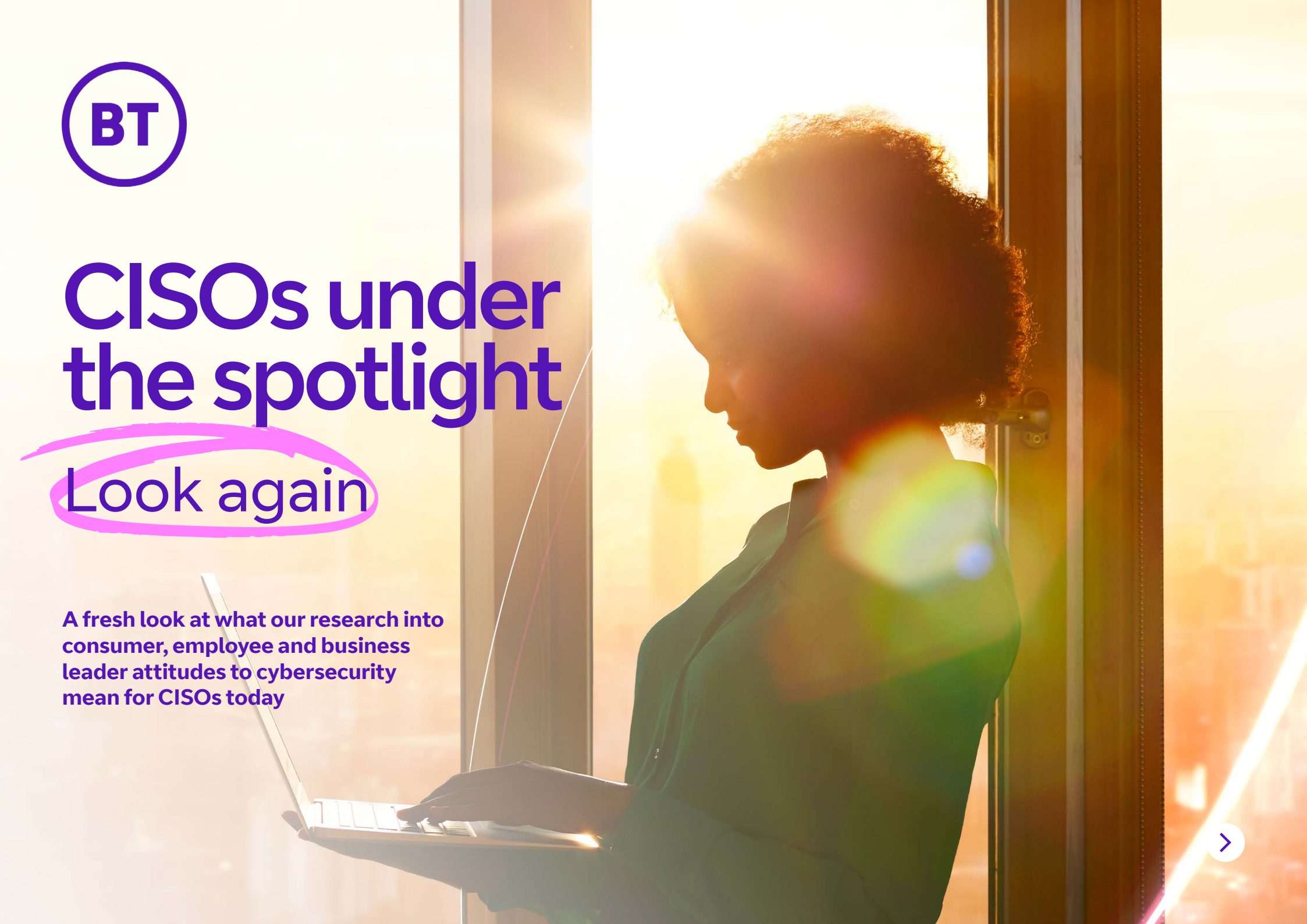
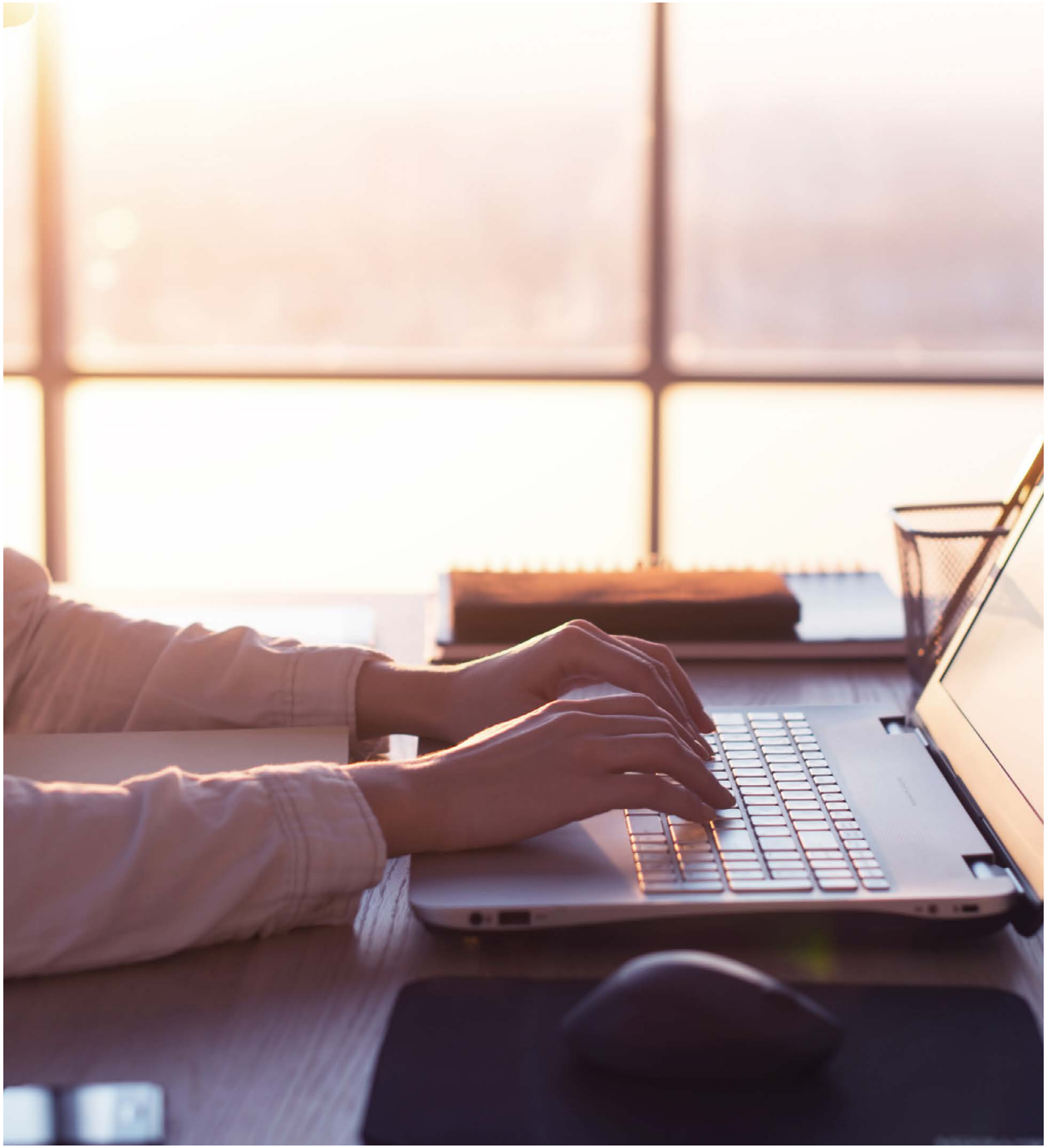


