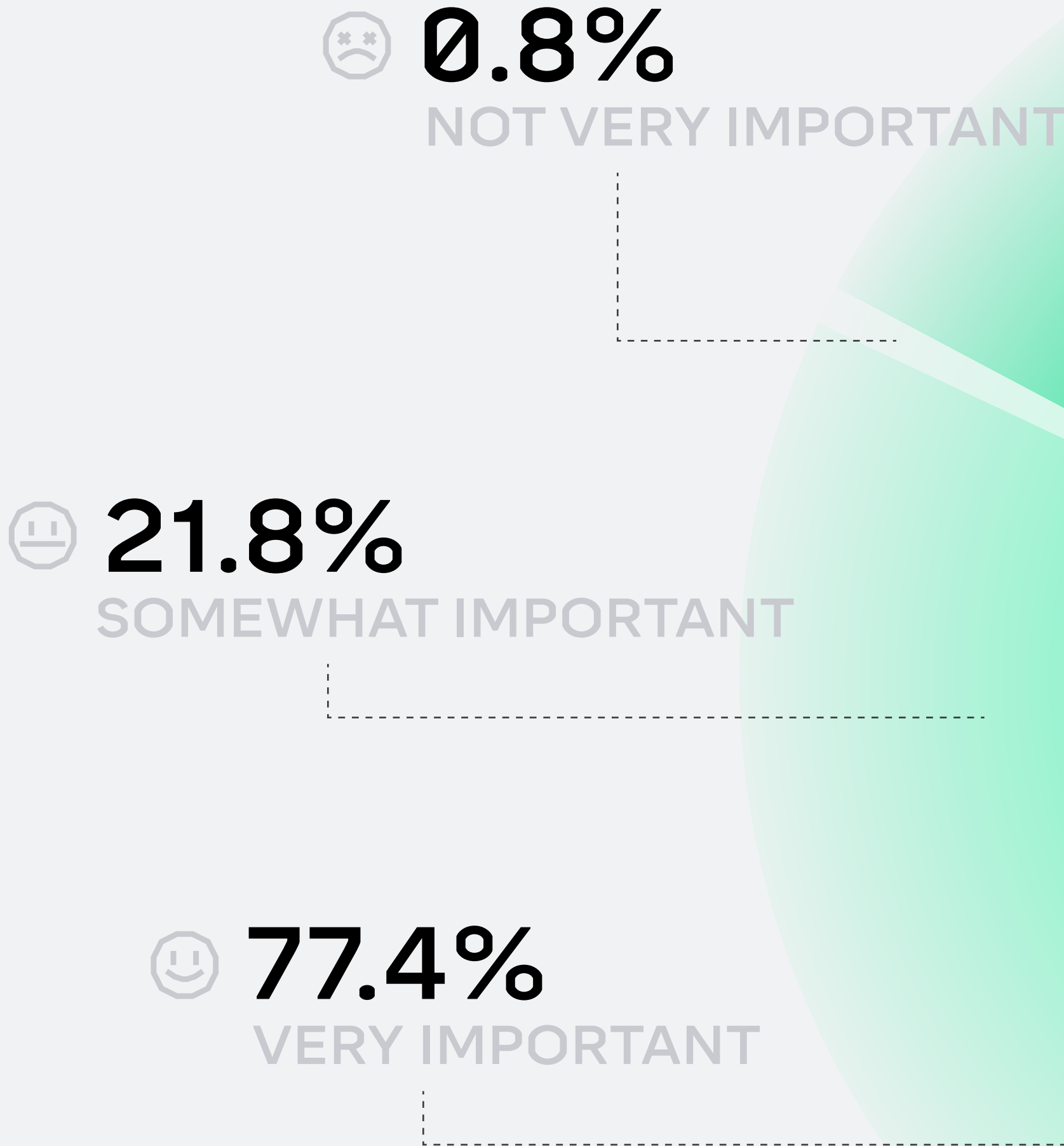
"Caution by staff and great preventative systems"



While the exact definition may vary, security leaders can agree on one thing:

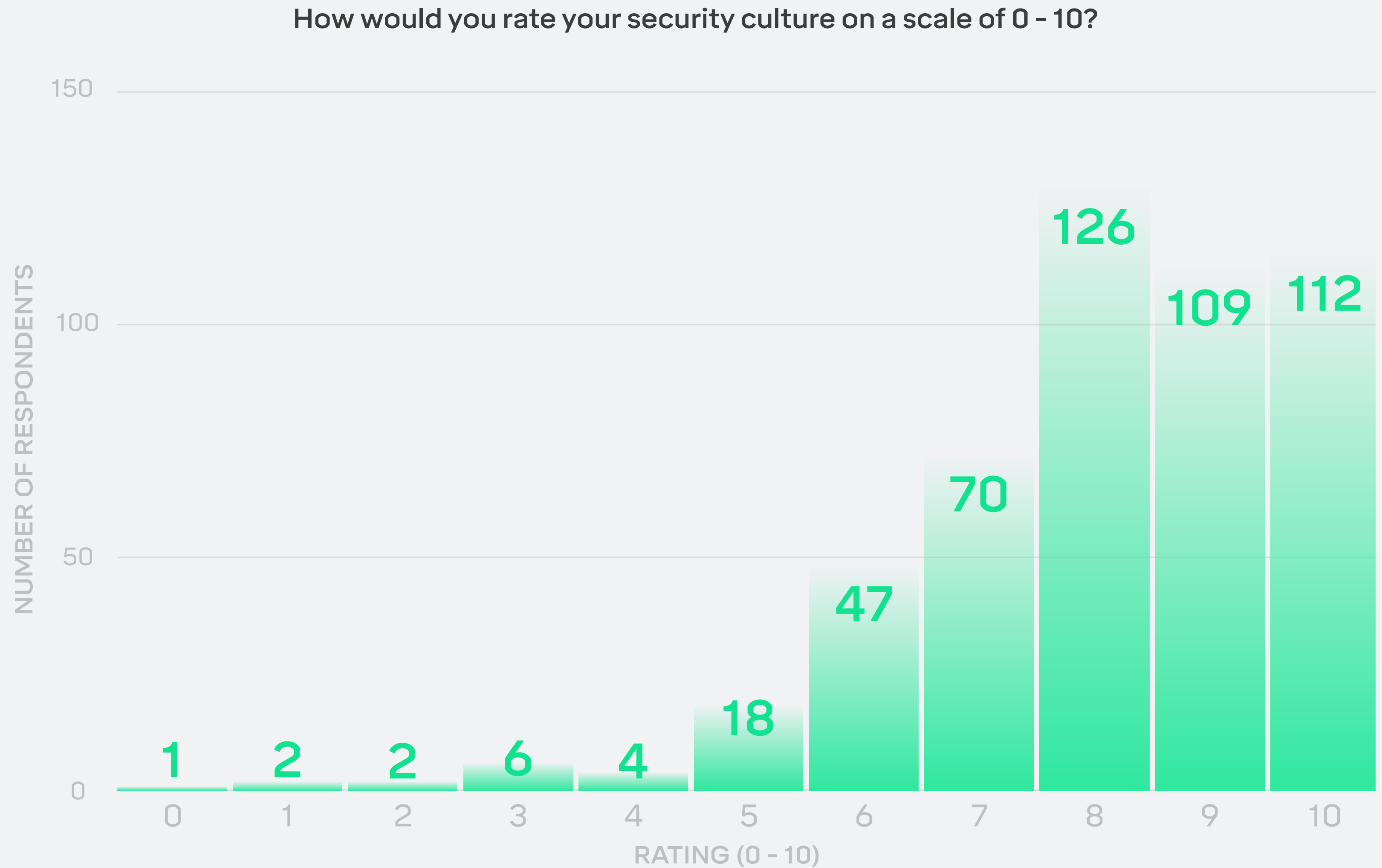
security culture is important.

