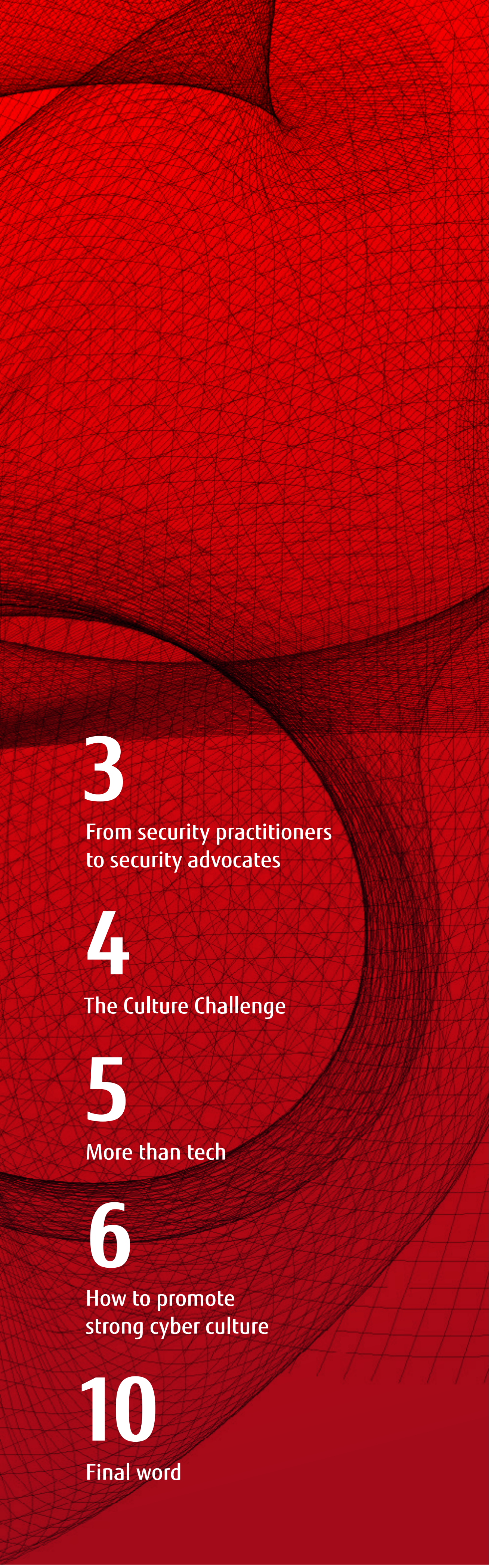
Building a Cyber Smart Culture

FUJITSU



3 From security practitioners to security advocates

4 The Culture Challenge

5 More than tech

6 How to promote strong cyber culture

10 Final word

Building a Cyber Smart Culture

Why and how leaders should prioritize stronger cyber security behaviors and mindsets

Many of the most worrying cyber security vulnerabilities involve human negligence or ignorance. This is not a new problem, but the Covid-19 pandemic has placed new emphasis on individuals and cyber secure behaviors. In the space of just a few months, workplace trends leapt forward several years, transforming much of the cyber security threat landscape. Industries have been forced to confront the security challenges of widespread remote working and a society that increasingly functions online.

This means that cyber secure behaviors need to become second nature to people across the workforce spectrum. What can organizations do to encourage this?

All results come from a research by
Longitude / Financial Times sponsored by Fujitsu

The strength of an organization’s cyber security culture is in the behaviors of every individual

From security practitioners to security advocates

We all think of cyber security as being about security frameworks and systems overseen by IT teams, but there is a lot more to it than that: an organizational culture that does not support those systems will undermine their defensive power.

A culture of cyber security includes the collective knowledge, habits and values shared by a workforce on all things digital safety. The strength of an organization’s cyber security culture is in the behaviors of every individual – from the C-suite and finance teams to HR departments and engineers – and depends on each person knowing their role and supporting the combined effort. Understanding this is more critical than ever to organizations’ future resilience.

Too few organizations fully appreciate and implement a strong cyber culture. For too long there has been a disconnect between the IT suite, which is formed of chief information security officers and other technicians, and everyone else. How do businesses bridge that understanding gap? By putting the development of a “cyber smart” culture at the top of their agendas and getting every individual to become a security advocate.