CISOs under the spotlight

Look again

A fresh look at what our research into consumer, employee and business leader attitudes to cybersecurity mean for CISOs today

Contents



Foreword - revisited

Environments evolve. Workplaces change. Threat landscapes shift. And, throughout this, the Chief Information Security Officer must enable business securely.

It's been a year since we asked business leaders, employees and consumers globally about their attitudes to cybersecurity. The findings are even more pertinent today.

The pandemic has generated a threat landscape that continues to become more intense and complex. Three quarters of business leaders say there are more and more security threats every year and we know that email scams, ransomware and brute force attacks have rocketed.

The hybrid working revolution has driven the convergence of network and security requiring CISOs to adjust their approach. More than ever, security needs to be built into a company's IT strategy rather than on top. And this needs to be achieved against a backdrop of a severe skills shortage that's posing a serious risk to the security of many organisations.

The CISO stands at the heart of this conundrum and has the power to lead the organisation through it.

By highlighting where CISOs need to focus, our research shows how they can unlock their time and energy and reduce their burden by bringing in an expert security partner to manage day-to-day security. The findings reveal a clear need for CISOs today to balance technological solutions with an understanding of human nature, encouraging people right across the business to adopt safe digital behaviours.

Respond to change, rethink your risks and unlock your competitive edge.

Kevin Brown,
Managing Director, BT Security

Foreword

The scale, pace and variety of cyberthreats continue to grow at an alarming rate – with uncertainty providing a further catalyst for change

In response, INTERPOL is constantly expanding and evolving our strategy to combat a wide range of cyber criminality – from organised criminal gangs to lone individuals. INTERPOL's Global Cybercrime Programme, in particular, is uniquely placed to prevent, detect and investigate cybercrime. We lead a global law enforcement response in support of our 194 member countries to reduce the global impact of cybercrime and protect communities for a safer world.

Given the instrumental role that the private sector plays in cyberspace, INTERPOL places public-private partnership at the core of its strategy. Our private partners have continually kept us abreast of the threat landscape and the changes and attacks within. Their skills, knowledge and insights also enhance our analytical and technical capabilities in identifying and disrupting the organised criminal networks behind cybercrime.

In this context, we have worked closely with BT for many years to achieve that, including BT becoming the first telecommunications provider to sign an agreement with INTERPOL to exchange data relating to cybercrime trends, malicious attacks and emerging cyberthreats. By sharing threat intelligence, we can make cybercrime far more difficult and costly for its perpetrators.

As this report demonstrates, CISOs have a similar role to law enforcement to protect organisations and individuals, and ultimately protect them from harm. While law enforcement focuses on enforcement and prosecution, the CISO is often on the front line of cyberattacks as the 'first responder'. Their actions, and the plans and strategy that they have put in place in advance of cyberattacks, are often the key decider on how successful criminal attacks will be.

This reaffirms the importance of a collaborative approach across the entire cybersecurity ecosystem, including law enforcement and the private sector, as the most effective way to tackle cybercrime.

With a clear commitment and trust to work together, our collective efforts will lead to more effective response and resilience against borderless and ever-evolving cybercrime.

