CLUBCISO™
Powered by Telstra Purple

Information Security Maturity Report 2023

clubciso.org

Founded and Funded by Telstra Purple

Executive Summary

Security culture making good progress despite human resource limitations.

The ClubCISO Information Security Maturity Report 2023 is a temperature check of 182 global CISOs, evaluating the security posture of organisations through the lens of culture, technology, risk, and people and comparing these findings against previous years. In 2023, there were **fewer material cyber incidents and breaches** across our respondents' organisations than in 2022 (which itself was a record low,) with 68% of respondents indicating that no material breaches had occurred at their organisation in 2023. On the whole, CISOs believe that their security culture is improving but is still a work in progress, yet the average rating for overall security posture was lower than last year.

Our respondents unanimously stated **that leadership endorsement is the most impactful factor in improving security culture**, and alignment between top management and security teams has improved compared to the previous year. While 51% of security teams have seen their budgets increase, on the whole, **it is to a lesser extent when compared with last year.** While the majority of our respondents feel that security culture is being negatively impacted by too many priorities and a lack of resources, it is personnel concerns that outweigh purely **financial constraints,** as CISOs feel their main barrier to meeting their objectives is insufficient staffing. In an effort to fix this, over 95% of organisations are trying **to retain talent and recruit new staff**, with a particular focus hiring for diversity to strengthen teams and bring different perspectives into the business.

of CISOs indicate that no material breaches had occurred at their organisation in 2023.

of CISOs listed leadership endorsement as the most important factor in fostering a better security culture.

of security teams have seen their budget increase.

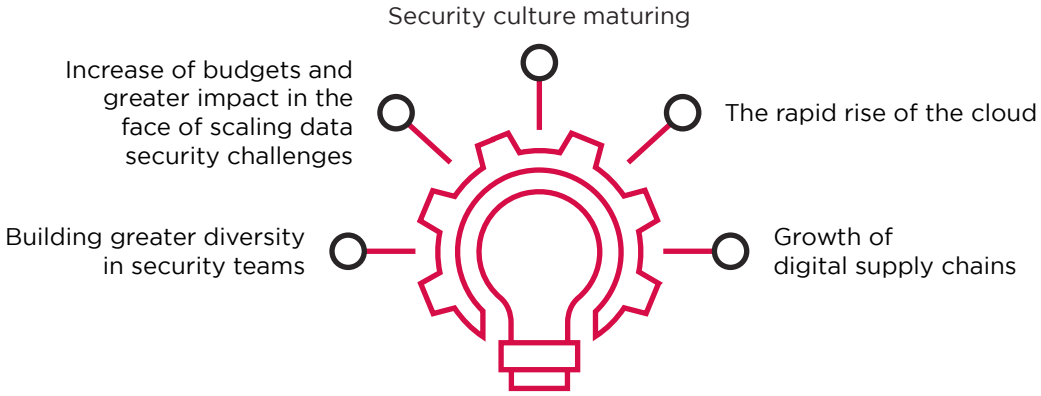
Contents

Executive Summary	2
Ten Years of ClubCISO	3
Culture	4
Technology	11
Risk	18
People	26
Telstra Purple perspective on the finding	36
Demographics	38
Methodology	40

Click here to see full survey results

Founded and Funded by Telstra Purple

Ten Years of ClubCISO



In the decade since its inception, the ClubCISO Information Security Maturity Report has provided a snapshot of the hopes, challenges, and opportunities of global information security leaders. In those ten years, more things have changed than have stayed the same.

Over the past ten years, the ClubCISO report has recorded and witnessed huge changes across the security industry itself and the CISOs attempting to navigate it. Alongside seismic global events like the COVID-19 pandemic, businesses and associated technology have evolved at break-neck speed. From the rapid rise of the cloud to the permeation of open-source components, or the growth of digital supply chains, CISOs have had to adapt to the times.

While early editions of the survey told a story of security awareness training and typically poor data breach prevention, in recent years, responses reflect a more mature environment with "security culture" concerns replacing awareness, and overall data breaches on the decline. The inaugural report from 2014 found that 67% of CISOs suffered a data loss incident in the last year. In 2023 however, 60% reported that no material cyber security incident had occurred in the same period - nearly a complete flip over the course of ten years. This sentiment that security posture has substantially improved is also shared by CISOs. In 2014, 75% rated their organisation's data loss prevention policy, strategy and solutions fairly poorly, either as level 1 or 2 ("initial" or "repeatable"). Compare this to 2023, and only 25% rated their organisations this low.

Another key question from the mid-2010s was CISOs' influence at the board level, but towards the end of the decade, we witnessed the CISO "come of age", with bigger budgets, more backing from their organisation, and a greater impact in the face of scaling data security challenges. In recent editions of the report, we've seen building greater diversity in security teams become more of a priority. The 2023 report has expanded on this theme, and digs deeper into how organisations aim to achieve this, and what the main perceived benefits are of doing so.

2014

of CISOs suffered a data loss incident in the last year.

2023

of CISOs reported that no material cyber security incident had occurred in the last year.

2014

of CISOs reported their organisation's data loss prevention policy, strategy, and solutions fairly poorly.

2023

of CISOs reported their organisation's data loss prevention policy, strategy, and solutions fairly poorly.

Click here to see full survey results

Founded and Funded by Telstra Purple

Culture

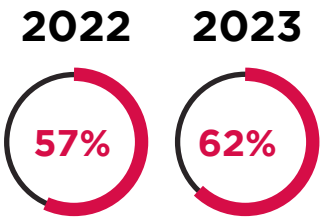
Culture
Technology
Risk
People

Click here to see full survey results

Founded and Funded by Telstra Purple

Culture

Leadership endorsement and alignment key to fostering a better security culture



of CISOs are feeling that their security culture is an ongoing priority but is making good progress.

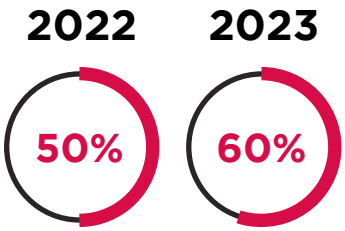
In last year's report, we observed CISOs continuing to make progress and improve organisational security culture in the disruptive environment of hybrid working. In 2023, we've seen this progression continue, with 62% of CISOs feeling that their security culture is an ongoing priority but is making good progress, compared to 57% in 2022. On the other hand, fewer respondents feel that their security culture is an exemplar of best practice, perhaps reflecting the bar gradually rising as the industry continues to collaborate and evolve. Overall however, CISOs feel they are moving in the right direction, with 80% believing that their organisation's security culture has improved to some degree in the last year.

As for factors that have the most influence in improving security culture, leadership endorsement was listed as the most important by the ClubCISO community, for the second year running with 60% listing it as a major influence. While proactive 'report it' no-blame policies (41%), simulated phishing (38%) and tailored training (37%) remain as the other key drivers of security culture, they did score lower than the previous year, perhaps showing reduced impact due to them becoming more of a well-established part of security culture. Alongside this, we are also seeing a stronger alignment between security and senior leadership teams compared to the previous year. This includes both the executive team (67% in 2023; 59% in 2022) and the board (54% in 2023; 49% in 2022).

On the other hand, the dual challenge of a growing list of priorities coupled with limited resources is holding security culture back. According to respondents, the top three factors most negatively impacting security culture over the last 12 months were too many competing priorities (61%), the security team being overstretched (44%), and a lack of resources to promote security awareness, behaviour, and culture (26%). On the whole, CISOs still feel that insufficient staffing is what is affecting their ability to deliver against objectives, but this has dropped slightly from last year (57% in 2022 vs 50% in 2023).

