



TESSIAN

Reclaiming Hours Lost to Cybersecurity Incidents

CISOs are overworked and missing important events in their personal lives due to work demands. How can technology help security teams claw back hours lost to security incidents?



A Lot of Love For the CISO.

CISOs are superheroes.

They defend against evil threats and crime, protect organizations, and keep employees safe. The overwhelming majority feel as though their work is appreciated and 66% of US and UK employees say they understand the role of the CISO.

But, like superheroes, CISOs need downtime. They have a life outside of work too, but the problem is: they aren't getting to spend as much time there as they'd like.

89%

OF CISOs BELIEVE THE WORK THEY
DO IS APPRECIATED BY EMPLOYEES
OUTSIDE THEIR TEAM

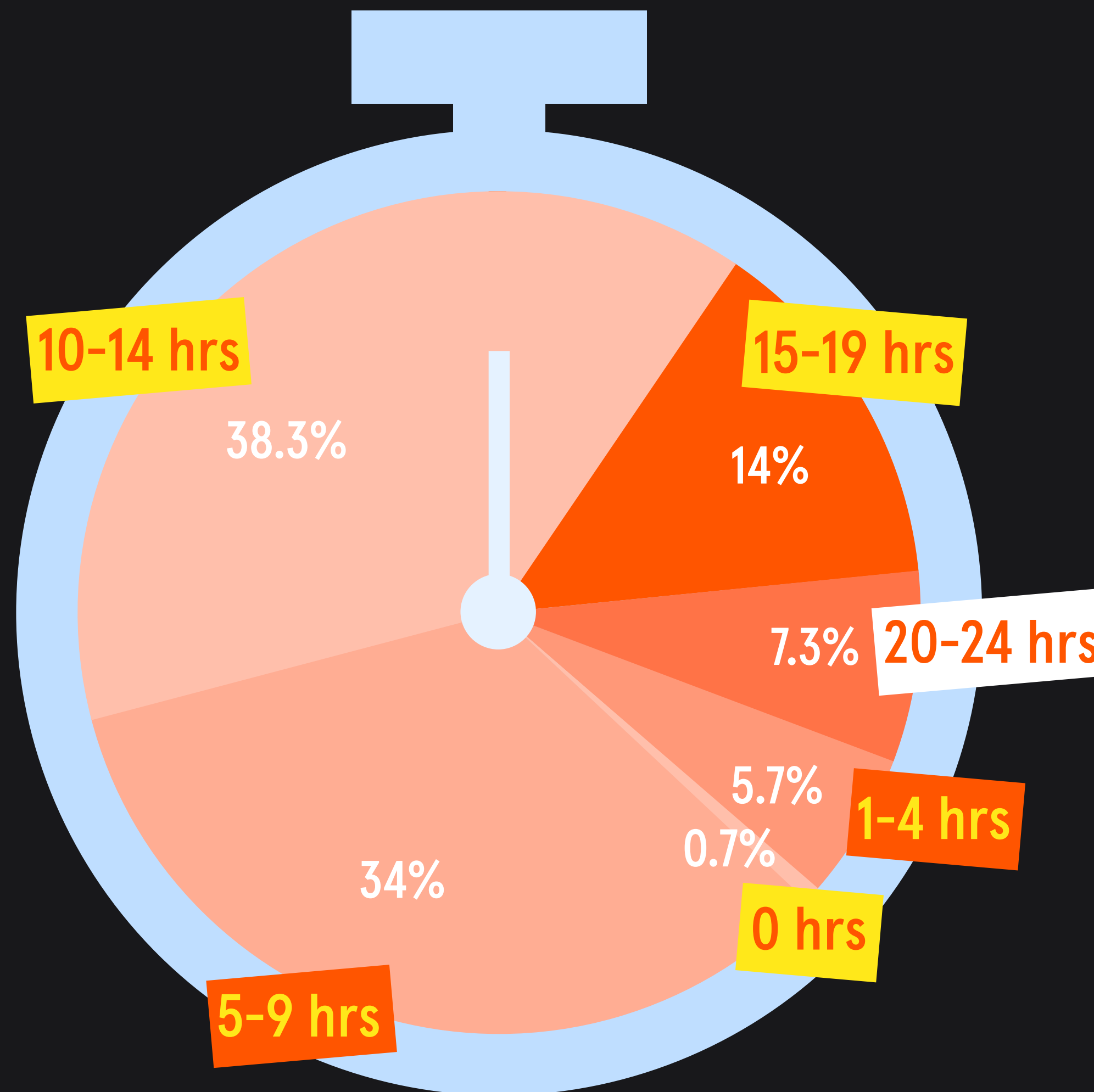
Work Hard, ~~Play~~ ~~Hard,~~ Work Harder

