SAMSUNG

Securing your digital future

Digital security is now key to success

Digital security has long been important for business. Recently, however, with more employees working away from the office, it has moved to the centre of everything companies do. Get it right and it's a source of genuine competitive advantage—and one that can allow businesses to reach new heights.

> "$57,000 (£41,500) loss to businesses per cyber incident."

In recent years data has become absolutely central to how we do business—as they say, there's no such thing as a data company anymore, because all companies are data companies. This means that cyber security has gone from being a bolt-on extra to mission-critical and should be part of every business's strategy. Indeed, according to Hiscox's 2020 Cyber Readiness Report, 39% of companies reported cyber incidents in the last 12 months; losing on average $57,000 (£41,500) per incident, which is a near six-fold increase on 2019 $10,000 (£7,285).

> "A managed mobile estate allows your business to become more secure overnight."

Even so, many organisations still view security as a chore. They shouldn't. Instead they need to embrace digital security as a source of competitive advantage. Companies that are secure are likely to attract new customers and retain existing ones. They will be ready to embrace new, collaborative, more productive, mobile ways of working. This, in turn, will make them a destination for the best employees. They will also be more attractive to investors and other stakeholders.

The good news is that it has never been easier to improve cyber security. With more employees working away from the office and at home, it's important to ensure they have everything they need to stay productive and remain secure. Business specific offerings like Samsung Enterprise Edition now include everything from providing premium mobile devices to fully managing your mobile estate. So, your teams can be fully equipped for remote working—ensuring their device and your company data remains secure at all times. A managed mobile estate allows your business to become more secure overnight, leaving you to focus on more important tasks.

An increasingly risky world

> "70% of people would stop doing business with a company if it experienced a data breach."

Data breaches are something that businesses need to take more seriously than ever. According to IBM's Cost of a Data Breach 2020, data breaches are costing UK firms an average of £3.9M and taking 256 days to identify and contain.

Outside the cost of the breach itself (and any fines that may be levied), reputational damage is probably the biggest of the second-order effects. Samsung's global director for enterprise business, Nick Dawson, says, "There's an increasing awareness about things like data leaks. Over the past couple of years this issue has really broken through into the public consciousness. People think, who's got access to my data and is it safe? Can I trust this business?"