We conducted a survey of 331 senior executives from various roles at organizations in 14 countries to find out whether they recognize the challenge – and what might be stopping them from pursuing a cyber smart culture. The respondents came from five broad industry groups: financial services, retail, manufacturing (including automotive), energy (including utilities), and central/federal government.

Below we present insights from this research, identifying the key challenges ahead for organizations looking to build a strong cyber security culture, and we provide you with some strategies that can help to embed cyber secure behaviors into the day-to-day activities of every employee.

The Culture Challenge

A striking 54% of respondents to our survey admit that in the past year they have bypassed security policies to keep pace with the changes taking place across their divisions as a consequence of the pandemic.

This suggests that many organizations have been more exposed to vulnerabilities this year. It could also mean that many previous processes were overly restrictive, preventing quicker deployment and hampering organizational agility. Either way, this result reinforces the need to solve long-standing issues.

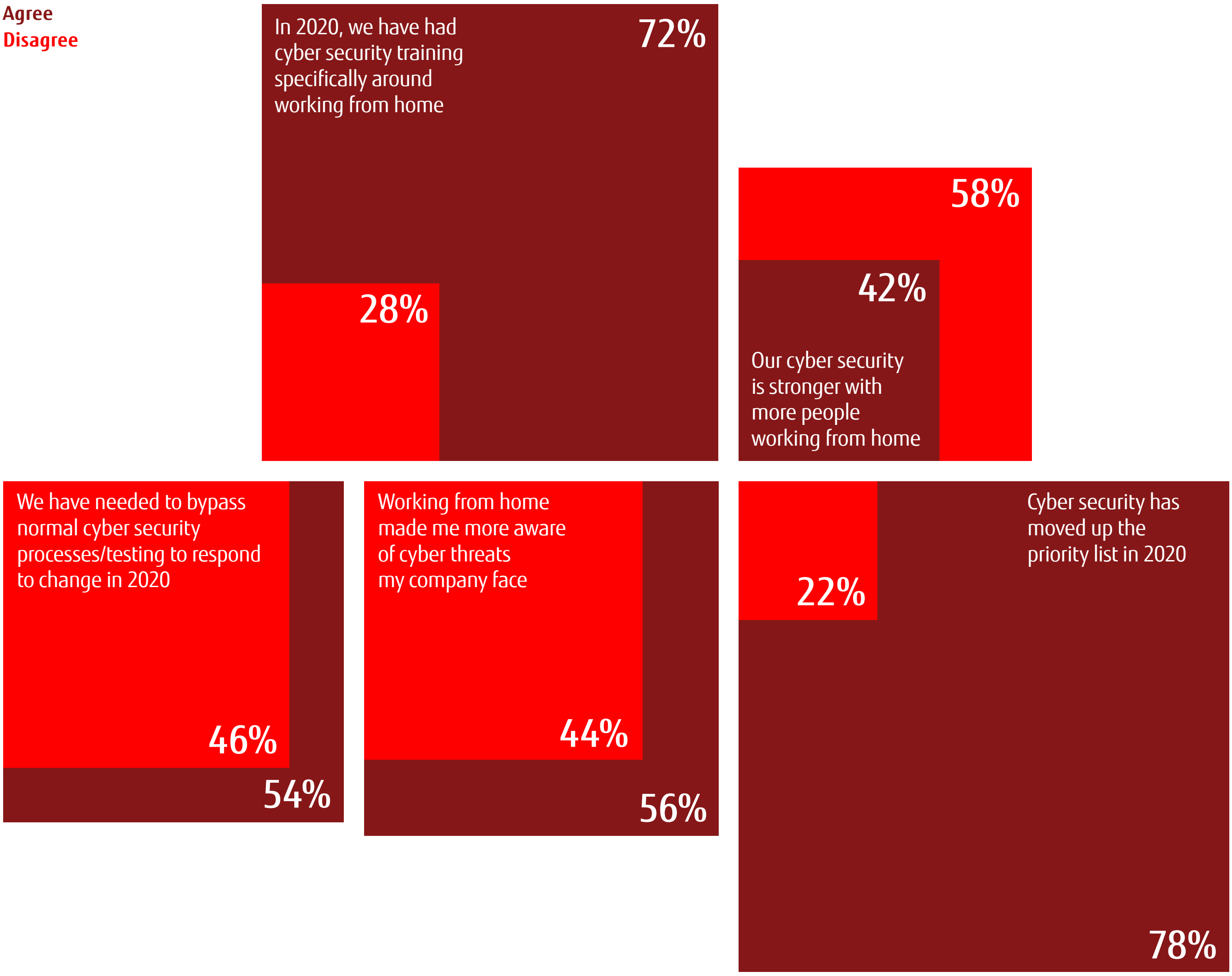
One of the problems that is stopping a change in culture is lack of clarity among employees about who is responsible for cyber security. More than four in 10 people in our survey (45%) believe that most people in their organization think cyber security has nothing to do with them. As we will see, beliefs like this differ markedly between technical and non-technical respondents.