According to 99% of security leaders in the US and the UK, a strong security culture is important or very important in maintaining a strong security posture, and benefits include: customer confidence, greater trust between employees and IT, less burden on IT/security teams, and more investment in security.



How important is security culture in maintaining a strong security posture in the workplace?

With so much riding on a strong security culture, it's no wonder it's a top priority for security teams who, on average, rate their company's security culture 😊 8.04 out of 10. Not bad...



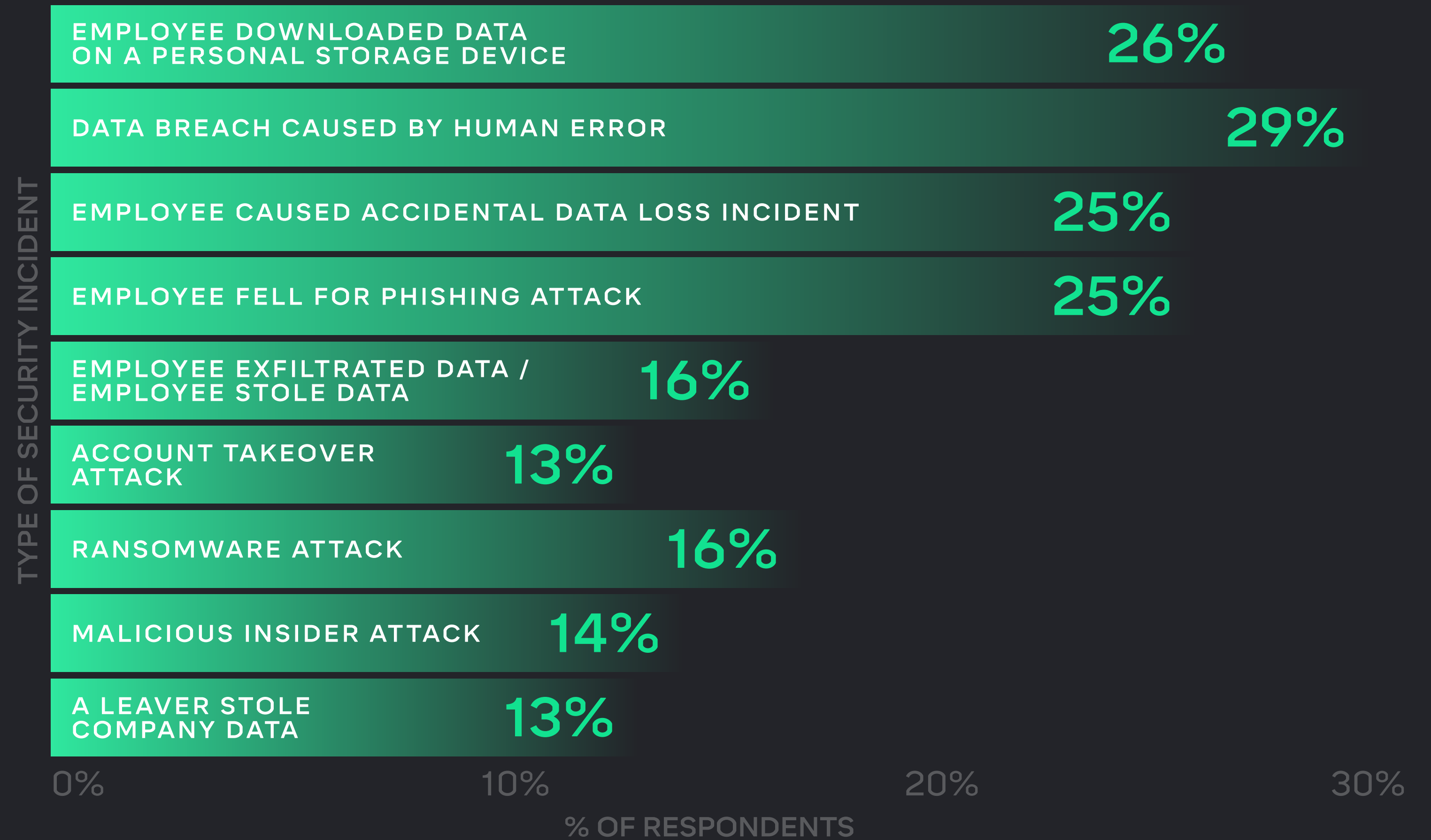
Total sample; Unweighted; base n = 250

But something doesn't add up.

According to security leaders, the #1 benefit of a strong security culture is fewer security incidents. Seems like a no-brainer, right? We would expect to see the likelihood of a breach decrease as security cultures become more mature.

Why, then, do 3 out of 4 organizations say they experienced a security incident in the last 12 months? And why do security leaders report breaches caused by or involving human error more than any other type of incident? Part of the problem is that employees aren't engaged.

Which of the following security incidents has your organization experienced in the last 12 months?



