Secure Together as One

FUJITSU

Why a healthy security culture starts with your people ›

shaping tomorrow with you

What culture is made of

If you're like most organizations, your non-technical employees will form the majority of your workforce. And, as you'll have seen recently, they play a significant part in driving your organizations' culture. Through their combined efforts – and your support – they've been able to adapt quickly to home offices, kitchen tables, and remote meetings.

Now, we can see the importance of employee behaviors and mindsets. They join smart processes and the right technology to form the basis for a great working culture.

So, why should a security culture be any different?

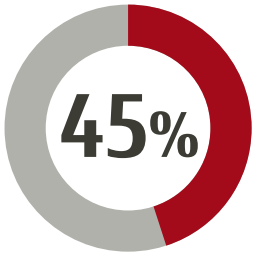
It’s their organization, too

The part of people in securing an organization has often come second to following processes or investing in technology. But in a world of rapid transformation and a wider attack surface, organizations are finding they need a new security model – one that unites every part of their operations and can adapt to changing conditions while following overarching rules. This means that, now more than ever, securing an organization depends on its people, as well as its processes and technology.

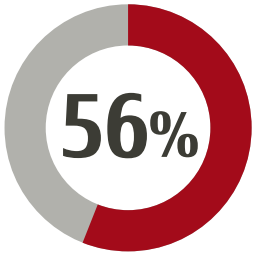
But, unlike working habits, employees aren’t always so quick to adapt to new security practices. They might not even be aware of their responsibilities at all. It’s a self-fulfilling prophecy – employees believe cyber security is someone else’s job, so that’s just what it becomes.

That “someone else” is often you and your fellow business leaders. But not for much longer. As you’ve done for new ways of working, it’s time to build a healthy security culture. In this guide, you’ll discover why it takes everyone to stay secure, where you can start with your organizations´ cyber security culture, and how we can help.

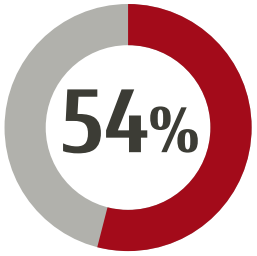
Who's responsible for cyber security?



of people believe that most employees in their organization think cyber security has nothing to do with them.



of non-technical employees look to their non-technical leaders (rather than their technical leaders) to encourage cyber security.



of non-technical employees believe their senior leaders understand and actively support cyber security culture and awareness initiatives.

Source: all information quoted in this report has been sourced from 'Building a Cyber Smart Culture', a global survey carried out in September 2020 by Longitude / Financial Times on behalf of Fujitsu.

The need to empower the CISO

Just as security isn't just the CISO's job, cyber security doesn't just come down to defending an organization from potential breaches. The modern CISO contributes to the business by designing a strategy for growth that identifies and mitigates potential risk along the way.

This allows organizations to take a proactive stance on cyber security – not just waiting to be attacked but finding ways to stop an incident from happening in the first place. From there, it also helps the company's reputation and maintains the trust of its customers.