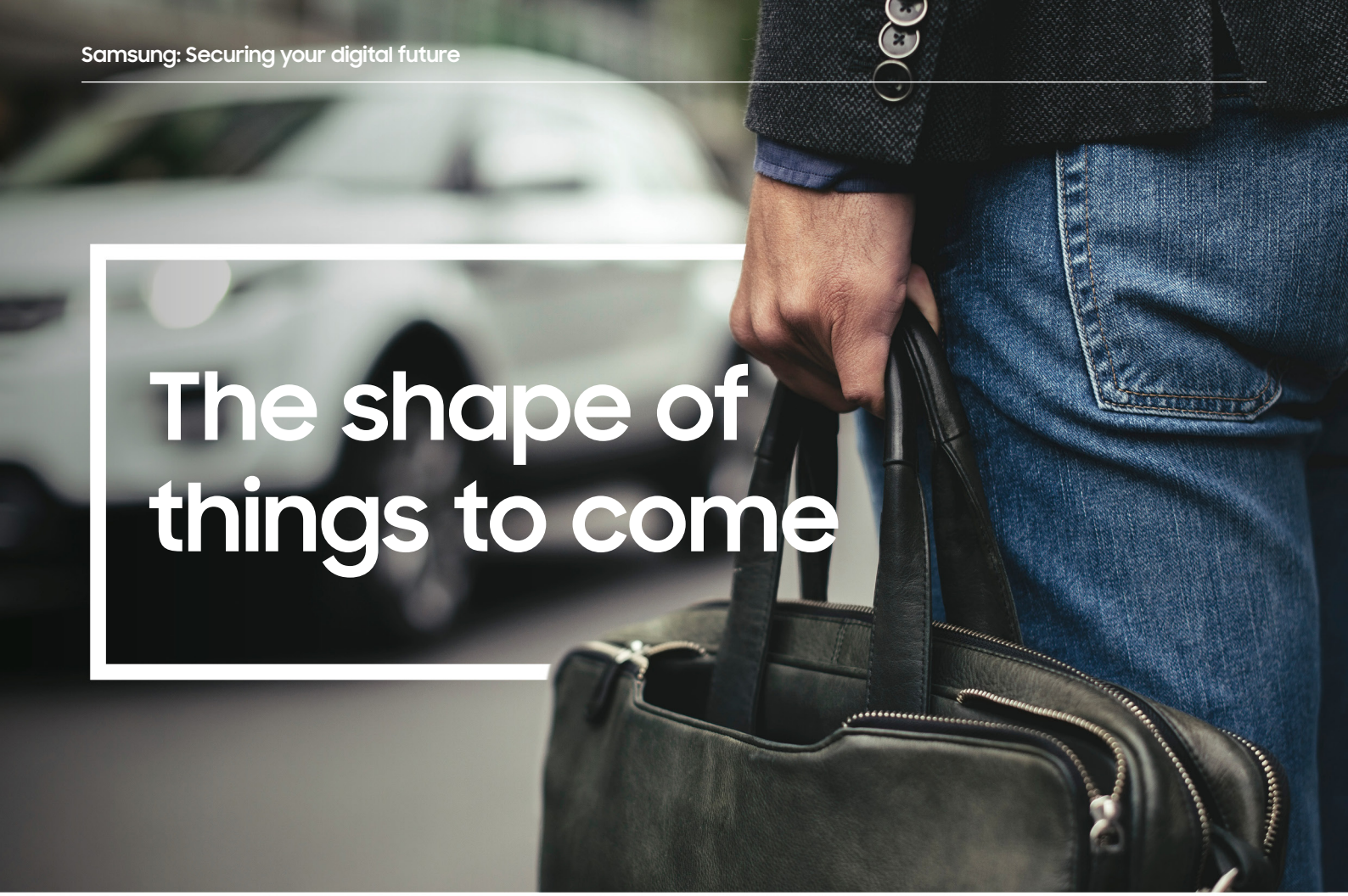
A stark illustration of how hacking can affect reputation comes from a survey of 10,0000 consumers undertaken by the security company Gemalto. This found that 70% of people would stop doing business with a company if it experienced a data breach. We can all name major companies that have been careless with customer data. One example is British Airways. The personal data of half a million customers was stolen by hackers and the company was fined £183m, which was 1.5% of its turnover. Clearly, the stakes are high—and are likely to get higher. With Samsung Enterprise Edition, you don't need to invest in lots of new technology—simply equip employees with the right mobile device for their needs, and they're good to go. It's also safer than equipping everyone with a new laptop, as all Samsung smartphones and tablets come with Samsung Knox defence-grade security built in to the hardware. All files and data are encrypted on the device, giving you extra peace of mind that everything is secure. Samsung Enterprise Edition also gives you greater control of your mobile estate—allowing you to configure, update, test and deploy mobile technology across your organisation easily and remotely.

> " Job losses happen in 31% of cases of cyber breach."

Indeed, the use of mobile devices, both business and personal are a major source of data breaches for companies. Often, employees are to blame (or partially to blame) for leaks. According to Spanning, the cloud backup company, 55% of employees admitted to clicking on links they didn't recognise. Indeed, it is an oft-repeated mantra that increasing staff awareness is one of the easiest and most important things you can do. Similarly, poorly thought through Bring Your Own Device (BYOD) policies can open you up to risks in all sorts of areas.

Breaches often have real effects on employees too—and some of these are surprising. Research by Kaspersky suggests that job losses happen in 31% of cases. Typically, the company said, "senior non-IT employees were held responsible [for the incident] and dismissed." Sacking and replacing employees, even relatively junior ones, is very expensive. Then there are the fallout effects from this. These might range from replacements taking time to train (and being inefficient while they get up to speed) to morale being lowered and employee engagement suffering.