All CISOs we surveyed work beyond their contracted hours, with CISOs working, on average, 11 hours more than they're contracted to each week. Nearly 1 in 10 work 20-24 hours more a week.

And when they're home, they're still "on".

The majority of CISOs (59%) struggle to always switch off from work once the working day is over.

And when we asked respondents what they would do if their schedule was cleared for the day, 13% of respondents would dedicate their time to catching up on pending work or researching ways to improve business operations at their organization.



ON AVERAGE, HOW MANY HOURS DO YOU WORK BEYOND YOUR CONTRACTED HOURS PER WEEK?

CISO TAKE

“Security is hooked on heroics. We love the story of pulling all-nighters and heroes saving the day. But to avoid burnout, there needs to be a shift. Recognize that heroics are a failure condition.”

Josh Yavor, CISO at Tessian 🚀

OH SH*T!

HALF OF ORGANIZATIONS

EXPERIENCE AT LEAST 6 EMPLOYEE-RELATED EMAIL SECURITY INCIDENTS PER MONTH.



Resolving the “Oh Sh*t!” Moments Takes Time

We conducted a survey of 317 security risk managers with analyst house Forrester, which revealed that investigating and remediating threats caused by human error are taking up a significant amount of CISOs’ time.

[According to Forrester’s research](#), organizations spend up to 600 hours per month resolving employee-related email security incidents.

A quarter of respondents say they spend 9–12 hours investigating and remediating each threat caused by human error, while more than one in 10 spend more than a day investigating and remediating each threat caused by human error.

It’s no wonder 37% of CISOs we surveyed say they spend excessive time on triaging and investigation.

