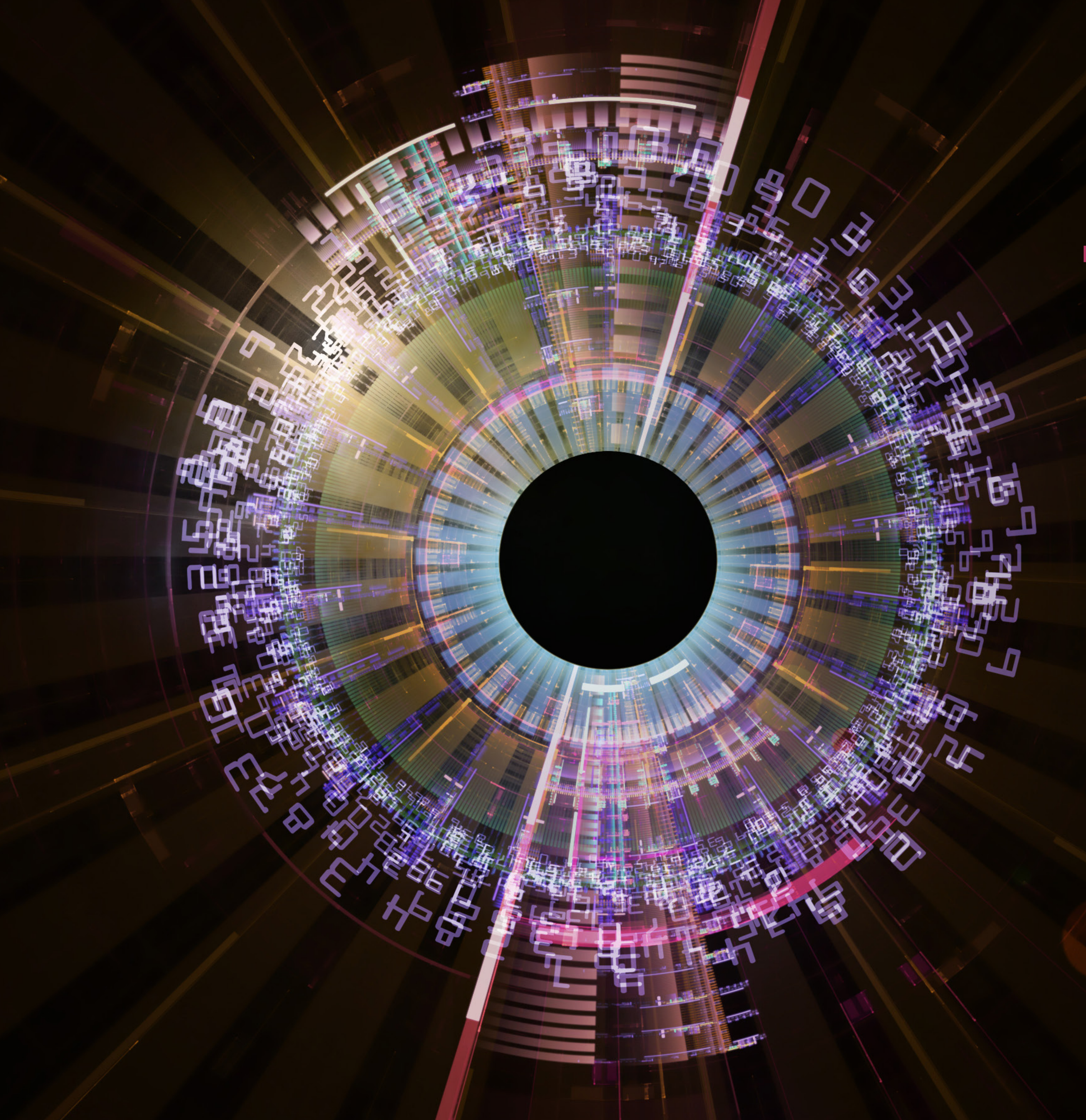


THROUGH THE CYBER LENS:

CYBER SECURITY'S EVOLVING FUTURE

Gemserv®

A Talan Company

A WORLD WHERE CHALLENGE AND CHANGE ARE CONSTANTS.

We live in a world of heightened geopolitical risks, from the conflicts in Russia-Ukraine and Israel-Hamas to precarious US-China relations and widespread economic slowdown, with the latter driving localised political tensions. Against this backdrop, cyber attacks have become more sophisticated, severe and frequent. The daily working of governments and their agencies, vital infrastructure such as healthcare services and corporations of all sizes are under threat. The UK's National Cyber Security Centre (NCSC)[1] has reported that more than **7 million** suspicious emails and websites alone were reported to authorities last year, equivalent to one every five seconds.

At the same time, more and more of our daily services and processes are being digitised, increasing their potential exposure to risk and demands for cyber resilience. More vital data and information is being gathered by more organisations and stored in the cloud. The growth in hybrid and flexible working in the wake of the pandemic is creating fresh challenges for organisations in maintaining cyber vigilance remotely.

The chief information security officer (CISO) has to respond to the challenges of this complex and fast-evolving environment, maintaining the security of nations, organisations and citizens. They are working within a technological environment that is itself changing dramatically, with this year notably bringing the leap forward in artificial intelligence (AI) in the launch and uptake of Generative AI powered language model, ChatGPT. This field of innovation is bringing both opportunities and new cyber risks.

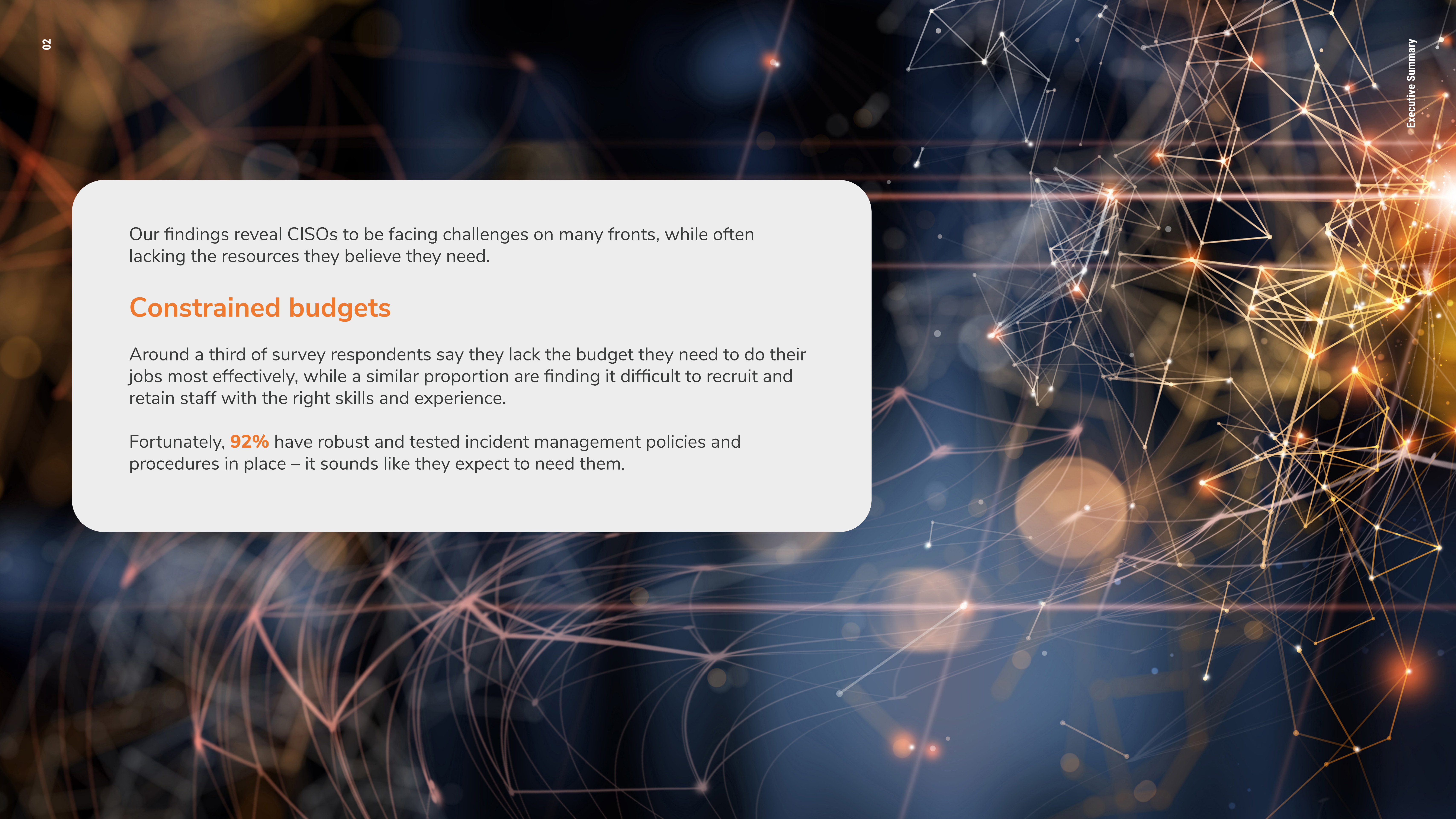
For the first time, Gemserv has commissioned a survey of CISOs to gauge their perceptions and experiences. Our survey, carried out in September 2023, looks at how well equipped CISOs felt to address their challenges - specifically those arising from AI innovation - and seeks to understand their expectations for the future.

To find out more contact BD@gemserv.com

[1] - Source: https://www.ncsc.gov.uk/news/british-business-support-crucial-in-removing-scams

01

Executive Summary



Our findings reveal CISOs to be facing challenges on many fronts, while often lacking the resources they believe they need.

Constrained budgets

Around a third of survey respondents say they lack the budget they need to do their jobs most effectively, while a similar proportion are finding it difficult to recruit and retain staff with the right skills and experience.

Fortunately, **92%** have robust and tested incident management policies and procedures in place – it sounds like they expect to need them.

The need for resourcing

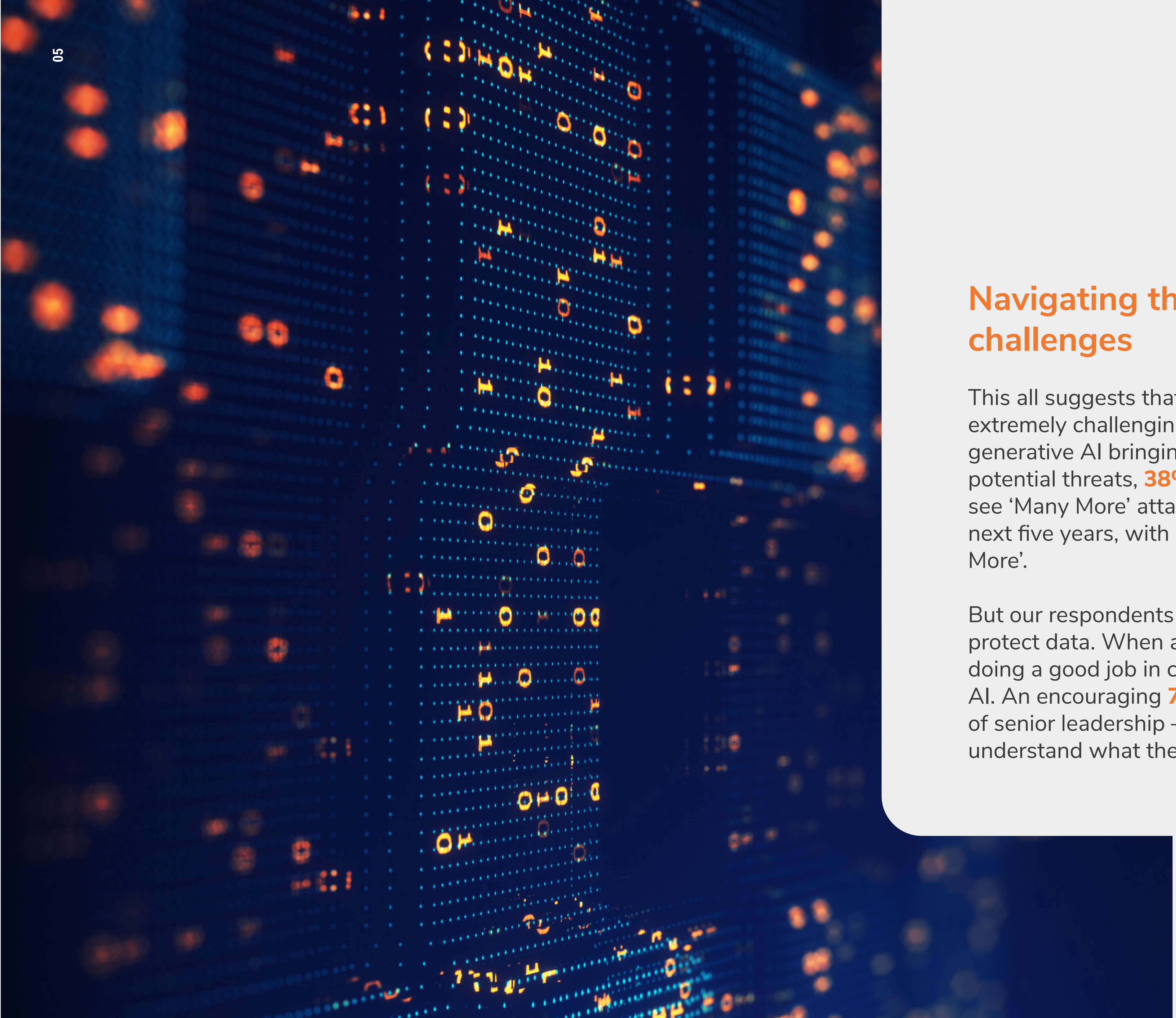
Cyber and privacy consultants can be doing more to support their CISOs. Only **19%** of CISOs rate cyber threat intelligence providers as ‘Excellent’ at providing clear, actionable and prioritised information. Privacy professionals fare slightly better, with **23%** of CISOs rating them as ‘Excellent’.

These communication deficiencies may partly explain why only **37%** of CISOs say their senior leadership have an ‘Excellent’ understanding of cyber security and privacy.

Technology & knowledge gaps

Our findings reveal clear technology and knowledge gaps that should give cause for concern. Only **31%** of survey respondents say they have both security information and event management (SIEM) tooling and cyber threat intelligence, and yet **78%** expect the cyber threat landscape to become more complex and challenging over the next 12 months.

In all, **83%** of respondents expect generative AI to be implicated in more cyber attacks, but only **16%** rate their organisation's understanding of these tools as excellent.

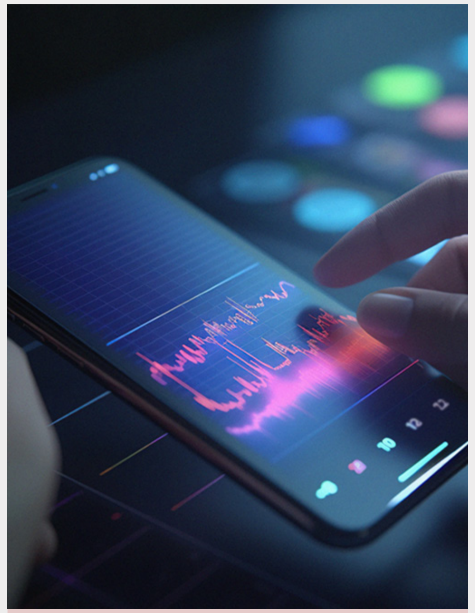


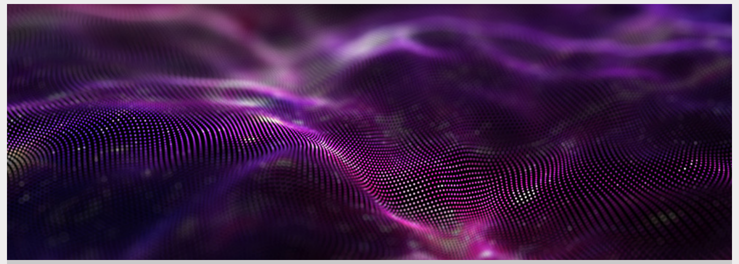
Navigating the AI landscape & other challenges

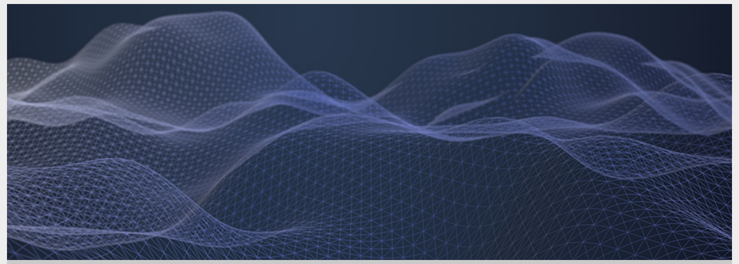
This all suggests that the working environment for CISOs is extremely challenging, with the evolution and application of generative AI bringing significant risks. When asked about the potential threats, **38%** of survey respondents say they expect to see ‘Many More’ attacks using deep fake AI technologies over the next five years, with a further **45%** expecting to see ‘Somewhat More’.