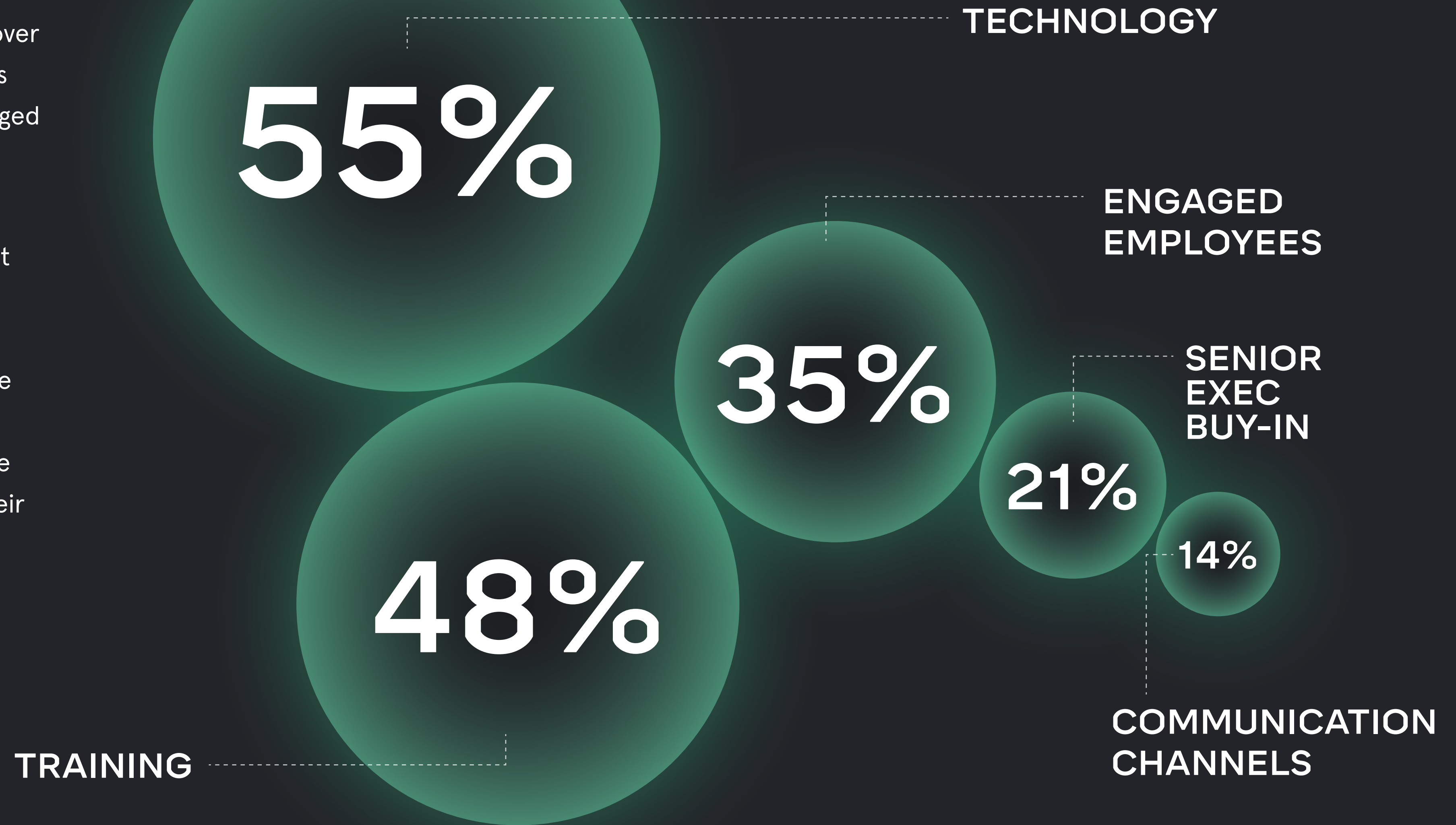
PART TWO

● Technology & Training, Without Employee Engagement

When asked what has the most influence over a positive security culture, security leaders favored technology and training over engaged employees, communication channels, and senior exec buy-in.

But training without employee engagement is little more than a tick-box exercise.

Technology and policies related to cybersecurity are ineffective unless they're clearly communicated. And more junior employees are only going to care about the company's security posture as much as their managers do.

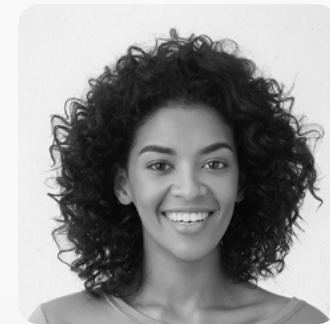


What do you think would have the most influence in your company in building a positive security culture?

The good news is, because security leaders are prioritizing training, 😊 **85%** of employees in the US and UK participate in security awareness programs

The bad news is, just 😞 **36%** of them say they're fully paying attention.

And while half (50%) do say it's helpful, only 28% say it's engaging. 36% say it's out-right boring. Perhaps that's why 1 in 3 employees don't even understand why cybersecurity is important, and nearly 30% don't think they personally play a role in maintaining their company's cybersecurity.



50%

"SECURITY AWARENESS TRAINING IS 🙌 **HELPFUL**"

"SECURITY AWARENESS TRAINING IS 😞 **BORING**"



36%



25%

"SECURITY AWARENESS TRAINING IS 🧑 **ENGAGING**"

This is especially problematic because, as we all know, cybersecurity is a team sport. The burden sits with everyone, across all levels and departments, from the Chief Finance Officer to a recently hired sales engineer. But only half (58%) of employees think senior execs at their company value cybersecurity. So much for top-down leadership...

And when it comes to communication, there's a clear disconnect between what security teams think they're delivering, and what employees are actually absorbing, especially in the US. 80% of security leaders say there's a feedback loop for employees to report security incidents. Meanwhile, nearly half (45%) of employees don't even know who to report security incidents to.