It's also important to realise that the business world does not exist in isolation. IT security is affected by and interacts with dozens of other factors in the world. In recent years these have ranged from the rise of social media to foreign governments. In the future, they are likely to include everything from climate change to inequality. Many of them will be wholly unexpected. In 2007, when the iPhone appeared and business ran on BlackBerry devices, few appreciated how smartphones would come to dominate business and, for many purposes, even replace laptops.



The shape of things to come

> "We will see an explosion of new types of "endpoints", and new connected devices."

The internet of things (IoT) is a new frontier for hackers. IoT devices are not things like smartphones or laptops—they're dedicated-function objects, such as vending machines, connected cars and a myriad of other examples. A recent report by Gartner predicts there will be "25 billion [IoT devices] by 2021, producing an immense volume of data". By way of comparison, there are around 14 billion mobile phones on earth—so these 'things' will outnumber phones by almost two to one.

The trouble with these things is that they represent a vast new "attack surface" for hackers. 5G is rolling out in Western Europe and will finally unlock the IoT at scale by providing the necessary quality of network service and low latency. We will see an explosion of new types of "endpoints," and new connected devices. Most of these will be small and cheap.

"The trouble is the manufacturers are not baking any security in at the hardware level on these things," says Dawson. "They're completely open and hackers will literally just have to find it on the network and then they have free access to your house or business."

One high profile example of this happened in an American casino, according to a report by the consultancy Darktrace. A fish tank in the casino had an internet-connected thermometer. Hackers gained access to the thermometer, and through it the casino's networks. Eventually, they found the database of high rollers. Darktrace's CEO told an audience, "[The hackers] pulled the data back across the network, out the thermostat, and up to the cloud." We can expect to see a lot more of this.

Heads in the sand

Despite the growing importance of security, many companies either get it wrong or stick their heads in the sand, refusing to deal with the problem at all. According to PWC 2021 Global Digital Trust Insights 39% of business are either reducing their cybersecurity budgets or keeping them static.

Businesses are finding it difficult to manage cybersecurity. Cisco's 2020 CISO Benchmark Report shows that out of the organisations surveyed:

- 52% say mobile devices are extremely challenging to defend
- 41% are struggling with data centre protection
- 39% have issues with securing applications
- 52% struggle with data stored in the public cloud