But our respondents are nonetheless confident in their ability to protect data. When asked about their capability, **59%** say they are doing a good job in controlling the risks associated with generative AI. An encouraging **72%** say they have the support and backing of senior leadership – even if those leaders don’t always fully understand what they are supporting.

Contents





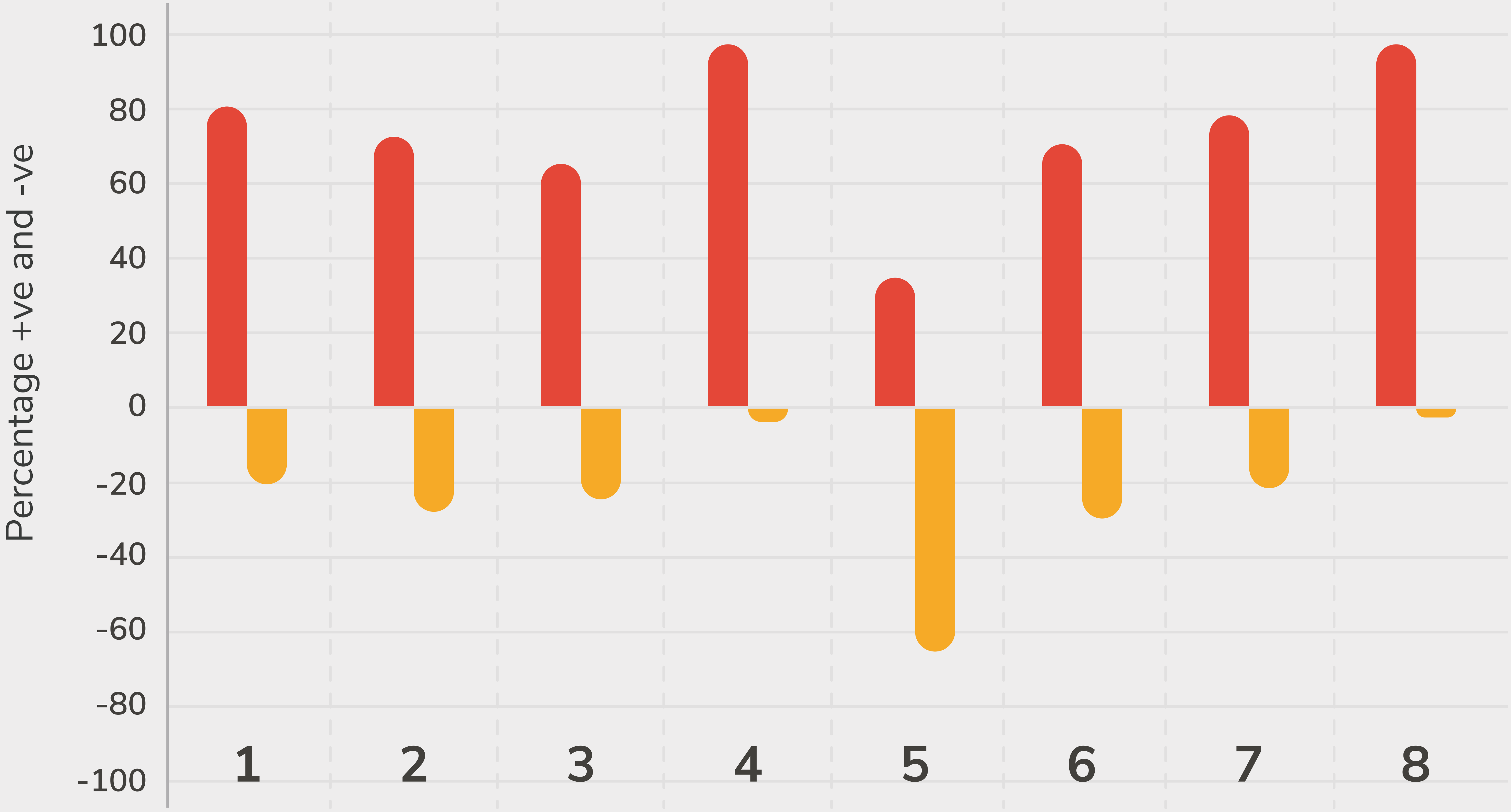


1

Sentiment: Being asked to do more with less

We asked our CISOs a series of questions that can be interpreted to give an indication of how positive or negative they are feeling.

Graph 1: Positive (in red) and negative (in yellow) sentiment across our survey questions.



1. Decision-making authority
2. Senior leadership support
3. Necessary budget
4. Confidence in resources to tackle threats in next 12 months
5. Concerns about being asked to do ‘more with less’ in next 12 months
6. Ease of recruiting & retaining talent
7. Concerns about increasing complexity of cyber threat landscape in next 12 months
8. Expectations that the EU AI Act & UK DPDI Bill will support growth

Source: OnePoll survey for Gemserv, September 2023

Overall, CISOs were **most positive** about:

- Having sufficient resources to tackle the cyber security and privacy challenges they expect to face in the next twelve months.
- The EU AI Act and the UK Data Protection and Digital Information (DPDI) Bill supporting their organisations to grow and expand their services.

They were most **negative about**:

- Being asked to do ‘more with less’ over the next twelve months.

More than 1 in 5 CISOs were concerned about:

- Lack of senior leadership support.
- Having the necessary budget.
- Recruiting and retaining talent.
- Increasing complexity and challenge in the cyber threat landscape.

Back to top

2

Risk management: A mixed picture on resourcing

We asked our CISOs how they are managing risks in their organisations. Our questions focused on the resources available to recognise and manage cyber and privacy threats, and the confidence CISOs have that they are getting this right.

Supplier risk management

We asked our CISOs how important cyber and privacy were when selecting products, suppliers and partners. In response:

- **76%** of CISOs said this was ‘Very Important’.
- **23%** said it was ‘Somewhat Important’.
- Only **2%** said it is not important to their organisations.

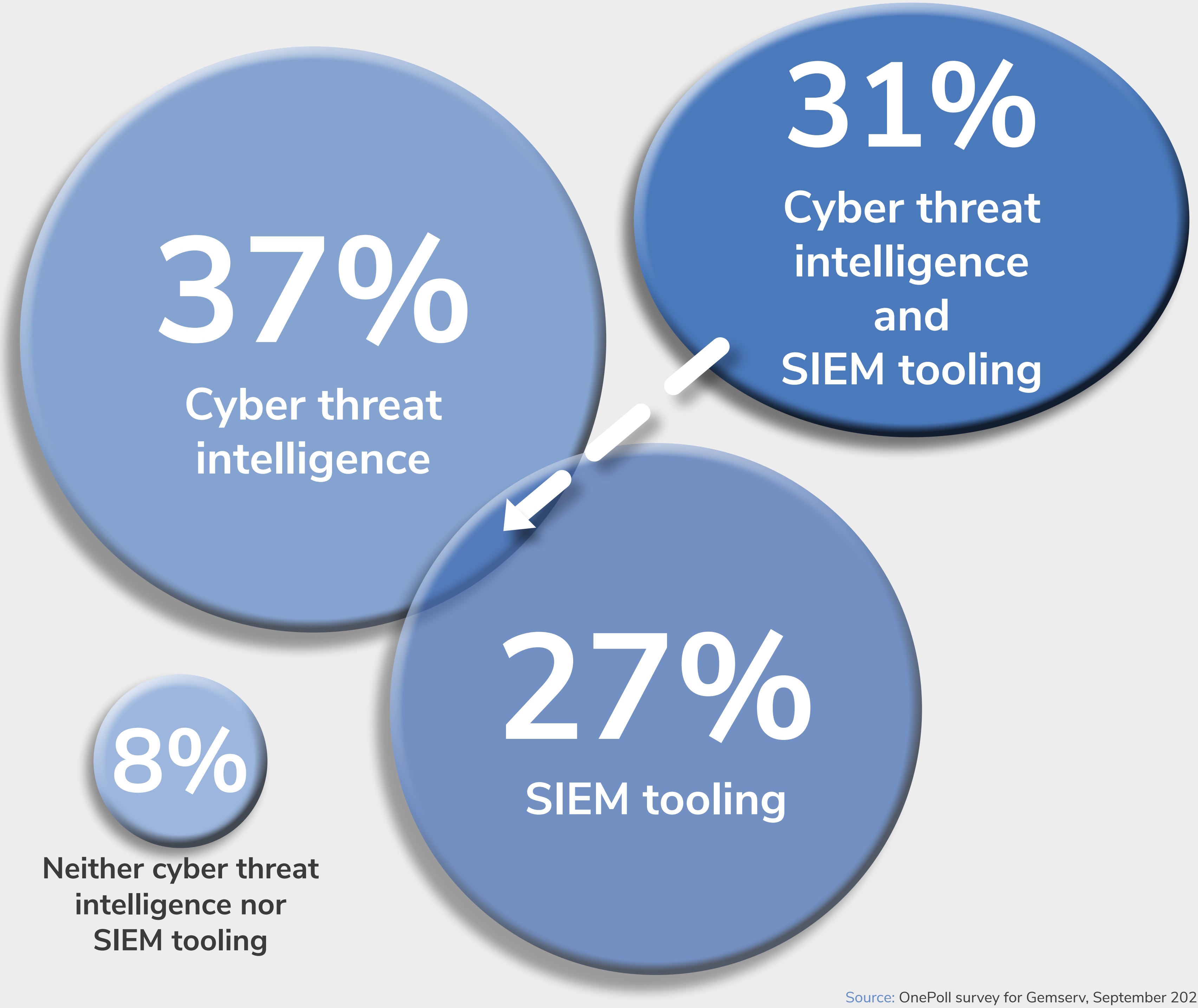
CISOs responsible for organisations that supply or partner with others should be under no illusions as to the importance of privacy and security by design, and should ensure that privacy and security measures are well conveyed through marketing communications.

Information and understanding

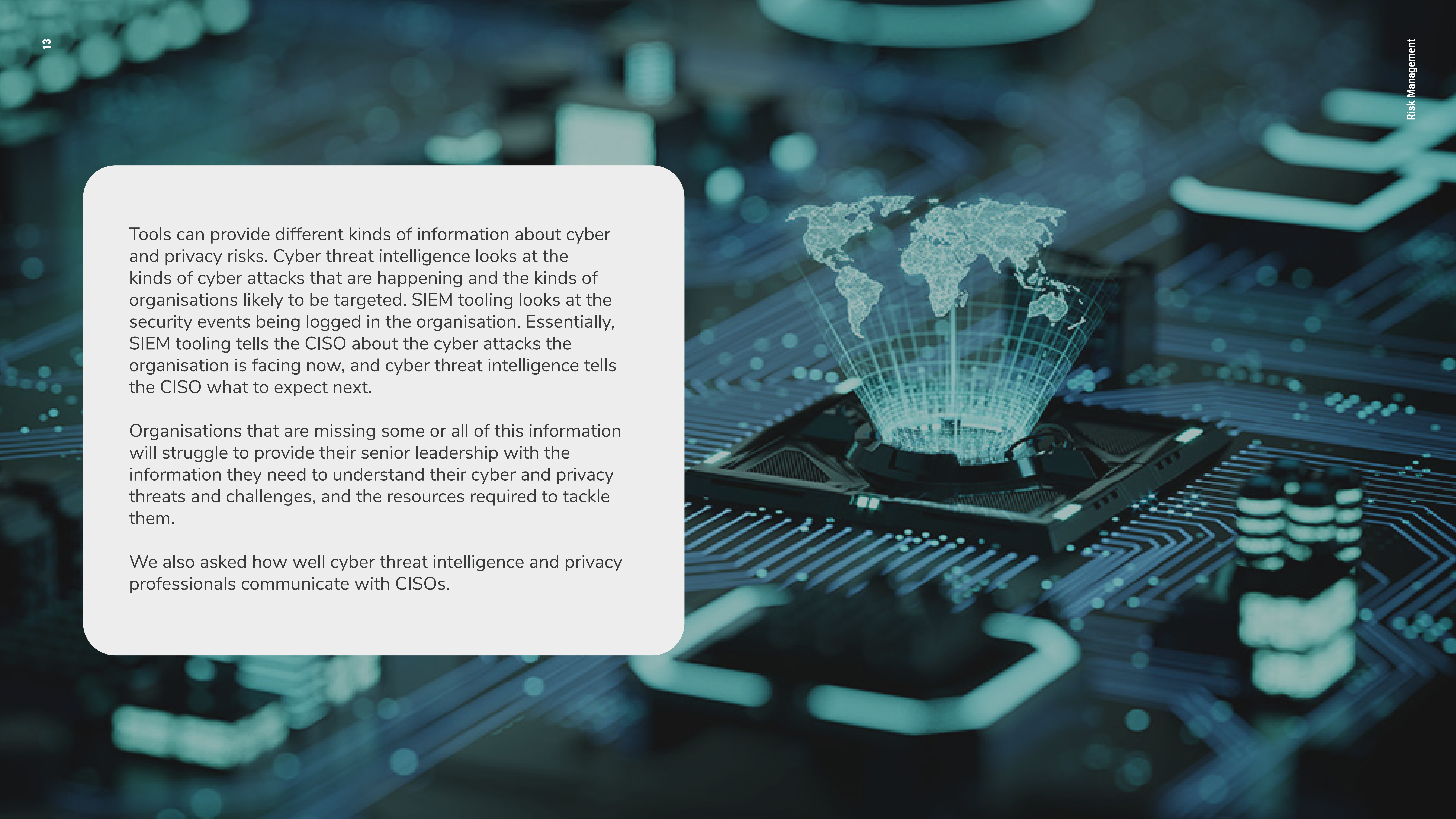
CISOs need senior leaders to understand the cyber and privacy risks they control and provide them with the resources they need to manage those risks. Our survey found:

- **37%** say their leadership has an 'Excellent' understanding of cyber security and data privacy risks and challenges, with a further **52%** rating their leadership as 'Good'.
- CISOs in the UK are less confident in their leadership than those in Europe, with **32%** of UK CISOs rating their leadership as 'Excellent' versus **42%** of EU CISOs
- **72%** of CISOs said they had the support and backing they need from their senior leadership.

Graphic 1: Cyber threat intelligence sources used by responding organisations (%)



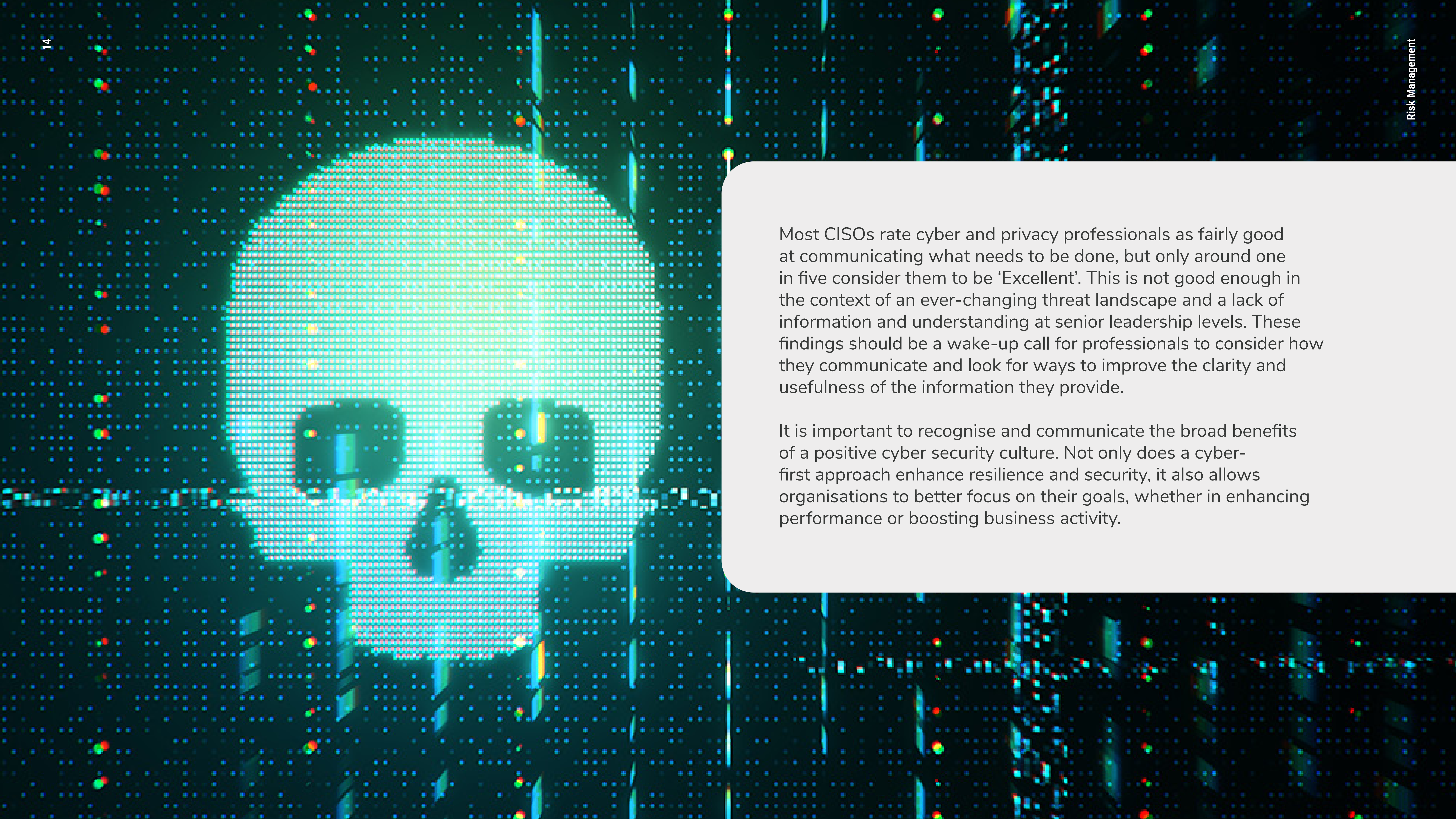
Source: OnePoll survey for Gemserv, September 2023



Tools can provide different kinds of information about cyber and privacy risks. Cyber threat intelligence looks at the kinds of cyber attacks that are happening and the kinds of organisations likely to be targeted. SIEM tooling looks at the security events being logged in the organisation. Essentially, SIEM tooling tells the CISO about the cyber attacks the organisation is facing now, and cyber threat intelligence tells the CISO what to expect next.