Having more individuals participating in security awareness training does not magically create a strong cyber security culture at organizational level. However, effective cyber security training does present an opportunity to correct misconceptions and shape a cyber smart culture. But many organizations are not taking that opportunity, or worse, they are harming the culture they hope to nurture.

For example, although individuals in different roles encounter different cyber risks, 60% of our respondents say that all employees at their organization get the same cyber security training. And where this does happen, just 37% say that security training tailored to their specific role and needs is effective.

“We've had a ‘crossing the fingers' approach for many years, because incidents were relatively rare,” says Gary Gaskell, a leading cyber security consultant in Australia. “If you gambled – you might be lucky.”

More than half have needed to bypass cyber processes to respond to change in 2020



Q5. To what extent do you agree or disagree with the following statements

More than tech

Our research suggests that many organizations lack creative and engaging practices that will truly build stronger cyber culture. That's despite the fact that 60% of respondents say that senior leaders understand and take an active approach to cyber awareness initiatives.

"I started out thinking that better technology would make a difference," says Gaskell. "It got us part way there, but we still need to improve how we manage and engage people."

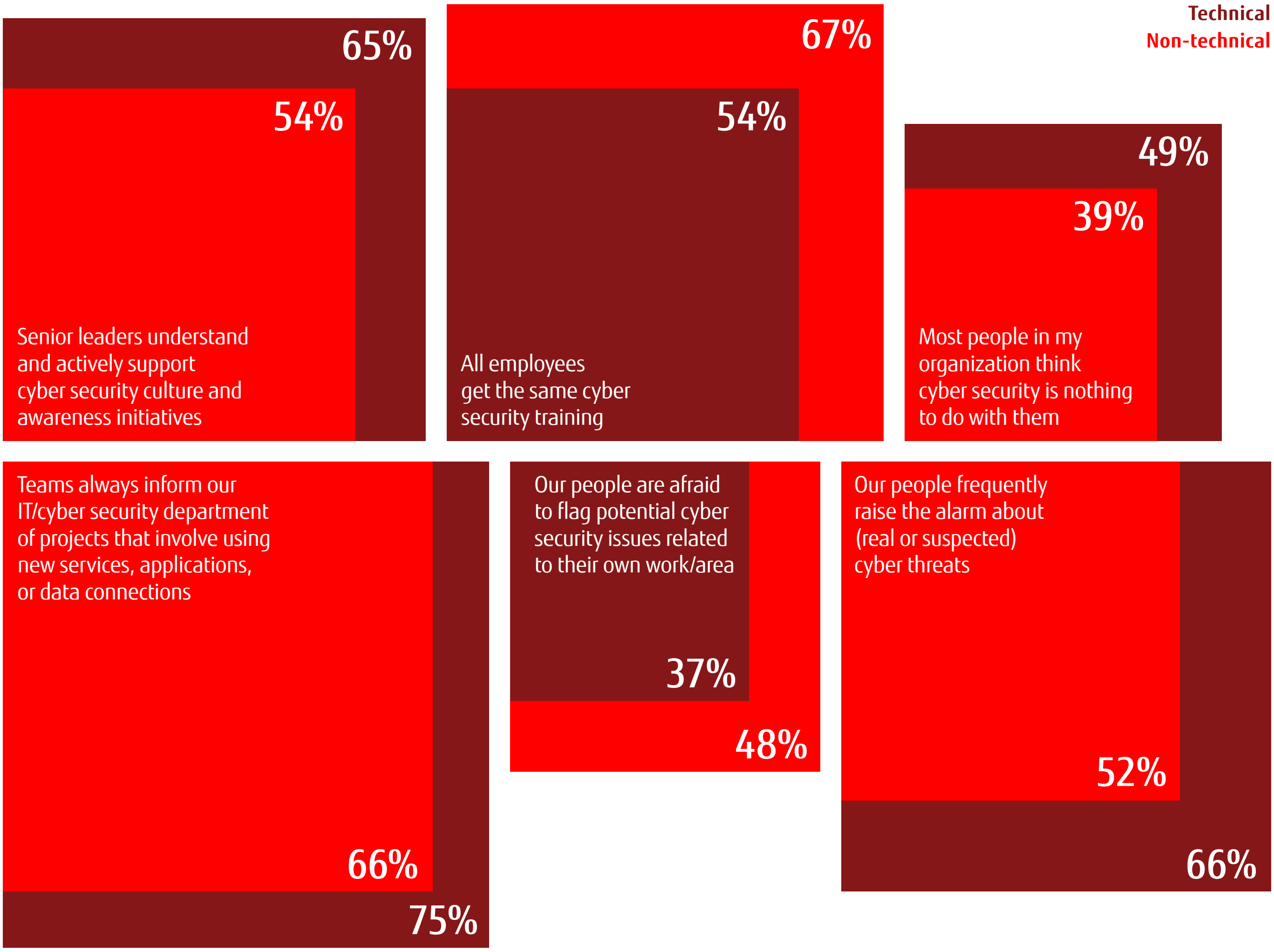
George Scott, Chief Information Security Officer of ROSA, which is a division of the UK's Foreign, Commonwealth & Development Office, explains that people are often the entry points for cyber threats – whether by clicking on a malicious link or sharing sensitive information to unvalidated contacts outside of a company. "It tends to be the humans that are the weak links in the chain," he says. So organizations need to recast cyber security from being an IT problem for CISOs, to the responsibility of every employee.