3 factors impacting the security culture:

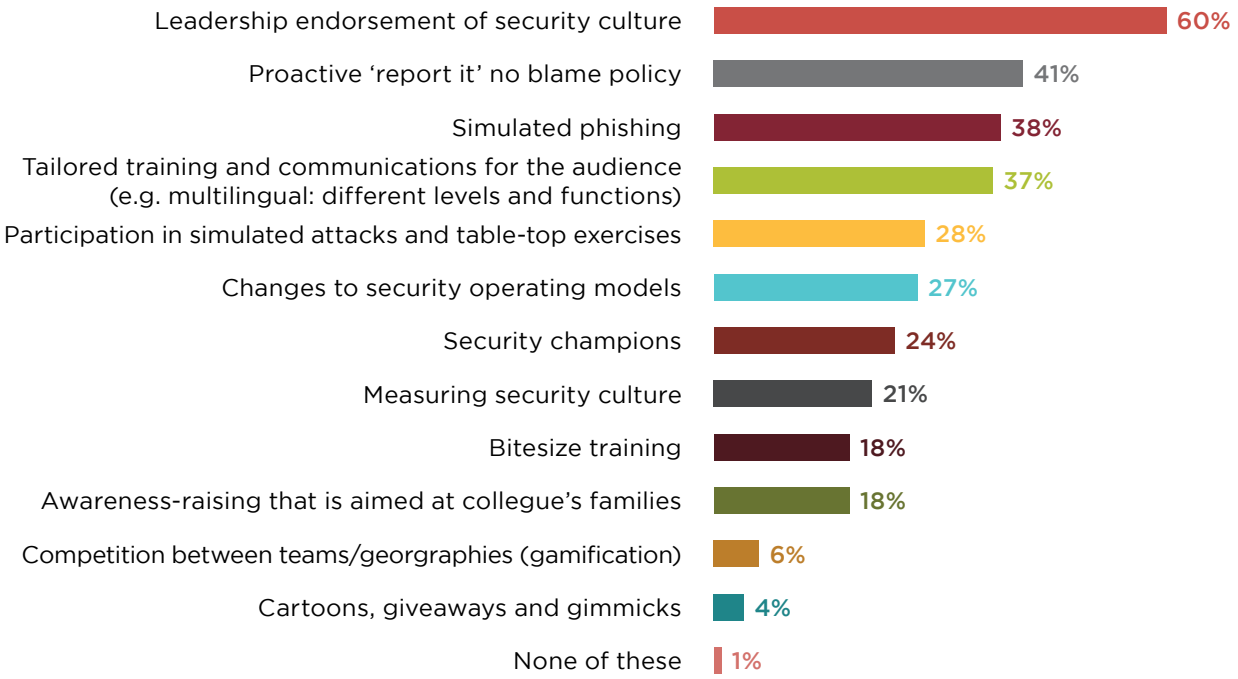
- **Security team is overstretched and under-resources**
- **Having too many competing priorities**
- **Lack of resources for security awareness, behaviour and culture**



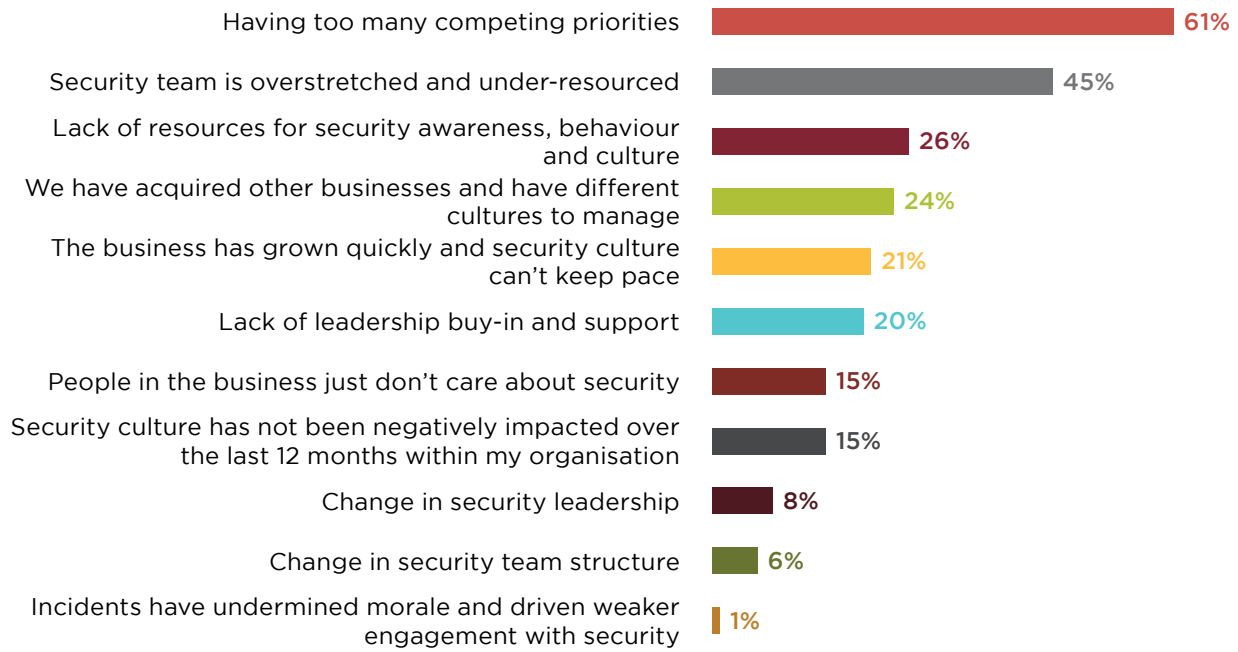
of CISOs listed leadership endorsement as the most important factor in fostering a better security culture.

Click here to see full survey results

Q7. Which of the following have been most effective at fostering a better security culture over the last 12 months within your organisation?



Q8. Which of the following have most negatively impacted security culture over the last 12 months within your organisation?



Advisory Board Perspective
Jessica Barker

As ClubCISO celebrates ten years of its community, we can reflect on progress made in the human side of cyber security - culture is a key part of the agenda like never before.

Our findings this year acknowledge the crucial role that leadership endorsement plays in security culture. Members also reported stronger alignment between security teams and senior leadership, suggesting greater harmony at an organisational level. This is highly encouraging progress. Without tone (and resource) from the top, building a healthy security culture is even more challenging.

Most leaders feel that their organisation is rising to the challenge. Yet, the number of leaders who believe their security culture is an exemplar of best practice has dropped compared to 2022. Does this mean that excellence in security culture has declined? It seems far more likely that this can be attributed to a deeper understanding of what it means to be an exemplar of best practice and how long it takes to change and improve culture.

Is this the year that security awareness, behaviour and culture have been elevated from a tactical to a more strategic level? Senior stakeholders recognise that security is a critical risk and are more engaged in cyber security as a whole, as well as security culture in particular. Alongside this, mechanisms for raising awareness and influencing culture, such as simulated phishing and tailored training, scored lower in terms of their effectiveness in influencing culture this year compared to 2022. Rather than seeing this as a sign of the dilution of their effectiveness, we should consider these findings more widely. Perhaps we need to recognise that it is not the tools themselves which raise the bar, but rather how they are used and the organisational context within which they are applied.

In light of the challenging circumstances we continue to find ourselves in, our findings suggest very promising progress. The greatest concern for CISOs this year is insufficient staff, followed by the culture of the organisation. It is no surprise that demanding priorities and limited resources are holding security culture back. Many teams are over-capacity, with even fewer people dedicated to security awareness, behaviour and culture. Despite the growing recognition of the importance of security culture, it is often harder for leaders to obtain a budget for the human side of security compared to technology. This challenge persists, despite the fact that social engineering remains the most common attack vector for material breaches.

Looking to the future, we can hope for a continuation of the elevation of security - and security culture - as a strategic, business issue. We must recognise the time and dedication it takes to build positive, proactive, and robust security cultures and we should acknowledge the progress we have made, and continue to make, despite the challenges and constraints.

Dr. Jessica Barker
Co-CEO and Co-Founder at Cygenta
Advisory Board

Connect on LinkedIn

Click here to see full survey results

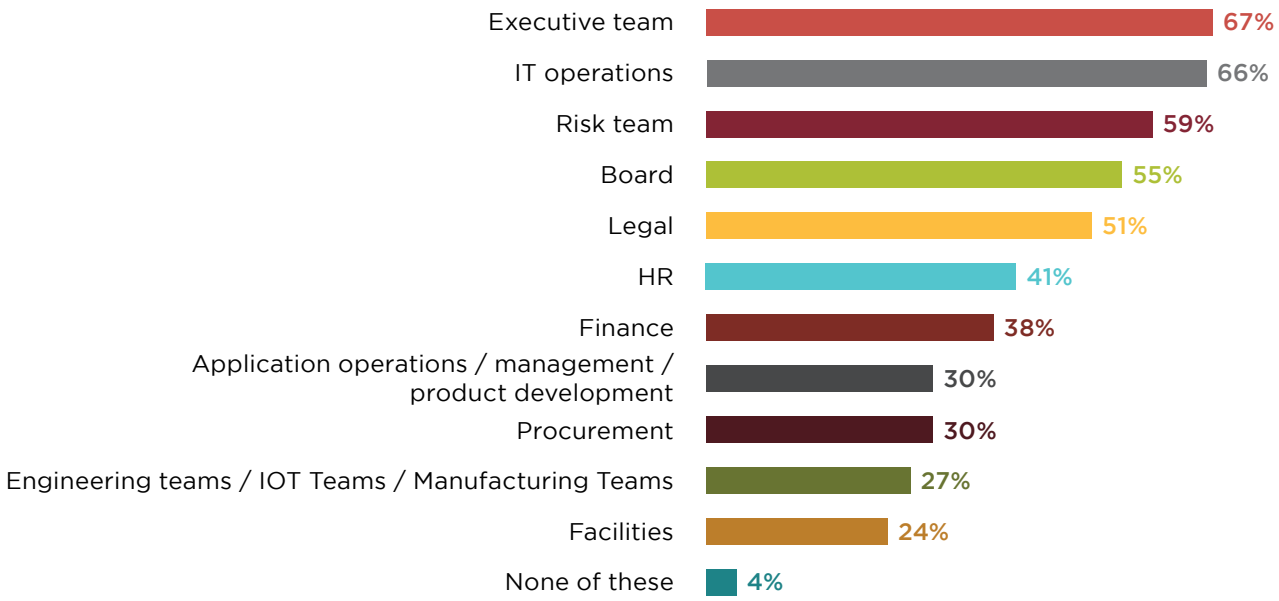
Additional Findings

Q6. Hand on heart, are you establishing a good security culture?