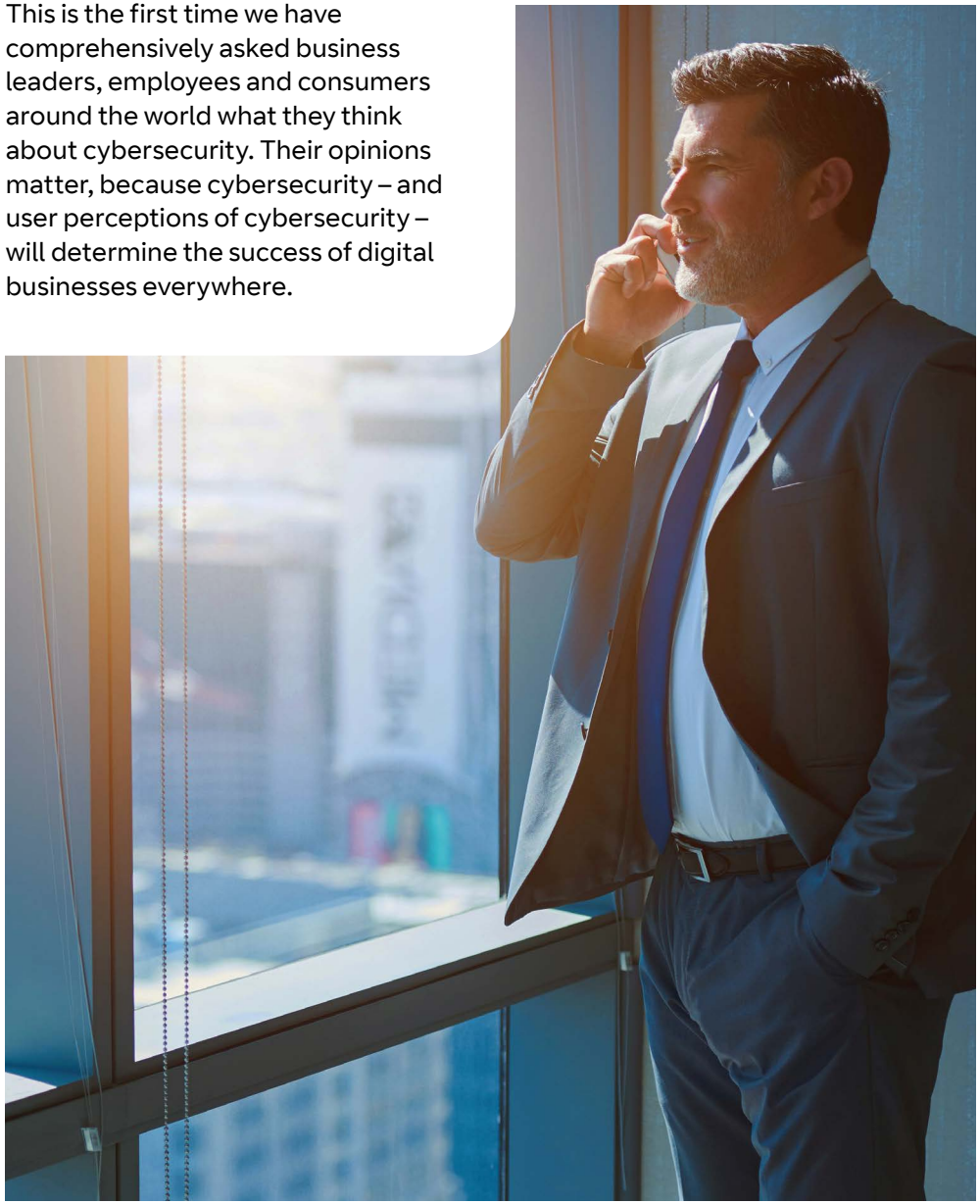
As well as providing examples of how the expectations and responsibilities of the CISO have evolved, this research also provides a number of recommendations around the clear steps you can take to better protect your organisation.

A proactive, forward-thinking approach to cybersecurity strategy is crucial for all organisations, big or small. We encourage you to turn these recommendations into action today.

Craig Jones
INTERPOL Cybercrime Director

Executive summary

This is the first time we have comprehensively asked business leaders, employees and consumers around the world what they think about cybersecurity. Their opinions matter, because cybersecurity – and user perceptions of cybersecurity – will determine the success of digital businesses everywhere.



We've uncovered five main insights.

1. First, while there's a general belief that organisations are operating securely, cybersecurity breaches are still an everyday occurrence. Why? Because too little attention is paid to basic cybersecurity measures.
2. Consumer behaviour doesn't help - people knowingly take risks online even though they understand the dangers. And that matters; how your customers behave day to day has huge implications for the viability of your digital products and services. The upside is that there is a real opportunity to make security a differentiator. Consumers value companies they perceive as more secure.
3. Happily, there's little resistance to greater security measures. Attitudes are maturing, people understand the scale of the problem. They recognise that more technology can help keep them safe. Two thirds of consumers now say security is more important than convenience. There's clearly a business case for investing in security measures and behaviours that enhance the employee or customer experience.
4. Human nature is part of the problem – and part of the solution. The fact remains that if you're only focused on technology, then you're missing the critical bit that is human behaviour. The easiest way to infiltrate any organisation is through someone who works there. We need to super-charge the human firewall.
5. CISOs have historically kept a low profile. Less than half of employees can put a name to their company's CISO. Yet without the expertise and leadership of the CISO, enterprises will struggle to achieve their digital transformation ambitions. Boardrooms now recognise that cybersecurity is their number one priority. They require CISOs to take a lead, to drive cybersecurity performance as a competitive advantage and help the enterprise take advantage of every digital opportunity. It's time for CISOs to take centre stage.

Insight one

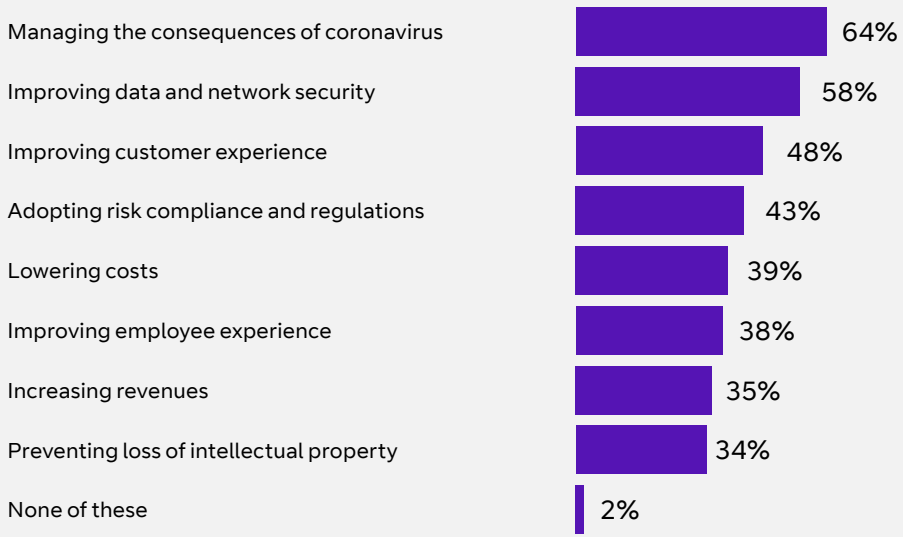
There's belief within enterprises that they are secure but that's not the full story: cybersecurity breaches remain at a dangerous level.

It's heartening to see that after years of encouraging businesses to prioritise cybersecurity, it has this year been ranked the main priority after the coronavirus crisis, ahead of customer experience, cost reduction and employee engagement.

Education by the IT industry and government has paid off. The likelihood and consequences of a cybersecurity incident are widely understood and executives appreciate the benefits of protecting data and networks.

Cybersecurity is now the number one priority for business leaders after the coronavirus crisis

Overall, which of the following has become more important for your organisation in the past year...