Organisations that are missing some or all of this information will struggle to provide their senior leadership with the information they need to understand their cyber and privacy threats and challenges, and the resources required to tackle them.

We also asked how well cyber threat intelligence and privacy professionals communicate with CISOs.



Most CISOs rate cyber and privacy professionals as fairly good at communicating what needs to be done, but only around one in five consider them to be ‘Excellent’. This is not good enough in the context of an ever-changing threat landscape and a lack of information and understanding at senior leadership levels. These findings should be a wake-up call for professionals to consider how they communicate and look for ways to improve the clarity and usefulness of the information they provide.

It is important to recognise and communicate the broad benefits of a positive cyber security culture. Not only does a cyber-first approach enhance resilience and security, it also allows organisations to better focus on their goals, whether in enhancing performance or boosting business activity.

The resourcing dilema

We asked our CISOs how they feel about the resources available to them to address cyber and privacy threats over the next 12 months.

We discovered:

- **65%** said they have the necessary budget.
- **36%** said they are ‘Very Confident’ that they will have the resources they need to tackle cyber and privacy threats over the next 12 months, with a further **61%** being ‘Somewhat Confident’.
- **22%** believe they are ‘Very Likely’ to be asked to do more with less in the next 12 months, with a further **45%** saying this is ‘Somewhat Likely’.
- **31%** say it is ‘Very Difficult’ or ‘Fairly Difficult’ to recruit and retain the right talent for their cyber and privacy teams.

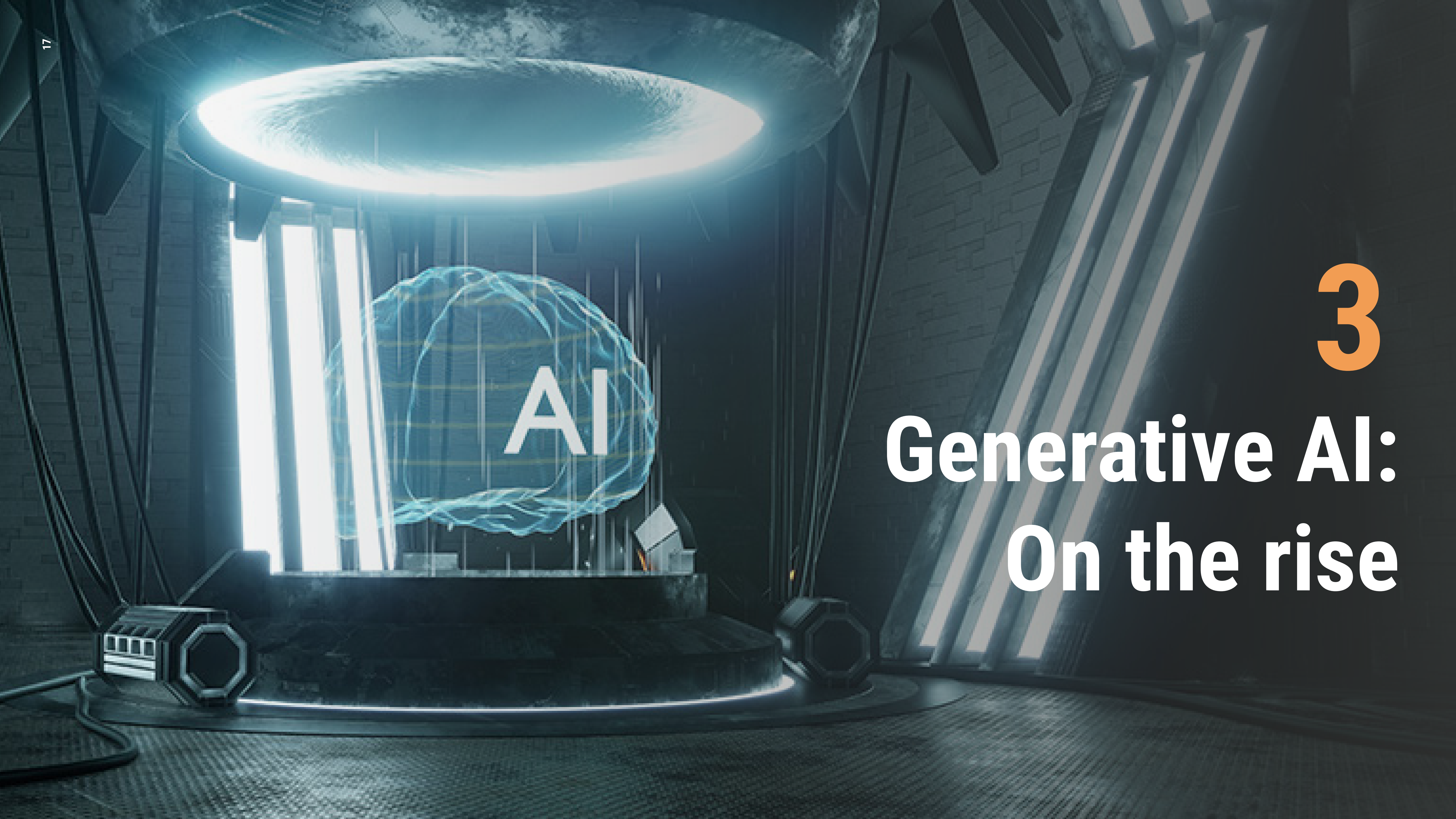
Our findings give a mixed picture, with many CISOs confident that they are adequately resourced to meet the cyber and privacy challenges facing them over the next 12 months. However, a significant number show signs of lacking resources. Around a third of respondents say they lack the budget they need, and a similar proportion are finding it difficult to recruit and retain staff with the right skills and experience. Overall, **67%** expect to be asked to do more with less in the next 12 months, indicating that many CISOs expect to be asked to find efficiency savings.

Meeting these challenges requires professionals who are excellent at communicating clear, actionable, prioritised information to help CISOs act efficiently, cope with budget constraints and fill any gaps caused by staffing difficulties. As we have seen, professionals need to urgently work on improving their soft skills in order to provide CISOs with the support they need.

OUR ADVICE IS

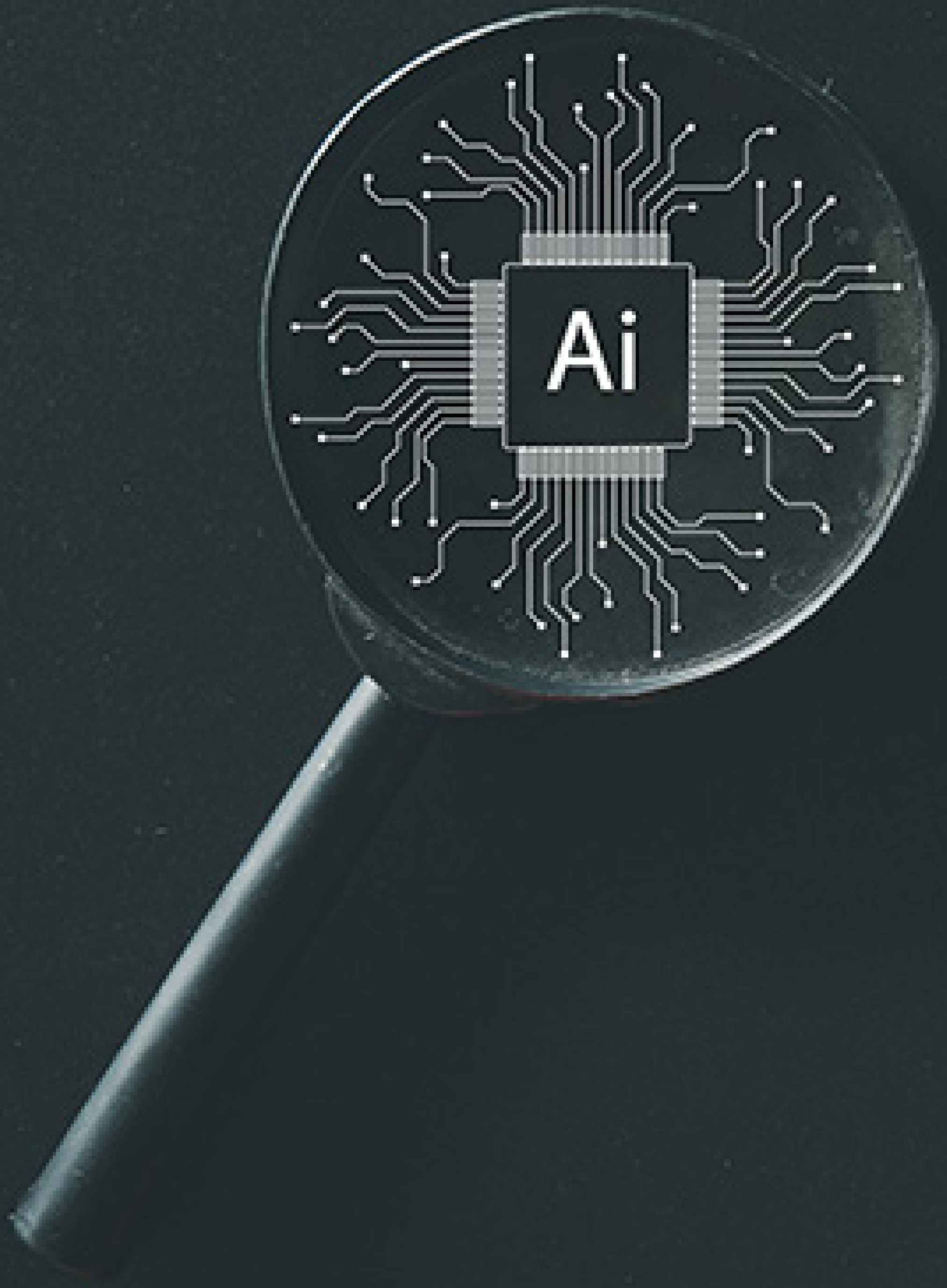
- Ensure professionals have a deep understanding of the organisation, its objectives, its context and the current knowledge levels of senior leadership.
- Work hard to relate cyber and privacy recommendations to the organisation’s requirements.
- Consider cost of implementation and availability of skilled resource when developing and prioritising action plans.
- Think about all stakeholders involved in making and implementing decisions, and design communications plans that consider their current level of knowledge, concerns and priorities and, therefore, their communication needs.
- Present information in a way that is concise and easy to interpret.

Back to top



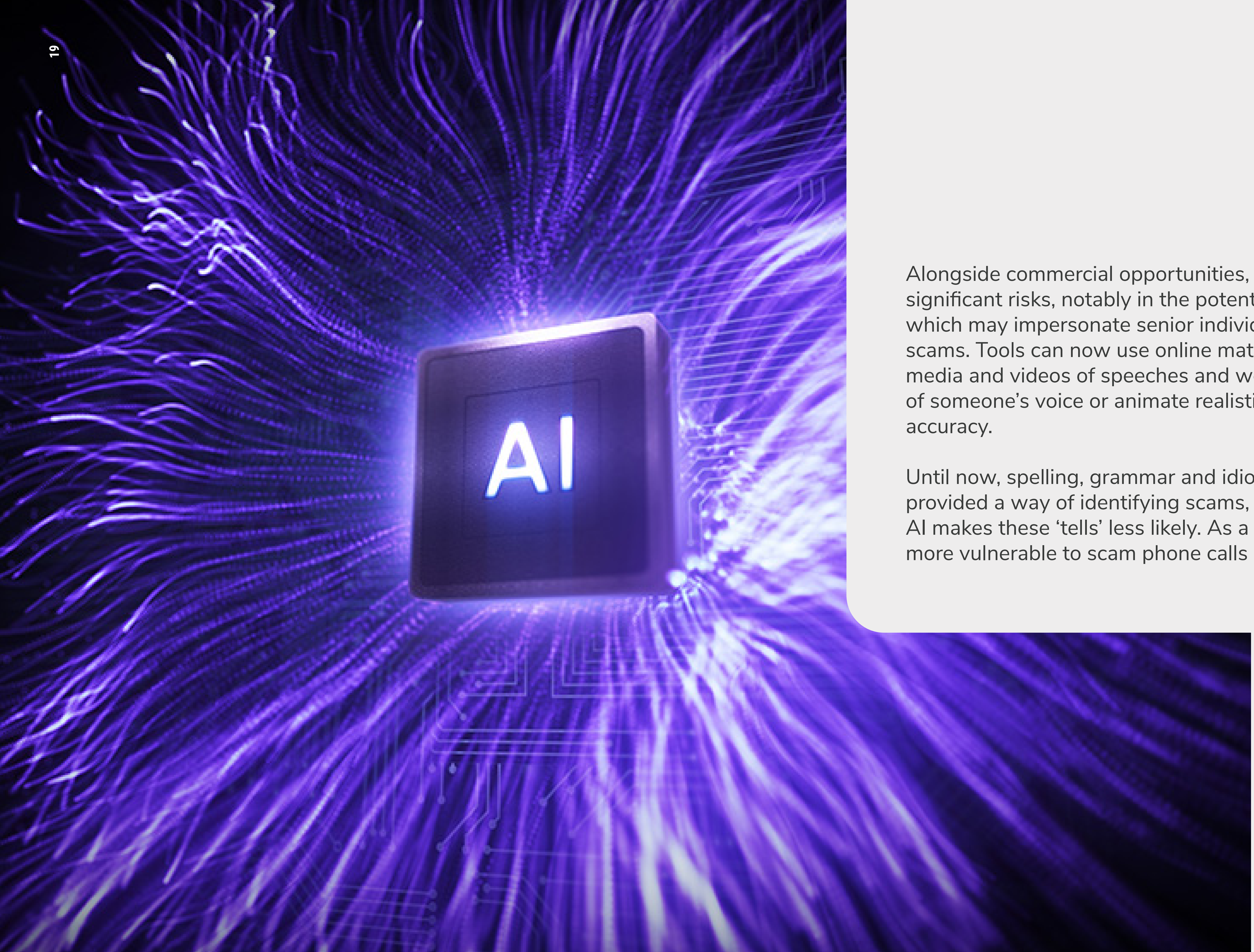
3

Generative AI: On the rise



For decades, AI has been seen as ‘the next big thing’, with researchers focused on developing a tool that could pass the Turing Test - for a computer that could pass as a human - and handle many tasks. OpenAI’s ChatGPT, the first tool to appear to meet these conditions, became the fastest app ever to reach **100 million** users, taking just two months from its launch.

Generative AI has the capability to create new content in response to stimuli, with ChatGPT handling text and other systems working with still and moving images and sound, including voices. Applications for generative AI continue to be explored but this already looks set to be a transformative technology with profound impacts for economic productivity and many industries.