Failing to address human problems can be costly. Phishing emails are increasingly sophisticated, making it harder for the untrained eye to tell an authentic message from an inauthentic one. Meanwhile, cyber criminals are taking advantage of the pandemic by increasing ransomware attacks. Figures from the UK's National Cyber Security Centre[1] revealed a rise in cyber incidents to 723 between September 2019 and August 2020, up from 658 the previous year.

"Malicious actors have taken Covid-19 as an opportunity to look at new ways of conducting their malicious behavior," says Scott. "There are considerations around things like how you're located at home – maybe you have smart devices in the house that are listening to the conversations that you have online and picking up on some, which may be sensitive."

[1] *https://www.ncsc.gov.uk/news/ncsc-defends-uk-700-cyber-attack-national-pandemic*

Technical respondents appear to overestimate how informed they are



Q1. To what extent do you agree or disagree with the following statements about employees at your organization?

How to promote strong cyber culture

Most CISOs today recognize the importance of stronger cyber security culture in reducing an organization's more human vulnerabilities, but not many can point to outstanding results. So what can be done to build the right cyber culture? Our research highlighted three practical measures that can help any organization immediately:

Listen to the non-experts

One of the key trends that emerged from our findings is a misalignment in the views of two categories of employees: **technical respondents**, who work in teams primarily dealing with software, cyber security, data governance and technology, and **non-technical respondents,** who include the finance, legal, management, research and marketing functions.

So non-technical employees, who form the majority in most organizations, do not appear to be telling IT as much as IT would like to believe, and are more worried about blowing the whistle.

These are the kinds of discrepancies that organizations can smooth out with better communication. It should be a dialogue, but given the sheer numbers of non-technical employees, technical specialists should listen more carefully to what their colleagues think and need.

"One of the things I've been involved in in the past is taking senior leaders in an organization – from directors down to senior management – through a program of training on the important elements of security policy and how their responsibilities are linked to that," says Scott. "And that conversation was only effective because it was a dialogue."

To build a more effective culture then, it is clear that cyber professionals must foster clearer modes of communication that allow them to listen to what non-technical employees think about cyber security and their role in it.

75%

of technical respondents feel confident about the extent to which they are informed about projects that involve using new services, applications, or data connections. That compares with 66% of the non-technical respondents.

37%

of technical respondents say that people in their organization are afraid to flag potential cyber security issues related to their own work/area, compared with 48% of non-technical respondents.

45%

of non-technical workers describe existing online security training as ineffective

2

Conventional training methods aren’t working as culture building

As we have seen, many organizations take a one-size-fits-all approach to cyber training. Gaskell says that this doesn’t work.

“If we’re a hospital,” he says, “We should have a different awareness training program for doctors compared with nurses and other sorts of allied health professionals.”