Confidence that the right security measures are in place is high

76%

of business leaders rate their organisation as excellent or good for protecting from cybersecurity threats

Four in five executives say their organisation's IT security strategy is strong and shareholders should be confident that the IT team has "done as much as is reasonable to be secure".

And yet. The evidence suggests that such confidence is misplaced. Eight in ten executives say their employer suffered a security incident in the last two years.

Of course, it's unrealistic to expect zero incidents but the uncomfortable truth is that cybersecurity breaches are still occurring at an unsustainable level.

Incidents continue to occur with great frequency

84%

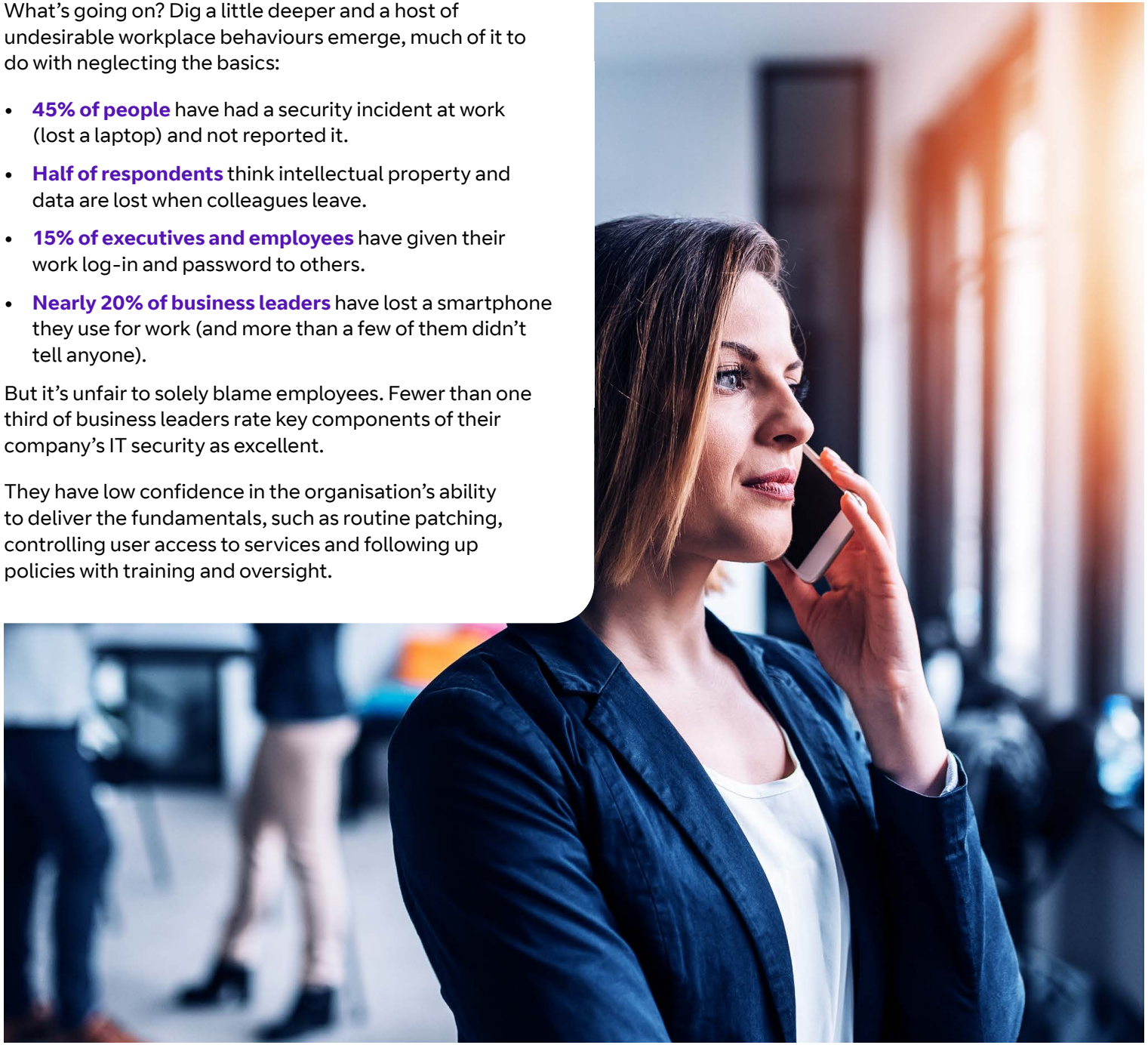
of executives say their organisation has suffered from data theft / loss or a network security incident in the last 2 years

What's going on? Dig a little deeper and a host of undesirable workplace behaviours emerge, much of it to do with neglecting the basics:

- **45% of people** have had a security incident at work (lost a laptop) and not reported it.
- **Half of respondents** think intellectual property and data are lost when colleagues leave.
- **15% of executives and employees** have given their work log-in and password to others.
- **Nearly 20% of business leaders** have lost a smartphone they use for work (and more than a few of them didn't tell anyone).

But it's unfair to solely blame employees. Fewer than one third of business leaders rate key components of their company's IT security as excellent.

They have low confidence in the organisation's ability to deliver the fundamentals, such as routine patching, controlling user access to services and following up policies with training and oversight.



This inattention to cybersecurity essentials will remain a drag on the business and its digital transformation ambitions.

It's the CISO's responsibility to fix it - and finding a specialist strategic partner for cybersecurity is part of the solution.

CISOs, think about:

- Prioritising basic cybersecurity measures: know your inventory and ensure routine software patching is never missed.
- Accepting that internal threat will always be with us. Take a 'Zero Trust' approach and establish controls that prevent carelessness.
- After a year of upheaval, many enterprises will be reviewing their business objectives. Use this opportunity to reassess your security strategy and policies to ensure they align with new boardroom priorities. The threat landscape is ever changing and architecture that was secure a year ago may now have vulnerabilities (especially in the wake of coronavirus and widespread remote working).

Insight two

Consumer behaviour doesn't help - people knowingly take risks online even though they understand the dangers.

Consumer cybersecurity behaviour matters to your business: how your customers act day to day has huge implications for the viability of your digital products and services.

It's not that people don't know the risks because they do. Two in three say life is riskier now than it was five years ago.

They accept the commercial deal: they get the digital services they value in exchange for their personal data.

Consumers are sceptical as to how safe their data actually is.