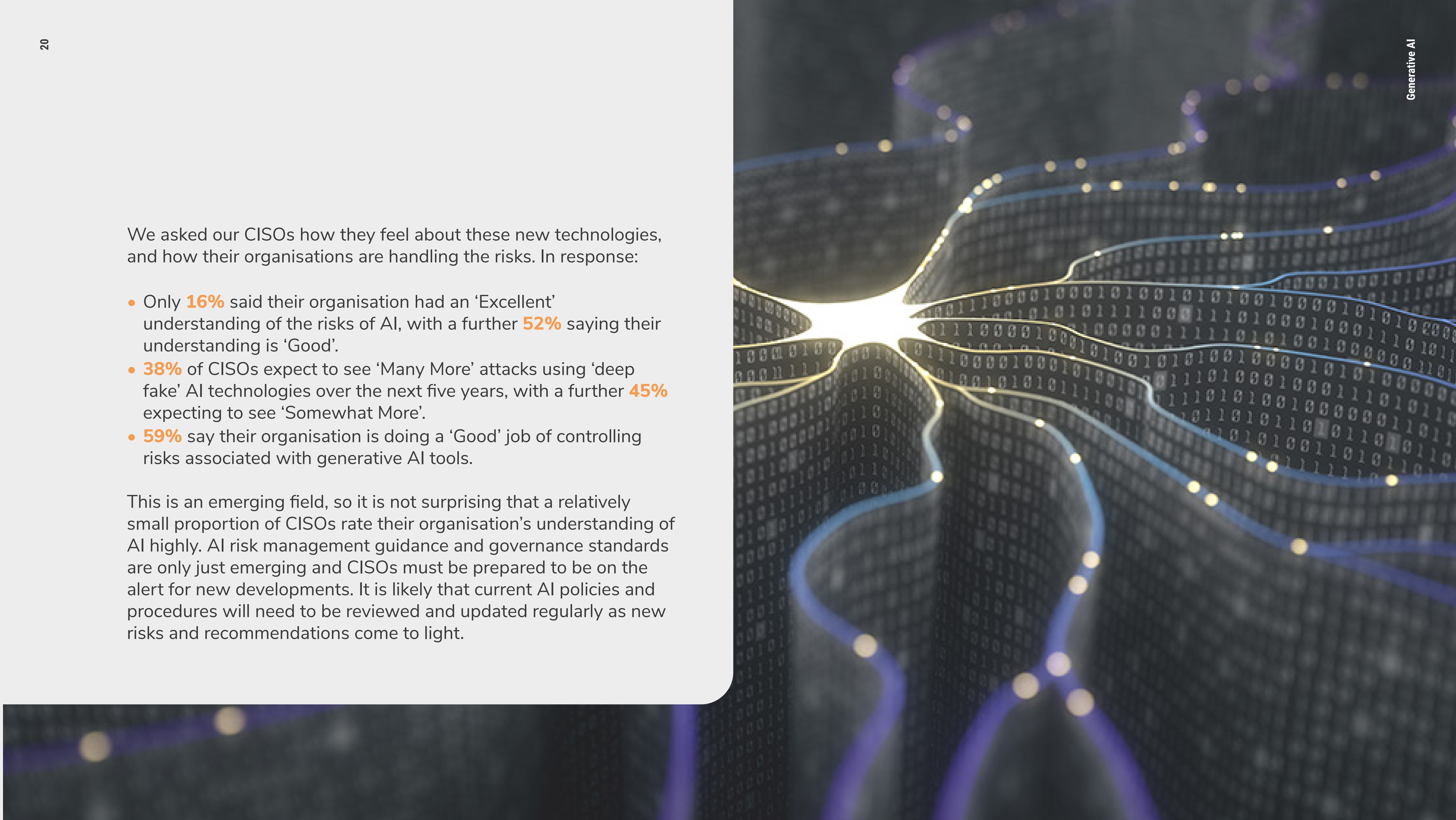
Alongside commercial opportunities, generative AI also brings significant risks, notably in the potential threat of ‘deep fakes’, which may impersonate senior individuals to perpetrate phishing scams. Tools can now use online materials, such as photos, social media and videos of speeches and webinars, to fake the sound of someone’s voice or animate realistic videos with high levels of accuracy.

Until now, spelling, grammar and idiomatic errors in messages have provided a way of identifying scams, but the advent of generative AI makes these ‘tells’ less likely. As a result, employees may be more vulnerable to scam phone calls and videos.

We asked our CISOs how they feel about these new technologies, and how their organisations are handling the risks. In response:

- Only **16%** said their organisation had an 'Excellent' understanding of the risks of AI, with a further **52%** saying their understanding is 'Good'.
- **38%** of CISOs expect to see 'Many More' attacks using 'deep fake' AI technologies over the next five years, with a further **45%** expecting to see 'Somewhat More'.
- **59%** say their organisation is doing a 'Good' job of controlling risks associated with generative AI tools.

This is an emerging field, so it is not surprising that a relatively small proportion of CISOs rate their organisation's understanding of AI highly. AI risk management guidance and governance standards are only just emerging and CISOs must be prepared to be on the alert for new developments. It is likely that current AI policies and procedures will need to be reviewed and updated regularly as new risks and recommendations come to light.



OUR ADVICE IS

- Consider the risks associated with the organisation's plans for AI, both from suppliers starting to incorporate AI into their products and services and from bad actors using AI to mount attacks. Individuals working in organisations may, for example, use cloud-based generative AI platforms to help them do their jobs, without understanding the risks of sharing information with these platforms, or the limitations of their outputs.
- Ensure that AI assurance frameworks are developed alongside new proofs of concept and new products and services, and that these take into account the – perhaps unexpected – ways that these tools will be used by employees.

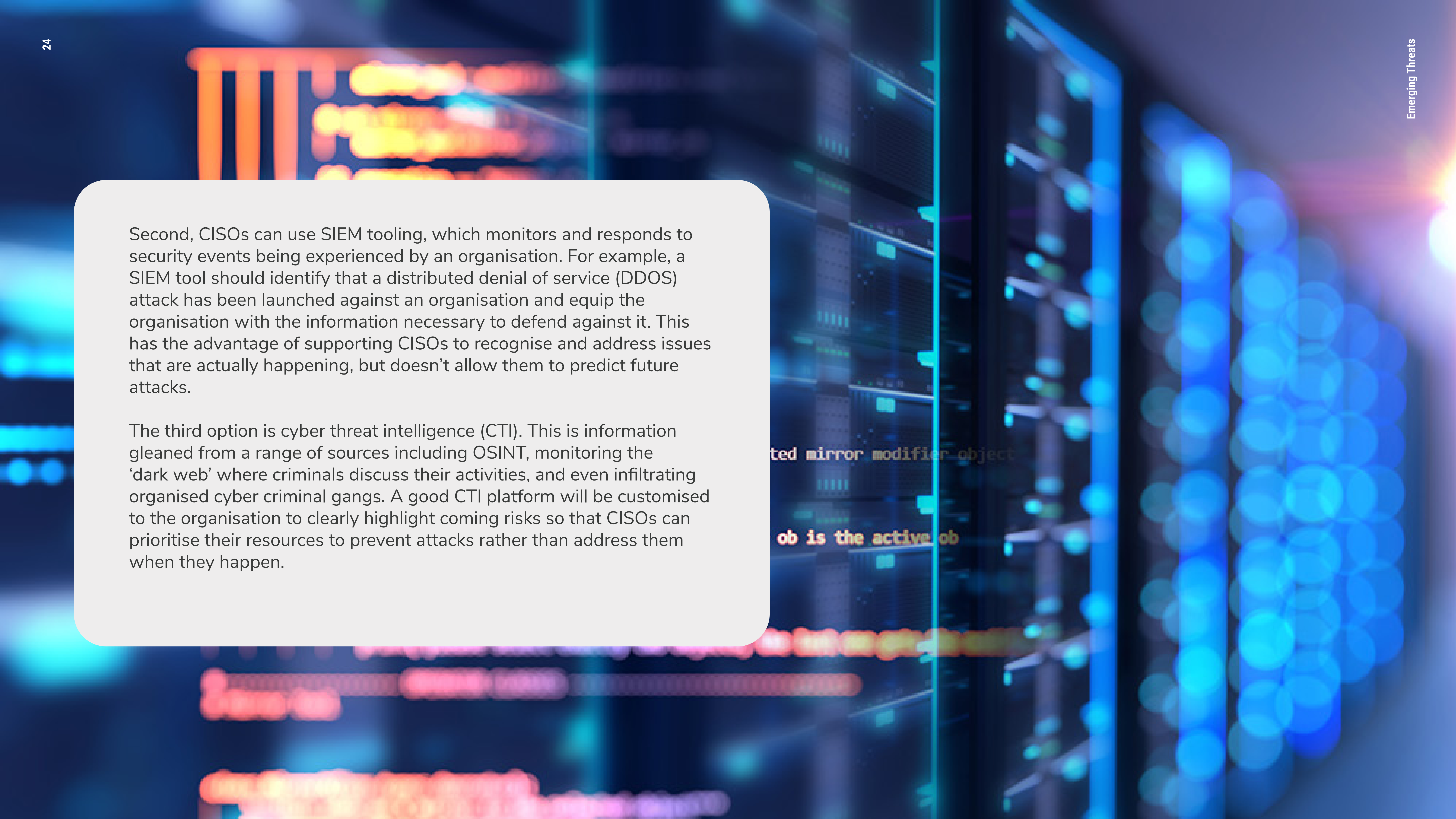
Back to top

4 Emerging threats: Being prepared

The cyber threat landscape is constantly changing, and one of the biggest challenges for any CISO is assessing where the next attack is likely to come from and what it might target.

CISOs need both information and budget to equip themselves to tackle emerging threats. There are three typical methods CISOs can use to gather information.

First, they can use open-source intelligence (OSINT), which basically means keeping abreast of what's making the news. This has the advantage of being readily available, often at little or no direct cost. However, it is not designed to be comprehensive or targeted to the organisation so relevant information may be missed and the indirect cost – in the time taken to gather and analyse information – can be high.



Second, CISOs can use SIEM tooling, which monitors and responds to security events being experienced by an organisation. For example, a SIEM tool should identify that a distributed denial of service (DDOS) attack has been launched against an organisation and equip the organisation with the information necessary to defend against it. This has the advantage of supporting CISOs to recognise and address issues that are actually happening, but doesn't allow them to predict future attacks.

The third option is cyber threat intelligence (CTI). This is information gleaned from a range of sources including OSINT, monitoring the 'dark web' where criminals discuss their activities, and even infiltrating organised cyber criminal gangs. A good CTI platform will be customised to the organisation to clearly highlight coming risks so that CISOs can prioritise their resources to prevent attacks rather than address them when they happen.

Our research shows that:

- **69%** of organisations lack access to either SIEM tooling or CTI, with **8%** having neither.
- **78%** of CISOs believe the cyber threat landscape will become more complex and challenging over the next 12 months.
- **83%** of CISOs expect to see more cyber attacks using generative AI tools.
- Only **36%** of CISOs are 'Very Confident' that they will have all the resources they need to tackle cyber threats over the next 12 months.

In a world where the cyber threat landscape is evolving significantly and good intelligence is essential, CISOs are facing challenges in responding as they expect their budgets to be under pressure and may find it difficult to recruit and retain the right talent. Choosing the right provider is important too – the **19%** of CISOs who rate their CTI providers as 'Excellent' at providing clear, prioritised and actionable intelligence are clearly already reaping the rewards.

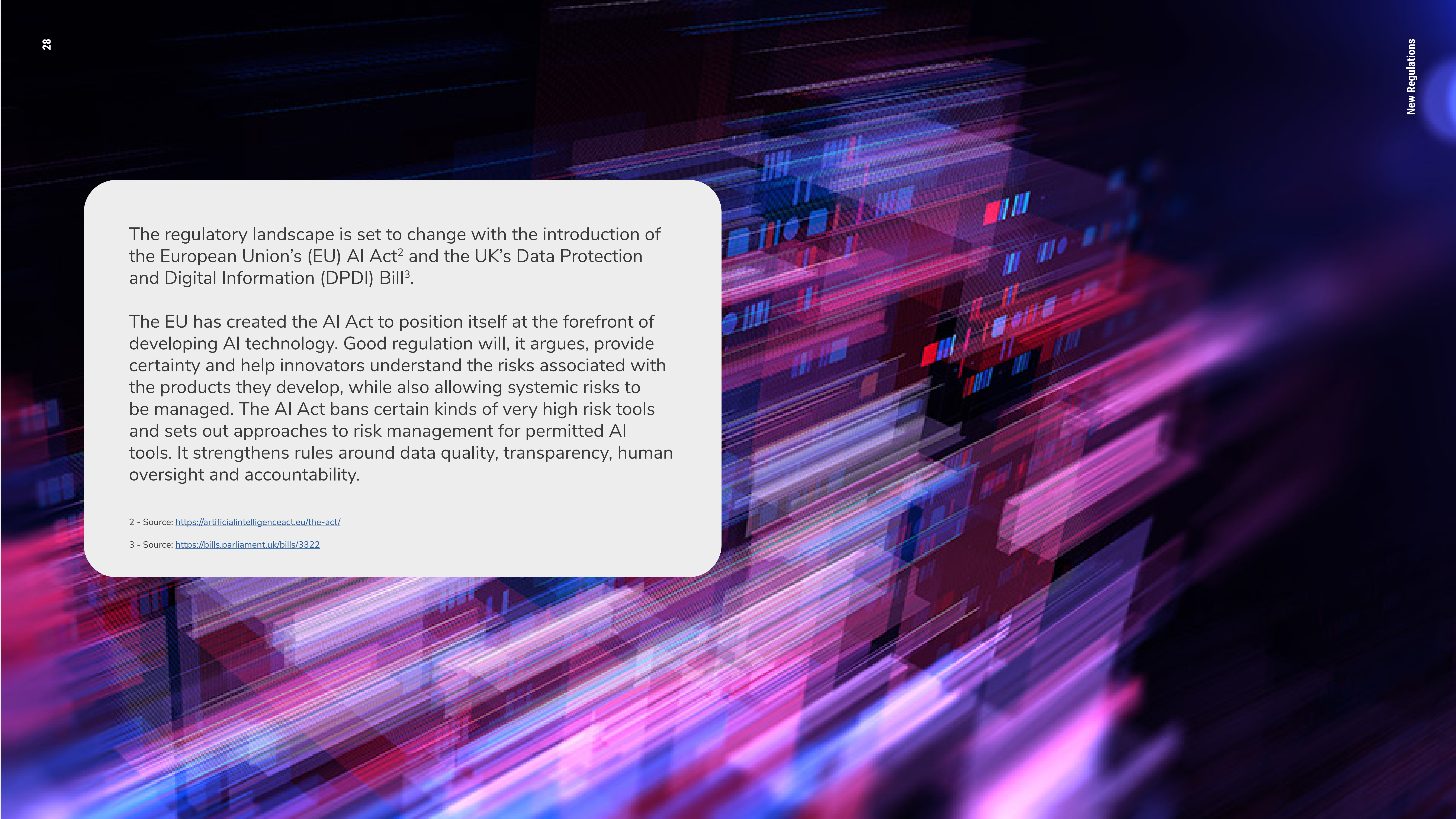
OUR OVERALL ADVICE IS

- Maintain vigilance; invest in good quality cyber threat intelligence.
- Undertake robust due diligence on your supply chains.
- Invest in training and awareness to ensure your people can be your first and most effective line of defence.
- Ensure you have an effective patching programme.
- Finance and embed governance, risk and compliance programmes.

Back to top

5

New regulations: Welcome moves

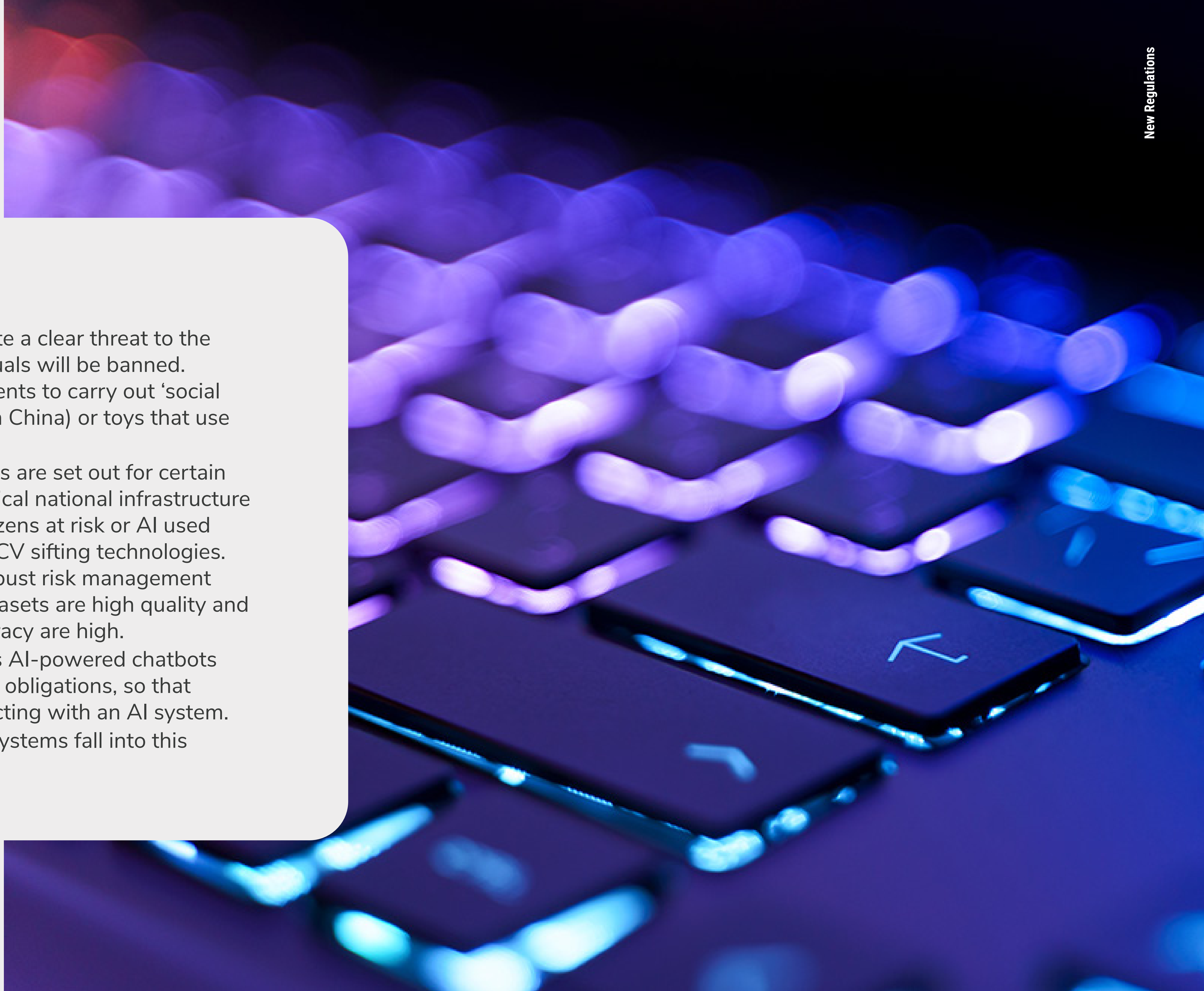


The regulatory landscape is set to change with the introduction of the European Union’s (EU) AI Act[2] and the UK’s Data Protection and Digital Information (DPDI) Bill[3].