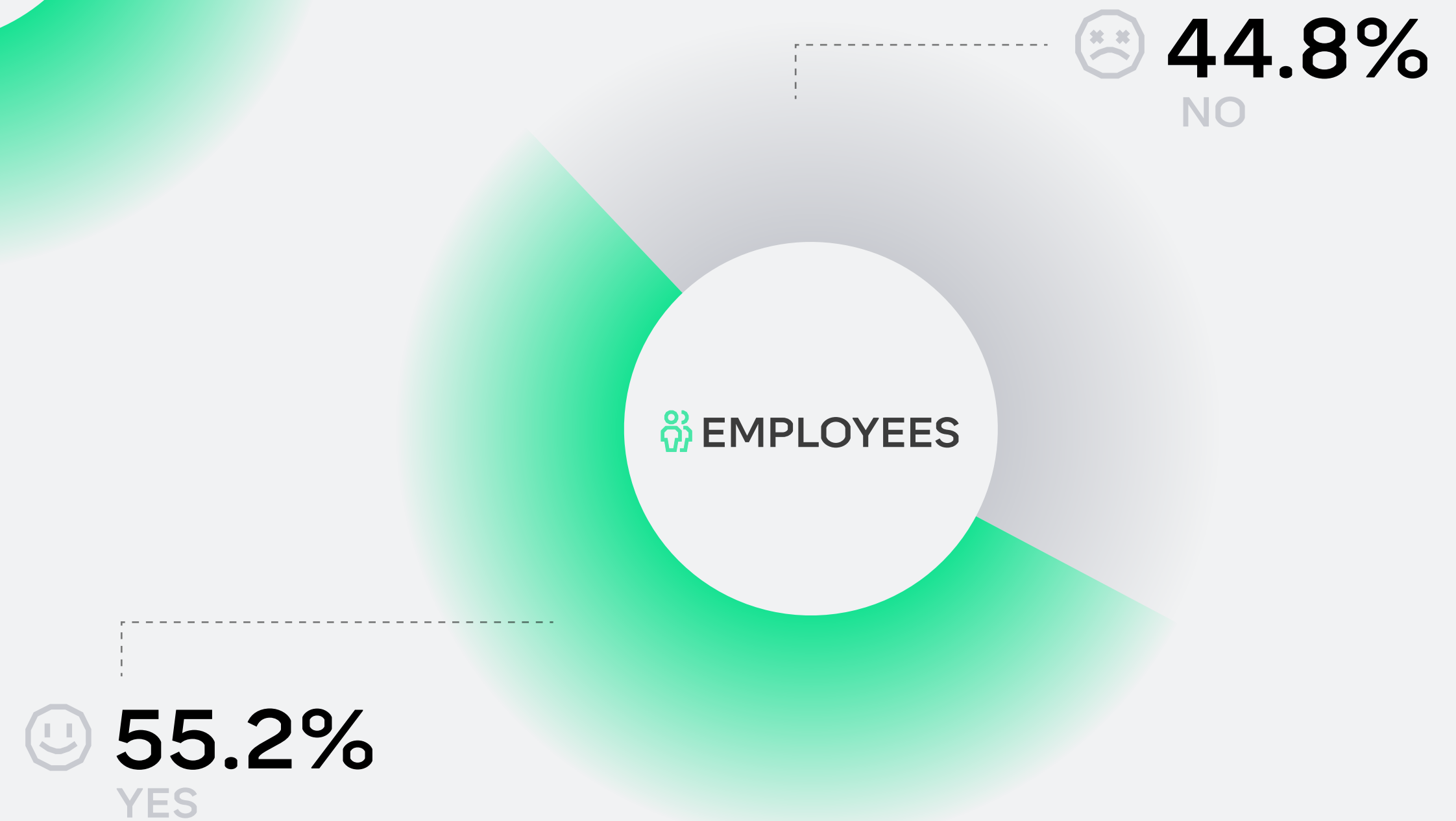
🧠 SECURITY LEADERS:

Is there a feedback loop for employees when it comes to reporting security incidents? (🇺🇸 US only)



👥 EMPLOYEES:

Do you know how to report cybersecurity incidents at your workplace? (🇺🇸 US only)



■ FEAR,
UNCERTAINTY,
AND DOUBT (FUD)
DOESN'T WORK

In some cases, employees aren't just unengaged or disinterested.

They're actually  turned off.

1 in 2 employees say they've had a negative experience with a phishing simulation. We've seen plenty of examples of phishing tests backfiring in the real-world, most often because they lean more towards punishment than positive reinforcement, and use questionable tactics like offering perks or bonuses to encourage employees to click.

This degrades trust, and according to Dr. Karen Renaud, Chancellor's Fellow at the University of Strathclyde, and Dr. Marc Dupuis, Assistant Professor at the University of Washington Bothell, can cripple employees' decision making, creative thought processes, and the speed and agility businesses need to operate in today's demanding world.

Fear Isn't The
Motivator
We Think It Is...

Business Management

Phishing Tests Are Necessary. But They Don't Need to Be Evil.

by Ryan Wright and Jason Bennett Thatcher

How a Phishing Awareness Test Went Very Wrong

Tribune Publishing Co. Employees Outraged at Phishing Test Teasing a Bonus

GoDaddy: Sorry We Promised Holiday Bonuses, That Was Just a Phishing Test

HOME > TRANSPORTATION

A company told about 2,500 employees they were getting a bonus during COVID-19 — but it was just a phishing test

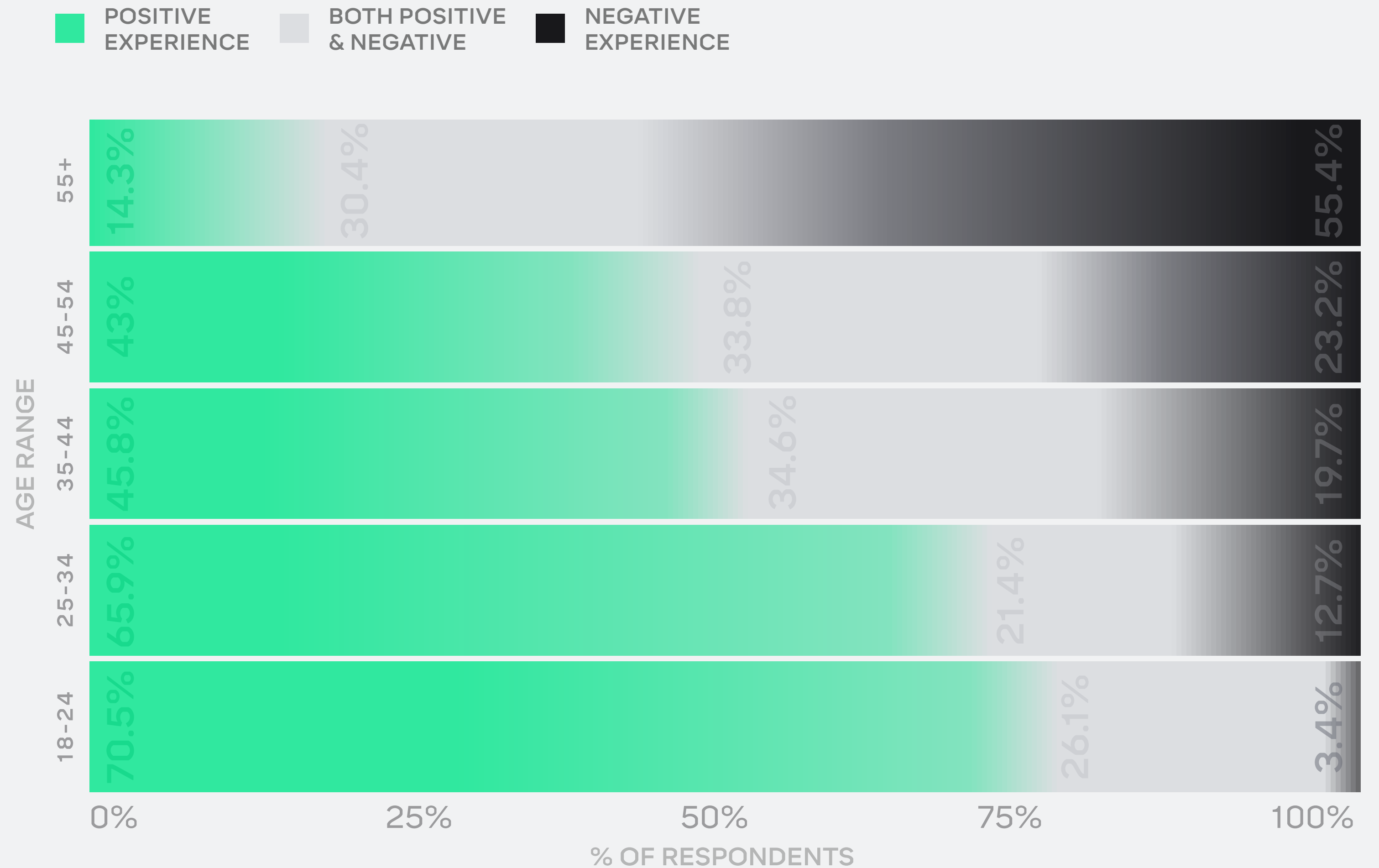
Brittany Chang May 11, 2021, 6:24 PM



Interestingly, the youngest generation is almost three times as likely to say they've had a 😞 negative experience with phishing simulations compared to the oldest generation.