Only 16%

of consumers strongly agree they trust large organisations to protect their personal data

Although they worry about losing data or being hacked, one third still neglect basic hygiene such as updating software, clearing cookies and routinely resetting passwords.

Why are millions of people putting themselves at risk every day? Have they become de-sensitised, perhaps overwhelmed by the flood of security protocols and messages? Certainly, the answer is not more bureaucracy. A fair number of executives think it's unreasonable to expect customers to read long privacy and data contracts. Which they don't do anyway: a social experiment in the US found only 1% of technology users read the 'terms & conditions' of a contract.

The upside is that this is a real opportunity to make security a differentiator. Consumers value companies they perceive as more secure.

A business with clearly visible cybersecurity will reassure consumers and create confidence in its digital products and services, carving itself a competitive advantage.

There is a real opportunity to make security a differentiator

64%

of consumers say they would recommend a large organisation that they think makes a big effort to keep their data secure

CISOs, think about:

- What's customers' perception of your cybersecurity? How do you know?
- To what extent is your cybersecurity profile attractive to customers?
- How can you better communicate the measures you have in place to protect customer data?

People knowingly take risks even though they understand the dangers

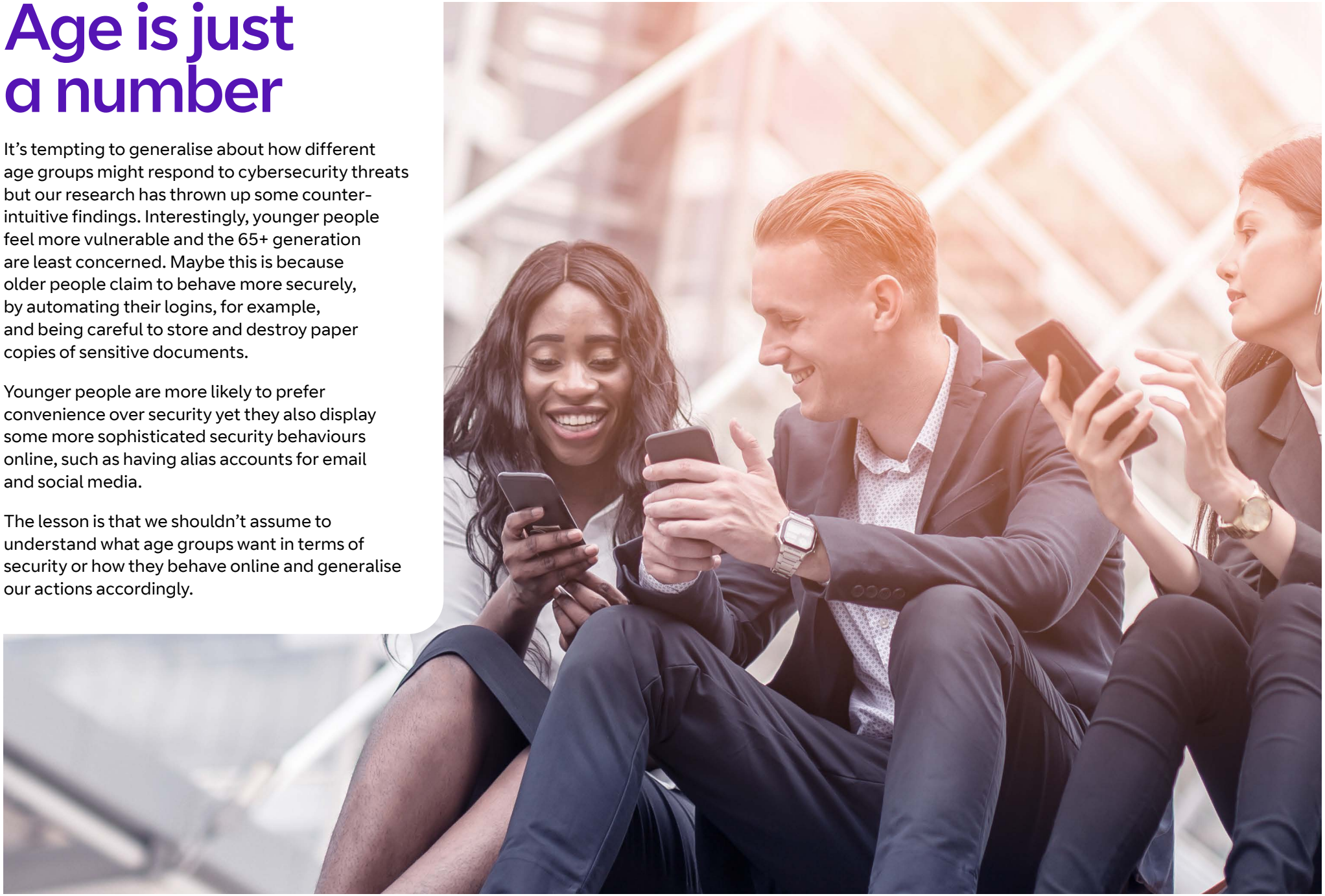
Consumers that say they forget or never...

Age is just a number

It's tempting to generalise about how different age groups might respond to cybersecurity threats but our research has thrown up some counter-intuitive findings. Interestingly, younger people feel more vulnerable and the 65+ generation are least concerned. Maybe this is because older people claim to behave more securely, by automating their logins, for example, and being careful to store and destroy paper copies of sensitive documents.

Younger people are more likely to prefer convenience over security yet they also display some more sophisticated security behaviours online, such as having alias accounts for email and social media.

The lesson is that we shouldn't assume to understand what age groups want in terms of security or how they behave online and generalise our actions accordingly.