The EU has created the AI Act to position itself at the forefront of developing AI technology. Good regulation will, it argues, provide certainty and help innovators understand the risks associated with the products they develop, while also allowing systemic risks to be managed. The AI Act bans certain kinds of very high risk tools and sets out approaches to risk management for permitted AI tools. It strengthens rules around data quality, transparency, human oversight and accountability.

2 - Source: https://artificialintelligenceact.eu/the-act/

3 - Source: https://bills.parliament.uk/bills/3322



The act creates four risk levels for AI:

- Unacceptable risk – any tools that create a clear threat to the safety, livelihoods and rights of individuals will be banned. This includes tools that allow governments to carry out 'social scoring' on their citizens (as happens in China) or toys that use AI to encourage dangerous behaviour.
- High risk – risk management obligations are set out for certain categories of AI, such as AI used in critical national infrastructure that could put the life and health of citizens at risk or AI used in the context of employment, such as CV sifting technologies. These require providers to carry out robust risk management activities, such as ensuring training datasets are high quality and levels of robustness, security and accuracy are high.
- Limited risk – providers of tools such as AI-powered chatbots have to ensure they meet transparency obligations, so that people understand that they are interacting with an AI system.
- Minimal or no risk – the majority of AI systems fall into this category and can be used freely.

The UK DPDI is designed to replace the General Data Protection Regulation (GDPR). It includes changes designed to make the UK an attractive place to carry out data-driven research and innovation, and to reduce the compliance burden on small and medium sized organisations. The goal is to differentiate the data protection environment in the UK from the data protection environment across Europe post-Brexit, without adversely affecting the 'adequacy decision' that allows data to move freely between the UK and Europe.

We asked our CISOs whether they felt these laws would enable their organisations to grow and enhance their services:

- **28%** 'Strongly Agree' that the laws will support their organisations
- **54%** 'Somewhat Agree'
- Only **3%** disagreed with our question and said they did not think the laws would help their organisations.

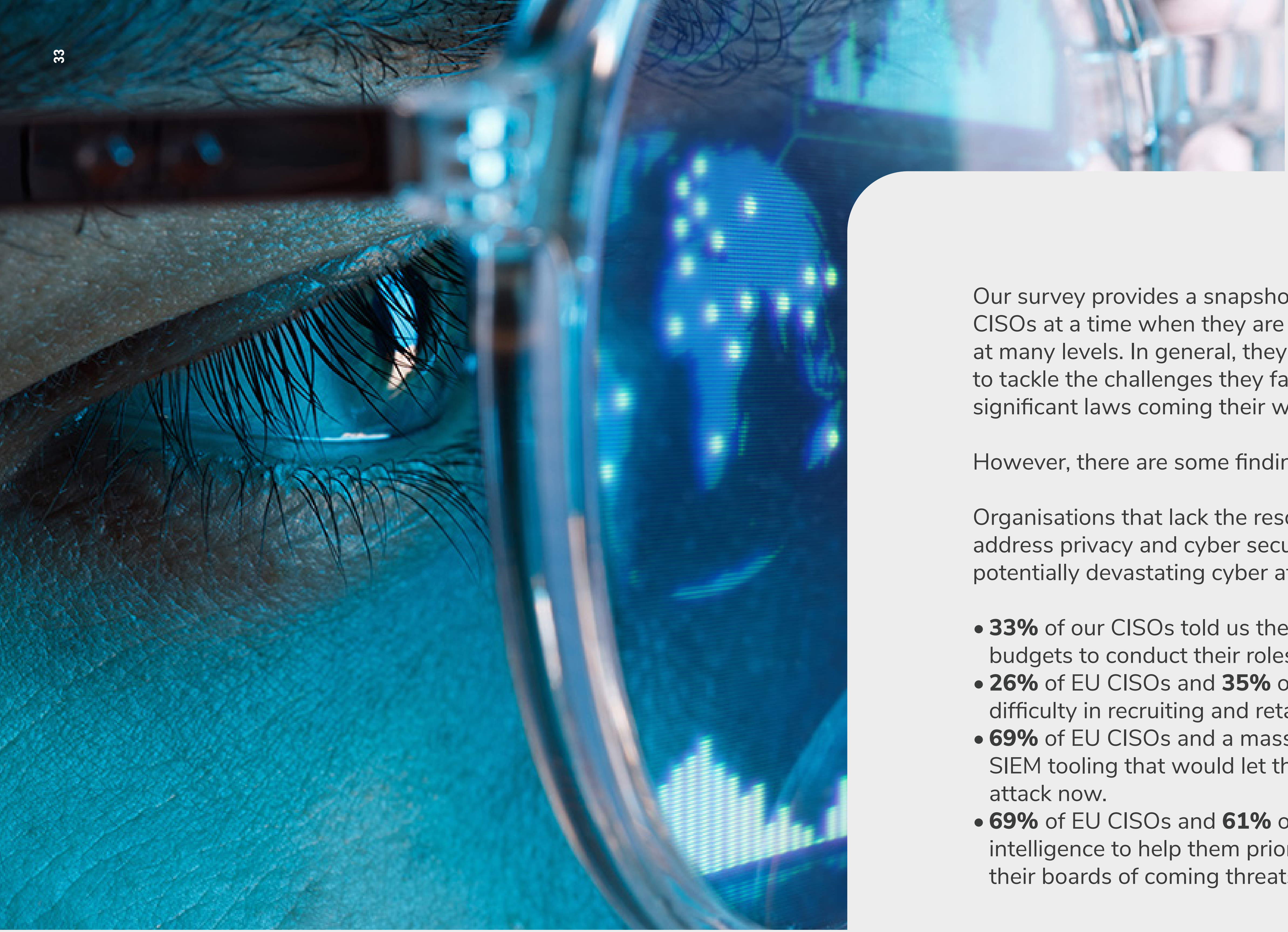
Interestingly, the numbers were broadly the same between European and UK-based CISOs, with the biggest difference being in the number who felt the laws would be unhelpful. Only **1%** of European CISOs felt this, compared with **5%** of UK CISOs. This may reflect the territorial scope of the laws.

It is good to see that our CISOs are largely positive about these new regulations and that it appears that these, at least, are not seen as unnecessary red tape.

Back to top

6

Conclusion: The need for more resources



Our survey provides a snapshot of the opinions of our 200 CISOs at a time when they are facing change and uncertainty at many levels. In general, they are positive about their ability to tackle the challenges they face and the impact of two significant laws coming their way.

However, there are some findings that should alarm us all.

Organisations that lack the resources and information to address privacy and cyber security challenges are at risk of potentially devastating cyber attacks. Our research shows:

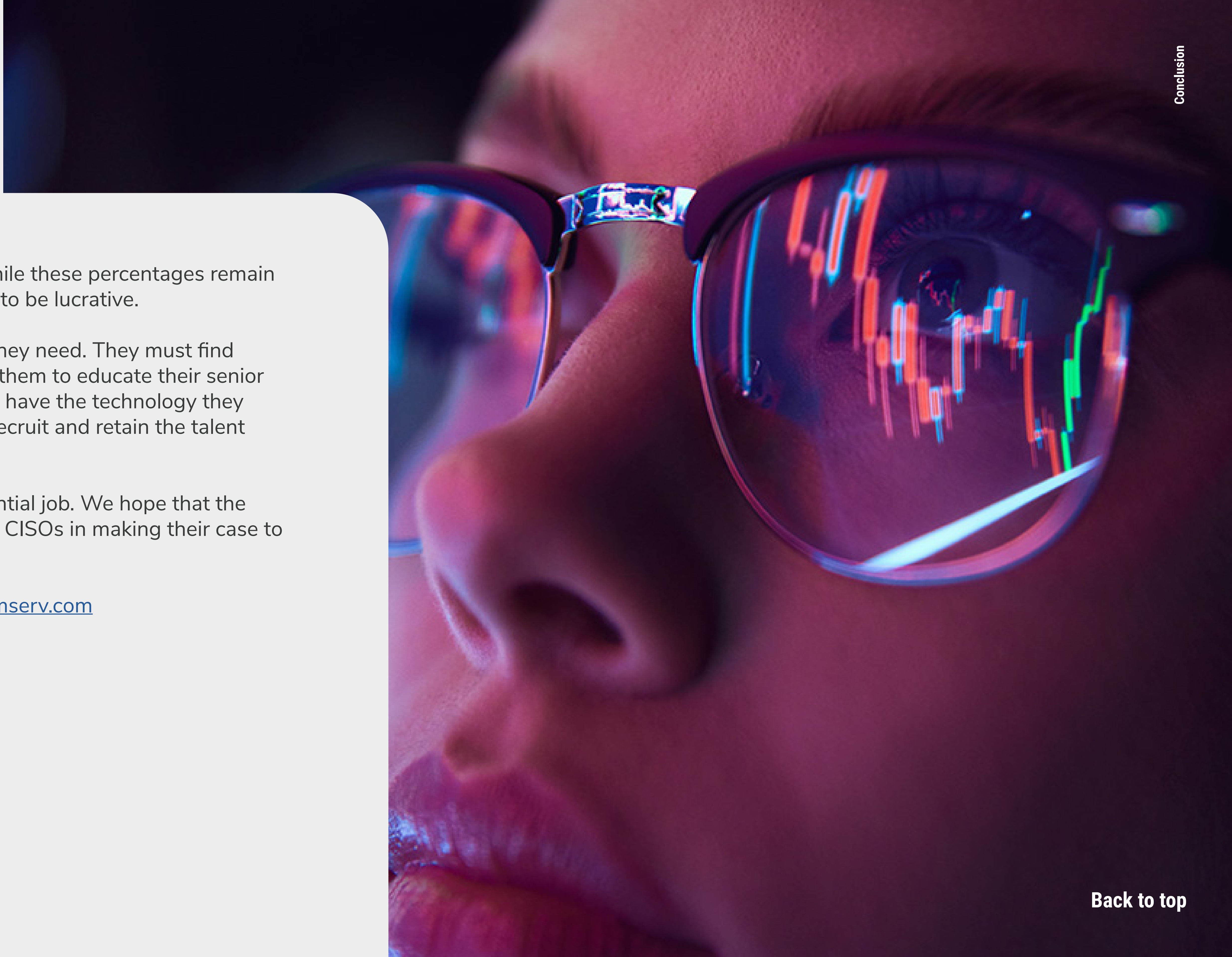
- **33%** of our CISOs told us they don’t have the necessary budgets to conduct their roles properly.
- **26%** of EU CISOs and **35%** of UK CISOs are experiencing difficulty in recruiting and retaining talent.
- **69%** of EU CISOs and a massive **78%** of UK CISOs lack the SIEM tooling that would let them know if they are under cyber attack now.
- **69%** of EU CISOs and **61%** of UK CISOs lack cyber threat intelligence to help them prioritise their budgets and inform their boards of coming threats.

These findings are significant. While these percentages remain so high, cyber crime will continue to be lucrative.

CISOs must fight for the budget they need. They must find the best professionals to support them to educate their senior leadership teams and ensure they have the technology they need. This in turn will help them recruit and retain the talent they need.

Being a CISO is a tough and essential job. We hope that the insights in this report will support CISOs in making their case to secure the resources they need.

To find out more contact BD@gemserv.com



Back to top

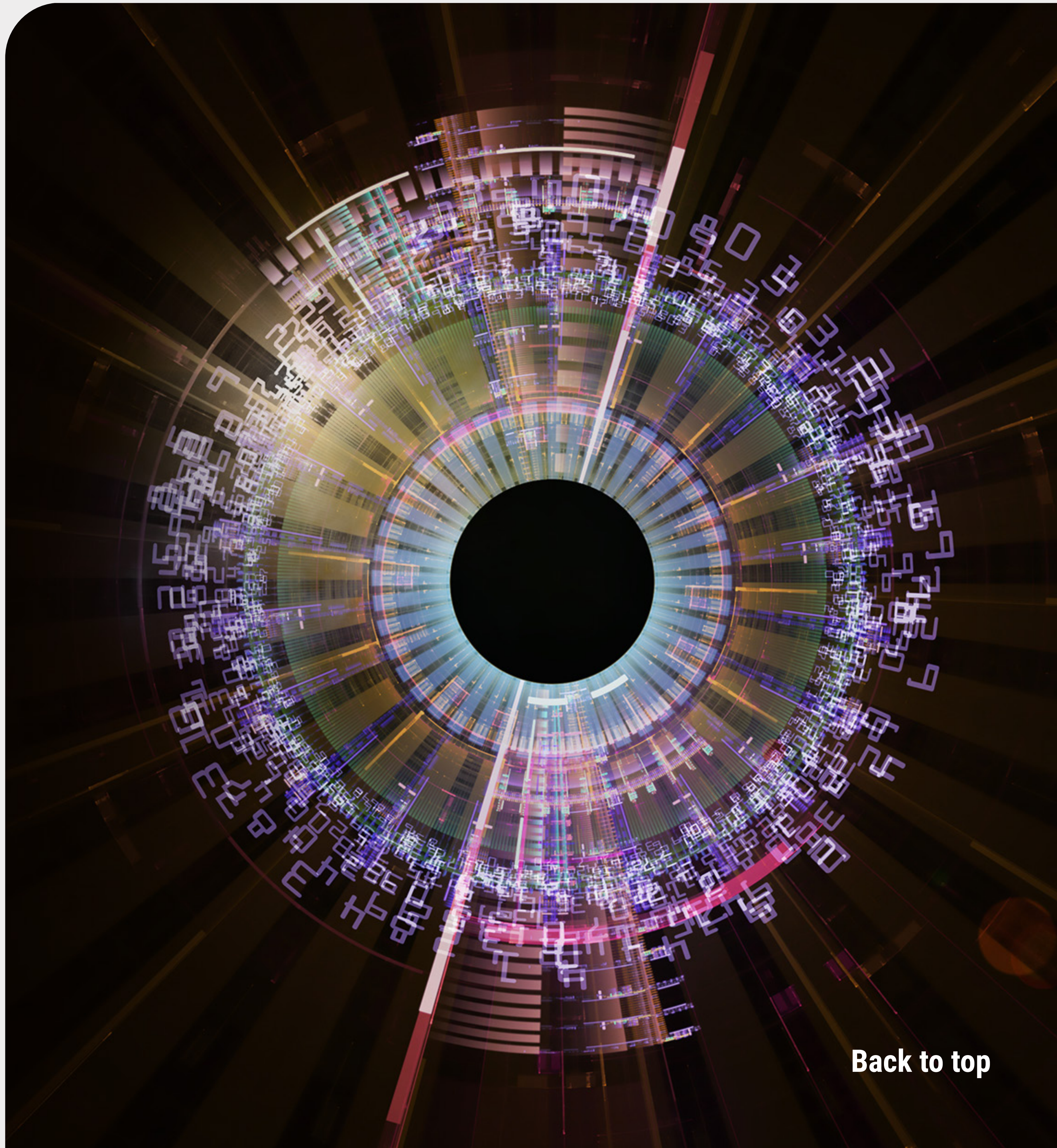
Key Contacts

Mandeep Thandi
Director of Cyber and Privacy

As the Director of Cyber & Privacy, Mandeep is a member of the Executive Team with responsibility to support the strategic development of the company, including the execution of the company's strategy plan.