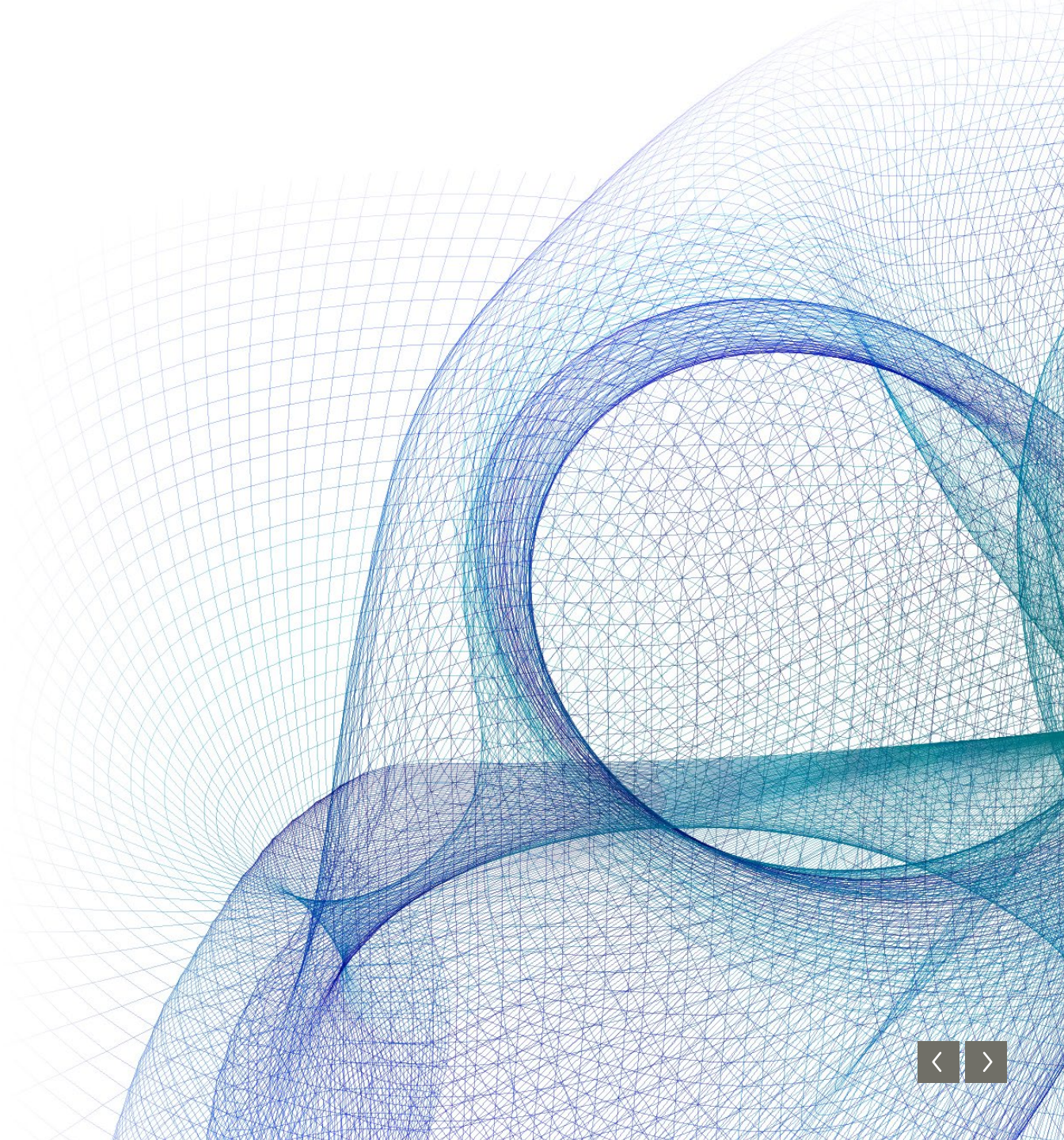
Put simply, it takes a lot to secure an organization. And all that takes more than just the business leaders to do. Let's take a look at some of the challenges surrounding cyber security – to see where your people might be able to help.

Responding to new priorities

Every day, week, month, and year comes with new challenges – some greater than others. And these challenges create new financial priorities for your organization.

Now, new ways of working, new service delivery models, and new business strategies are cropping up in every industry. The way you interact with everyone from your suppliers to your competitors has become fluid – even experimental. And still, industry standards govern everything. The GDPR has become a new high watermark for data security, with new data protection and privacy regulations really taking off, including the new California Privacy Rights Act 2020.

Your organization's priorities are not just set internally – but externally, too. And in your pursuit of new, better ways of working, there are more priorities than ever demanding a secure approach (and the budget to make it possible).



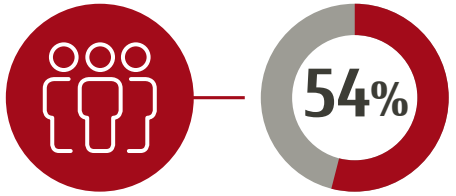
Finding opportunities in change

What started as a short-term solution has become a long-term vision.

Your organization and its people are resilient – able to turn change into opportunity with new technologies and an open-minded approach. But don't forget that cyber criminals have access to all the same emerging technologies and industry insights you do. Data breaches have become a lot more difficult to detect. And cyber criminals take every opportunity to gain entry – like phishing emails disguised as key updates on topical and newsworthy items. At the same time, cyber crime has become a well-resourced industry, ranging from agile and tenacious individuals to nation-funded groups with deep pockets. Free of any rules or regulations, they're usually faster to put these technologies and insights to work, too.

As your organization has responded to new ways of working, it needs to respond to new attack surfaces, too. Because, while the working culture has moved on, the security culture has mostly stayed the same. It's why more than half (54%) of business leaders bypassed some security policies in 2020, reasoning that it was more important to keep up with change than follow security best practices.