But our findings show that even when training is tailored to a role, 61% say it is ineffective (37% say it is effective, while 2% say it has never been done). Why is that, and what can organizations do about it?

For one, they must pay closer attention to the content of the training they provide to their employees as a whole. Just 26% of non-technical workers say they find training interesting, 32% find it too long, 35% say it is boring, and the same proportion say it is too technical.

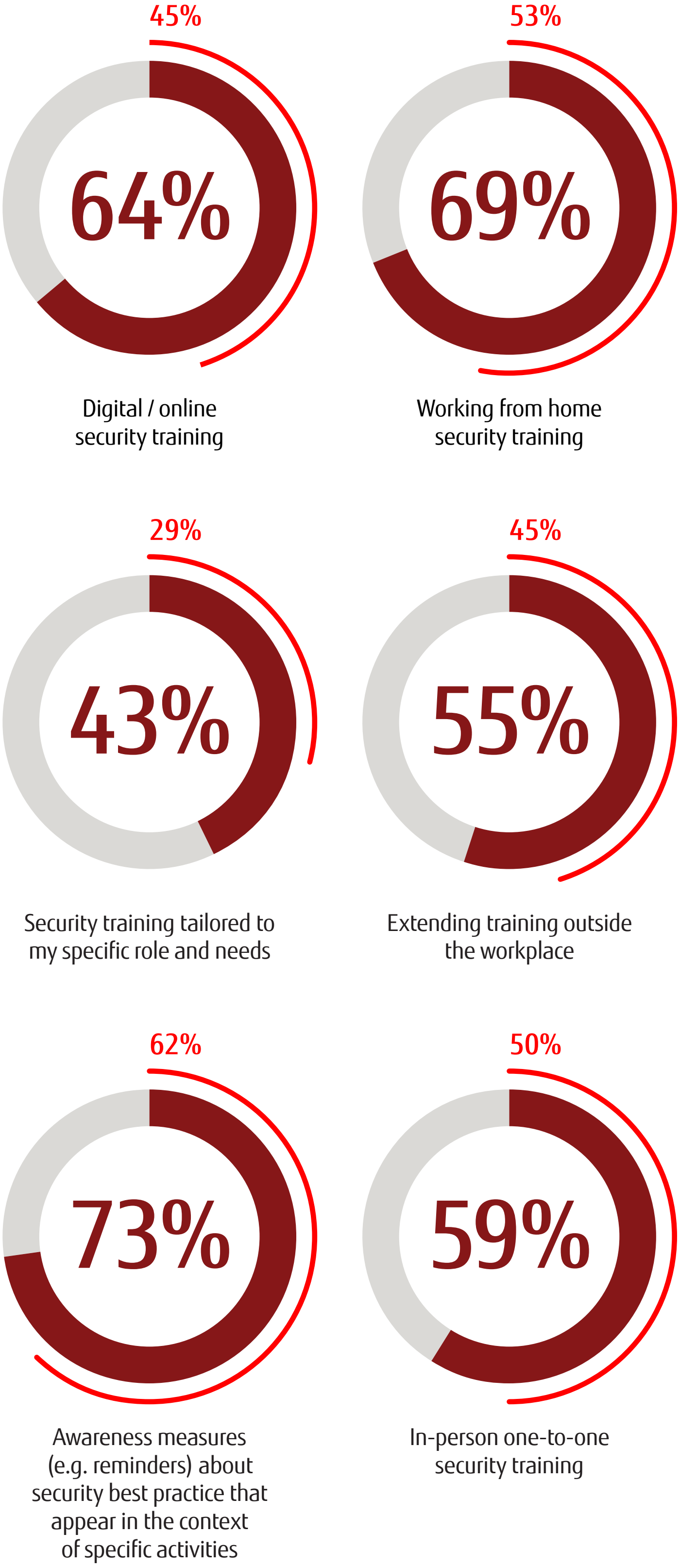
The effectiveness of digital training in particular should be scrutinized. As the pandemic has forced almost all training to move online, it is startling to hear 45% of non-technical workers describe existing online security training as ineffective.

There are ways to address this. Most non-tech respondents (69%) say that training is most effective when it involves games, rewards or quizzes to improve security awareness or behaviors.

And two-thirds (66%) believe in the effectiveness of signs, posters and notices (physical and digital) that promote awareness and security best practice.