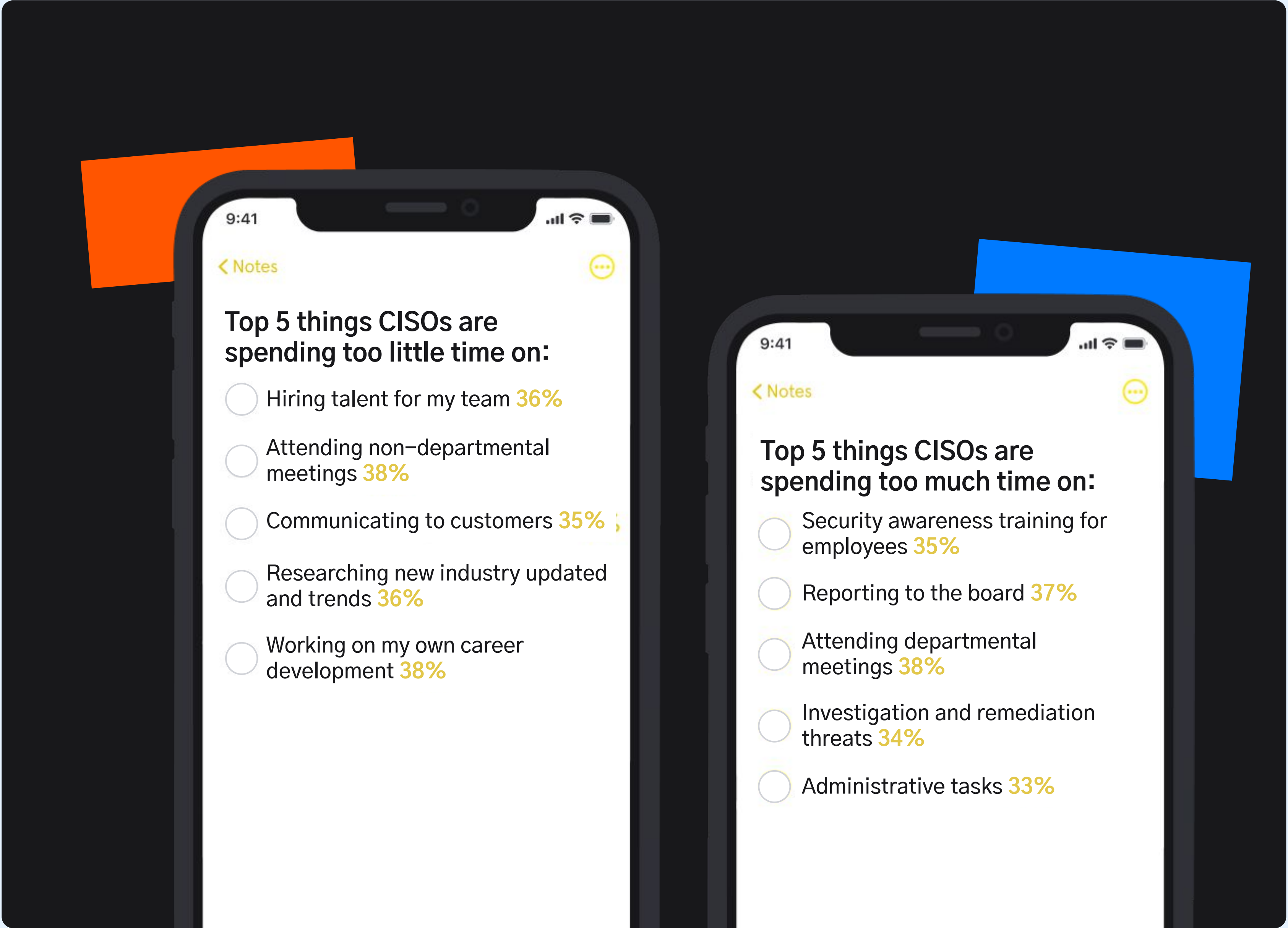


Download the full
Forrester report [here](#) →

What Else is Taking Up Time?