Q9. How has your security culture evolved over the past year?

More than **80%** say it has improved

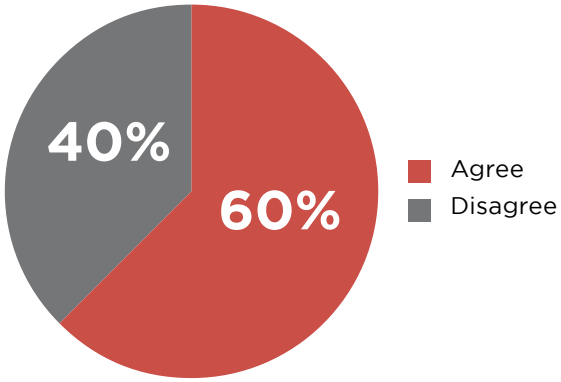
Q10. I am comfortable with how well security is aligned with these areas of my organisation right now



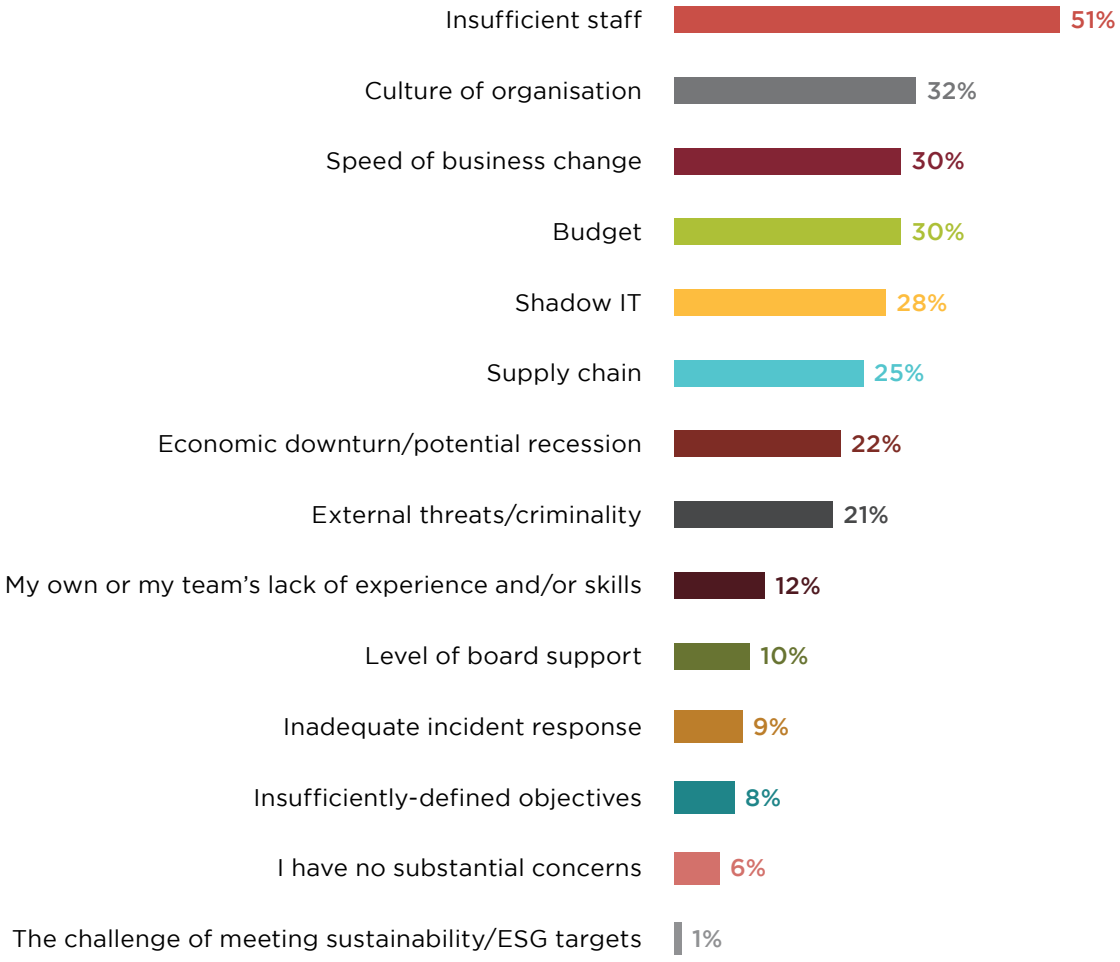
Click here to see full survey results

Founded and Funded by Telstra Purple

Q11. The business measures and / or reports on the value I add to it



Q12. Which of the following concerns most affect your ability to deliver against your objectives?



Q13. Do you think risk and threat management challenges are getting easier, harder, staying the same?

4.9

Average Rating

Much Worse  Much Better

Q14. How does security culture drive value and encourage innovation within your organisation?

Technology

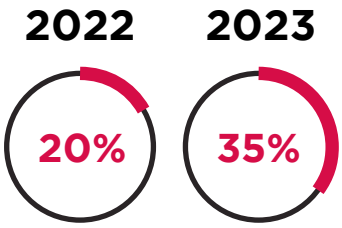
Culture
Technology
Risk
People

Click here to see full survey results

Founded and Funded by Telstra Purple

Technology

Keeping pace with the industry while security spend slows



number of organisations whose security budgets remained flat.

A lack of resources for security teams is a common theme in the Information Security Maturity Report. Despite security budgets continuing to increase, this year's survey suggests that this may be slowing down. While 51% reported that their budgets had increased compared to last year, compared to the 2022 report, the degree of increase was typically lower across the board. The number of organisations whose security budgets remained flat also increased from 20% last year to nearly 35% in 2023. Finally, 13% of this year's respondents reported having reduced budgets or no access to any budget whatsoever - while alarming, these numbers are consistent with last year.

When asked about the **key factors contributing to an increase or decrease in security spending,** most of the increases seem to be driven by a need to keep up with the pace of change. The evolution of the cyber threat landscape was listed as the single biggest factor (39%) while keeping up with peers (21%) and investing in recruitment and training (18%) were also common influences. On the flip side, limitations on budgets appear to be in response to economic downturn (34%), profit and loss pressure (30%), and geopolitical unrest (17%).

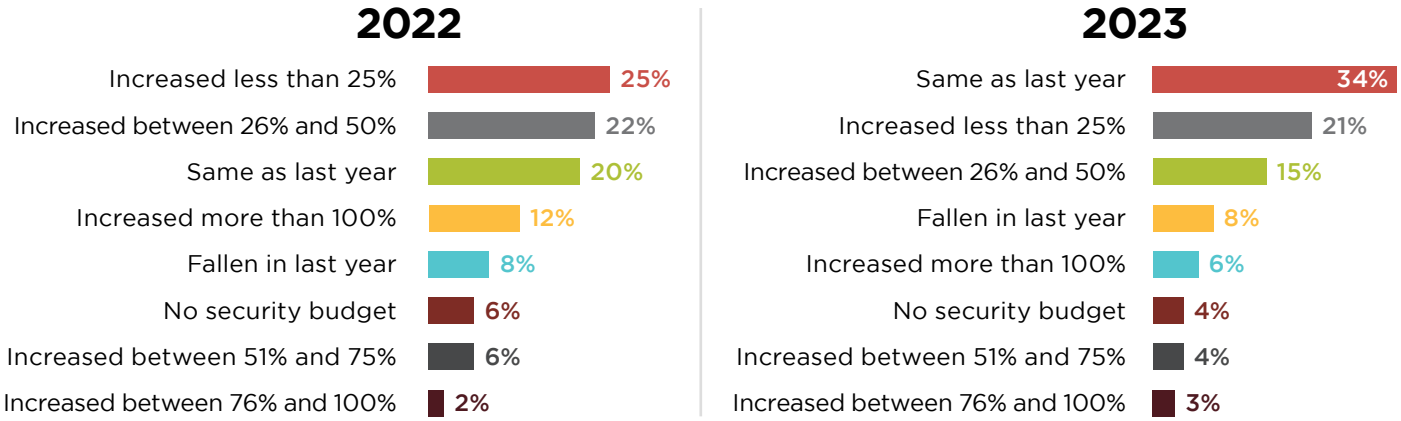
Key factors contributing to an increase or decrease in security spending