Technical employees may over estimate the effectiveness of online training

Percentages indicate effective ratings split by **Technical** *and* **Non-technical** *respondents*



“I think we’ll get better at motivating behavior change for different audiences and better ways to increase buy-in on the skills”

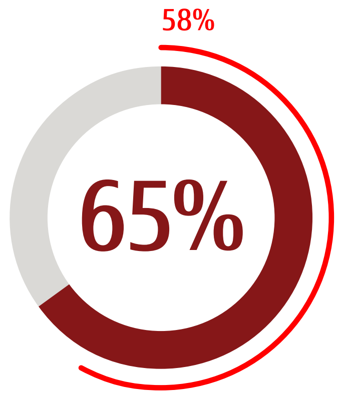
Gary Gaskell, leading cyber security consultant in Australia.

“I think we’ll get better at motivating behavior change for different audiences and better ways to increase buy-in on the skills,” says Gaskell. “Organizations are doing computer-based training – click here, click there – but some companies are gamifying it and making it fun in some way.”

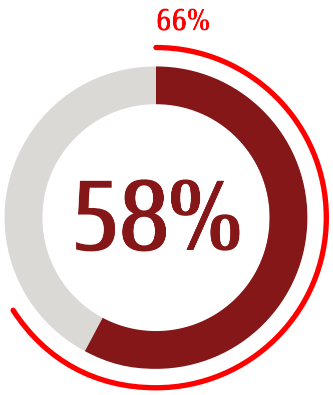
Technical respondents do not seem to think as quite as highly of these gamifying measures. Conversely, technical respondents are more positive about the effectiveness of context-specific awareness measures, such as customized reminders about security best practice that appear during specific activities.

However, these two do offer some degree of common ground in terms of overall effectiveness, and therefore could offer useful starting points for new training approaches.

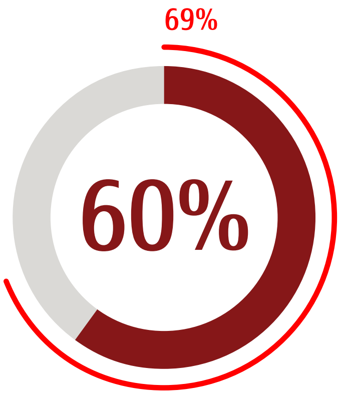
Percentages indicate effective ratings split by **Technical** *and* **Non-technical** *respondents*



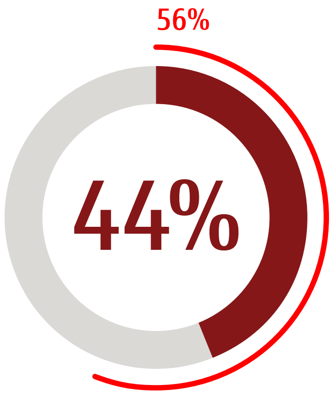
In-person group security training seminars/classes



Signs, posters, and notices (physical and digital) that promote awareness and security best practice



Games, rewards, or quizzes to improve security awareness or behaviours



Non-technical senior leaders that endorse stronger cyber security behaviours

Employees need something different

Get personal and be creative

Building a healthy cyber security culture does not have to involve dull, passive presentations or box-ticking exercises. Employees need something different.

According to Gaskell, good awareness training focuses on two fundamental aspects. The first is behavior change – motivating people to think and act differently. This kind of training should recognize that different sections of the workforce are motivated in different ways, as we have seen in the different attitudes to various types of training.

The second aspect of good awareness training is knowledge: people need to know what to do. When employees encounter phishing attempts, they should immediately know what to do, what not to do and who to inform.