As you and your employees venture into new enterprise practices, cyber security needs to strike a balance between protecting your organization as a matter of course – and propelling it forwards as a competitive advantage.



of business leaders bypassed some security policies in 2020, reasoning that it was more important to keep up with change than follow security best practices.

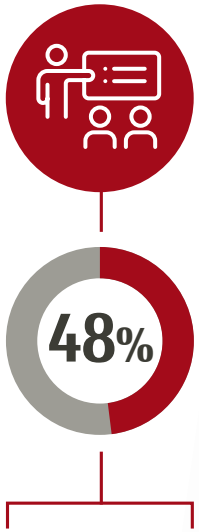
Source: all information quoted in this report has been sourced from 'Building a Cyber Smart Culture', a global survey carried out in September 2020 by Longitude / Financial Times on behalf of Fujitsu.

Encouraging awareness

Business leaders – whether they're technical or non-technical – can do everything right. But the reality is that it only takes one mistake to threaten the cyber security of your organization. And that mistake can come from anywhere.

Lack of cyber security awareness among employees is one thing. But misunderstandings around cyber security and who is responsible for it can also drive inaction in the event a breach does occur. In fact, 48% of non-technical employees believe people in their organization are afraid to flag potential cyber security issues. Employees think business leaders will be looking for someone to blame – when really, you're just looking for somewhere to start.

Cyber security awareness is about more than annual training and quarterly refreshers, especially since 45% of non-technical employees describe existing online security training as ineffective. Good cyber security awareness combines behavior change – encouraging people to think and act differently – and knowledge – sharing your vision for cyber security with everyone in the organization. You're all on the same team, after all.



of non-technical employees believe people in their organization are afraid to flag potential cyber security issues.

Source: all information quoted in this report has been sourced from 'Building a Cyber Smart Culture', a global survey carried out in September 2020 by Longitude / Financial Times on behalf of Fujitsu.

You're secure together as one

Many factors stand against your business's security. However, it only takes one of them to break through your defenses. It means your entire organization is only as secure as a single part of it – and strongest when you're working together.

Building a culture with security at heart takes everyone and everything – people, processes, and technologies – working together to support the CISO and secure the organization.
Of course, as individual risk-owners, every individual will want to approach security in their own way – much as they might approach their own day-to-day tasks.

The solution is to explore more creative and interactive ways to encourage secure behavior every day. Security will be at the center of a cultural shift – one of several defenses your business can use against digital threats.

At Fujitsu, we know because it's something we've done ourselves.