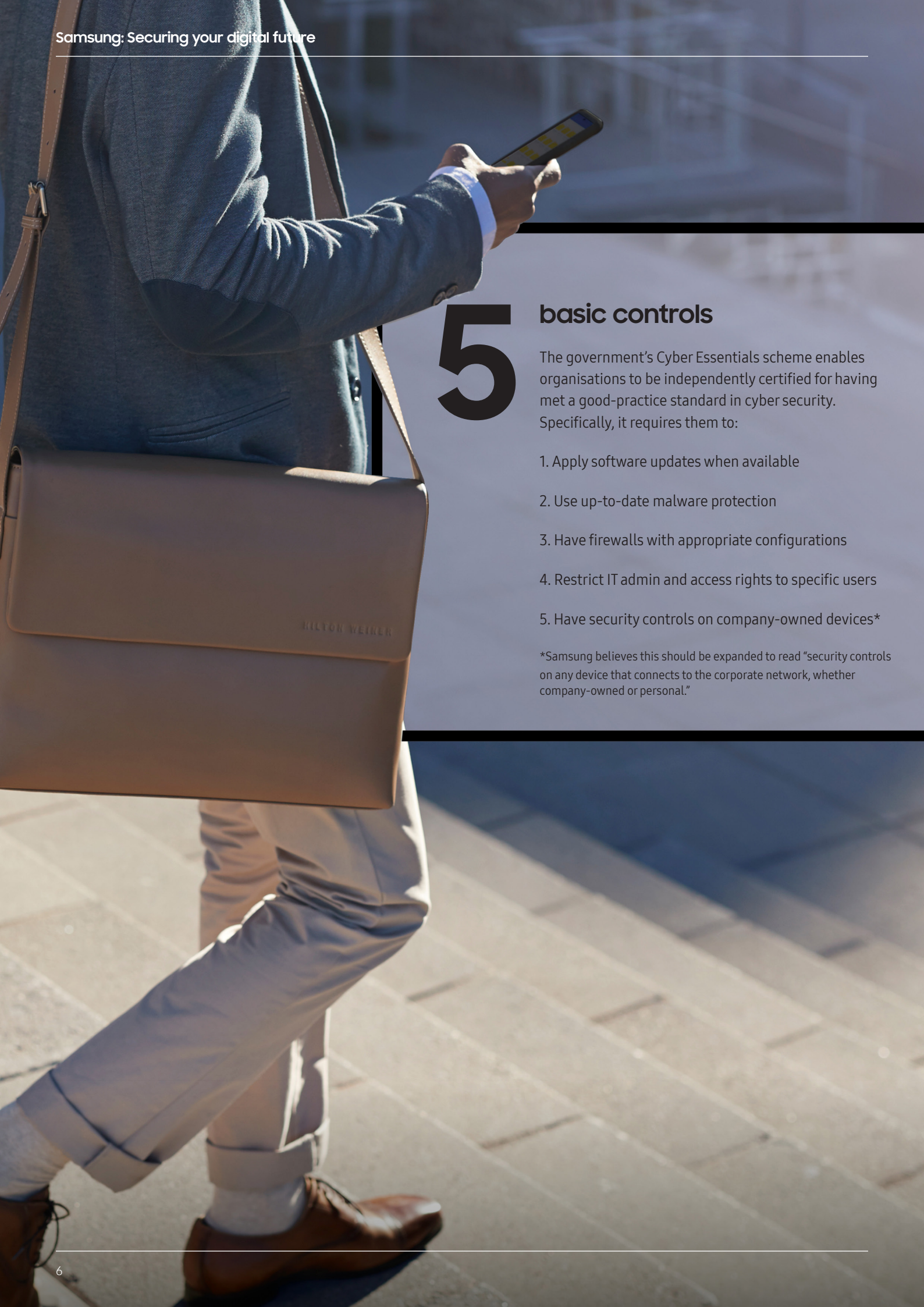
Indeed, it has simply become too much for many, with 42% of respondents suffering from cybersecurity fatigue, which is defined as "giving up on proactively defending against malicious actors."

In a similar vein, according to the UK Government's Cyber Breaches 2019 report, only 51% of businesses have implemented the five basic controls it suggests (see box below).

It's not that businesses don't recognise what technology can do. According to FSB/Cisco, more than three quarters of decision-makers believe that technology can empower agile working and increase productivity. However, nine out of 10 spend under 25% of their budget on IT. The survey also indicated that when very small companies did invest in IT, they soon grew and became larger companies. The trouble is, taking the first step is daunting.

"Businesses want to address security but often they don't know what to look out for and where to begin. It's up to us in the industry to address this and point out just some of the basics," says Dawson. That's why for example, Samsung Enterprise Edition packages up devices and services to give businesses more value from their mobile investment.

> **"Only 51% of businesses have implemented the five basic controls of security suggested by UK Gov."**



5 basic controls

The government's Cyber Essentials scheme enables organisations to be independently certified for having met a good-practice standard in cyber security. Specifically, it requires them to:

1. Apply software updates when available

2. Use up-to-date malware protection

3. Have firewalls with appropriate configurations

4. Restrict IT admin and access rights to specific users

5. Have security controls on company-owned devices*

*Samsung believes this should be expanded to read "security controls on any device that connects to the corporate network, whether company-owned or personal."

Collaboration is the future

If IT security is an important part of the present, its role in the future is only likely to grow. This is down to changes in both the way we work and the world as a whole. Over the last few decades, companies have gone from being largely standalone entities to participants in ecosystems. You see this at every level. Twenty years ago, you were on the staff or you weren't. Now freelancers, contractors and consultants are everywhere; modern organisations are very fuzzy at the edges.