Mandeep is responsible for the development and growth of the Cyber & Privacy business unit, including the commercial development of services across cyber security & privacy, digital services, codeworks platform and data analytics across key sectors such as energy, health, public sector, telecoms, transport, financial services and defence.

mandeep.thandi@gemserv.com



Back to top

Camilla Winlo
Head of Data Privacy

Camilla is an experienced leader of data privacy consultancy teams. Key achievements include winning Best Privacy by Design at the DMA Awards and Best Privacy and Data Ethics Initiative at the DataIQ awards, both for work with WarnerMedia and DQM GRC. In 2022, Camilla was named as one of the top 100 Women in Tech.

She is a regular media commentator noted for her commercial, pragmatic and strategic view of data privacy issues. Prior to moving into data privacy, she was a senior marketer and part of the leadership teams that launched three new financial services brands to market in response to regulatory change.

camilla.winlo@gemserv.com

Ian Hirst
Partner, Cyber Threat Services

Ian joined Gemserv in November 2018 as a security consultant. Ian has over 29 years' worth of experience in the cyber and security field gained through a combination of both military and Consultant employment.

Experience includes ISO compliance and security evaluation, CESG systems accreditation, risk assessment and management and Cyber Essentials certification. Significant experience of operating in security governance and assurance settings.

ian.hirst@gemserv.com

Back to top

Ian Rutland
Head of Cyber Security

Ian has over 30 years of experience within the Information and Cyber Security fields, gained via a combination of both military service and private sector consultancy across a broad spectrum of industry sectors, including defence, aerospace, automotive and energy.

Ian's experience includes ISO certification, system certification, risk management, incident response and security governance and compliance.

Ian Davis
Head of Information Security

Ian is a highly experienced information security and business continuity consultant with over 20 years' experience in the design, implementation and management of information security projects across diverse sectors.

He is responsible for the development of the information security practice of Gemserv Ltd following the integration of Red Island Consulting into the Gemserv consultancy practic.

ian.rutland@gemserv.com

ian.Davis@gemserv.com

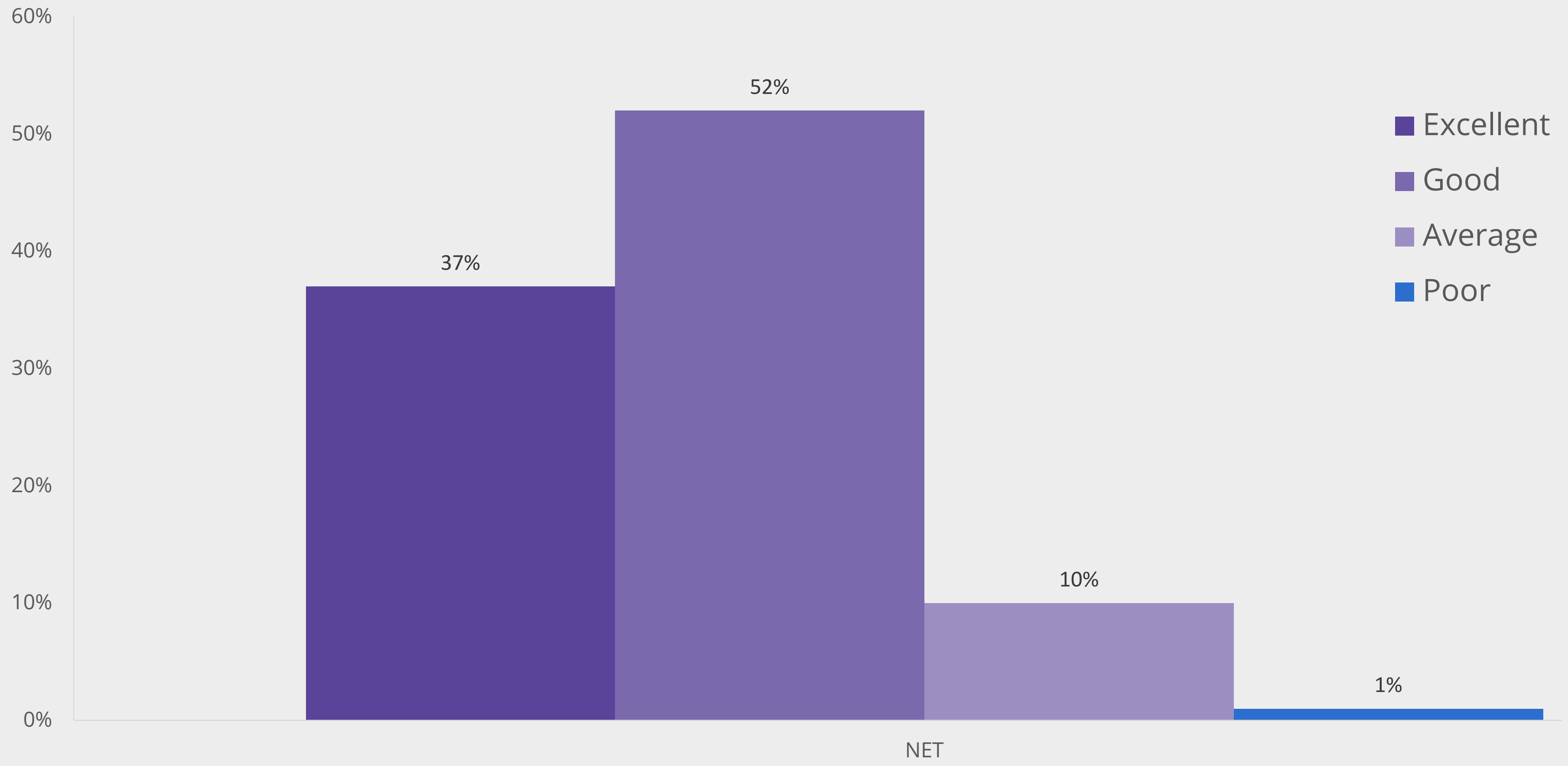
Back to top

Appendix:

Methodology

Our survey was conducted online by OnePoll, who contacted 200 CISOs: 100 based in the UK and 100 across the EU. Each CISO was asked the same questions and given the opportunity to choose the best fit from a list of options. This report sets out our findings, as well as our interpretations and insights based on the responses.

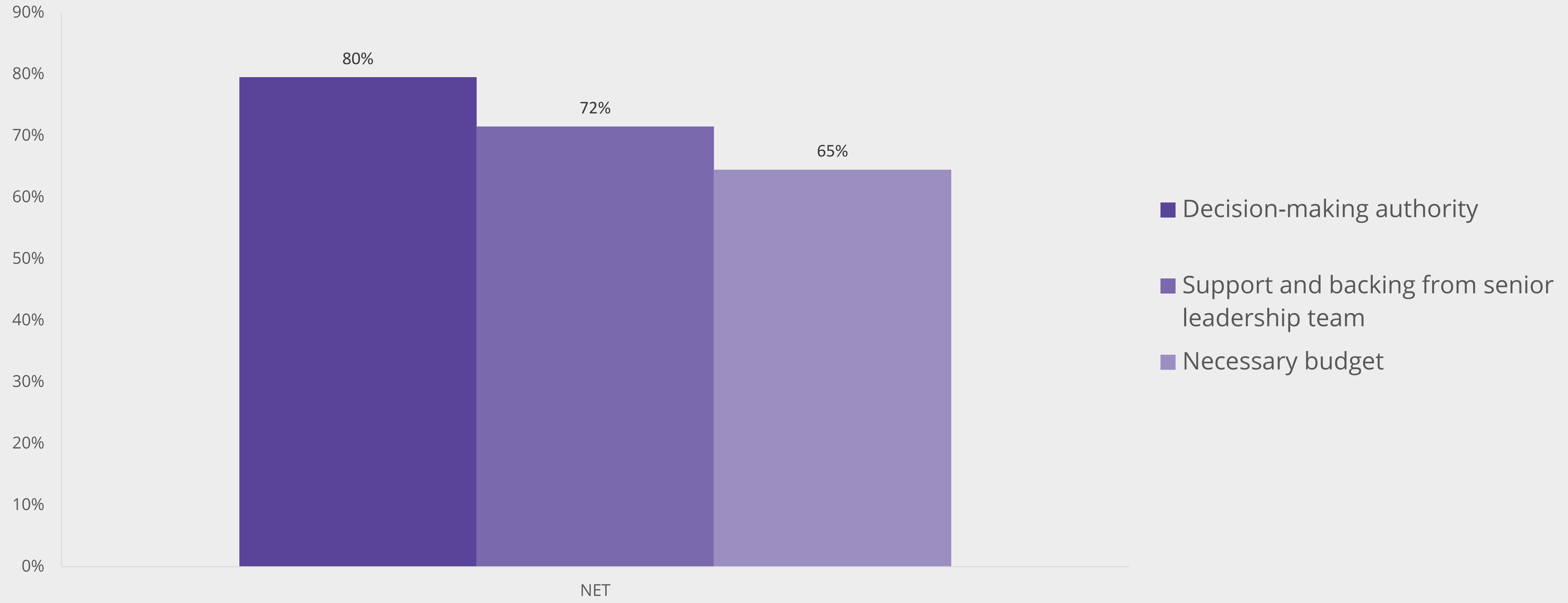
1. How would you describe the senior leadership team within your organisation's level of understanding of cyber security and data privacy, specifically risks and challenges? by All



(C) OnePoll 2023; base n = 200

Back to top

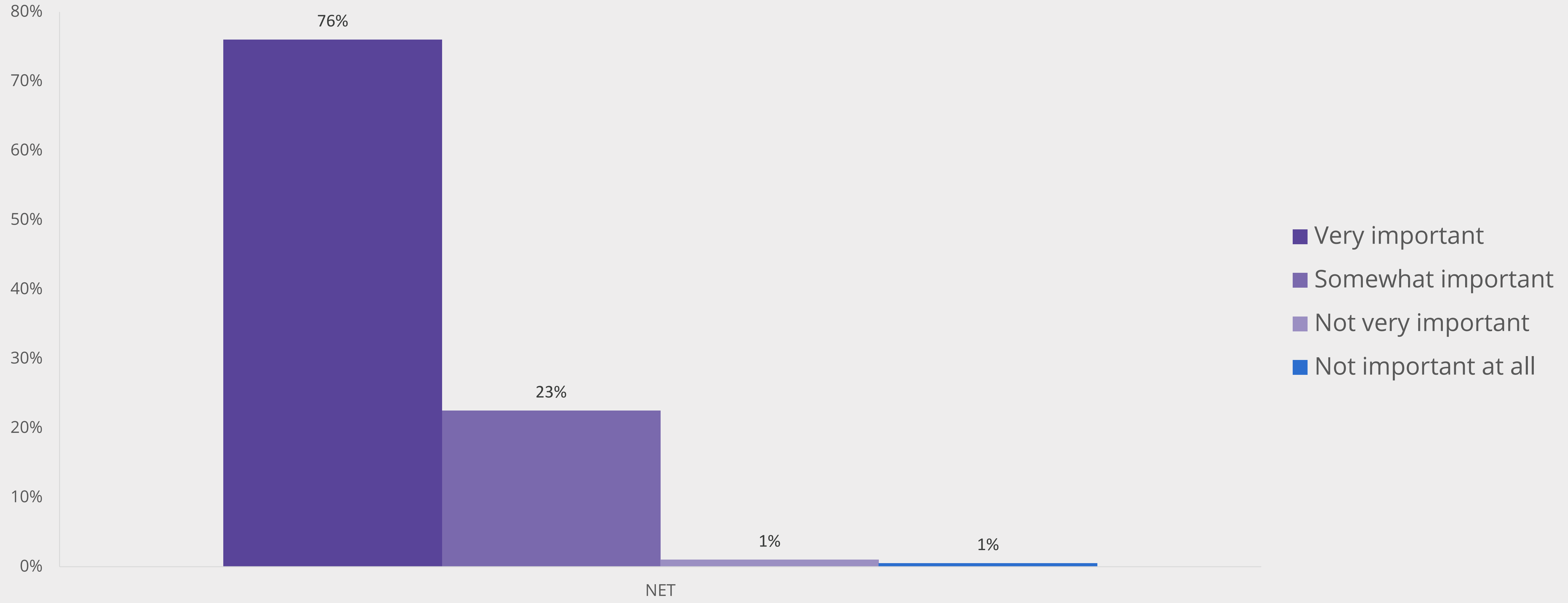
2. Which, if any, of the following do you feel you have access to so you can conduct your job role properly in the business? Selected all that apply by All



(C) OnePoll 2023; base n = 200

Back to top

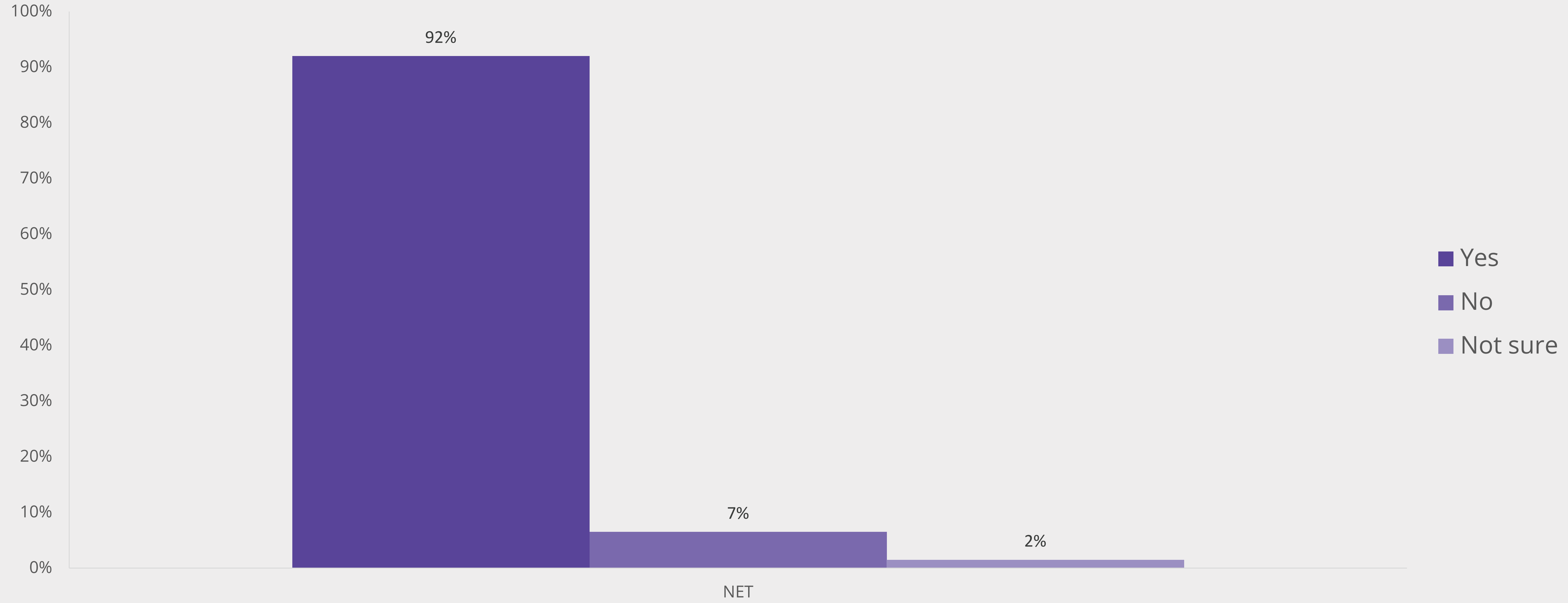
3. How important, if at all, is cyber security and data privacy to your organisation when selecting products, suppliers and/or partners? by All