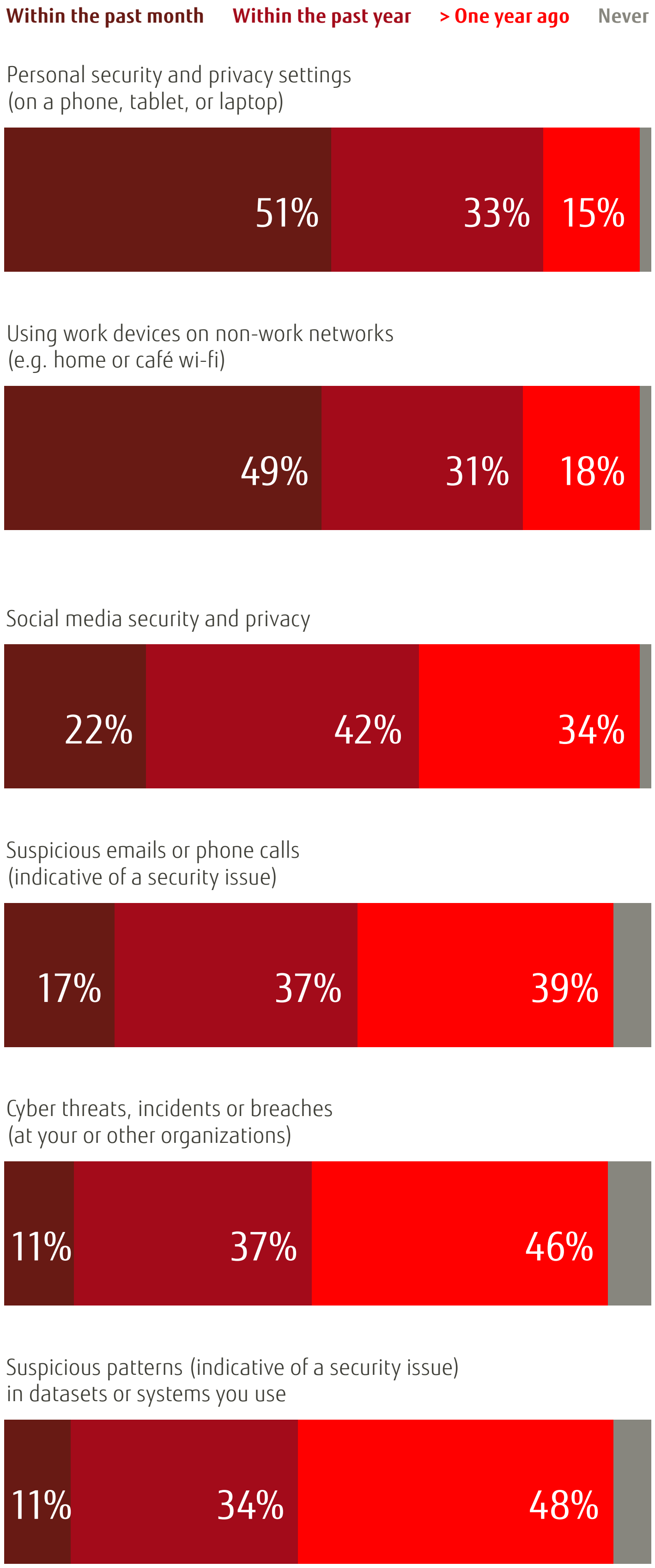
Our research suggests one way to combine behavior change and knowledge: getting personal. The most common cyber security-related conversations respondents have with colleagues are about personal settings (such as the use of work tools on non-work devices – and vice versa) and working remotely.

This natural interest presents organizations with an opportunity. Innovative and interactive training on issues employees encounter in their personal context is likely to get strong engagement, yet it could convey many of the same behavior shifts and lessons that are needed in the work context.

This is the kind of technique that organizations can use to turn employees from security practitioners into security advocates, a hallmark of a cyber smart culture, while making it more likely that those employees will remember how to act.

Interest in personal data security presents an opportunity to improve engagement

Percentages indicate responses to the question:
"When was the last time you were involved in a conversation (by phone /online call, email / chat box or in person) with a colleague (or a group) about the following?"



Final word

Organizations can build a cyber smart culture by getting creative with the content and delivery of their training, ensuring it is convenient and easy to digest. But they need to do more than just training: they should also ensure that everyone's views are heard and endorse behaviors that are cyber safe in all functions of a business.

According to our research, 78% of respondents believe cyber security has moved up the priority list in 2020, and 77% expect cyber security training to increase over the next two years. This gives organizations an opportunity to tackle the culture challenge as employees are anticipating it.

Most (72%) also anticipate stricter rules on allowable devices, software, or services before 2022. However, company's need to be careful with strict measures, even if people expect them. Many people do not respond well to top-down procedures, and a strong cyber security culture is about empowering people to be aware and proactive – neither of which flow from strict rules.