- **Cyber security landscape (39%)**
- **Keeping up with peers (21%)**
- **Investing in recruitment and training (18%)**

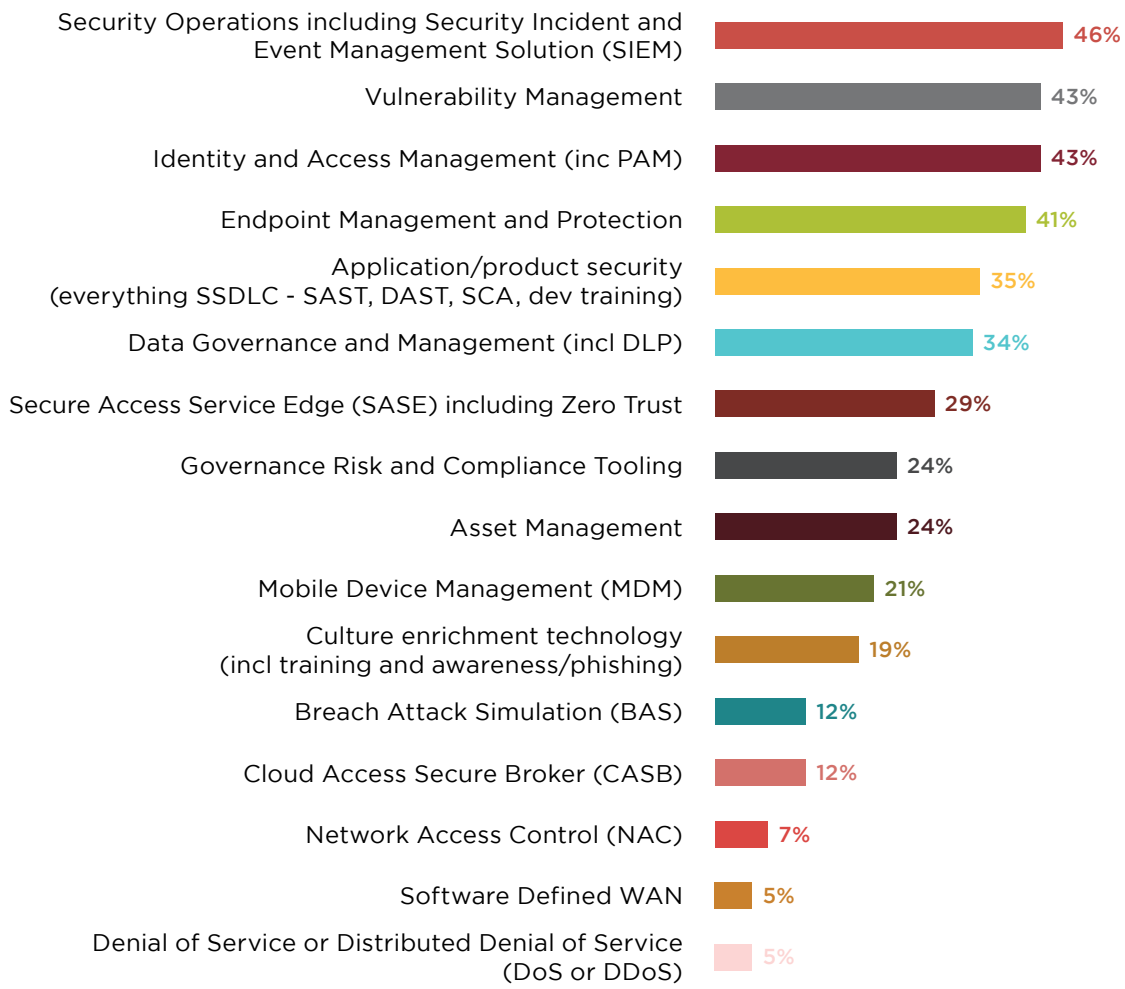
In terms of where organisations invest their security budget, we can see a fairly even spread across our respondents. Within the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, and Recover) there is a three-way split between prioritising investment in protection and detection (46% for both), and funding across all five processes equally (see Q30 - Risk). While specific technology investment priorities are similarly disparate, the most common solutions at the top of CISO's lists are **Security Information and Event Management (46%), Vulnerability Management (43%), and Identity and Access Management (43%)**. This is very similar to last year, with only Governance, Risk and Compliance Tooling seeming to have fallen down the list of priorities in 2023, with 10% fewer respondents listing it as a priority.

Click here to see full survey results

Q16. Describe your organisation's current information security budget relative to last year



Q21. Which of the following are your highest technology investment priorities?



Click here to see full survey results

Advisory Board Perspective
Manoj Bhatt

Focusing on the last four years, cyber security has been through a major transformation. Four years ago, I remember discussing the need for cyber security to be given a seat at the boardroom table and not to be seen as an overhead. We wanted businesses to recognise the importance of cyber security, and sometimes it felt like an uphill battle to get our point across.

Roll forward to 2023 and the majority of budgets have increased or at least remained the same. This demonstrates the increasing importance of cyber security within our businesses. We are seen as leaders not just in the cyber security space but also within the main operations of our businesses at board level. As the complexity and volume of cyber attacks and threats increase, more and more businesses are recognising the need for continued investment in order to manage these day-to-day cyber problems.

Cyber security, once seen as a hygiene factor or a nice to have, is now able to demonstrate that it's more than that. Cyber security can be seen as a business enabler, and this was clearly demonstrated in supporting our businesses during the pandemic.

Cyber security can give companies a competitive advantage and is now seen as a revenue generator as citizens and businesses become more and more selective about what the security credentials of a business should be. More importantly, boards are increasingly concerned with how they compare to their peers in the market, something the CISO needs to understand at a macro level rather than just focusing on themselves as a business.

Cyber security, for the first time through the use of technology, has the ability to save businesses money. In 2021 and 2022, the hot topics that CISOs mentioned included cyber resiliency, security culture and cloud security. For the first time this year, cloud security did not feature in the top three. This year, however, security culture and cyber resiliency continue to be the top two hot topics on CISOs' radars.

This shows that we are utilising the cloud as a part of day-to-day business and the move to the cloud has allowed CISOs to utilise cloud-native tools to improve their security posture and subsequently reduce their risks. Conversely, even as we become more used to the cloud, we still do not feel confident in the cloud and the maturity of our cloud environments still remains "Defined", where it has remained for many years. My view is that as the cloud evolves we are recognising it's not just one technology that we need to understand, but a collection of technologies which we then need to integrate into our business, along with the people and processes.

We have made some really great progress and as technology allows us to better align with the business, there are still a number of areas that we have not solved. As we continue to use cloud in different ways, and as the cloud continues to evolve, all of the elements that we might have in place may need revisiting. Security culture and monitoring of our environments, through a SOC / SIEM are still high on the list of tactics that we will be focussing upon. These are not new topics, however, as the environments that we utilise keep evolving to support the business, the likelihood is that we are going to review some of the foundational elements such as policies that we have in place to ensure that they remain fit for purpose.

Manoj Bhatt
Cyber Security Team Lead
Advisory Board

Connect on LinkedIn

Click here to see full survey results

Additional Findings

Q15. Which of these hot topics are on your radar for the coming year?

Q17. Which factors have contributed to an increase or decrease in your organisation's current information security budget relative to last year?

Click here to see full survey results

Founded and Funded by Telstra Purple

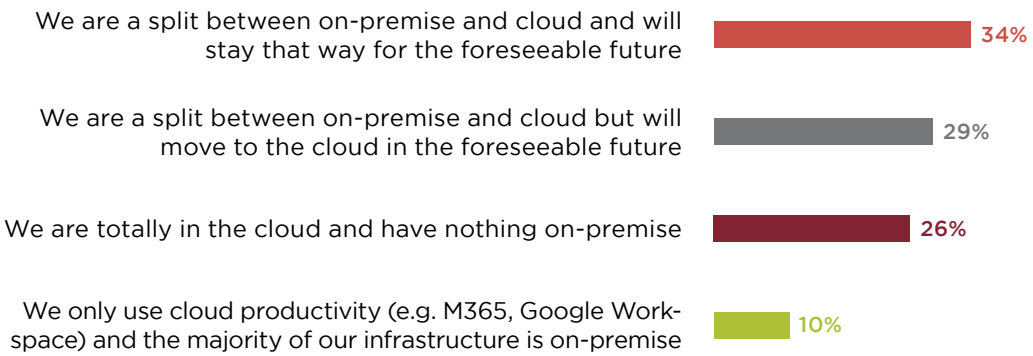
Q18.Where you have business critical workloads running in the cloud, how do you rate the maturity?