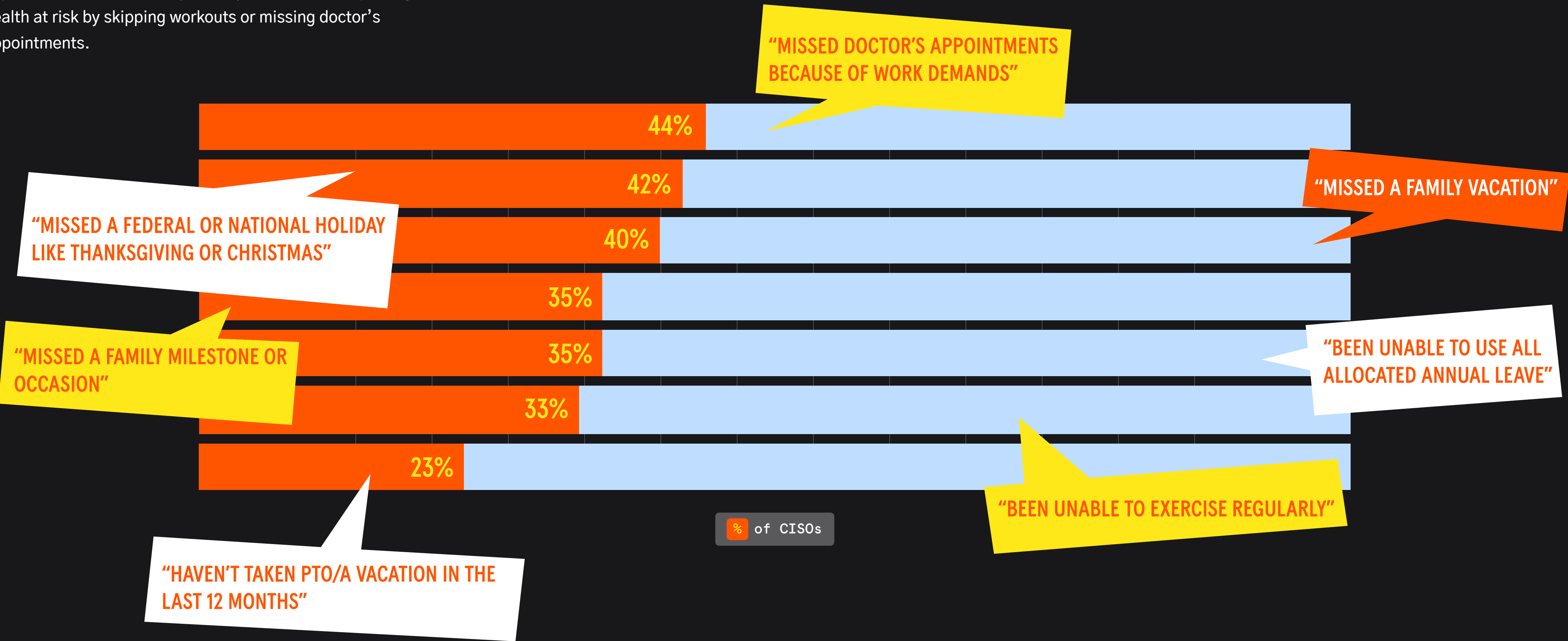
38% of CISOs believe they're spending too much time in departmental meetings and reporting to the board on cybersecurity. And a third (33%) also feel as though they are being drained of time because of administrative tasks.

Conversely, 38% said they are spending too little time on their own career development, attending non-departmental meetings to collaborate with other parts of the business, researching new trends in the industry and communicating with customers. They also feel as though they aren't spending enough time hiring new talent.



Work Demands Keep Play at Bay

As a result of their demanding day jobs, CISOs are missing out on important events and family holidays, and are even putting their health at risk by skipping workouts or missing doctor's appointments.



CISO TAKE

“As security leaders, we need to do a better job of communicating capacity constraints. I’m accountable for ensuring that my team is committed to reasonable expectations around delivery of work.”

Josh Yavor, CISO at Tessian 🚀

Reclaiming The Hours Lost to “Oh Sh*t!” Moments

It’s clear that CISOs love their jobs and are dedicated to their work. But they’re overworked.