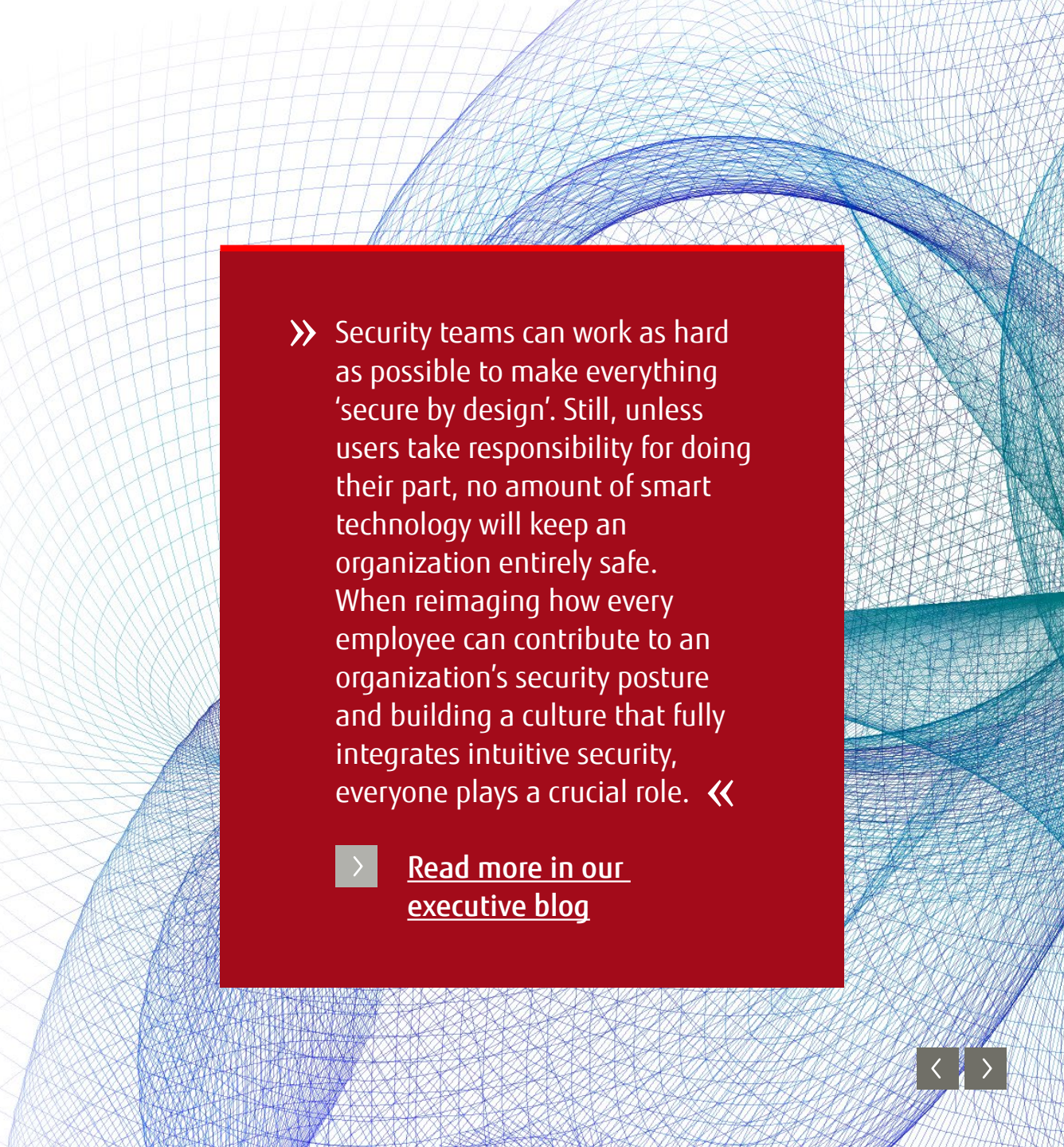
It's one way we secure our business

When you've got **over 3,700 security professionals** across 100 countries and **you serve 1,400 customers globally**, **working together becomes essential**.

We think of our security culture like a human firewall, held together by collective knowledge, habits, and values. In this firewall, all of our people are focused on playing their part to keep our customers secure and create business value. It's part of a wider security strategy – and a bigger ambition to put people at the heart of everything we do. Talent, strength, and diversity are our most valuable tools for any challenge, including cyber security.

And when it comes to shaping your own security culture, what we've learned along the way can help.

Using our people-centric cyber security solutions, you too can support your existing strategy to minimize disruption and maintain continuity. So, your organization can work towards a more resilient strategy and operations, with the elasticity to meet whatever your employees and industry might demand next. All built on a foundation of integrated, collaborative technologies that everyone can use.



» Security teams can work as hard as possible to make everything 'secure by design'. Still, unless users take responsibility for doing their part, no amount of smart technology will keep an organization entirely safe. When reimaging how every employee can contribute to an organization's security posture and building a culture that fully integrates intuitive security, everyone plays a crucial role. «

› Read more in our executive blog

Why Fujitsu?

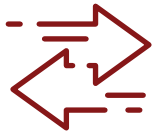
We believe that strong collaboration is key to securing your organization.

We work with you to drive high-performing security strategies capable of creating business value in challenging times.

We act as a trusted advisor as you build secure measures that enable digital transformation.

It goes further than securing your organization

A culture of cyber security, as part of a holistic approach to security, helps you protect your organization, its employees and customers, and their data. But with everyone and everything working securely together, you'll find you can solve some of the surrounding challenges, too.



A security culture works within your wider strategy to help you **respond to new priorities**. By taking on some of the basic and most preventable cyber security tasks, your employees can help you free resources that might be better spent on emerging priorities.

A security culture works within your wider strategy to help you **understand opportunities in change**. When everyone can identify and assess the risks of a new way of working, you can move forward faster and with greater confidence – to keep progress from bottlenecking.

A security culture works within your wider strategy to help you **encourage awareness**. More open conversations mean you can find processes that everyone understands and follows. Remember, encouraging your employees to take responsibility for cyber security means giving them some ownership of it, too.

What better place to start?

Culture depends on people as much as it does on processes and technology. So, how do you get your people on board with a cyber security culture?

Find out more about the human side of the business case for a cyber security culture in this research study, **Building a Cyber Smart Culture**. Inside, you'll discover the challenges organizations like yours face when trying to build a strong cyber security culture. You'll also pick up some recommendations that can help you change your employees' cyber security mindset – to become secure together as one.