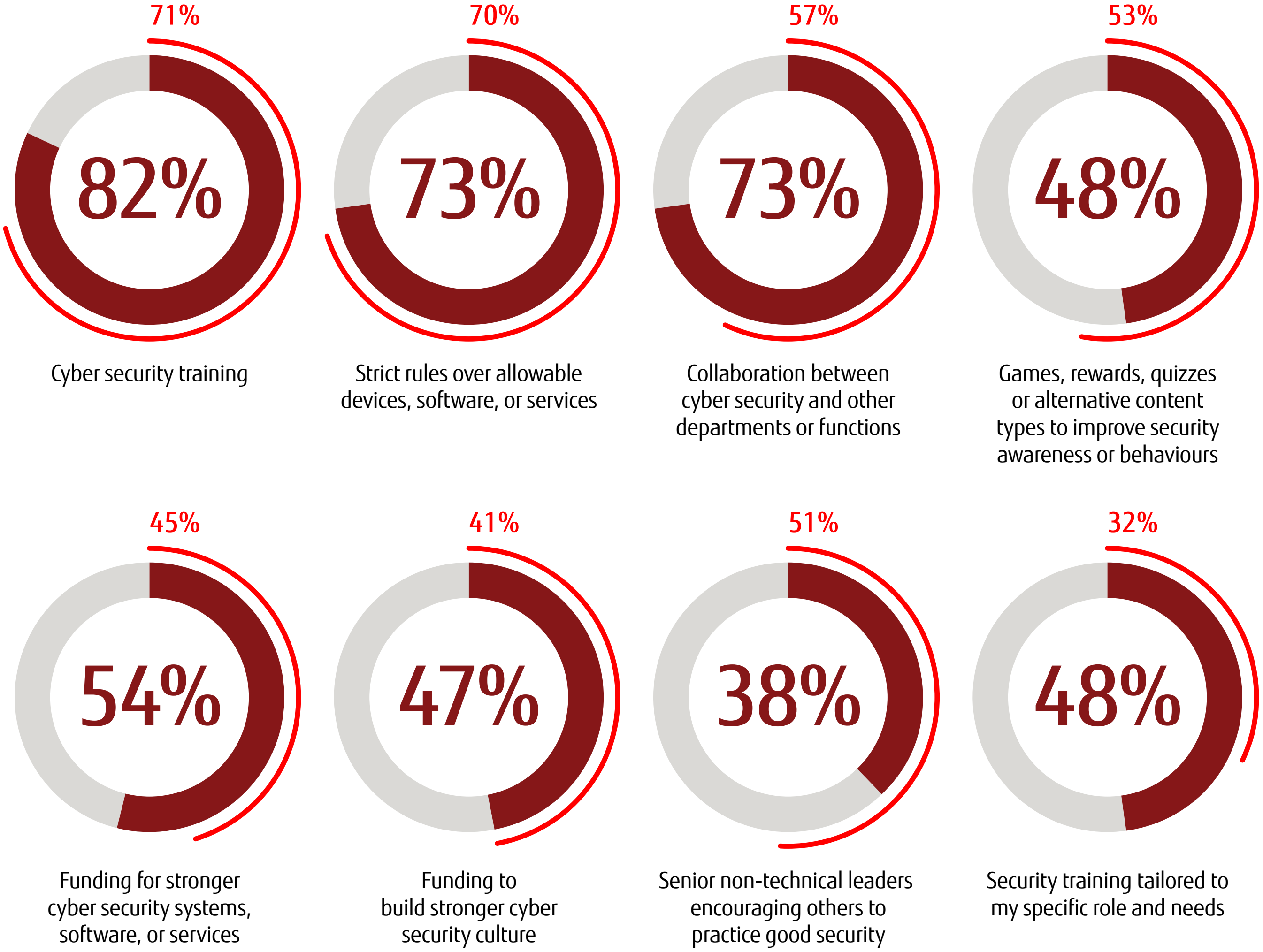
It is therefore vital to improve communication between security teams and the wider business, while introducing more creative and interactive ways to influence behaviors. This will help organizations drive the mindset and cultural shift that will become a powerful defense against cyber threats.

"The objective should be not to tick a completion box, but to actually make the organization more secure," says Scott. "It's actually getting people to think of the implications of what they're doing, and to consult others if they need to."

It is time to put to rest the idea that CISOs and their teams are the only ones who are responsible for cyber security, and the only ones that should advocate for better practice: everyone in the organization should play a role. That is what builds a strong cyber culture, which in turn makes organizations genuinely resilient to modern cyber threats.

Technical respondents anticipate greater internal collaboration

Percentages indicate those that expect an increase in the activity over the next two years, split by **Technical** *and* **Non-technical** *respondents*



Learn how Fujitsu can help your business gain value from advanced security services:

www.fujitsu.com/global/themes/security