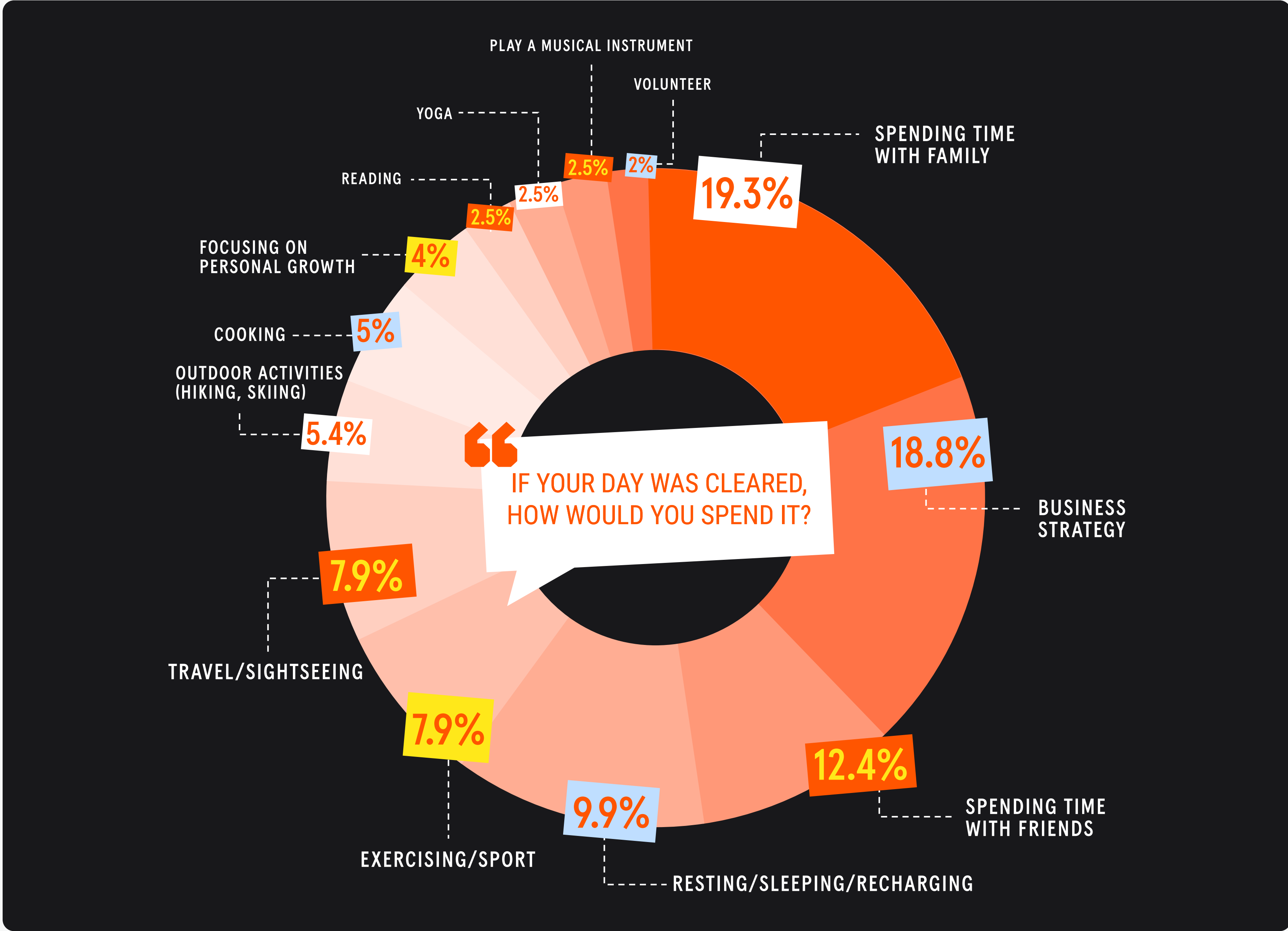
So how can they use technology to free up time?

Tessian data shows that by automating security to prevent security threats on email – like accidental data loss, data exfiltration, advanced spear phishing attacks – an enterprise with 1,000+ employees can get back **26,357 hours in a year.**

We asked CISOs what they would do with that time back and asked them to imagine what they would do if their schedules were cleared.

Some would be committed to driving *even more* business value for their organization. After spending time with their families, tasks related to bettering business strategies or finding ways to benefit their organization were top of mind.

And 10% would spend it resting or sleeping...we don’t blame you!



“I WOULD LIKE TO WORK ON MY
FUTURE GOALS”

“I WOULD DO ALL MY
PENDING WORK”

“I’D REST AND RELAX, MAYBE
PLAY A LITTLE GOLF!”

“I WOULD SPEND THE DAY IN MY GARDEN
PAINTING”

“I JUST WANT TO REST”


“I WOULD TRY MY BEST AND FIND
SOMETHING INNOVATIVE TO BENEFIT
MY COMPANY”

“I WOULD SPEND TIME WITH
MY CHILDREN”

“I’D HAVE MY BREAKFAST, LUNCH AND
DINNER WITH MY FAMILY”

“I WOULD SPEND MY FREE TIME
WITH MY FAMILY”

“I WOULD LIKE TO FOCUS
ON MY PERSONAL GROWTH”

A collage of various family photographs, including parents with children, a man holding a baby, and a family walking, all in a light blue, semi-transparent overlay.