Insight three

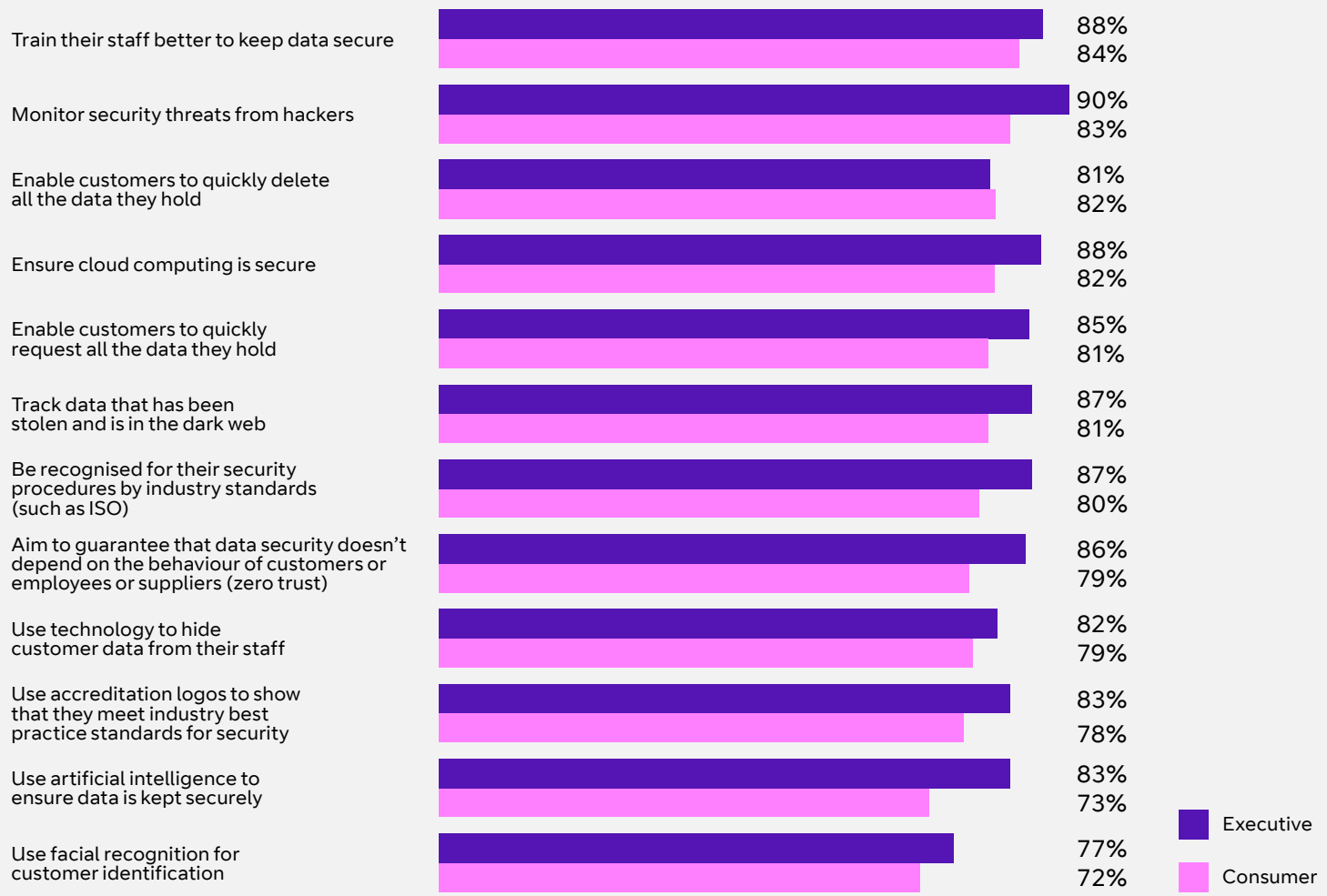
Good news: there's little resistance to greater security measures (as long as they don't get in the way).

Attitudes are maturing. People understand the scale of the problem. Three quarters of business leaders say there are more and more security threats every year. And two thirds of consumers now say security is more important than convenience. There's clearly a business case for investing in security measures and behaviours that enhance the employee or customer experience.

Today's digital citizens are open to greater cybersecurity measures, at work or play. Generally, we're more familiar with all sorts of new technologies and ready to welcome their deployment if it helps keep us safe online. Now more than ever, there's recognition that recent changes in working styles require a new approach - eight in ten executives say in the future working away from the office will become more important due to the coronavirus - and that current technology can be improved.

There's broad agreement on future focus

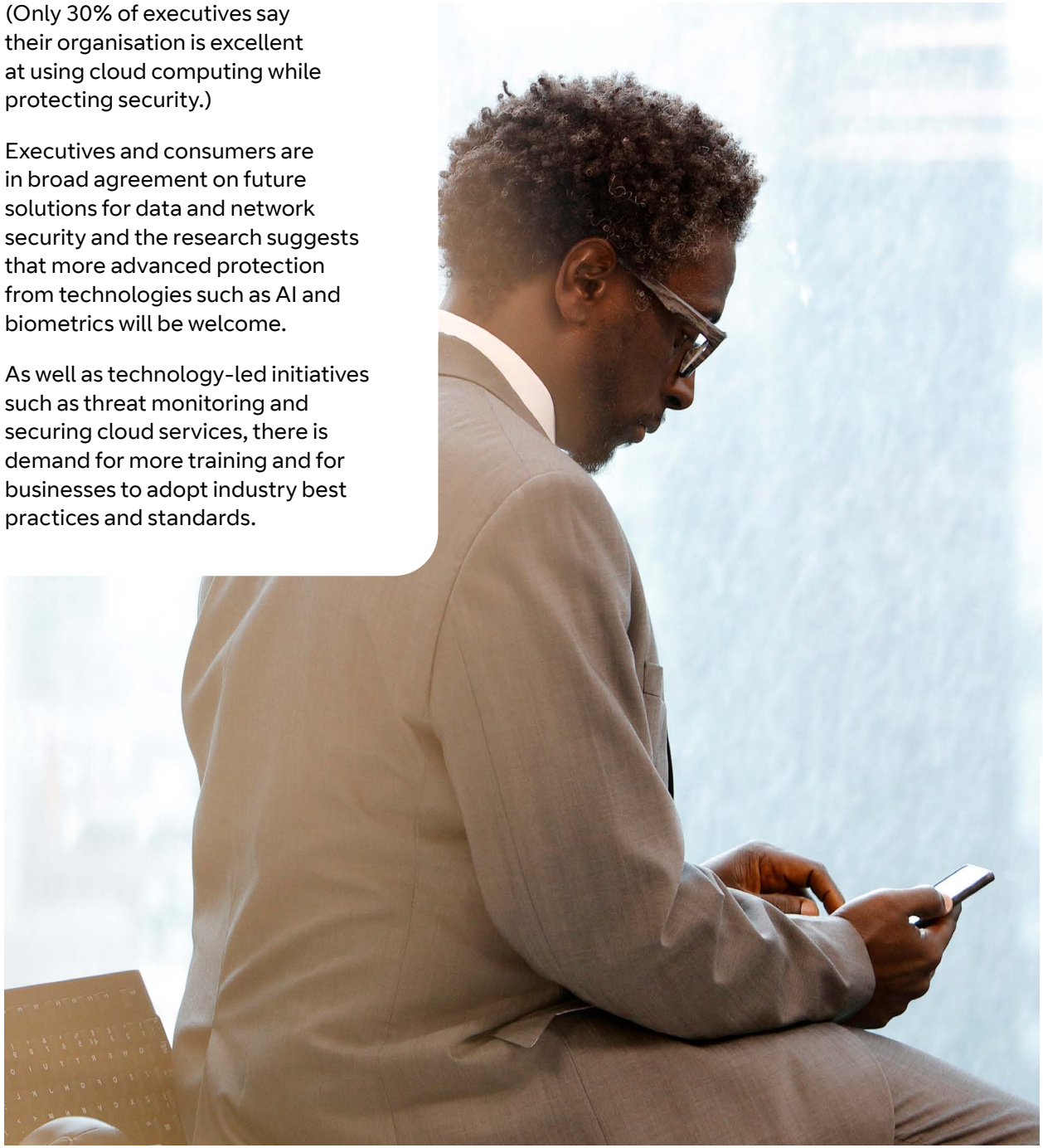
Should large organisations do the following to improve the security of their networks and data?