2.9

Average Rating

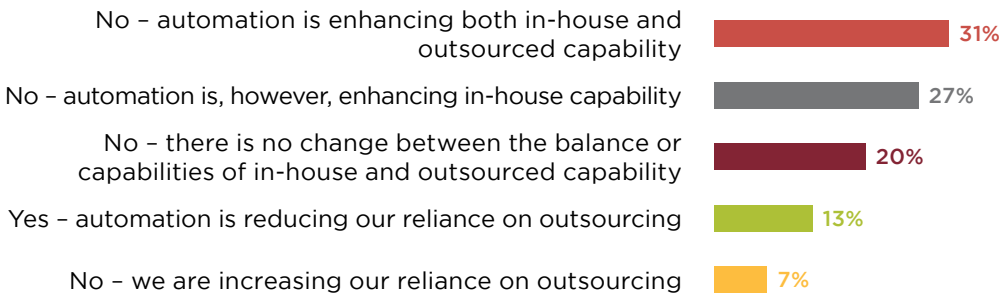
Initial (Lowest)	Repeatable	Defined	Managed	Optimising (Highest)
9%	**25%**	**33%**	**25%**	**6%**

Q19. How is cloud currently implemented in your organisation?



Q20. Which of the following tactics are you focusing on to accelerate your cyber security strategy from last year?

Q22. Is automation of security technologies changing the balance of insourcing vs outsourcing for your organisation?



Risk

Culture
Technology
Risk
People

Click here to see full survey results

Founded and Funded by Telstra Purple

Risk

Material cyber security incidents and breaches on the decline

2022

of CISOs stated that no material breaches had occured at their organisation.

2023

of CISOs stated that no material cyber security incided had occured at their organisation.

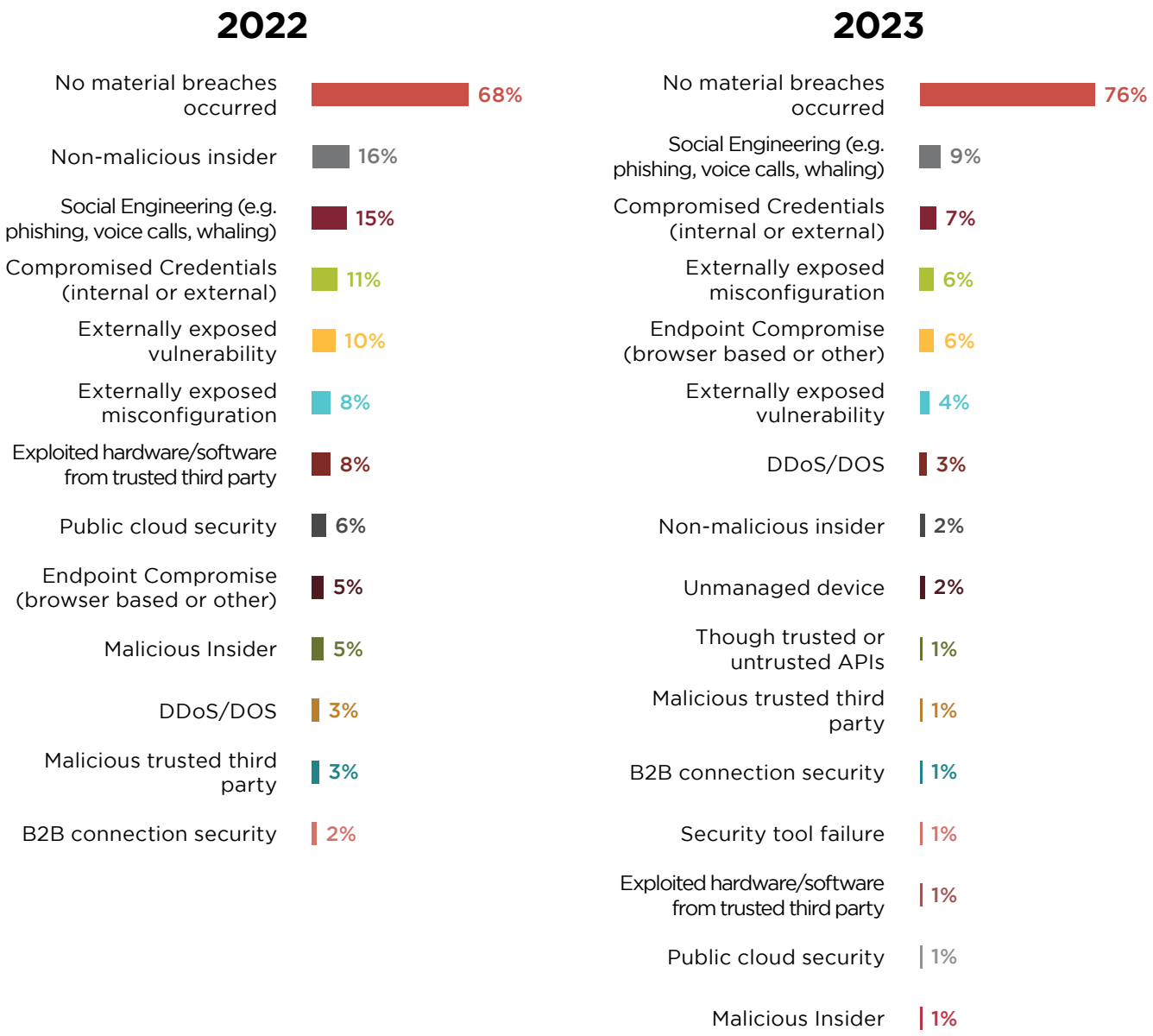
Despite ongoing internal and external challenges, this year's ClubCISO Report once again paints an optimistic picture of organisational resilience from security threats. In 2022, 68% of respondents indicated that no material breaches had occurred at their organisation and 54% stated that no material cyber security incident had occurred. This year, there has been even less, with 76% stating that no material breaches had occurred and 60% stating that no material cyber security incident had occurred in the past 12 months.

This apparent success of security teams is particularly interesting given that CISOs on average rate their organisation's overall security posture lower than they did last year. In 2022, we saw the best scores of the report's ten-year history in this regard. This year, however, saw a relative drop in confidence from CISOs. Last year, 46% rated themselves as above average (at least 4/5 stars) while this year, only 38% rated themselves the same. Additionally, more than 13% of respondents don't feel confident that their organisation will be able to meet key security objectives - an exact repeat of last year's result.

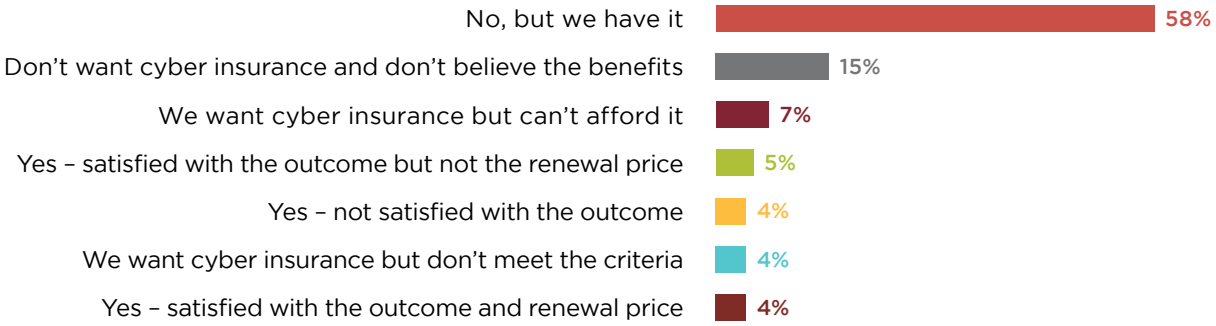
Cyber Insurance

Cyber insurance remains a very divisive issue amongst the ClubCISO community. Almost identically to last year, 15% of CISOs don't want cyber insurance and don't believe in the benefits. However, most of our respondents (72%) do have it. Of the organisations with insurance, 18% have attempted to make a claim. There is further division among this group, as 29% were satisfied with the outcome and the renewal price, 38% were satisfied with the outcome, but not the renewal price and 33% were dissatisfied with the outcome altogether. This final group is the one area where we saw a real change from last year, where not a single respondent said they were unsatisfied with the outcome of their insurance. Finally, on the more philosophical side of the debate, over half (54%) of respondents agree that cyber insurance is exacerbating the issue of ransomware to some extent, while 14% disagree.