(C) OnePoll 2023; base n = 200

Back to top

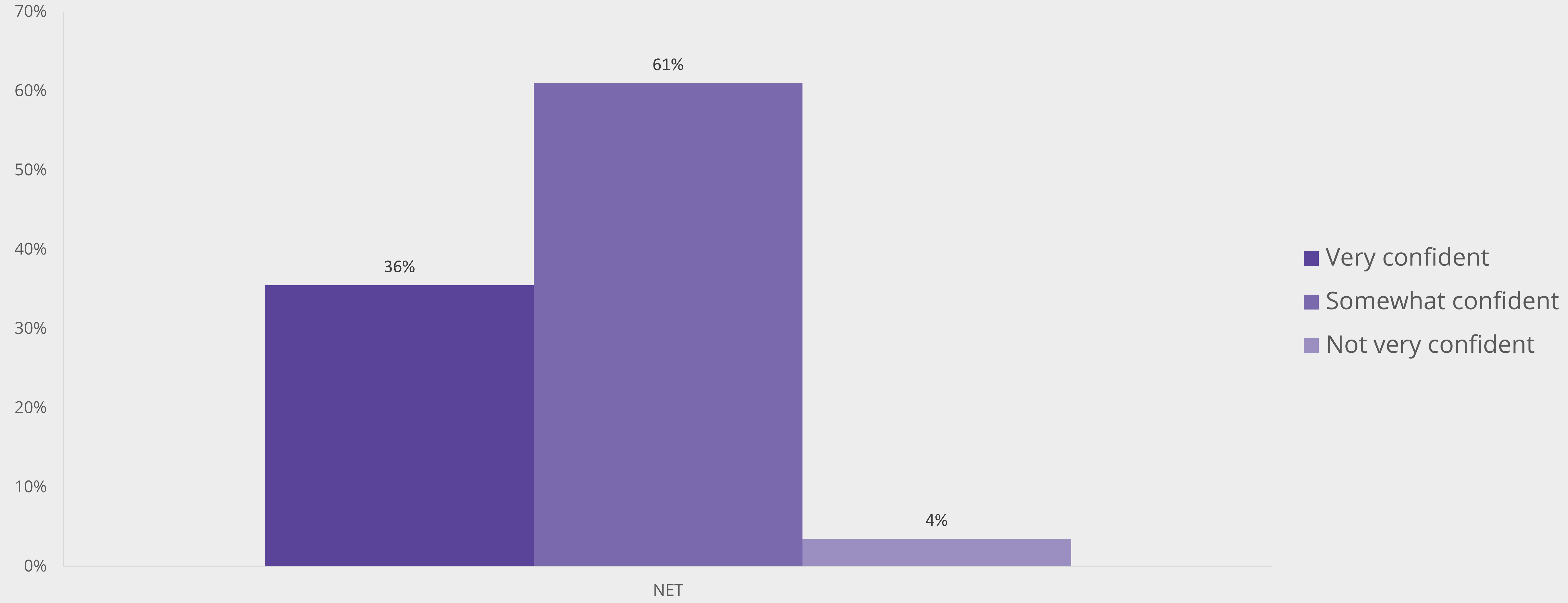
4. Does your organisation currently have robust and practiced policies and procedures for the conduct of Incident Management and Incident Response? by All



(C) OnePoll 2023; base n = 200

Back to top

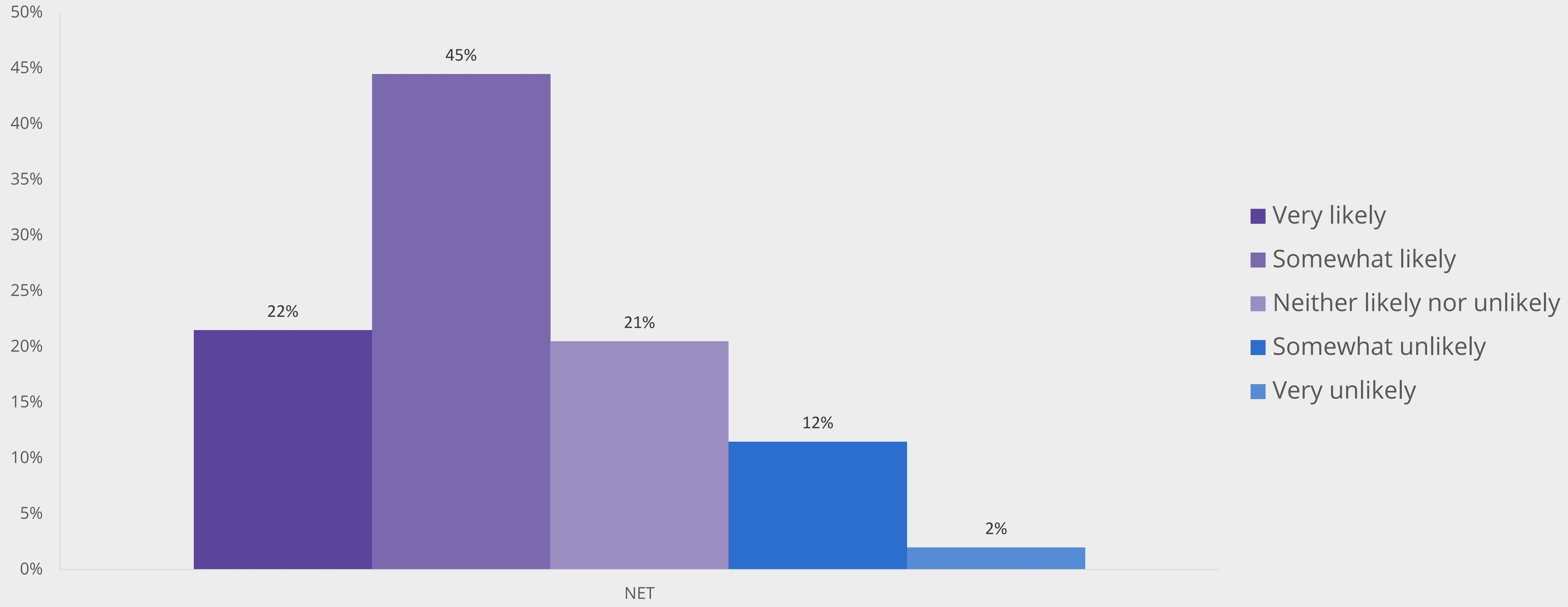
5. How confident are you, if at all, that you will have the resources you need to tackle any cyber and privacy threats over the next 12 months? by All



(C) OnePoll 2023; base n = 200

Back to top

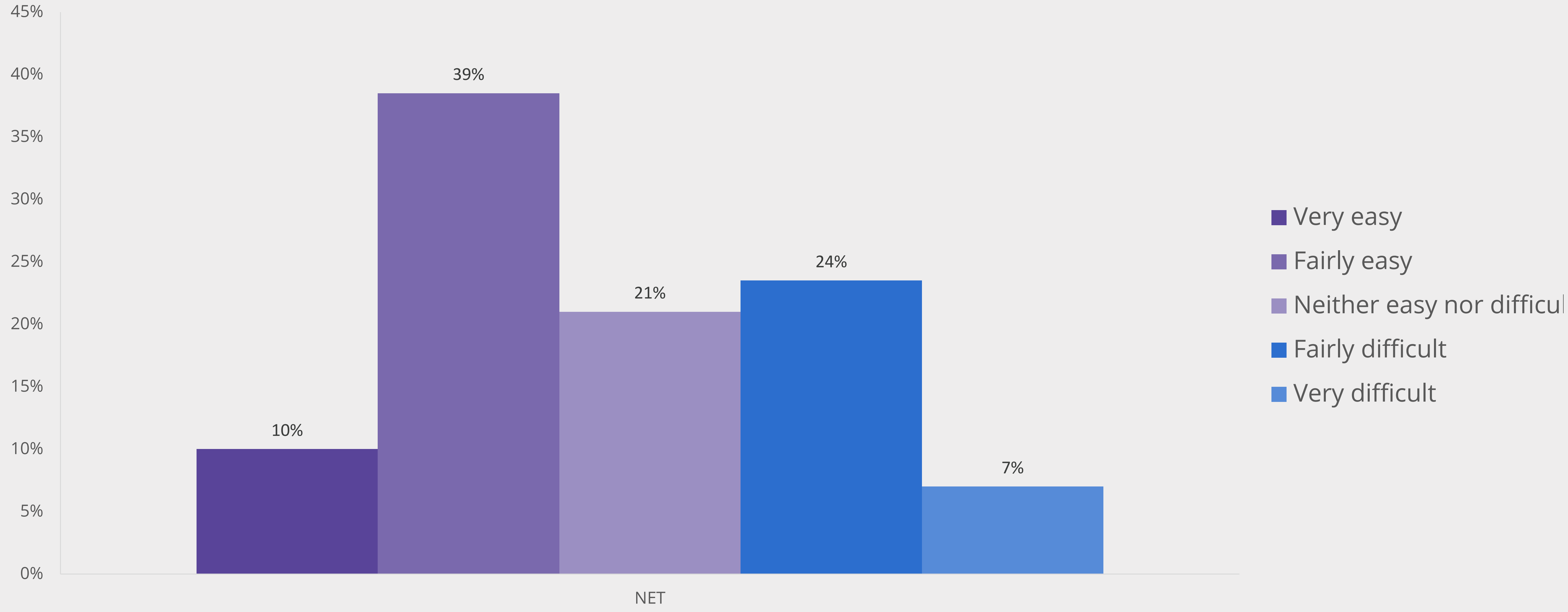
6. How likely or unlikely do you think it is that the cybersecurity and privacy teams will be asked to 'do more with less' in the next 12 months? by All



(C) OnePoll 2023; base n = 200

Back to top

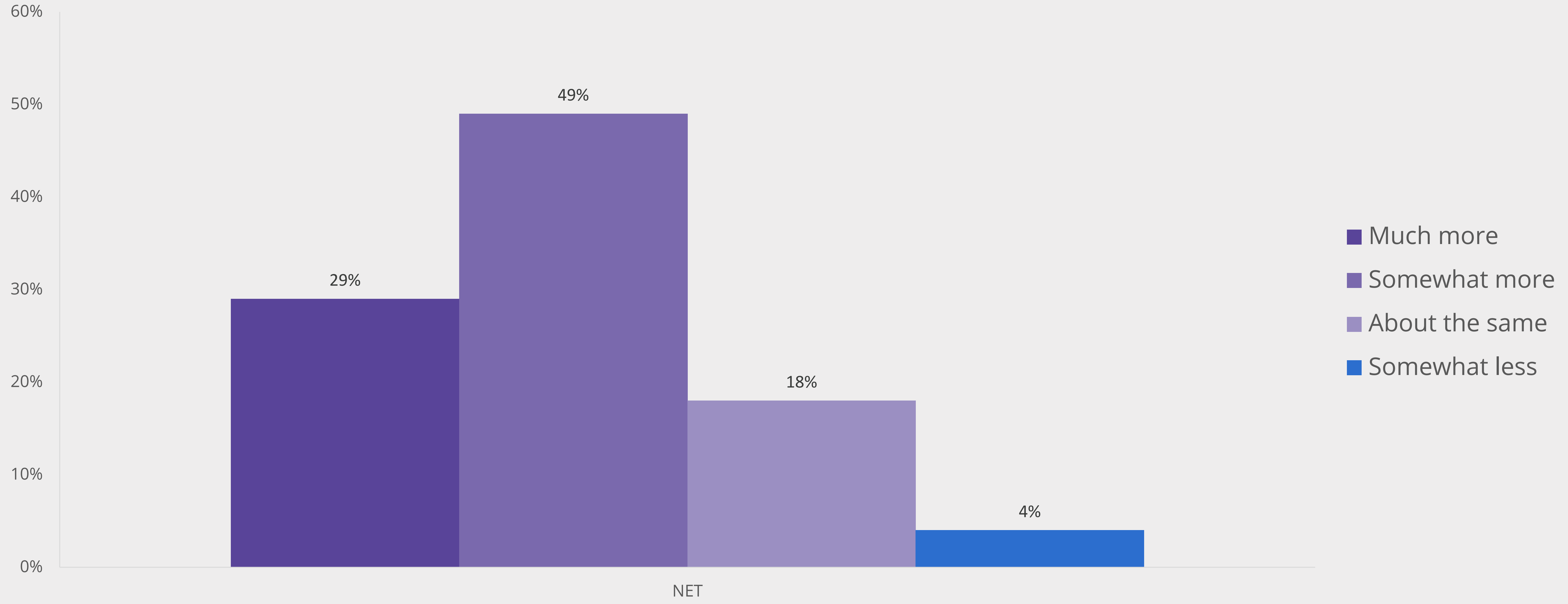
7. How easy or difficult does your organisation typically find to recruit and retain the right talent for its cyber security and privacy teams? by All



(C) OnePoll 2023; base n = 200

Back to top

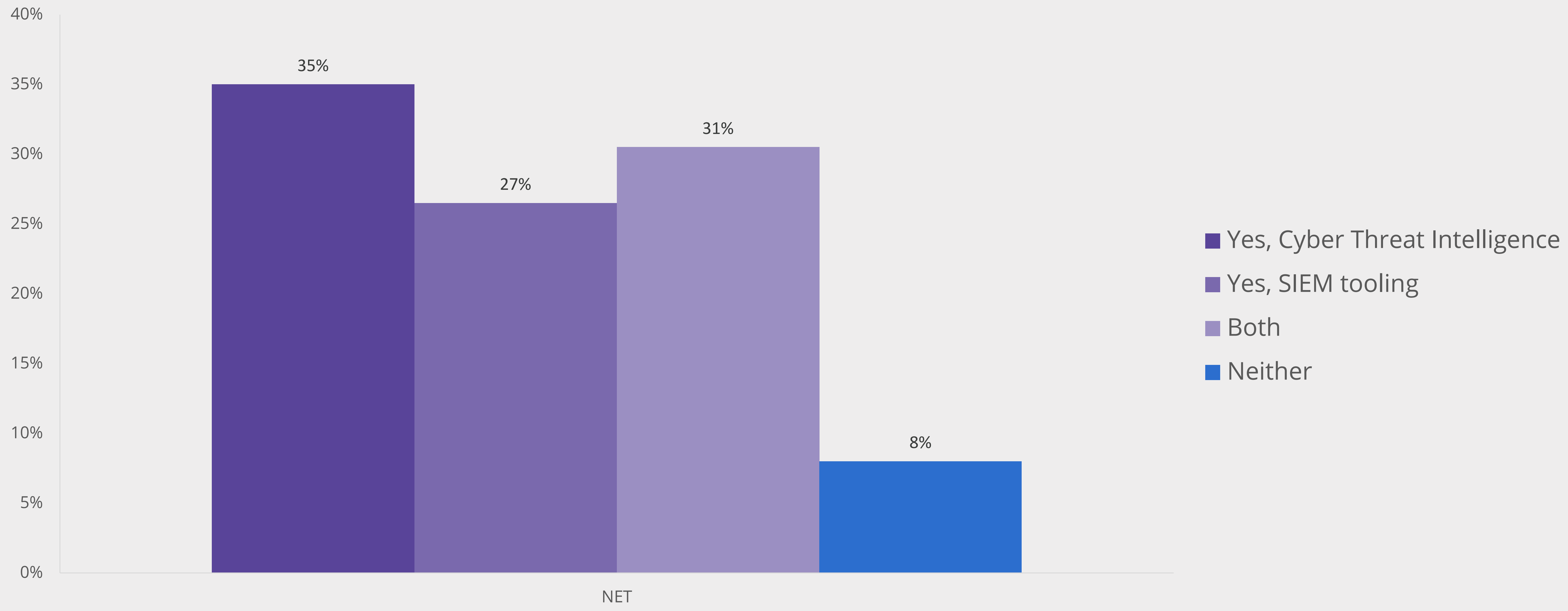
8. Will the cyber threat landscape become more or less complex and challenging over the next 12 months? by All



(C) OnePoll 2023; base n = 200

Back to top

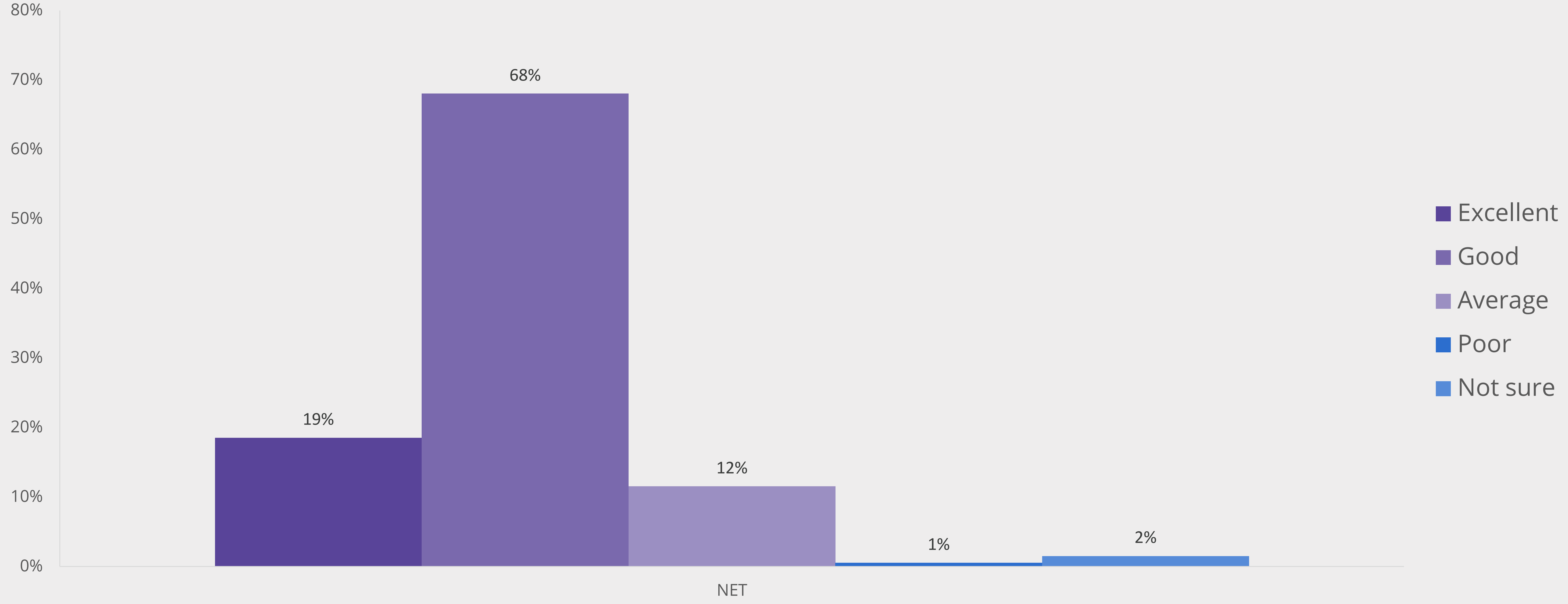
9. Does your organisation currently invest in Cyber Threat Intelligence (CTI) or SIEM tooling? by All