But this difference in attitudes based on age isn't an anomaly. Across our survey data, we see that the older employees are, the more likely they are to understand and care about their role in maintaining their company's security culture.

Have you had a negative experience with a phishing simulation/test at work? (by age range)



A GENERATIONAL → DIVIDE

Over half (54%) of respondents 55+ care about cybersecurity at work “a great deal” compared to just 15% of 18-24 year olds.

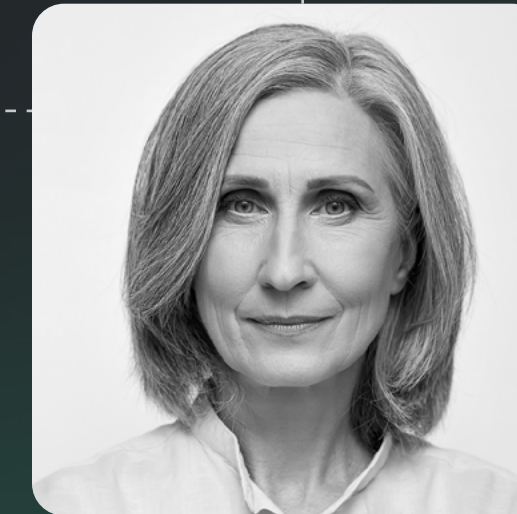
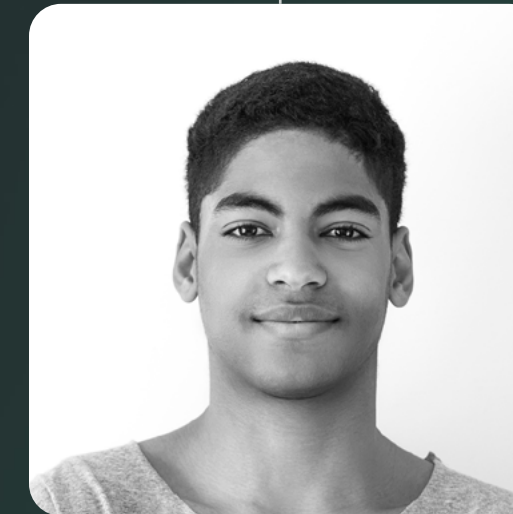
That explains why older employees are 4x more likely to have a clear understanding of their company’s cybersecurity policies compared to their younger counterparts, and 5x more likely to follow those policies.

54%

care about cybersecurity at work “a great deal”

15%

care about cybersecurity at work “a great deal”



5x

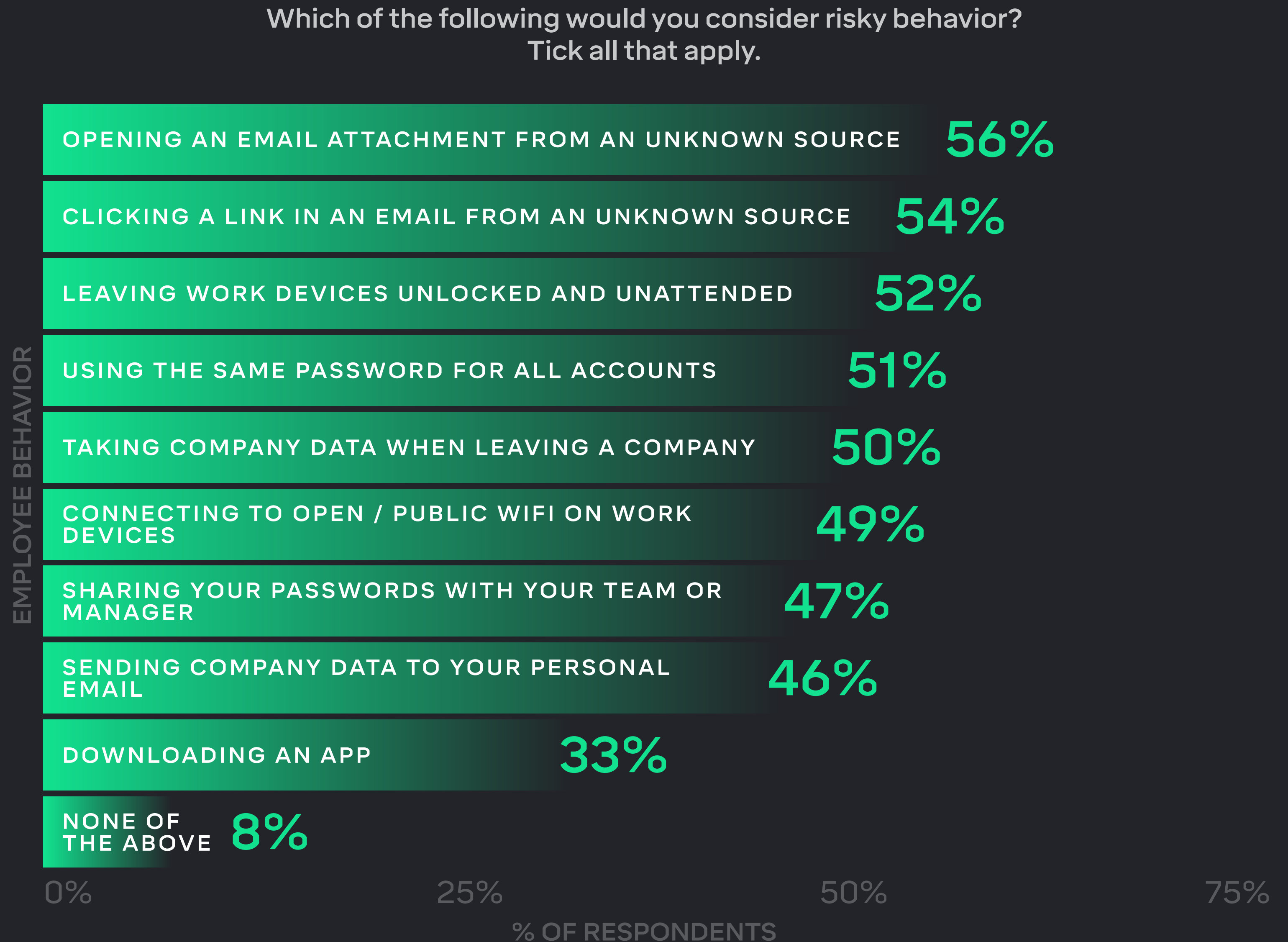
5x more likely to follow cybersecurity policies

4x

4x more likely to have a clear understanding of their company’s cybersecurity policies

It goes without saying these attitudes and beliefs about cybersecurity influence behavior. And while the vast majority of security respondents – regardless of age – see nothing wrong with re-using passwords, taking company data, leaving work devices unattended, or opening email attachments from unknown sources...younger employees are the least likely to see anything wrong with these unsafe practices.