> "Organisations that can harness the collective capabilities of an extensive network of collaborators... ...outperform their peers."

It's not just individuals either. Collaboration happens at every level. Integrated supply chains mean far deeper connections between businesses. On the retail side, customers will often buy products through multiple retailers and referrers. And, right at the other extreme, it's now virtually impossible for a single company to build large items like commercial aircraft or a large satellite alone. It requires collaboration between several or even dozens of organisations.

As well as being inevitable, collaboration is good for business. A recent IBM study of over 1,600 CEOs suggests that organisations that can harness the collective capabilities of an extensive network of collaborators—staff, customers, freelancers, experts and partners—outperform their peers. For example, Raconteur states "businesses that connect their people enjoy 32% more production innovation." Conversely, those who do not embrace collaborative, flexible practices are likely to suffer.

So what should businesses do? If they are to embrace this collaborative future, it will mean devices and systems sharing information at every level—from freelancers logging into shared storage to suppliers having access to systems. Those who do not embrace this future will be held back.

Fortunately, it has never been easier to buy in the expertise you need. Samsung has long recognised the need for integrated, across the board, multi-device security. As Dawson says of Samsung Knox defence-grade security, "No one has ever got through all of the defence mechanisms that Samsung has put in place."

Towards a secure future

> "Not having the right security is a huge risk, both commercially and reputationally."

> "Since the COVID -19 outbreak 71% of security professionals say they've noticed an increase in security threats or attacks."

For businesses, leveraging the power of security is the key to being able to grasp the opportunities a collaborative, technologically-enabled future offers.

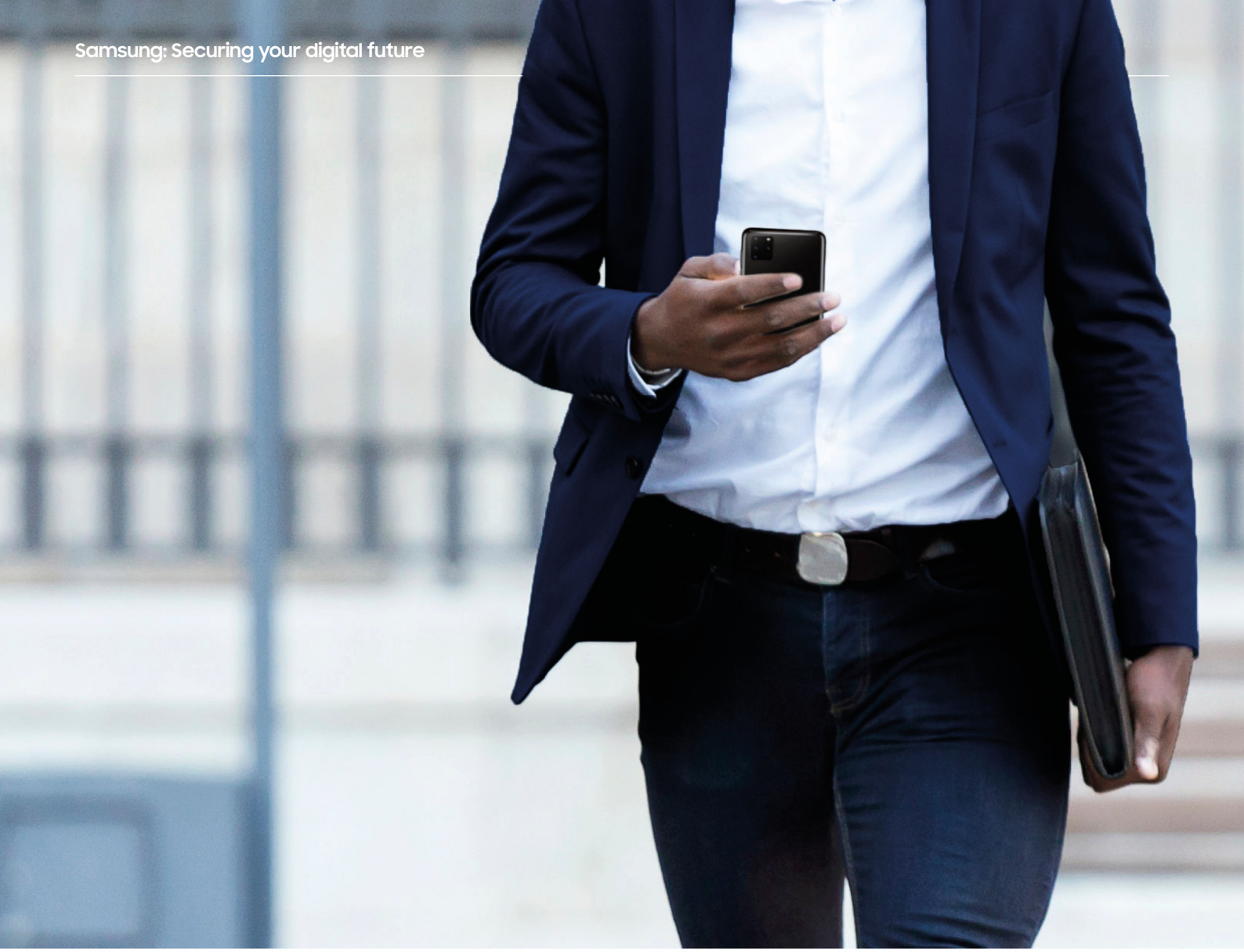
Securing mobile devices and networks that may stretch beyond your company is a big task—and there are few shortcuts. However, businesses need to stop thinking of security as just a cost and start thinking of it as central to what they do. Not having the right security is a huge risk, both commercially and reputationally.