(C) OnePoll 2023; base n = 200

Back to top

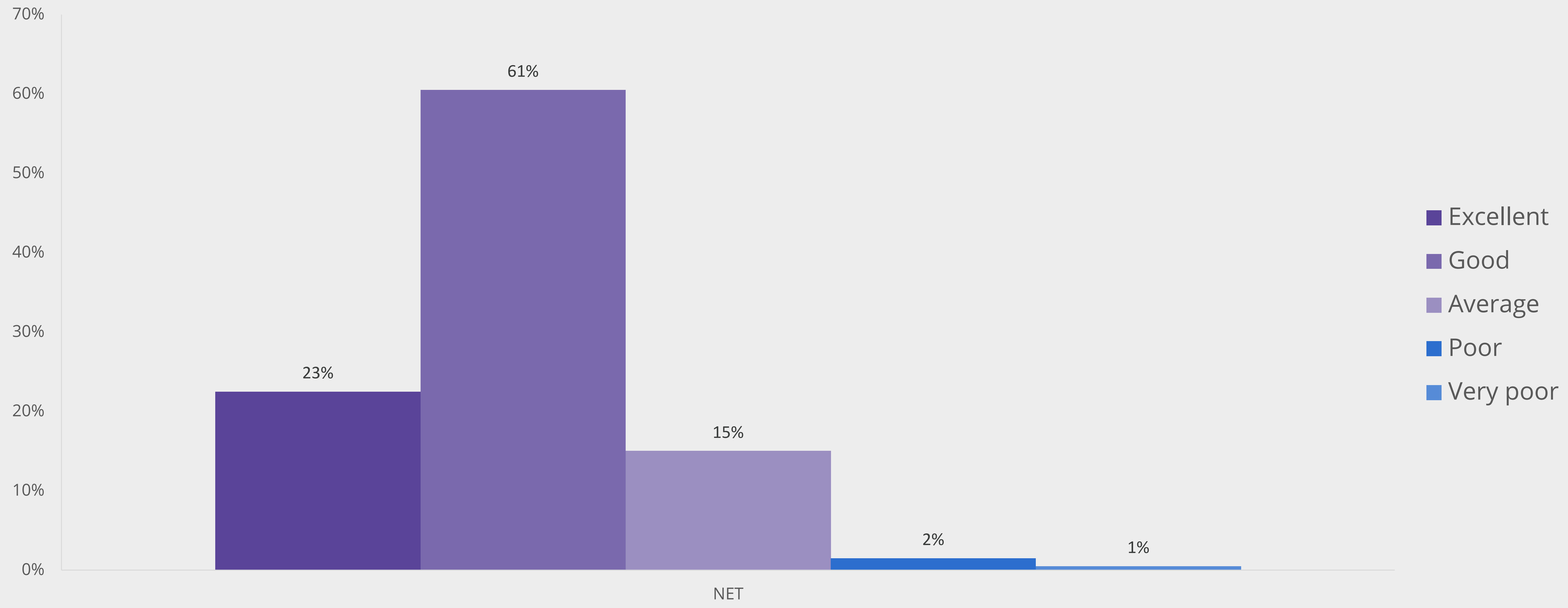
10. In general, how would you rate Cyber Threat Intelligence (CTI) providers ability to provide clear, actionable and prioritised information and reporting? by All



(C) OnePoll 2023; base n = 200

Back to top

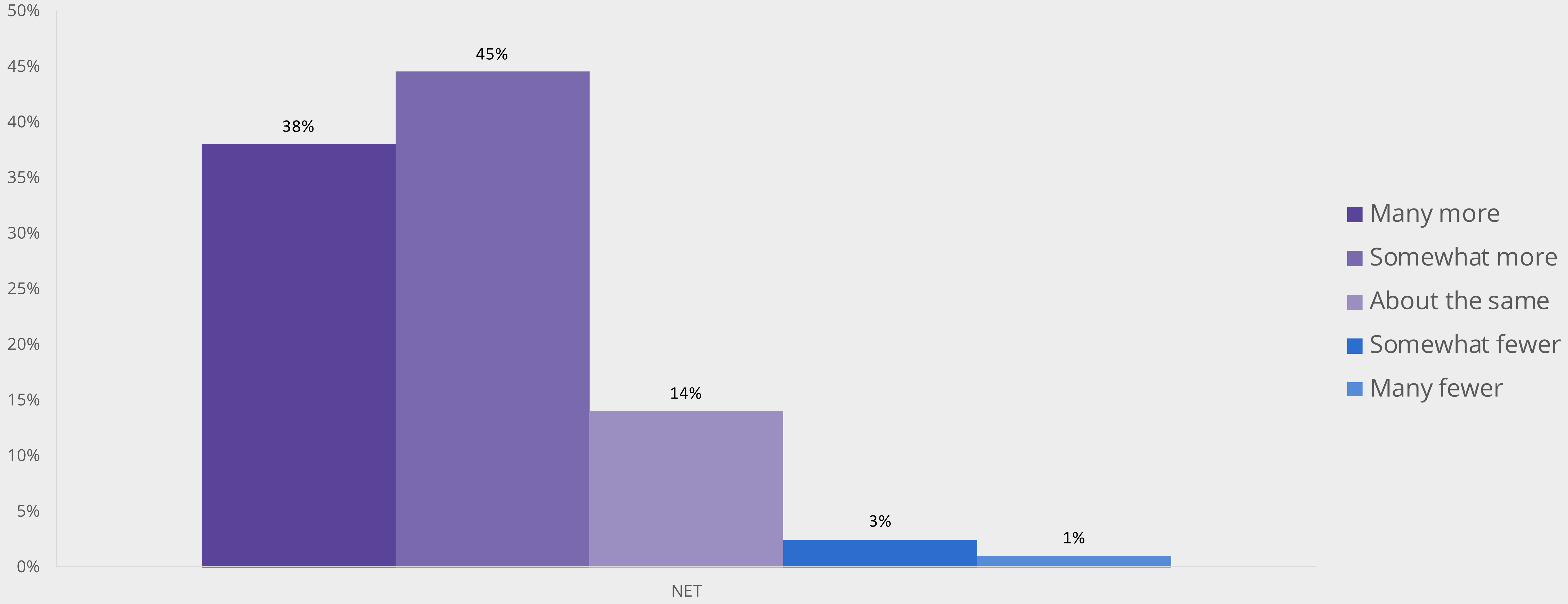
11. In general, how would you rate privacy professionals’ ability to provide clear, actionable and prioritised information? by All



(C) OnePoll 2023; base n = 200

Back to top

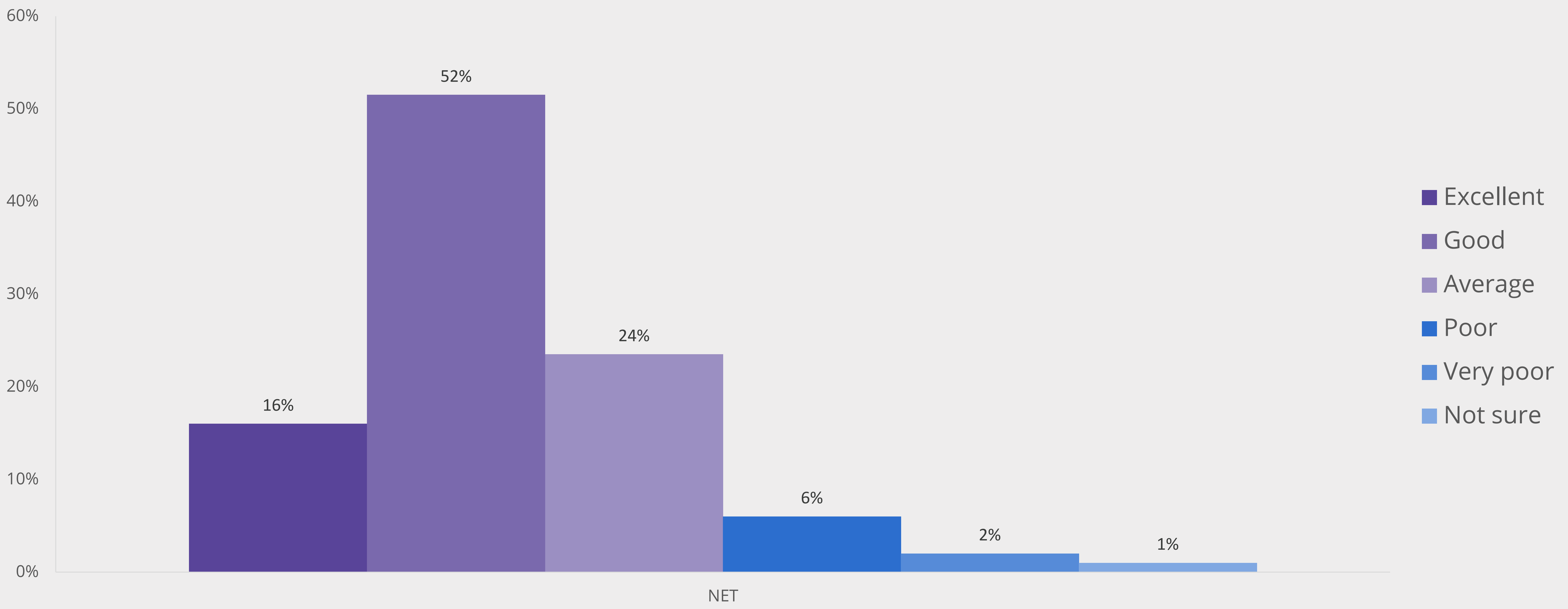
12. Over the next 5 years, to 2028, do you think we will see more or fewer cyber-attacks using GenAI tools such as ChatGPT and DALL-E (deep fake technology) than we currently see? by All



(C) OnePoll 2023; base n = 200

Back to top

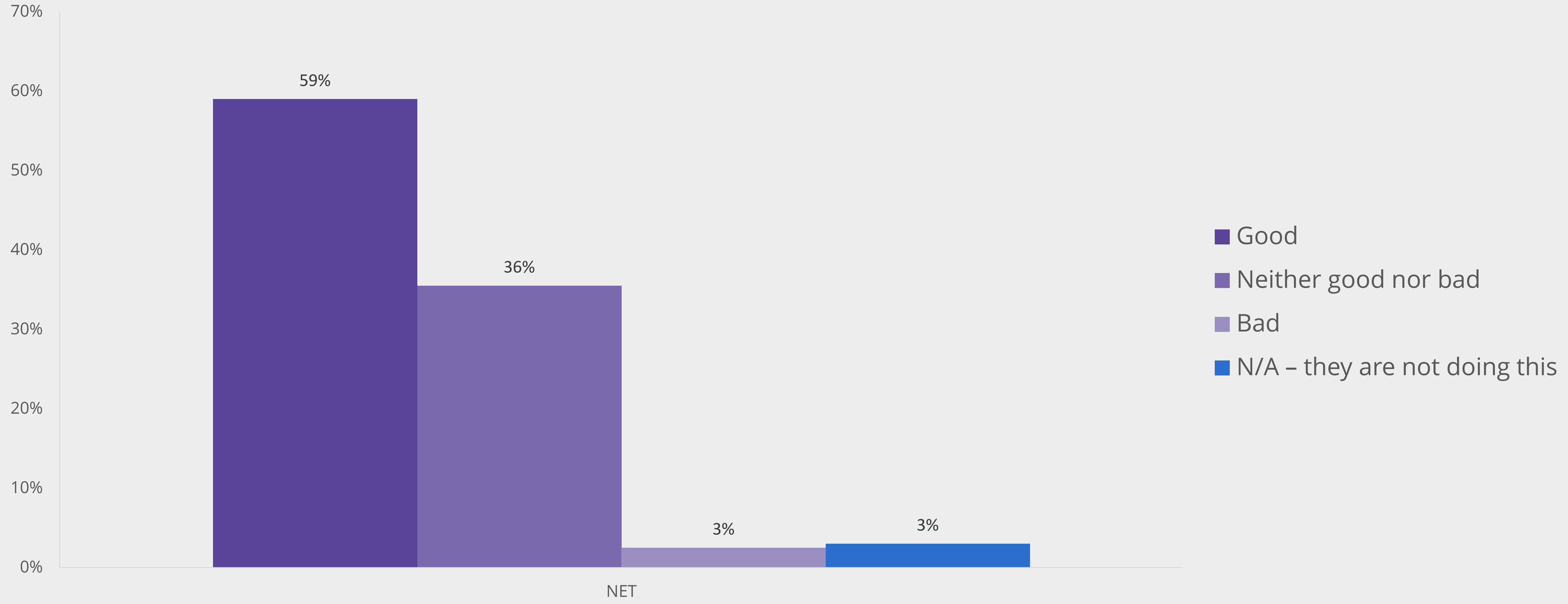
13. How would you rate your organisation's understanding of the risks of GenAI tools such as ChatGPT and DALL-E? by All



(C) OnePoll 2023; base n = 200

Back to top

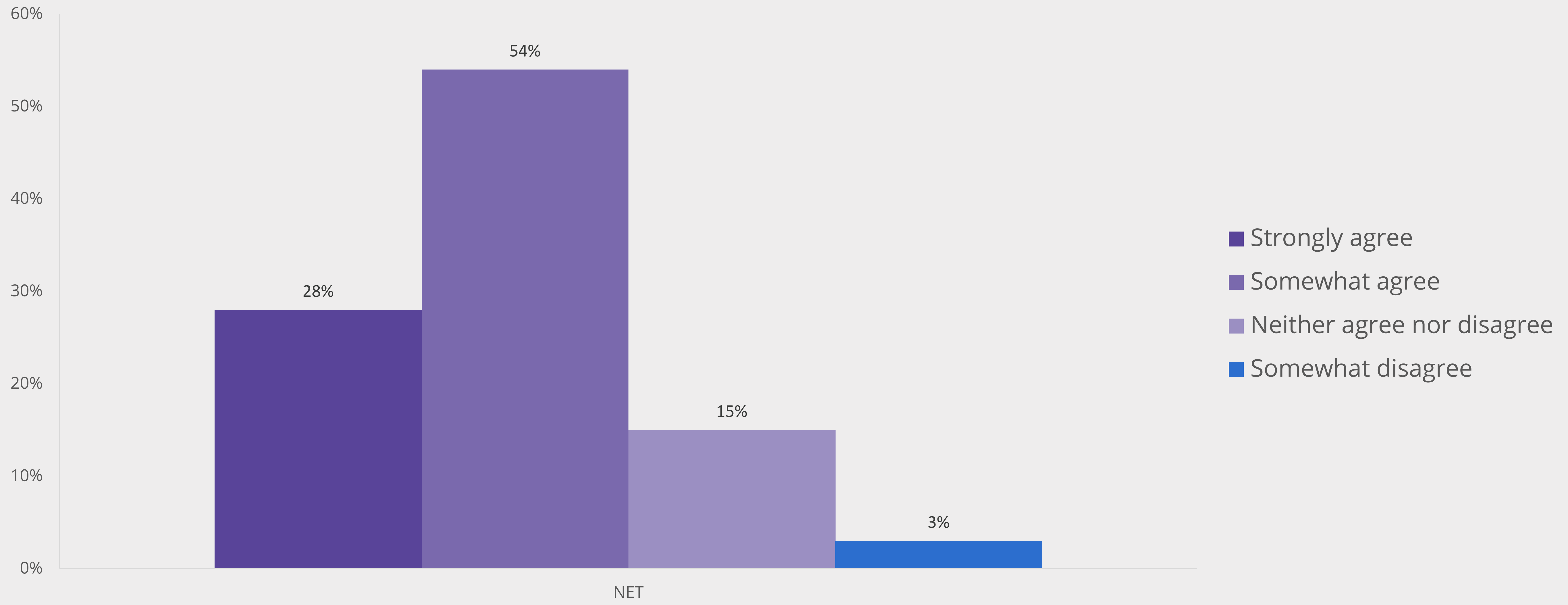
14. Is your organisation currently doing a good or bad job of controlling the risks associated with GenAI tools such as ChatGPT and DALL-E? by All



(C) OnePoll 2023; base n = 200

Back to top

15. To what extent do you agree or disagree with the following statement: “The upcoming Data Protection and Digital Information Bill and EU AI ACT, enable my organisation to develop and grow/or enhance our services”? by All



(C) OnePoll 2023; base n = 200

Back to top

Back to top

Visit us at www.gemserv.com or email BD@gemserv.com

Gemserv®

A Talan Company

Certified B Corporation