But each of these actions leave employees and the organizations they work for vulnerable. This is made worse by the fact that only 39% of employees say they're very likely to report a security incident, making investigation and remediation even more challenging and time-consuming for security teams. When asked why, almost half (42%) of employees said it's because they wouldn't know if they had caused an incident in the first place. 1 out of 4 said they just don't care enough about cybersecurity to mention it.



Which of the following would you consider risky behavior? Tick all that apply. (US/UK)

US

UK

18-24 25-34 35-44 45-54 55+

50%

25%

0%

0%

25%

50%

75%

Opening an email attachment from an unknown source

Connecting to open / public WiFi on work devices

Clicking a link in an email from an unknown source

Leaving work devices unlocked and unattended

Using the same password for all accounts

Sharing your passwords with your team or manager

Taking company data when leaving a company

Sending company data to your personal email

Downloading an app

None of the above

This begs the question:



How can  **security leaders** more effectively communicate the importance of cybersecurity, and encourage all employees to take an active role in maintaining their company's security posture?

PART THREE

How can you make ● employees care?

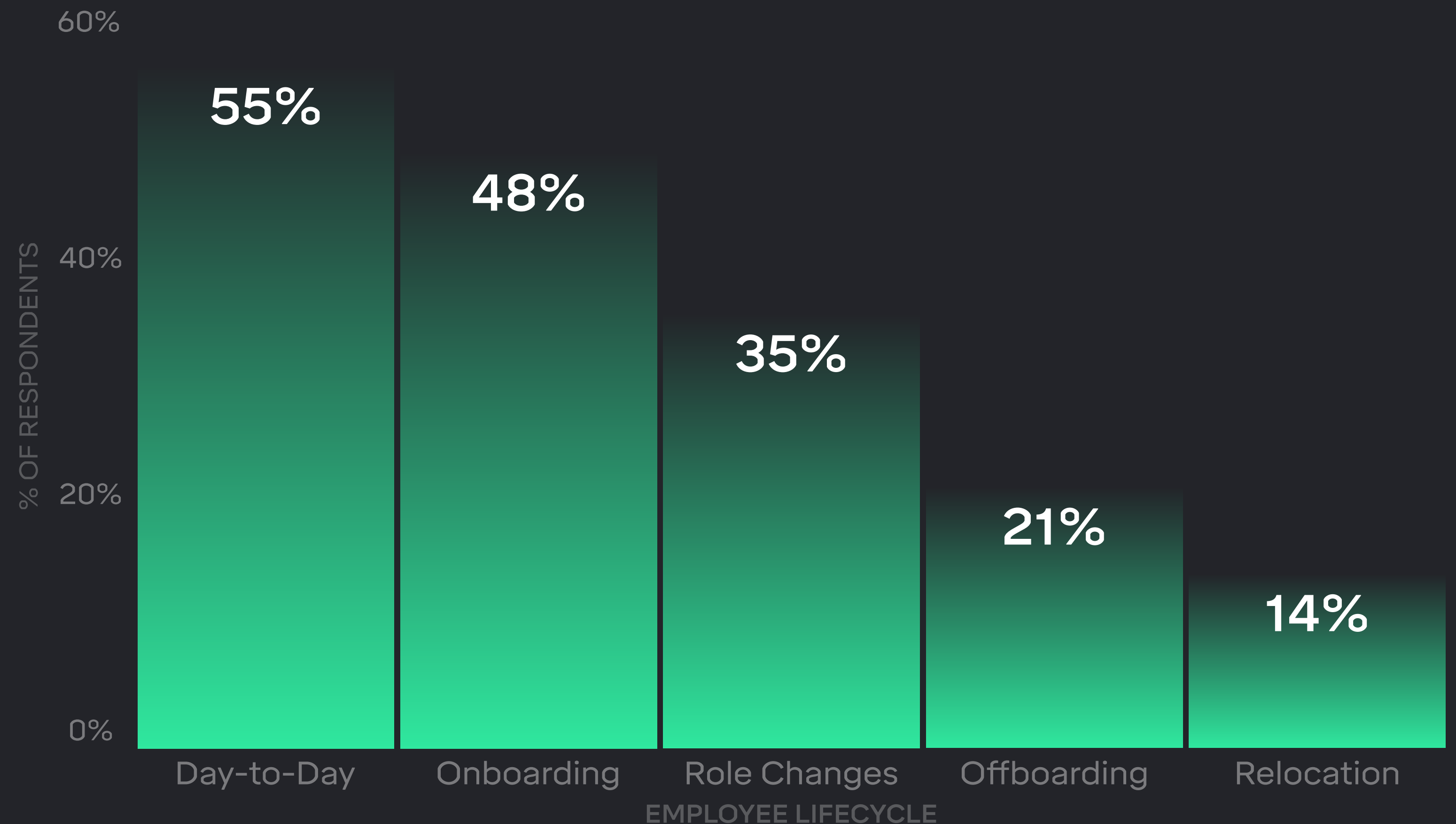
Like most things related to cybersecurity, there is no silver bullet when it comes to employee engagement. But touch points throughout the employee lifecycle, clear communication, and technology that helps build self-efficacy are all good places to start. Let's tackle these one at a time...

Touchpoints throughout the employee lifecycle

In order to foster and maintain a risk-aware workforce, security teams should play an active role in onboarding, offboarding, and day-to-day. This is especially important now, with remote and hybrid set-ups being the norm. But, according to our research, security leaders underestimate just how much they should be a part of the employee experience. When asked which parts of the employee lifecycle are most important for a security team to be involved in, just 39% said onboarding, and only 1 in 5 said offboarding.

While – yes – ongoing training is essential, onboarding represents a huge opportunity to introduce eager and attentive employees to your company’s cybersecurity policies and procedures. And a thoughtful, comprehensive, and closely monitored offboarding process can help prevent data exfiltration attempts (both negligent and malicious).

Which part(s) of the employee lifecycle are most important for a security team to be involved in?