Mobile security should be seen as the frontline protection from that risk, and also a source of competitive advantage and new opportunities. It enables businesses to embrace new ideas and new approaches that will make them more attractive to customers, suppliers, partners and collaborators.

What's more, businesses can gain competitive advantage by implementing off-the-shelf offerings in areas ranging from cloud computing to Artificial Intelligence (AI). No matter the size of the business, the internet has levelled the playing field through technologies such as the Cloud. And mobile will make it easier for businesses to work globally.

With Samsung Enterprise Edition, businesses can access industry-leading mobile devices that are quick and easy for IT teams to set up—without even opening the box. Enterprise Edition provides access to Knox Suite—a collection of additional Samsung Knox licences including Knox Mobile Enrolment, Knox Manage, Knox Platform for Enterprise, Knox E-FOTA and Knox Service Plugin.

Enterprise Edition customers can remotely register and pre-configure multiple devices, Wi-Fi networks, contacts and company profiles and settings. They can also pre-load essential files and documents, and tailor devices for specific employees before sending directly to them.



To find out how Samsung can help your business be more secure with Enterprise Edition, go to: **samsung.com/uk/business/enterprise-edition**

Enterprise Edition even features a Quickstart build service for customers that want to take advantage of Knox Manage and E-FOTA, but don't have the skills. Samsung creates all the Knox and Android Enterprise accounts, sets everything up and hands it over to the customer. And support staff are on hand to provide technical and hardware support for the next three years.

Customers also receive up to five years of security updates*, meaning devices have the most up-to-date Android and Samsung security and maintenance patches. Security updates can be easily controlled with Knox E-FOTA. And, customers can choose how and when updates are delivered across their fleet, and even force critical updates—without users having to take any action.

Finally, with Knox Platform for Enterprise, customers can monitor device activity, and restrict employees from downloading anything that might leave their mobile device exposed to attacks.

Nick Dawson concludes, "Increasingly, businesses will be asked by suppliers, customers and partners if they are secure and if they have put certain measures in place. Particularly if their competitors don't do these things, it can give them a real leg up." Businesses that can sell themselves as secure are more likely to succeed in a collaborative world. "They can talk about trust," Dawson adds. "They can say, 'We've got it covered. We can take care of this."

*5 years from first global launch for S20 and S21 Series, Note20 Series, XCover 5, Tab Active3. 4 years for all other devices.