Did you know that organizations with over 1,000 employees could save as many as **26,357** hours a year by automating security?

Want to find out how your security teams and employees can reclaim the lost hours? Get in touch with the Tessian team today to learn how Human Layer Security can help stop “Oh Sh*t!” moments from clogging up your schedule.

GET IN TOUCH →



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

Methodology

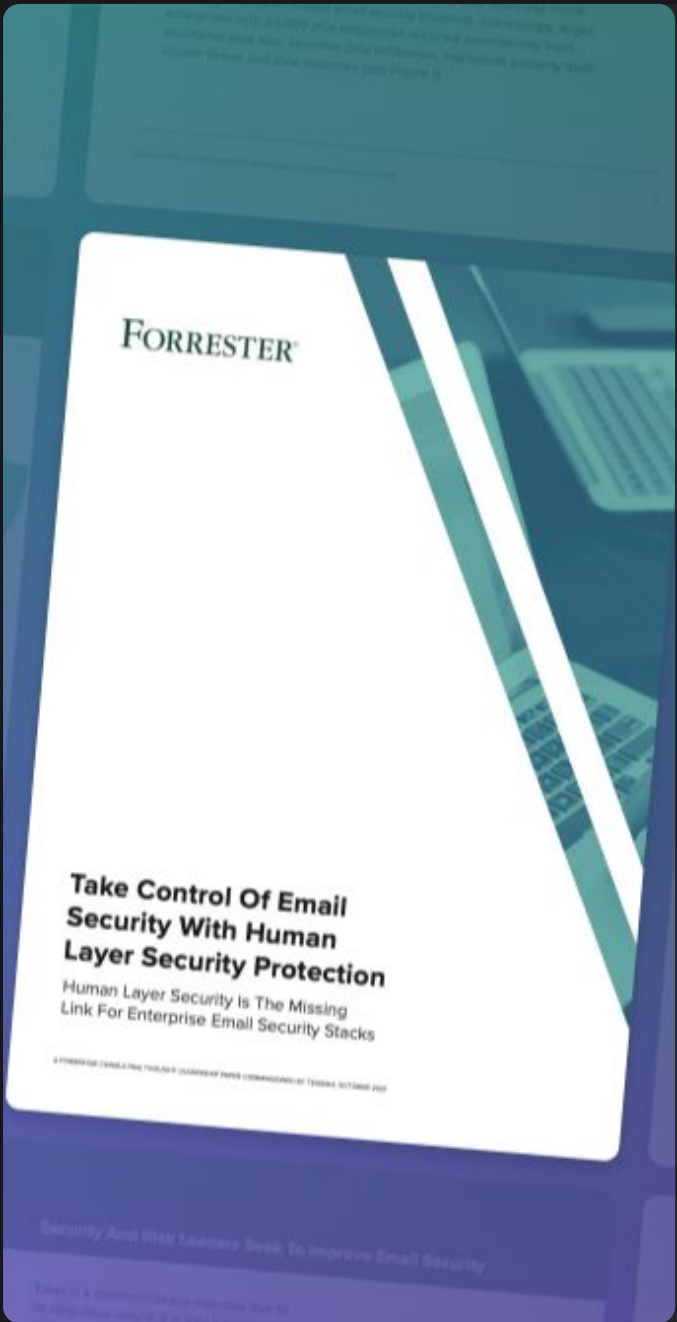
This report is based on survey findings from 300 CISOs in UK and US organizations. The poll was conducted by Censuswide in September 2021.



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 →



Download our Forrester Report:

Understand why Human Layer Security solutions are necessary to achieve the full value of your existing security tech stacks and to also empower employees to be your best security asset.

DOWNLOAD NOW →

Share this report



TESSIAN.COM/RESEARCH →