↳ DID YOU KNOW?

45%

45% of IT leaders say incidents of data exfiltration have increased in the last year, as people took data when they left their jobs

↳ FIND OUT MORE

1 2 3

3 DAYS

It takes up to three days for security and risk management teams to detect and remediate a data loss and exfiltration incident caused by a malicious insider on email


↳ FIND OUT MORE




1 IN 3

One in three employees admit to having taken data with them when they quit

↳ FIND OUT MORE

 **James McQuiggan,**
Security Awareness
Advocate at KnowBe4
offers some tips for
→ onboarding:

- 1 **Work closely with the HR department to coordinate the set-up or delivery of employees' new work machines and accessories on time. This will prevent employees from ever logging into the company network on their personal devices**
- 2 **Because in-person inductions have been replaced with online training, it's essential that training presentations (whether related to data privacy or company policies) are interactive**
- 3 **New users should receive their first phishing assessment within a few weeks of starting. This is especially important because new starters are prime targets for bad actors.**
- 4 **Keep employees engaged with daily "special events" as a part of the onboarding process. For example, virtual trivia based on GDPR requirements, or a Q&A with the CISO.**
- 5 **At the very least, make sure new joiners know who to contact with questions, and understand the importance of reporting incidents (including near-misses). This will help build trust and transparency early on, which is key to a strong security culture.**

 **Josh Yavor,**
CISO at Tessian, offers
some tips for
↳ offboarding:

1

Give people an approved and secure way to get personal documents (like family photos or tax documents) off their work laptop ahead of offboarding

2

Communicate offboarding expectations and needs with both the employee and their manager

3

Ensure that offboarding from core and critical systems happens as soon as possible

4

Have a plan in place for how you'll address any post-employment data requests from former employees

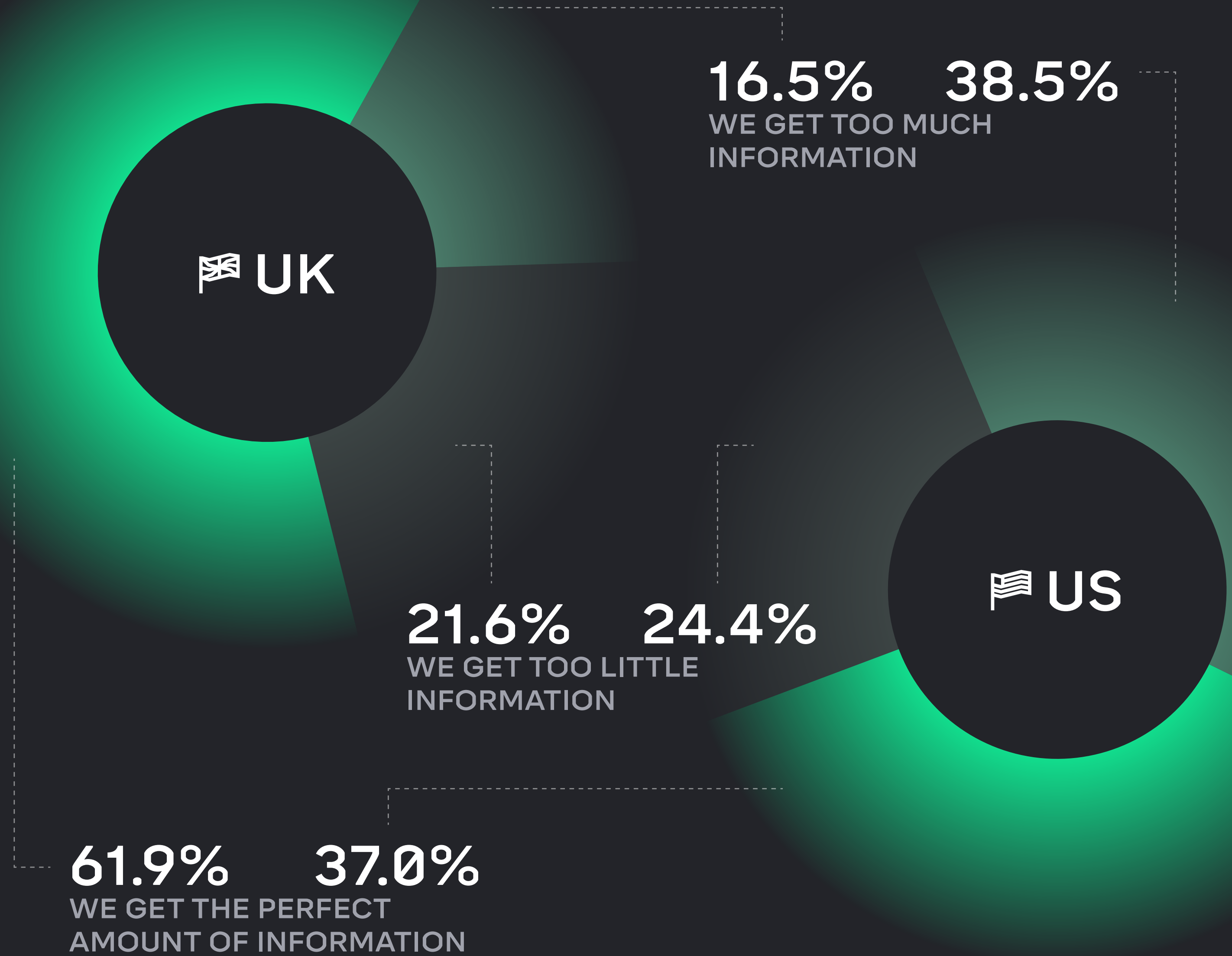
5

Ensure that all critical systems have audit logs to enable you to identify any mistakes, or malicious activity, that may occur leading up to an employee's last day



Clear Communication

Because every organizational function is impacted by security, its imperative policies, procedures, risks, and relevant news are regularly and universally communicated. This helps drive awareness, encourage engagement, and improve the success of security programs. But this is all easier said than done. Security teams have to consider how much information they share, who it comes from, via what channels, and how frequently.

According to employees, IT/security teams in the UK are on the right track, with 62% saying they get the perfect amount of information. But those in the US have some work to do, with 39% of employees saying they get too much information, and 24% saying they get too little. That leaves just 1 in 3 employees satisfied with the communication they receive from their IT/security department.



How would you describe communication with your IT/security team?

Security leaders and academics like  Kai Roer,  Lola Obamehinti, and  Jeff Hancock offered advice on our podcast:

1

To communicate effectively, you have to speak the same language as employees. That means stripping out the jargon, technical terms, and acronyms, and only providing need-to-know information.

2

Tailor comms to specific people, teams, or departments to help everyone understand threats, consequences, and solutions. Data, real-world examples, and specific “what-if” scenarios can help you paint a clear picture.