(Only 30% of executives say their organisation is excellent at using cloud computing while protecting security.)

Executives and consumers are in broad agreement on future solutions for data and network security and the research suggests that more advanced protection from technologies such as AI and biometrics will be welcome.

As well as technology-led initiatives such as threat monitoring and securing cloud services, there is demand for more training and for businesses to adopt industry best practices and standards.



Everyone understands the scale of the problem

75%

of executives say there are more and more security threats to their organisations each year

Attitudes are maturing

67%

of consumers say security is more important than convenience when dealing with organisations

CISOs, think about:

- Security measures shouldn't get in the way of letting employees do their jobs. Introduce authentication methods that don't require users to remember complex passwords.
- You can give users a better, more secure experience by adopting cloud services and a hybrid network.
- Artificial intelligence is an emerging technology you'll want to incorporate into your cyber defences. Start looking now at how you might deploy AI and identify the right partner so you can be off to a flying start.

Insight four

Technology can never replace the human firewall.

There are big gaps between policy and practice. Only...

29%

of executives say IT security is excellent at educating colleagues about the need for security

45%

of executives say they have definitely received training on data security

28%

of executives say IT is excellent at ensuring staff that leave don't take data with them

The fact is, if you only focus on the digital, then you'll miss the most critical element: human behaviour. The easiest way to infiltrate any organisation is through someone who works there. It's rarely malicious. People get distracted, make mistakes. It's human nature.

Executives are optimistic about what technology can deliver in the workplace but what users do, or fail to do, can defeat the best-conceived security policies and solutions. Attacks don't need to be sophisticated. Phishing emails that include 'LinkedIn' in the subject line have an open rate of almost 50%.

There are big gaps between policy and practice:

- Employees don't admit to mistakes. **Nearly half of employees** say they personally have had a security incident and not declared it. Ouch.
- **Only one in three** are 100% aware of the policies and procedures they should take to protect the security of their organisation's data and less than half say they have definitely received training on data security.
- **There's a lack of confidence in training** for new employees, and that steps are taken to protect data when people leave the company.

What this suggests is that it's time to power up and reinforce the human firewall. Employees need to understand that they are a key line of defence in securing their organisation.

This requires (a) providing education and coaching in how to behave safely online, (b) helping employees appreciate the impact a breach would have on the organisation and brand and (c) creating a culture in which it's OK to speak up, to admit mistakes.

CISOs, think about:

- The pandemic has magnified the need to deploy your human firewall. How easy is it for someone to confess to a cyber-error in your organisation? What's the process and the payback for reporting? To what extent do leaders in the business set an example?
- Building regular cybersecurity training into your year to reinforce good behaviours.
- One of the approaches we use at BT is to help our co-workers to understand the difference between fast thinking and rational thinking, and encourage them to take the time to consider their response or action.

Read more about our approach in this blog post.

Insight five

CISOs are under the spotlight: their expertise and leadership are central to the success of the digital business.

Business leaders say that their organisations are at more risk over the last year from a wide range of threats. But a CISO no longer just has to protect against threat and manage risk. Now, they have a major contribution to make to brand perception, employee engagement and the strategic adoption of new technologies.

Moving beyond threat management to trust and reputation building

69%

of consumers suspect that many more organisations lose customers data than gets reported and that there is more financial fraud than companies admit

The speed and scale of the digital transformation triggered by the global pandemic has underlined how security is a true enabler for business. It has also created the opportunity for a reset of the cybersecurity mindset, to better balance technology with the whole-hearted engagement of users, be they employees or customers. The CISO should lead this reset.

But leaders need to be visible. It's dispiriting that fewer than half of executives and employees can put a name to their CISO (or DPO). Would they be equally unknowing of the CFO, we wonder?

And whose fault is it that only half of executives say their colleagues will involve the CISO or IS security team when appropriate? If, of course, they know who to contact in the first place?

Enterprises urgently need to elevate cybersecurity leadership, processes and people to the first division. To this end, boards must ensure their CISO colleagues have the authority, the resources and the status to drive cybersecurity across the organisation and ensure that no-one is ever in doubt about how central it is to business success.

The days are gone when the role of the CISO was to maintain the security of the network and corporate data. Now the job is about protecting the enterprise against fast-evolving business risks so it can deliver for all its stakeholders. One way to step in the right direction would be to hand over routine security operations to a trusted partner, freeing up the CISO to champion the safe deployment of digital products, services and workspaces.

Security is at the top of the boardroom agenda. The door is open for CISOs to raise their profile and their voice, in the boardroom and across the organisation.

CISOs, think about:

- How you might leverage advisory services to help you prioritise and build a compelling vision for the future.
- Outsourcing day to day security operations to managed services can give you time and space to focus on wider business issues.
- Talking to a global managed security services provider about aligning your security challenges with your business outcomes.