Get the report and start building

If you want to learn more about what your own cyber security culture could look like – or find out more about the people, processes, and technologies united under ours – just get in touch.

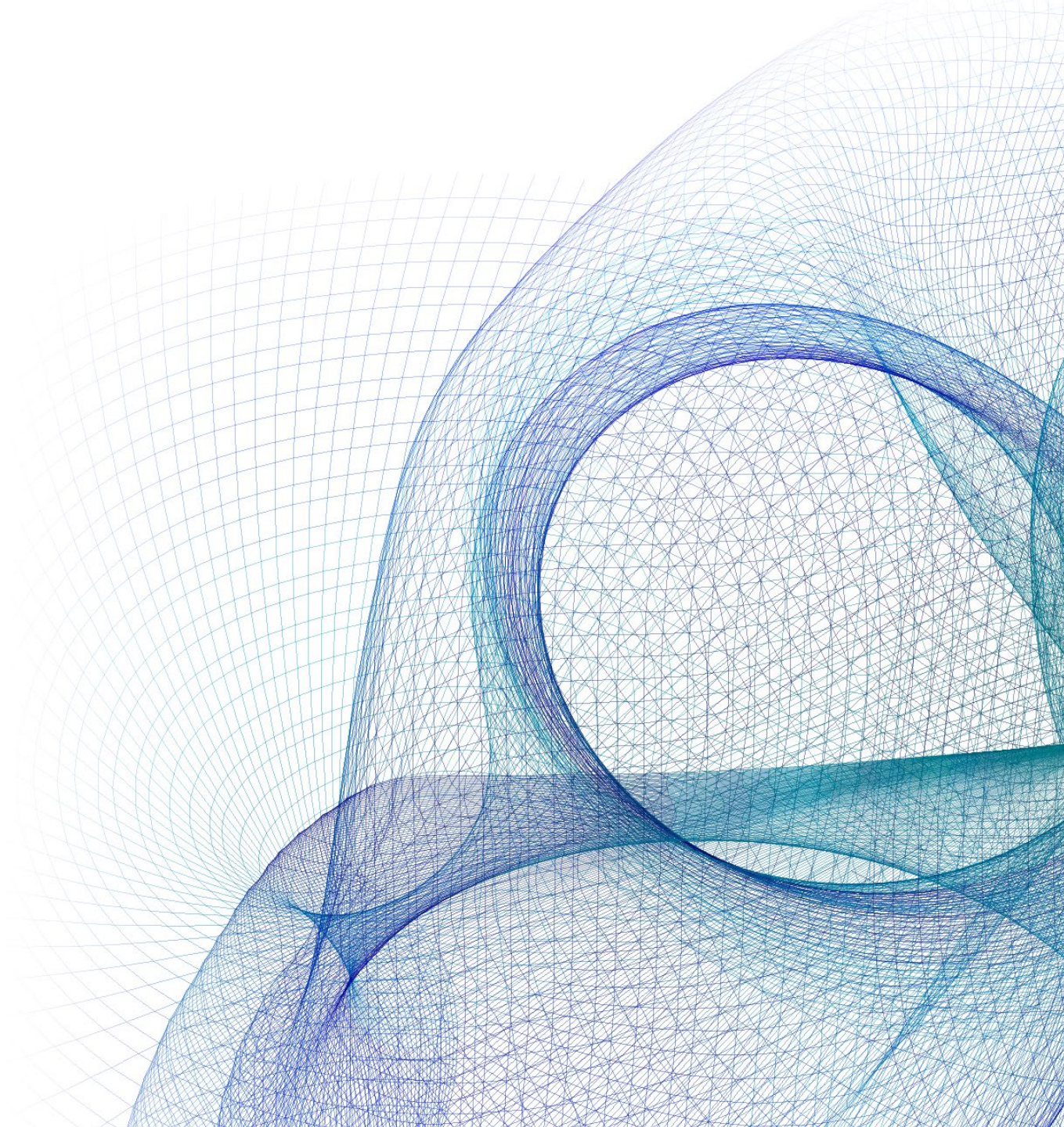
Get in touch with us today

Become secure together as one.

Telephone: +44 (0)870 242 7998

Email: askfujitsu@uk.fujitsu.com

Web: fujitsu.com/global/themes/security/



FUJITSU

ID-7218-004/04-2021 | Ask Fujitsu ID: 4042

Source: all information quoted in this report has been sourced from 'Building a Cyber Smart Culture', a global survey carried out in September 2020 by Longitude / Financial Times on behalf of Fujitsu.