3

Security teams should identify one person to deliver updates or make requests and be the point of contact for all questions

4

Develop a consistent format and cadence (for example, a monthly bulletin) to streamline communication and ensure employees have a source of truth to reference



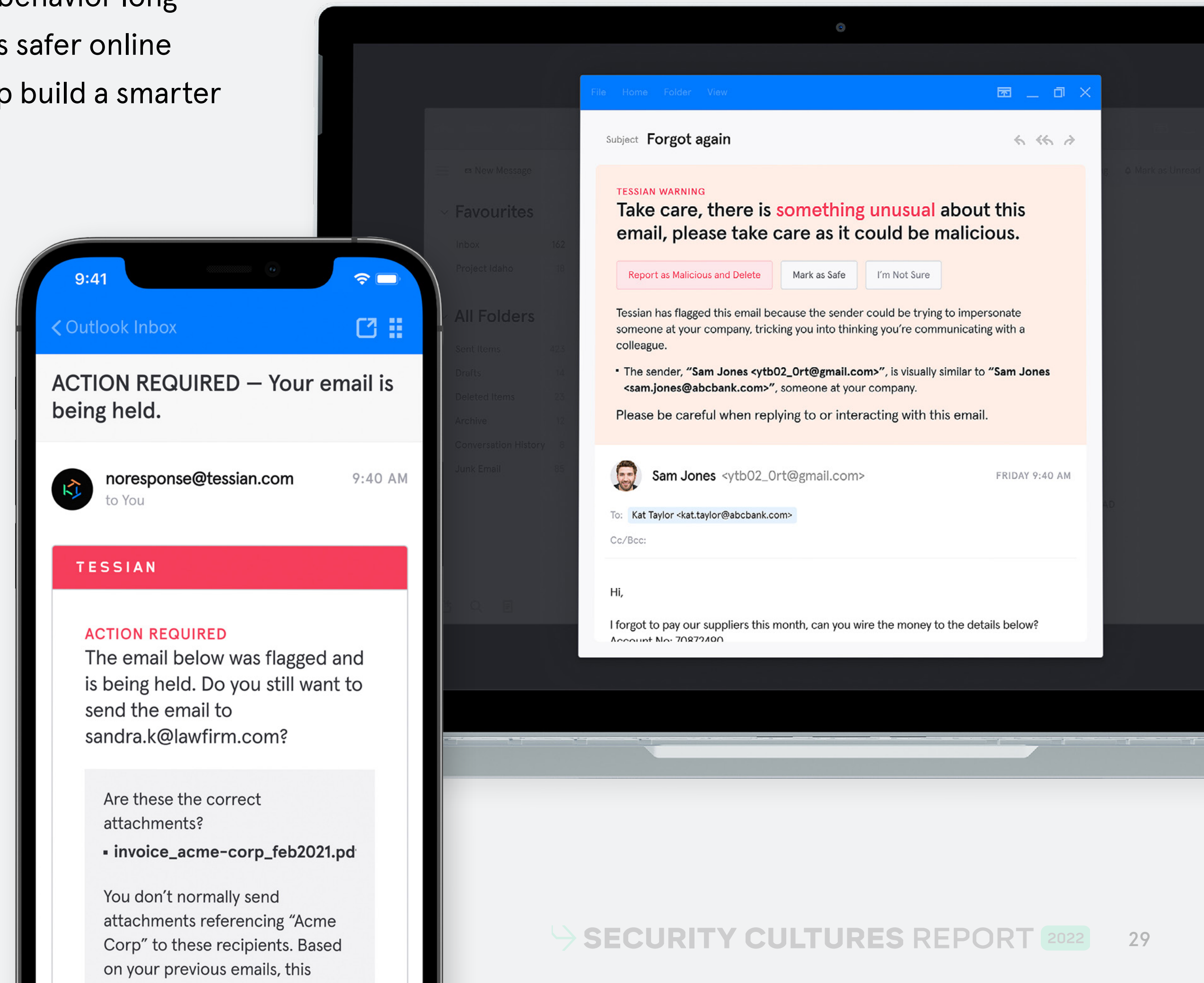
Technology that helps build self-efficacy

Monthly phishing simulations can help employees spot inbound attacks. Quarterly training sessions can help reinforce existing policies and procedures around data handling and password hygiene. And introducing new joiners to the cybersecurity team during onboarding is a great way to build a positive security culture. But as we've seen, despite all of this, employees still get phished, still ignore or workaround cybersecurity policies, and still mishandle data. That's why security leaders have to find ways to consistently educate their people.

In-the-moment warnings can help.

When Tessian detects a threat, employees see a warning message. It's written in plain English, and offers context around why the email was flagged.

These in-the-moment warnings do more than just prevent threats in real-time. They help change employees' security behavior long-term, coaching them towards safer online behavior, and as a result, help build a smarter security culture.



Tessian customers have seen click-through-rate on phishing simulations **drop below 1%** after deploying Tessian.

And, on average, customers see an **84% reduction** in data exfiltration.

“You have to train your users. You have to help them get better at spotting threats by helping them understand the threats. Tessian does that.”



Thierry Clerens
GLOBAL IT MANAGER AT SPG DRY COOLING

“Traditional training and awareness can only go so far. That’s where we look at technology solutions like Tessian to help us close the gap.”



Adam Jeffries
CIO AT JTC

“Tessian is a security product that’s about the people. It’s about engaging people and making security intrinsic to what they do, without getting in their way.”



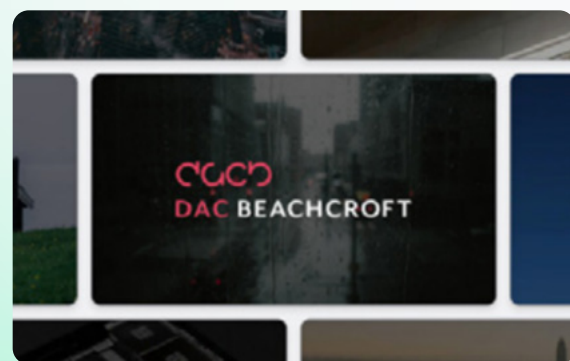
Mark Parr
GLOBAL INFOSEC MANAGER AT HFW

“Tessian explains the “why” which is very important for awareness. It also appears within the email itself versus employees having to click through a pop-up or link to view the warning. It’s impossible to ignore and easy to understand.”



Marie Measures
CTO AT SANNE GROUP

Don't Take It From Us. Hear It From Them.





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. Tessian's intelligent approach not only strengthens email security but also builds smarter security cultures in the modern enterprise.

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



Learn 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

[SUBSCRIBE →](#)

Methodology

Tessian commissioned OnePoll to survey 500 security leaders and 2,000 working professionals in the US and the UK. Survey respondents varied in age from 18-51+, and occupied various roles across departments, industries, and company sizes.

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 THE REPORT:

