In 2025, cyber security is both a challenge and a catalyst for growth – putting the CISO at the heart of business transformation. This report explores how the role is evolving to meet rising threats, new tech, and growing expectations, and how partners like BT can help CISOs turn risk into opportunity.

CISOs Under the Spotlight 2025

Cyber Security is everyone's business

August 2025

Foreword

A lot has changed since we last explored the CISO role four years ago, so now is a good time to take stock, assess the trajectory of threats, and get a sense of the direction of travel. This, we hope, will help bring new clarity to the ever evolving role against an economic, political, and technological backdrop that is anything but clear.

For many businesses, 2025 represents a crossroads. Artificial intelligence (AI) is fuelling new technologies used both for building up and breaking down cyber security, depending on what side of the fence the user sits on. Now is the right moment for businesses to revisit their cyber strategies and decide how they will move forward in light of the latest opportunities and risks.

We see customers considering how their investments in resilience can also fuel innovation and growth, keeping them ahead of the market. We call this being Cyber Agile: companies at every scale must take action to reinforce defences that not only protect them from online harm but also clear a path for experimentation, collaboration, and sales.

Now is the ideal time to laser-in on that main driver of cyber agility: the CISO. We want to know whether the role has changed, what new pressures they are under, what new responsibilities there are and, in general, how the priorities and focus of CISOs have changed in the last couple of years.

Our view is that it is an increasingly vital role within organisations. The job description, handed down from leadership but also influenced by CISOs themselves, is expanding with CISOs taking on new responsibilities to keep organisations safe. CISOs' seat at the boardroom table is all but guaranteed because of the increasingly strategic dimension of their role.

But along with the changing nature of the job, we see them navigating a new competitive environment, global regulatory changes, emerging technologies, and pressure to recruit, retain, upskill and engage the best, most appropriate people to safeguard security.

Add to these widespread macro trends, such as staff returning to the office, the rapid adoption of artificial intelligence, the swelling demand for interconnectivity and the seismic impact of global political change.

It goes without saying that all this is taking place under the umbrella of a complicated and morphing risk matrix. Such is the sophistication of new threats that an organisation-wide response is the only answer, with employees taking accountability for their own security and not relying solely on dictates from higher up in the organisational hierarchy.

Organisations should also connect with expert third parties capable of providing the best technology and advice to help get the job done. After all, cyber security is a team sport, and we are on your side.

We think it's an exciting time for CISOs; they're in the perfect position to drive positive change within their organisations, bringing the wider team along with them. With help from partners like BT, CISOs can make the most of the cyber agile approach, enabling transformation and addressing risks while freeing up capacity for individuals and teams to hit targets and drive growth.

Tris Morgan
Managing Director, Security, BT

About the study

CISOs under the spotlight is based on a global survey of:

827 business and IT executives at organisations employing more than 1,000 people across eight countries

4,036 consumers and 2,413 employees across eight countries

Respondents were from a range of industries, roles and demographics in eight markets: the UK, Ireland, Australia, France, Germany, Singapore, UAE and the USA.

Executive summary

Since our last CISOs under the Spotlight report, Chief Information Security Officers have experienced considerable change. They are increasingly likely to sit on the board, upskill employees and partners, and shape the organisation's future vision by building trust in new technologies. These three focuses enable CISOs to lead by example while protecting the organisation from attacks.

A seat in the boardroom

The last four years have seen many CISOs promoted to a seat on the board, thanks to a greater understanding of IT priorities at the senior executive level. Our research shows that CISOs have become the custodians of trust, responsible for making good on security promises to customers and fellow employees alike.

It's working: there was a steep increase between 2020 and 2024 in executives who think their board has the right knowledge and strategy to protect their IT security, rising from 60% to 73%.

Skills in the picture

Another growing aspect of the CISO role is ensuring executives and employees are adequately trained, a key part of building cyber agility within an organisation. This is reflected in the growing number of executives who say they've received data security training in the last year, hitting 53% in 2024, up from 46% in 2020, but there is still much more progress to make.

However, there is still evidence of the ongoing skills shortfall, with just under half (49%) of IT executives claiming a lack of resources and skills gaps were a 'main barrier' to the cyber resilience of their organisation.

Future focus

Pressure is building on CISOs to safeguard their organisations from the complicated challenges that AI brings. More than a third (37%) are 'very concerned' about AI-related data leaks, while 33% are very concerned about augmented attacks on cyber infrastructure.

But technology will also play a part in repelling threats and dealing with the consequences. For example, more than six in 10 CISOs in our study (61%) said AI will help them monitor threats as they arise.

Achieving CISO best practice is getting harder; it's more complicated with a broader, changeable brief; meaning modern CISOs are on a never-ending learning curve, requiring them to be agile, responsive and receptive to change.

By adopting the best tools, systems and principles, your organisation can steal a march on the competition and grow faster, potentially establishing a stronger foothold in your market and a platform for further advances. There's no better time than right now.

Contents

Part One | The evolving environment for CISOs 2020-2024 6

Part Two | CISOs build trust as risks evolve 11

Part Three | Educating employees, suppliers and consumers 14

Part Four | A host of future challenges 18

Conclusion | The CISO's moment to lead 21

Appendices | 23

Part one

The evolving environment for CISOs 2020-2024

An uplift in IT security capability

In the past four years, CISOs oversaw an increase in awareness, skills and technology – all part of the solution to address increases in cyber crime. This is in evidence organisation-wide, not simply confined to the IT department, as non-tech leaders embrace the benefits of cyber security and the pitfalls of a lax approach.

More generally, this has led to growing confidence in IT leadership among employees. There was a large uplift between 2020 and 2024 in executives who believe their board has the right knowledge and strategy to protect their IT security, rising from 60% to 73% in just that four-year timeframe.

This was partially due to a greater understanding of security protocols across organisations. The proportion of executives saying they're '100% aware' of the policies and procedures expected of them to protect their organisation's data also rose by around a quarter, from 39% in 2020 to 49% in 2024.

This statistic chimes with the growing number of executives receiving data security training, reaching 53% in 2024 compared with 46% in 2020.

Preparedness has increased too, with 43% of those who experienced a data breach in the previous year saying they felt prepared, while one in three execs say their organisation uses AI to track data and its usage.

The downside for CISOs is that a growing number of employees think increased security precautions make it harder for them to do their jobs, perhaps because of the extra hoops they must jump through to log in and get going with systems. Despite attacks still having a major impact on businesses, in 2024 more employees said security 'gets in the way', 15% in 2024 versus 13% in 2020.

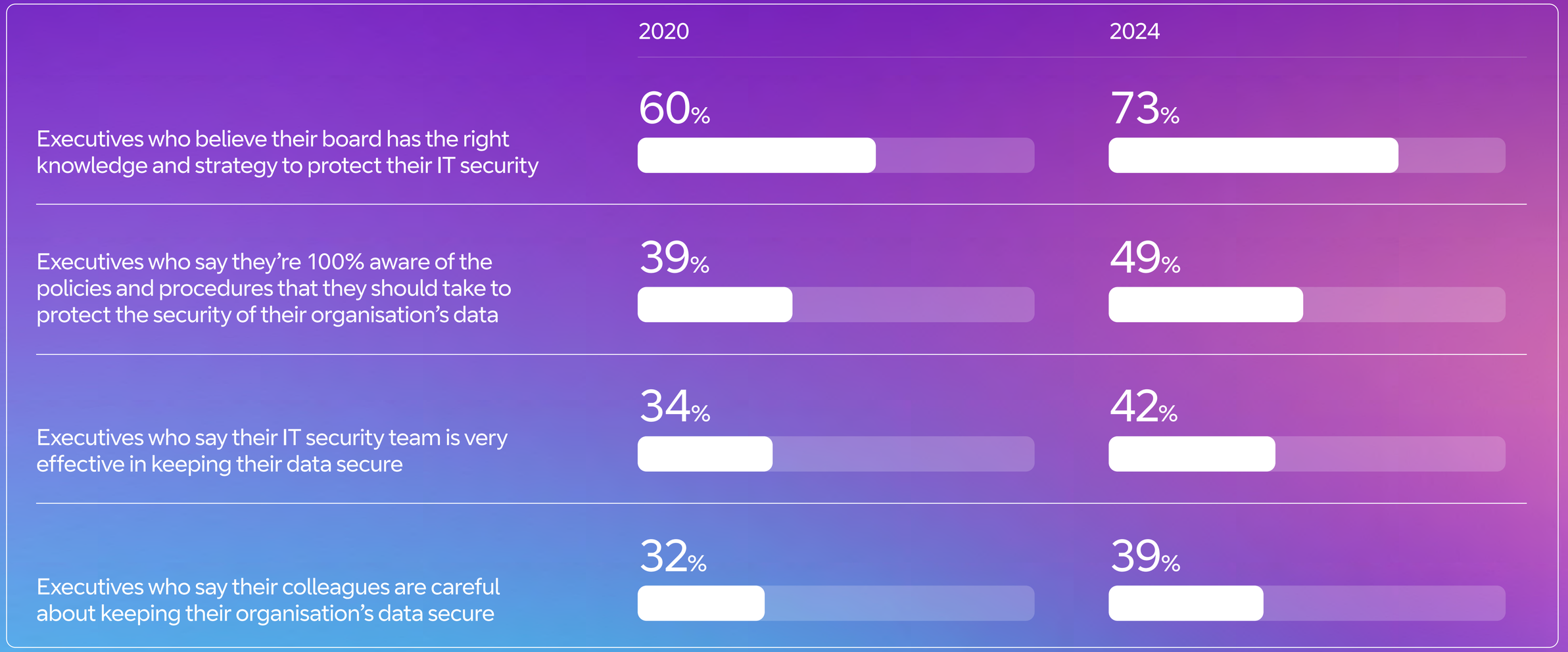
Contents

"CISOs have ever increasing and evolving levels of accountability. Their responsibilities extend way beyond the traditional IT security aspects of infrastructure and systems, to the human aspects of securing organisations. For example, ensuring everyone has the required levels of security awareness and knowledge with regular and relevant training. And one of the CISO's biggest challenges is how to achieve balance between employee agility and empowerment versus ensuring a secure environment and set of behaviours."

Iain Logan
Director of Cyber Operations, BT

CISO cyber security uplift 2020 - 2024

Contents



Contents

Security breaches still shocking organisations

Executives feel more prepared for cyber attacks, but this hasn't reduced the damage inflicted on organisations when attacks are successful. With security threats rising year-on-year, and the number of devices and network connections also on the rise, CISOs must manage a broader attack surface.

Often it can take days, even weeks, to recover from attacks, a sobering thought given the 28% of executives who said their employer suffered compromised data through an attack in the last year alone.

The ability to get back up and running after an attack is a key tenet of cyber agility, yet, of those who experienced a breach, just 42% said their organisation was 'extremely prepared', while 15% of businesses took longer than a week to recover.

This is why operational resiliency is becoming an essential part of a CISO's toolkit.

It's a change compared with four years ago, when the focus was on the organisational 'security fortress' – now there is increasing investment in minimising the impact of an attack and bouncing back quickly when it happens.

This is where resiliency and awareness come into play, as CISOs must manage various strategies and mitigation measures to ensure they're ready to respond to attacks if, or when, they happen.

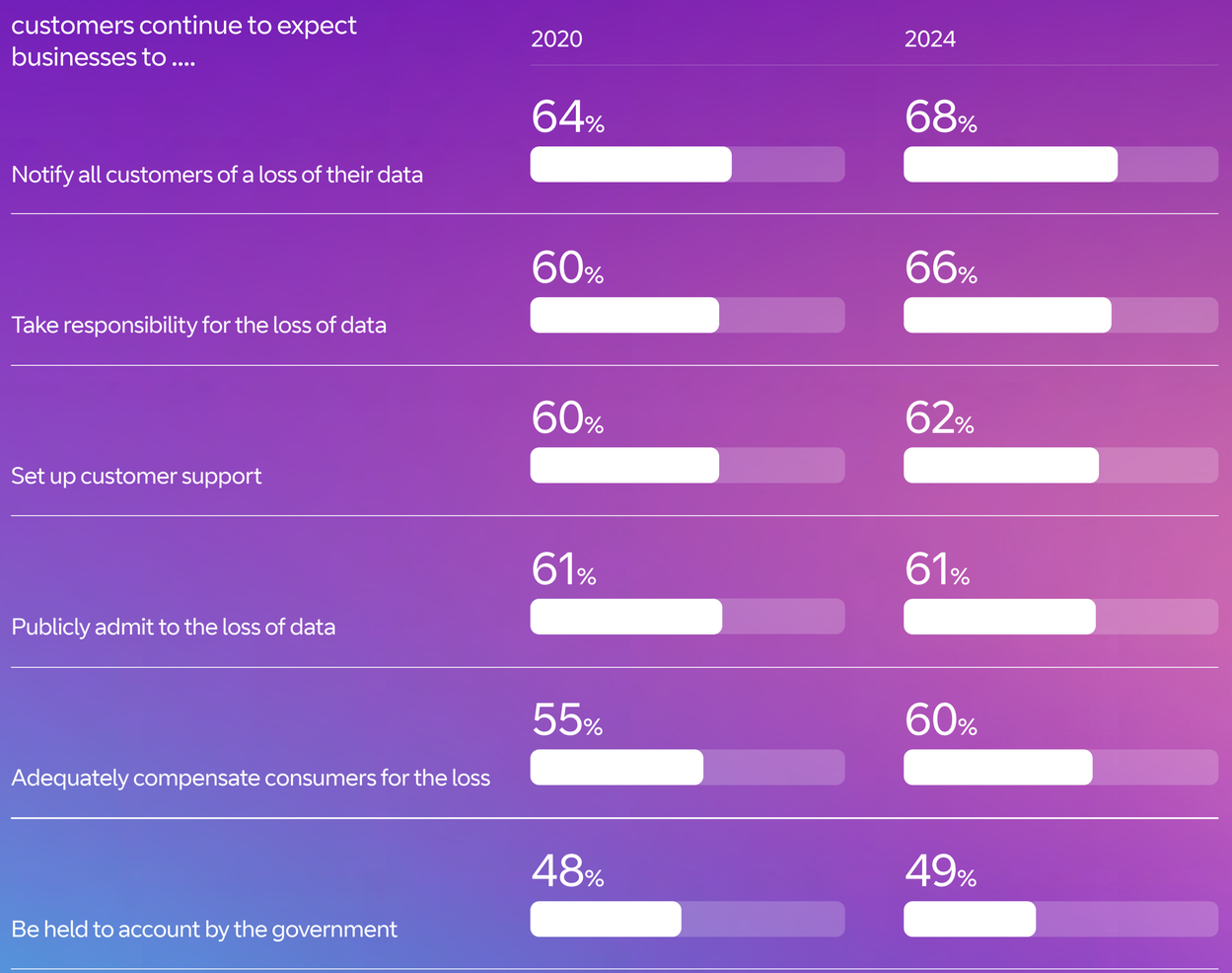
Customers want more accountability

With cyber attacks becoming more destructive as sophistication increases, customers increasingly expect organisations to act quickly, decisively and with resilience following a data breach. Top expectations include notifying customers, with 68% pointing to this in 2024 compared with 64% in 2020.

Two-thirds (66%) want companies to take responsibility for loss of data, versus 60% in the previous study. There was also a small increase in expectations of businesses being held to account by the government, cited by 49% of customers, up from 48% previously.

Contents

Customer expectations remain high



Part two

CISOs build trust as risks evolve

Trust is on a tightrope

With the turbulent security landscape, diversity of tech tools and sophistication of scams, many customers are warier of their cyber risk than ever before. Trust is declining as attacks rise, obliging CISOs to lead the process of building back confidence among employees, customers and the supply chain. They must lead organisations by developing procedures, systems and protocols that build and maintain trust. This is a fundamental attribute of cyber agile resiliency.

When consumers were asked about the top benefits to large organisations of keeping their networks and data secure, 47% said it was building trust with customers, up from 38% in 2020. This was by far the biggest proportion of respondents. In second place was ‘avoiding brand damage’, quoted by only 12% of respondents, unchanged from four years before. In third was ‘being part of the fight against organised crime’, from just 11%, down from 15% in 2020.

On the other side of the coin, 85% of executives say losing customer trust is the top concern following a data breach. But, despite their fears, this problem isn’t going away. Between 2020 and 2024, there was a slight increase in the number of consumers saying they noticed reports in the media of organisations losing customer data (58% vs 56%).

When asked the main reason why large organisations are hacked or lose customer data, 54% said it was because they hadn’t invested enough or kept systems up to date, slightly down from the 58% who said the same in 2020.

Conversely, there was a marked increase in the number of respondents pointing to hackers getting better at attacking organisations, up from 28% in 2020 to 35% in 2024. The findings underline the importance of organisational resiliency, mapping out protocols not just to prevent attacks, but to recover quickly and as painlessly as possible if and when an attack is successful.

Contents

A trusting foundation

47% According to consumers, the most important benefit for large organisations if they keep their data and networks secure is building trust with customers

85% of executives say losing trust is the top concern of a security breach

58% of consumers notice reports in the media of organisations losing customers’ data

Customers feel more vulnerable

Consumers report feeling that life is riskier than it was five years ago, and trust in organisations is low, with 74% believing there is more financial fraud committed by organisations than is currently reported publicly and 71% saying the same about customer data loss.

Technology and data are two areas of particular concern for respondents, 57% of which do not feel secure about AI and 50% are unconvinced about organisations keeping data safe online. Surprisingly, perhaps, 39% admit to being wary of technology in general.

Some 78% of consumers think hackers are able to find out almost everything about individuals if they want to, a fear which has led to questions about personal details held by businesses. The same number believe more people will want to know where their personal data sits and what it is used for.

Consumers are savvy to the threat, but less so to the remedies. More than three-quarters (76%) say they care about personal data but don't do enough to keep it safe, and some 68% think national infrastructure is at risk from cyber attacks by foreign states and terrorist organisations.

Contents

"A cyber attack can knock customer trust back to square one – and regaining that trust takes time, consistent effort and tangible results. CISOs play a crucial role in building and maintaining customer confidence. In an ever-evolving digital world, which can feel unpredictable, their leadership helps customers to feel safe and reassured."

Yasemin Mustafa
Cyber Security Portfolio Director, BT

Part three

Educating employees, suppliers and consumers

Educating employees, suppliers and consumers

Regardless of whether CISOs put in place the best policies and procedures, it is the responsibility of the business as a whole to keep an organisation's data secure. Cyber agile organisations empower their employees to be the first line of defence, so it's important to equip people with appropriate training.

For those that don't, the level of risk remains higher than it needs to be. Organisations recognise that insufficient training means employees stand a greater chance of losing data via simple errors, while consumers put themselves at risk if they neglect to take their own data security seriously.

It's clear from the data that as a society, we all need to keep the focus on good security practices. For example, there was a marked decline in the proportion of consumers using passwords in 2024 (54%), compared with 2020 (61%), although some of this is likely due to the rise of other forms of security, such as biometric data.

But those taking basic protective measures also fell, like covering their PIN at an ATM, down to 50% from 56% in 2020 – although perhaps also tied to the decline in ATM usage – while shredding documents with personal details on them and ensuring software is up to date both fell to 40% vs 47% in 2020.

For organisations to become cyber agile, it's crucial to build awareness, enrol employees in rigorous training programmes and ensure strong lines of communication between teams.

> The employee network should be the first strong barrier to prevent attacks and help alleviate any single point of responsibility on the CISOs.

Employees are making as many errors as ever

The number of employees admitting to making simple security errors in the workplace and beyond has remained broadly static. Some 11% had given their work login and password to others at their work, down slightly from 13% in 2020, but 8% admitted failing to declare when they lost organisational data, up from 7% four years before.

This data is a little anomalous when contrasted with the above findings about skills provision and executives' high level of confidence in the management of cyber security in their organisation. An obvious next step for CISOs is to discover why mistakes continue, despite wider awareness, and take steps to minimise them.

Transparency needed over suppliers

Supply chains are an area of concern for CISOs. More than one in four executives (27%) said a supplier had reported a data theft or loss, or a network security breach, in the last two years alone. Just 56% said this had not happened, while 16% weren't sure.