Q28. Through what vectors did a material breach occurin your organisation in the past 12 months?



Q32. Has your organisation ever claimed on cyber insurance?



Click here to see full survey results

Founded and Funded by Telstra Purple

Advisory Board Perspective Stephen Khan

The last 12 months have highlighted some interesting observations from our global membership as we adjust to new ways of working, and organisations have fully embraced a hybrid working model.

Most of our members have not suffered material incidents, and most organisations believe their board and stakeholders are largely focused on maintaining or operating within risk appetite.

Although many members believe no material incidents have been observed. Of those who had incidents, many were attributed to non-malicious insiders through accidental or human error, with a similar number indicating incidents were attributed to malicious outsiders. Due to the varying nature of assessing incidents within organisations, two areas are worthy of note; vulnerabilities and misconfiguration were of particular concern to members when it came to protecting their organisations.

Despite the complexity of supply chains, and the distributed nature of ecosystems to deliver services using Cloud, on-premise, and outsourced security capabilities, most members believe they have good supply chain practices in place.

When it comes to maintaining an organisation's security risk posture, most members have well-managed and repeatable processes in place; complimented by continuous improvements to adapt to the changing security landscape.

In relation to where security investments are being directed to protect organisations; the top was for protect and detect capabilities, followed by response and identity with recovery coming in third place. Whilst recovery is in third place, it must be noted, this area is often managed and operated by IT teams and may not be reflective of the effort of organisations to ensure they have adequate BCP/DR planning in place to recover from major ransomware attacks.

Despite the challenges around the changing threat landscape and hybrid working patterns, the majority of our members are confident in maintaining their security posture. Members are also very cautious about claiming any kind of victory as maintaining and continually securing their organisations has always been a challenging, and stressful endeavour.

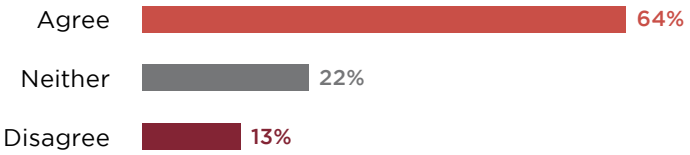
Whilst members are in broad agreement on the strategic direction to protect their organisations, they are less in agreement when it comes to cyber insurance. This remains a very divisive issue amongst the diverse cross-industry ClubCISO community. Most members believe Cyber insurance has a part to play, however they express clarity on the outcomes from policies must be understood. Members believe cyber insurance must complement in-house capabilities, with specialist advice, and support from credible suppliers.

Stephen Khan
Chairman, ClubCISO
Advisory Board

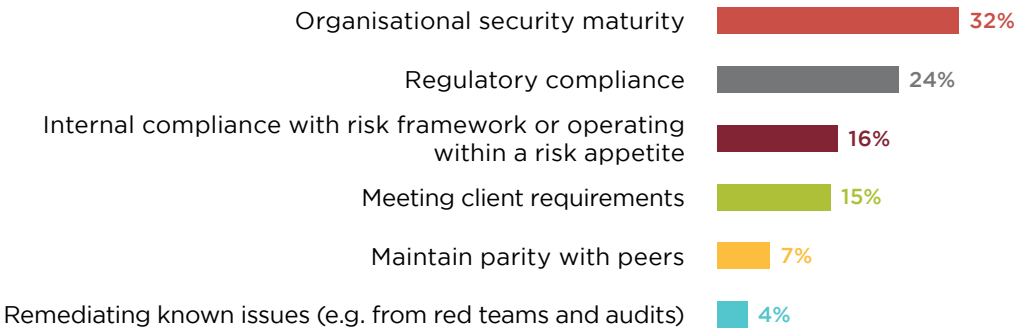
Connect on LinkedIn

Additional Findings

Q23. I am confident my organisation is currently able to meet key security objectives



Q24. Which of the following is your board currently most focused on with regard to cyber security?



Q25. Rate the maturity of your process to measure, manage and assure supply chain risk

2.8

Average Rating

Initial (Lowest)	Repeatable	Defined	Managed	Optimising (Highest)
17%	**16%**	**41%**	**23%**	**1%**

Click here to see full survey results

Founded and Funded by Telstra Purple

Q26. Rate the maturity of your organisation's overall risk management programme

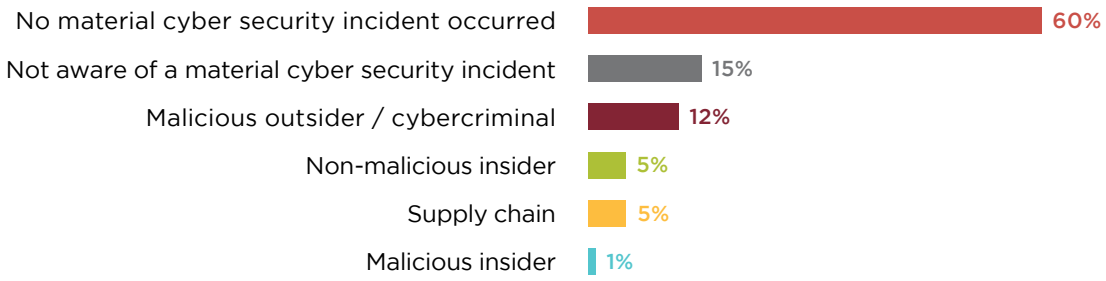
3.0

Average Rating

★★★☆☆

Initial (Lowest)	Repeatable	Defined	Managed	Optimising (Highest)
9%	20%	35%	29%	3%

Q27. What activities have led to a material cyber security incident in the past 12 months? (Incidents may be material if they have significant impact on the company's financial position, operation, or relationship with its customers.)



Q29. Rate your organisation's security posture

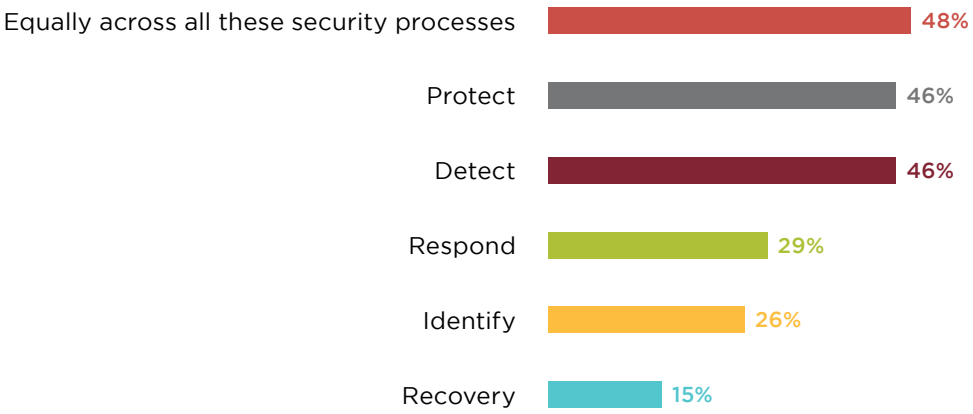
3.1

Average Rating

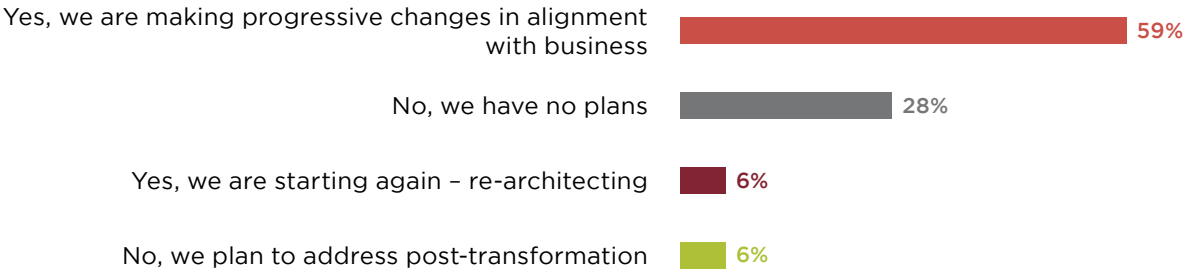
★★★☆☆

Initial (Lowest)	Repeatable	Defined	Managed	Optimising (Highest)
4%	20%	37%	31%	6%

Q30. With the NIST Cyber Security Framework in mind, where and how does your organisation direct investments to improve your security maturity and capability?