CISO's are managing an evolving threat landscape as well as a widening remit

Executives say their organisations are at more risk over the last year from…

49% professional hackers trying to steal data

49% scammers cheating consumers

43% hacktivists with a political agenda

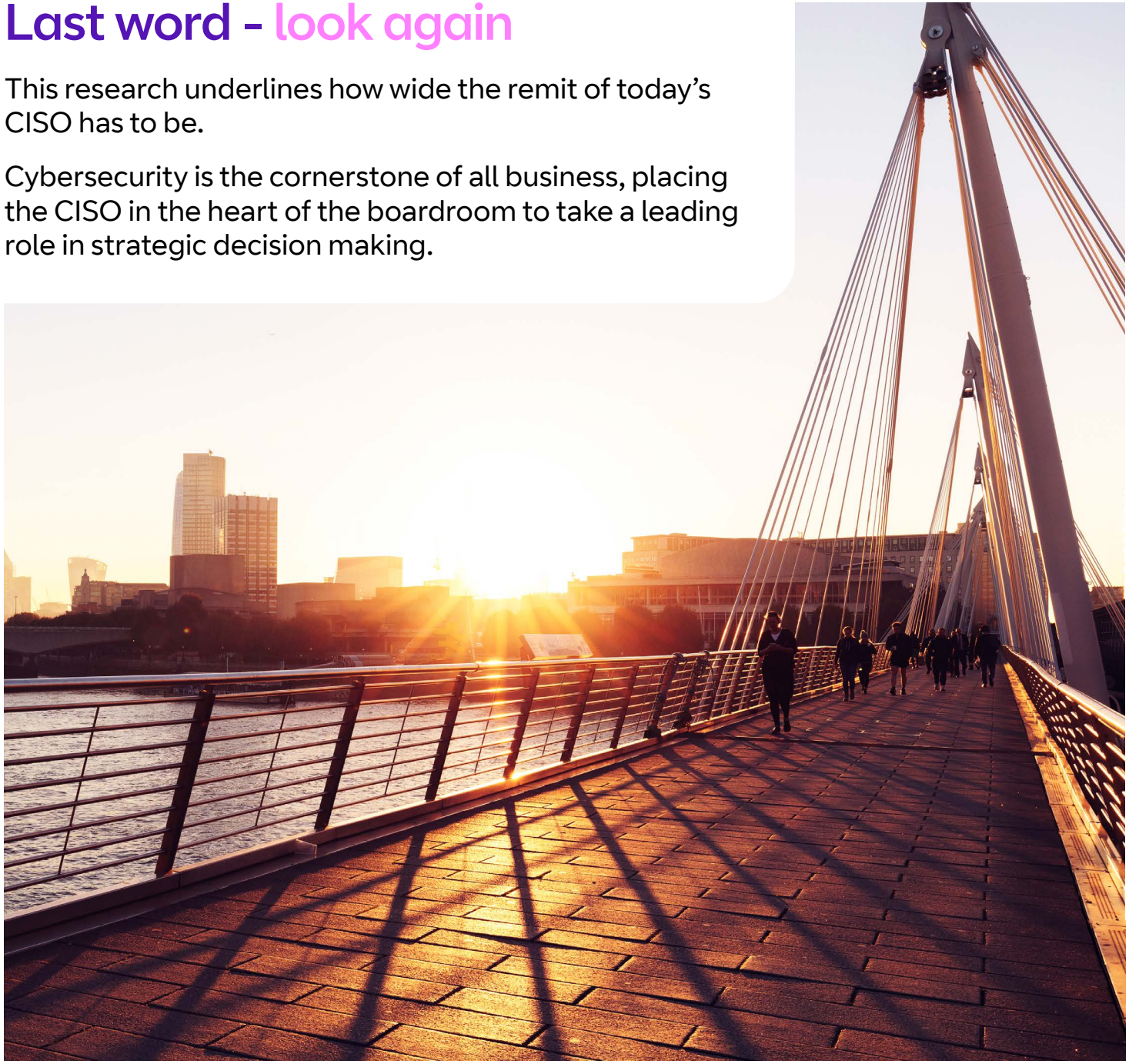
43% dark web selling organisations' data

23% customers making mistakes

Last word - look again

This research underlines how wide the remit of today's CISO has to be.

Cybersecurity is the cornerstone of all business, placing the CISO in the heart of the boardroom to take a leading role in strategic decision making.



It's understandable, that the reaction is to double-down, holding tightly to responsibilities, taking more control, spending more. But, in reality, the way through this challenge involves overturning this thinking:

1. Get the basics right
   Make them repeatable and reusable (like having pre-flight checks for aircraft).
2. Leverage automation
   Get smart about managing the uptick in alerts that comes with an increase in technology. Instead of trying to expand your team and continuing to use existing monitoring measures, re-look at your approach to automation to increase your vigilance. This will free you up to focus your energy on generating insights, motivating people and refining processes.
3. Expand partnerships
   Expand your ability to react through a considered, collaborative approach. Map your security team's strengths against your security requirements and bring in an external partner to bridge the gaps, so you can lead on your priorities and delegate supportive roles.

The CISO is the key to unlocking the future of security, so start exploring the possibilities today.

BT – a global security partner like no other

BT has an exceptional global security practice.

We have more than 3,000 skilled security experts and consultants globally. They are protecting governments and their agencies, national infrastructure, large global corporations and BT's own assets.

Our ringside seat at the world's global networks give us an unrivalled understanding of cybersecurity threats and performance around the world. With sophisticated tools and tradecraft, we can see what few others can.

Every day, we protect BT and its customers from 6,500 potential cyber attacks. With the data we collect and analyse, we can see further and learn faster. We've seen most things and we're often the first to spot new threats. While it might be a first for you, it certainly won't be new to us.

The depth of our expertise and the breadth of our knowledge means we have a pragmatic, not theoretical approach to cybersecurity. We can help you enhance your existing security measures and deliver world-leading protection for your business.

Research methodology

In September 2020, independent research company Davies Hickman Partners surveyed 4,016 consumers in eight countries (Australia, China, France, Germany, Hong Kong, the UAE, the UK and the USA, UAE) plus 715 business executives working in a range of sectors and roles. The employee data was derived from a 2,727 sub-set of the consumer respondents.

January 2021