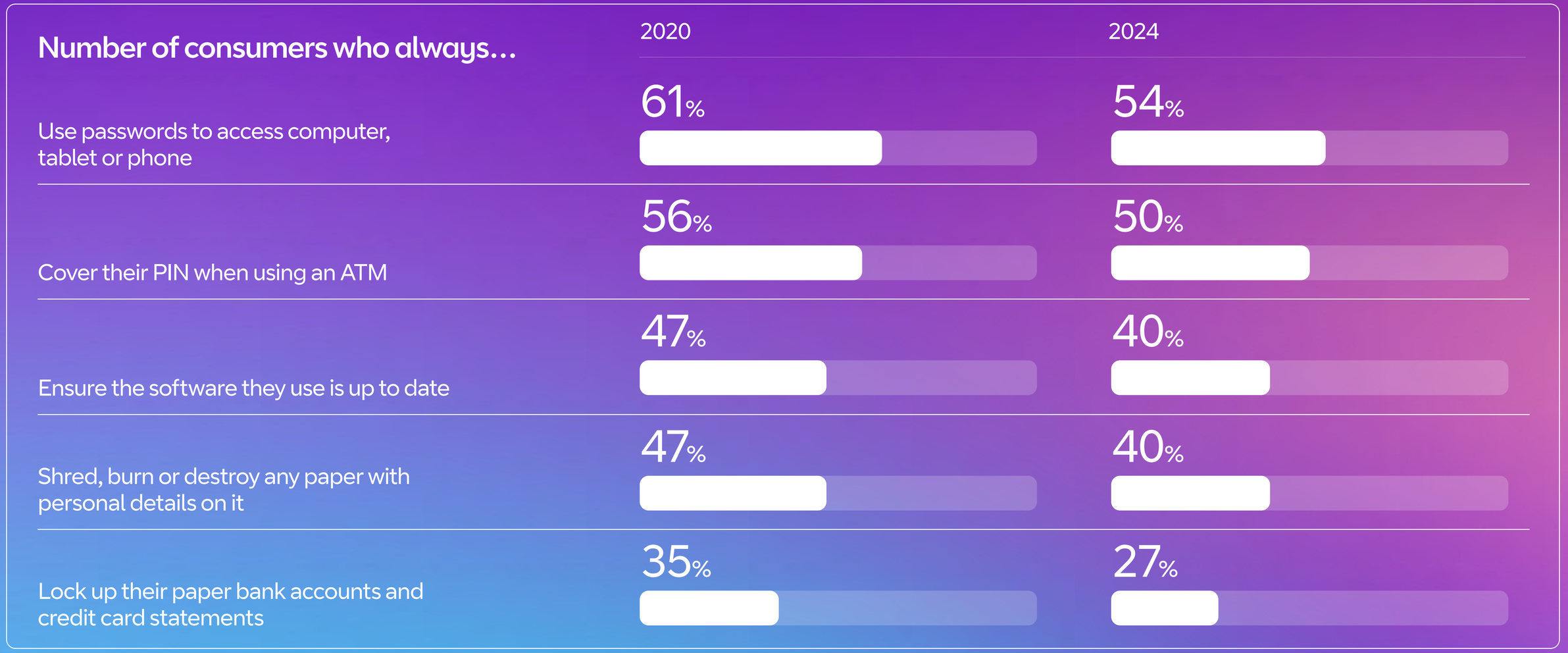
Despite this, security coverage remains patchy, with just 74% of global enterprises having a firewall, 66% having anti-virus software and 62% having network security solutions.

Contents

> "The safety of an organisation is not the responsibility of just one job role. While CISOs enable transformation, a lot of real change stems from training and upskilling everyone around them, giving them the space to enact their all-important role."

Lee Stephens
Director of Security Advisory Services, BT

Consumers are not prioritising safety



Part four

A host of future challenges

A host of future challenges

Rapid technological advancement brings new opportunities, but not without challenges. AI helps to monitor security threats and improves resiliency, but it can also be the root cause of data leaks and breaches, so it's important to ensure employees have the right skills to prevent or respond to the latest threats. Even more so with hybrid working, which extends an organisation's attack surface to the homes of employees and adds an additional layer of complexity for the CISO.

AI is a blessing and a curse

AI is both an area of concern and a centre of opportunity for CISOs. While 70% of executives are concerned about AI-related data leaks, 61% say new AI will help them monitor threats.

Other fears relate to augmented cyber attacks (69% concerned), the advance of phishing, malware and deepfakes (68% concerned) and AI-disseminated disinformation in large volumes. To control these risks, it helps that 69% of IT executives have a zero-trust policy, although 24% do not and 6% don't know either way.

Ongoing skills shortfall warning

While 59% of executives receive regular training to keep data secure, just under half (49%) of IT executives said a lack of resources and skills gaps were a 'main barrier' to the cyber resilience of their organisation, while a further 36% pointed to a potential lack of executive support and 30% added that 'not knowing where to start' or understanding 'best practices' were significant barriers.

The good news is that more executives understand their role in keeping their organisation safe, with 47% believing they are primarily responsible for keeping data secure, 32% claiming it is the responsibility of the IT department and 22% saying responsibility is shared.

Half of executives say they have definitely received data security training, while 31% said this was probably true.

Almost the same number, 47%, said they definitely were aware of all the policies and procedures to protect organisational data, and just 39% claimed their IT security team was very effective at keeping data secure.

Main barriers to cyber resilience according to IT executives

Resources and skills gaps	49%
Cost of transforming legacy systems and processes	41%
Executive support	36%
Cultural resistance to change (leadership or employees)	34%
Not knowing where to start and/or what best practices are	30%

New working practices cause concern

While we see impetus in some sectors to return employees to the office, hybrid working remains the norm, embedded in the expectations of workers across industry.

Just 46% of executives work in their employer's office every day, while almost the same number (44%) work between two and four days per week. Despite this, only 25% rate their employer as excellent for setting up apps to secure remote working environments.

A similar number, just 24%, rate their organisation as excellent at letting employees work from anywhere on mobile devices but protecting them from identity misuse and endpoint threats.

When it comes to technologies that are potentially useful for cyber security, AI and machine learning were cited as increasingly important by 51% of IT executives, while 39% said the same about cloud infrastructure entitlement management, the same number about operational technology security and 37% about digital risk management.

> "AI is a game-changer in the race to build cyber security defences. Automated threat detection, planning and response can significantly enhance security measures. But it's not without its challenges, so CISOs must exercise caution when introducing new practices, especially when rolled out to the wider workforce who may not be as aware of the dangers."

Colin Bannon
Chief Technical Officer, BT

Conclusion

The CISO's moment to lead

Conclusion

As we have seen, CISOs are working through a period of fundamental and profound change, encompassing the work they do and the world they occupy. New essential aspects of the CISO role became embedded in the last few years, including the responsibility to establish and maintain trust in digital systems, not just within organisations, but also across the customer base and down the supply chain.

In this volatile climate, CISOs are prioritising the search for the right solutions, now and in the future. As our research shows, there's plenty of work to be done to shore up organisations, so now's the time to move the dial and strive for action.

CISOs have made a solid start when it comes to equipping executives with a broader skillset to defend against – and recover from – cyber attacks.

We believe an increased focus for the next four years will be turning education into action, ensuring the right skills are shared among everyone within the organisation, while safely and securely introducing new technologies such as AI. These focus areas will help CISOs build their boardroom presence by continuing to be a strategic part of the business.

At BT, we strive to be a strong ally to CISOs. This is why we develop our skills across network and security solutions to support customers where they need to outsource managed services. But essentially CISOs need us to be a dependable partner, to support their bid to ensure security is an enabler to their business growth.

Our recent report, the Cyber Agile Organisation, gives a wealth of guidance on how organisations can become more secure without encumbering growth, finding the perfect balance to move forward without fear and tackle challenges head-on. The cyber agile framework, six key dimensions of cyber agility, helps you not only discover your place on the cyber agility spectrum but also find out what you need to do for your organisation to improve.

By adopting the best tools, systems and principles, your organisation can steal a march on the competition and grow faster, potentially establishing a stronger foothold in your market and a platform for further advances. There's no better time than right now.

Get in touch

1. BT can help CISOs and other security professionals to carve out areas of opportunity as well as protect against threats. To understand your organisation's current position on cyber security, analysing the six pillars of cyber agility can be a useful starting point. For more on how to become cyber agile, check out the **Cyber Agile Organisation report.**

2. We'd love to discuss the findings in this report, contact your account team or security.advisory.services.uk@bt.com.

3. If you'd like to go deeper, assess and understand your risk in detail, our Security Advisory team can work with you to build a more comprehensive assessment of threats, risks, what needs protection, your current security controls, policy, process and more – all aligned to one of the key frameworks.

We've got your back

Appendices

About BT

BT Group is the UK's leading provider of fixed and mobile telecommunications and related secure digital products, solutions and services. We also provide managed telecommunications, security and network & IT infrastructure services to customers across 180 countries.

BT Group consists of three customer-facing units: Consumer serves individuals and families in the UK; Business covers companies and public services in the UK and internationally; Openreach is an independently governed, wholly owned subsidiary wholesaling fixed access infrastructure services to its customers - over 700 communications providers across the UK.

British Telecommunications plc is a wholly owned subsidiary of BT Group plc and encompasses virtually all businesses and assets of the BT Group. BT Group plc is listed on the London Stock Exchange.

For more information, visit www.bt.com/about

Disclaimer and acknowledgements

The research was carried out by BT and Davies Hickman Partners in 2024. The report was developed by BT and thought leadership consultancy, Man Bites Dog.

To find out more about BT’s security offerings, visit **bt.com/security**

August 2025