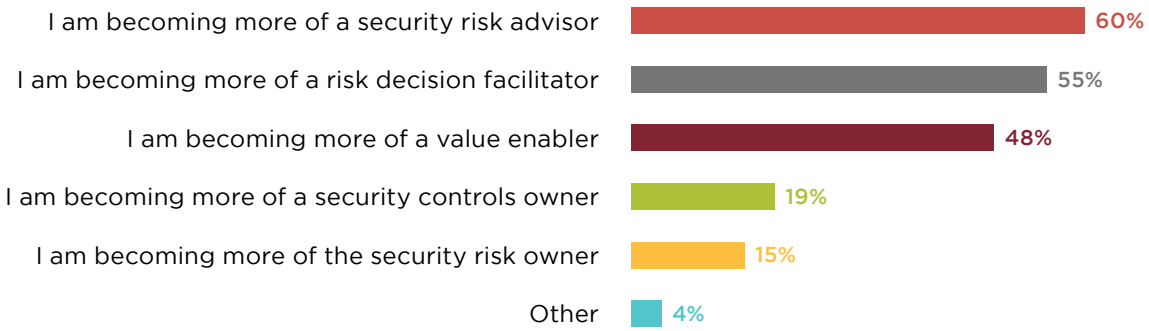


Q31. Are you reducing or consolidating your security vendors?

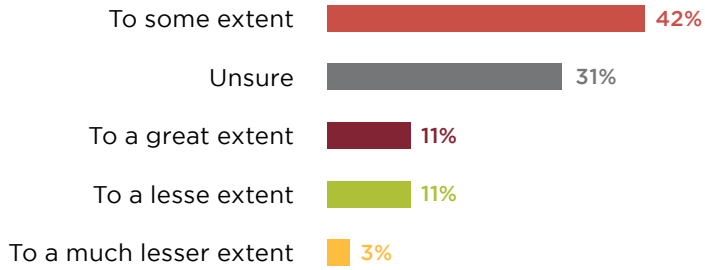


Q33. What changes have you made in your security operating model in response to changes in the way your organisation adopts and governs technology?

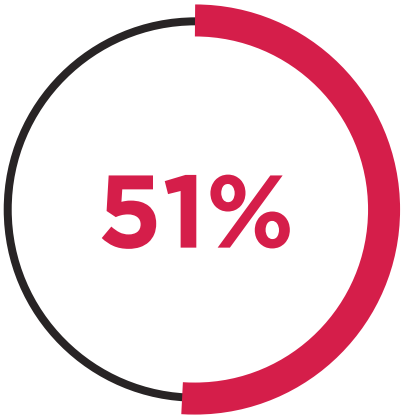
Q34. How is your role changing in the face of the changes in the business technology adoption and governance?



Q35. To what extent do you think that cyber insurance is exacerbating the issue of ransomware?



Q36. How is are your organisation's security investments being impacted in the face of economic head winds?



Click here to see full survey results

People

Culture
Technology
Risk
People

Click here to see full survey results

Founded and Funded by Telstra Purple

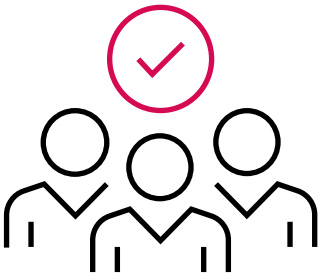
People

Diversifying the cyber security industry amid a global talent shortage

of CISOs considered people and cultural challenges more impactful on the ability to deliver against objectives than macro challenges such as budget, the supply chain, and the economic downturn.

As seen in question in Q12 under "Culture", insufficient staff is the top (51%) concern for CISOs when asked which factors most affect their ability to deliver against their objectives. The next biggest concern for respondents was the culture of the organisation (31%). It's interesting to see that people/cultural challenges are still considered more impactful on the ability to deliver against objectives than macro challenges such as budget (29%), the supply chain (25%), and the economic downturn (22%).

Despite widespread redundancies across many sectors, CISOs are continuing to hire, with 38% focusing on enhancing their security team, including recruitment and training to accelerate their security strategy post-pandemic (see Q20 - Technology). On the recruitment side, just over half (52%) of respondents plan on adding staff to their team in the coming year, while most others (43%) plan on retaining all of their current teams. Less than 5% are planning on reducing the size of their teams.



69%

of CISOs are recruiting from diverse backgrounds

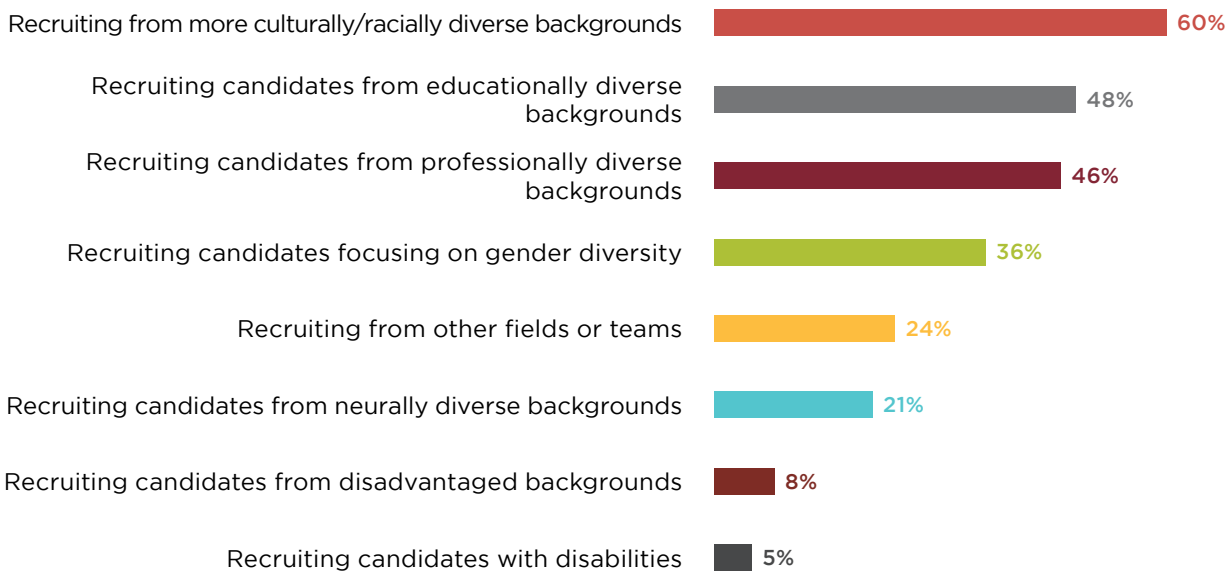
When it comes to building teams that complement existing skills and working styles, recruiting from diverse backgrounds remains at the top of the agenda for CISOs in 2023. With 69% placing it among their top three priorities, it was the only initiative that received a majority of the vote. When asked why it's important to build these diverse teams, most CISOs (78%) believe that it is beneficial to **bring different perspectives into the business, while improving culture (54%) and fostering greater innovation (48%) are the next most common reasons.** With social engineering still being the leading cause of material breaches over the last years (accounting for 38% of the respondents who reported a material breach, higher than any other vector) recruiting diverse teams with a range of perspectives and experience could also help in this regard.

While the vast majority (84%) of respondents feel confident or very confident that their organisation has a strategy in place to offer equality of opportunities for candidates, there is a wider spread of opinions on how best to actually recruit these diverse teams, CISOs are hiring most from culturally/racially diverse backgrounds (60%), but the next highest-scoring strategy was, interestingly, recruiting from educationally diverse backgrounds (48%). Recruiting candidates from professionally diverse backgrounds was almost as common (47%) but focusing on gender diversity is rarer, with only 36% giving it specific focus.

Click here to see full survey results

Q42. What are you doing to build teams that complement your and other team members' skills and working styles?

Q45. What actions are you taking to create a more diverse workforce in your organisation?



Advisory Board Perspective Kevin Fielder

Diversity remains a key concern for most organisations and security teams. Given the benefits around team/organisation performance coupled with the ongoing hiring challenges in security, this is not surprising. It is refreshing to see how many CISOs are actively looking to hire from multiple diversity angles including cultural racial, educational and professionally diverse backgrounds.

As we mature our industry and become more diverse, we need to move the conversation forward from 'equality' to 'equity'. We need to do more than just treat everyone the same or fairly and ensure we are providing genuine equity. This will ensure we are genuinely providing people from diverse backgrounds with what they need to enter and succeed in the field of security. This will be key to building a truly inclusive and diverse workforce.

We should look to this as an area for further discussion and investigation to really understand what is being done and to share success stories - have you run any successful initiatives to attract more diverse talent? Share with the community what you have done and how you tracked your success, this will be really valuable to help everyone learn and improve!

The other key findings in the 'People' section of the survey focussed on having enough people in the security team, culture, uncertainty and broader macro challenges. While insufficient staff came out on top, it would be great to understand what drives this challenge. Is it the 'talent shortage'? In which case, our work in attracting more diverse talent will help here. Or is it driven by tightening budgets, hiring freezes and even headcount reductions in many organisations? Would focusing on improving organisational culture and engagement improve security outcomes and reduce the need for such large security teams? Can you multiply your team's impact by having networks of security champions and working to make things like secure development a key priority and performance metric for your engineering teams?

During times of economic uncertainty, we can aid our organisations by focusing on efficiency, automation and cultural engagement. These can all improve our security without requiring more hiring. Focusing on these areas will help you show business awareness and alignment. If your organisation is tightening budgets and cutting back hiring due to the global and economic uncertainty, a security team demanding people and budget does not align with current business goals. Instead, if you create a strategy focusing on doing more with less, automation and leveraging people across the organisation, you can show your alignment to the organisational goals.

Where things need to be pushed back, be open about the extra risk your organisation will carry, as this allows risk-based decisions to be made, but you can do this while showing you are cognizant of the economic environment.

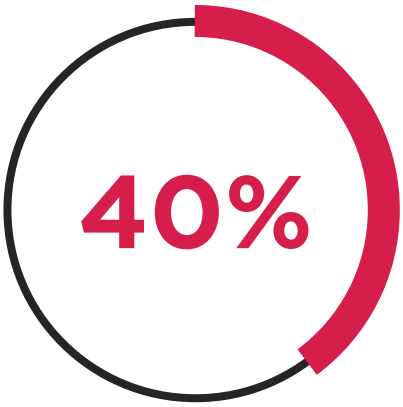
To summarise, work to build a hiring process and working environment that is as equitable as possible for all. Build a security strategy that shows clear alignment with the business goals and economic environment. Focus on automation, improving organisational security culture and engagement and force multiplying your team with support from across your organisation!

Kevin Fielder
CISO at FNZ Group
Advisory Board

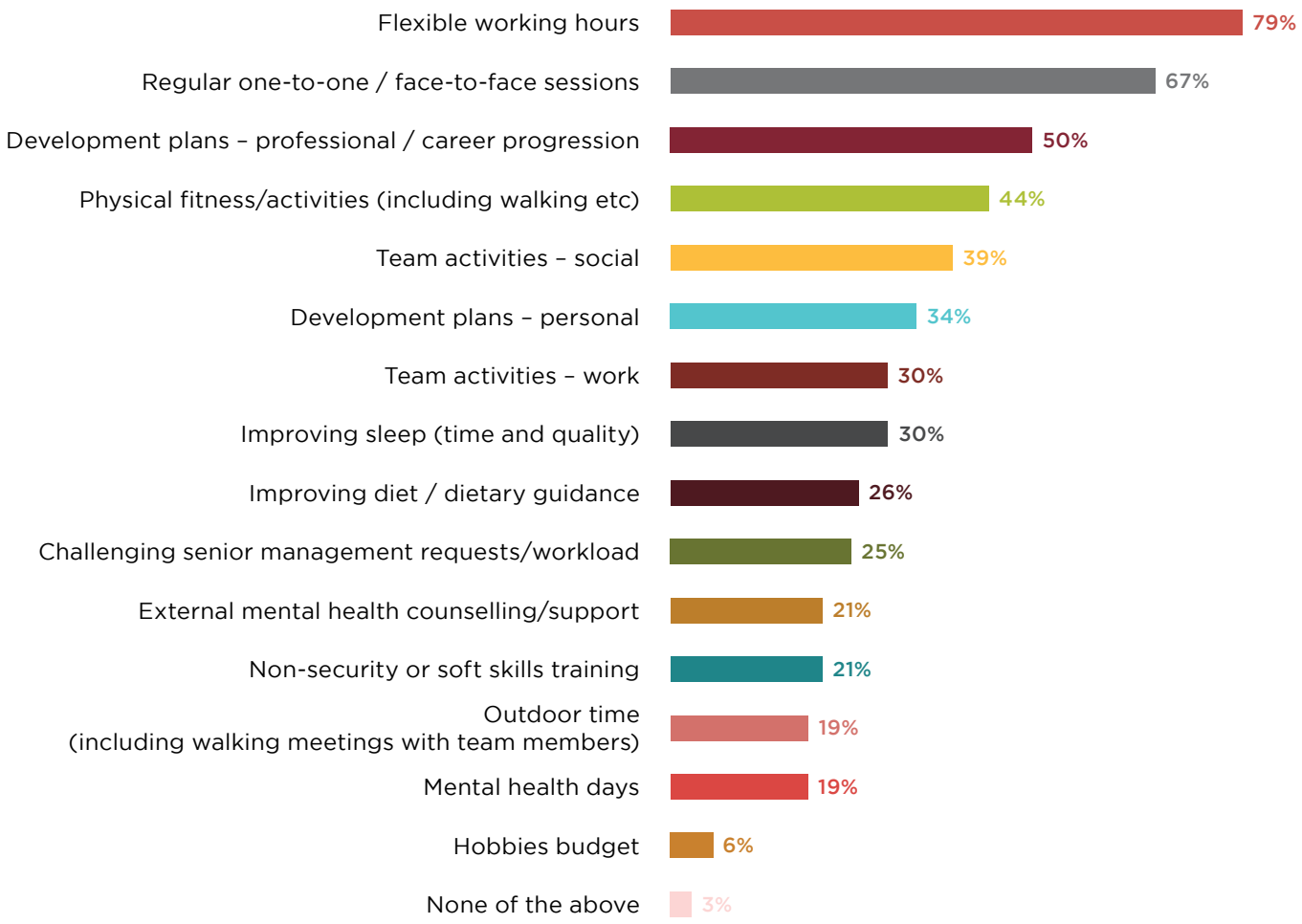
Connect on LinkedIn

Additional Findings

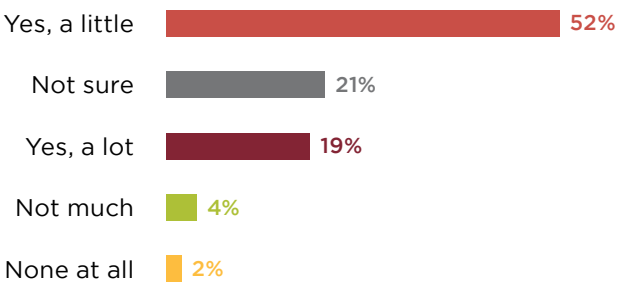
Q37. How stressful is your job?



Q38. How are you addressing stress for yourself and your team?

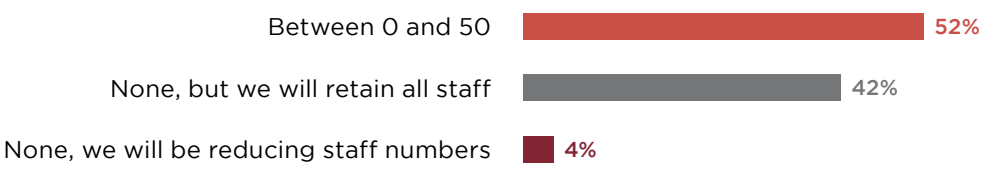


Q39. Are the actions you are taking to address stress having any impact?



Q40. How are you and your organisation supporting and retaining your team?

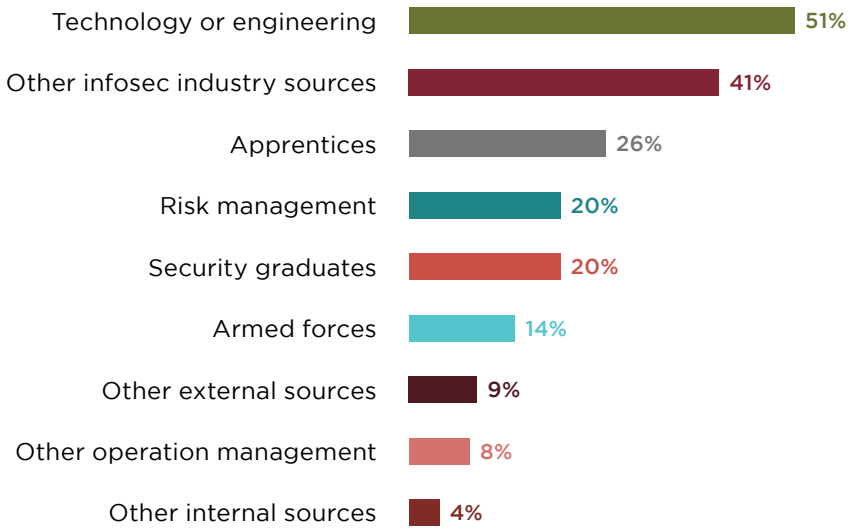
Q41. How many staff do you plan to add to your team in the coming year?



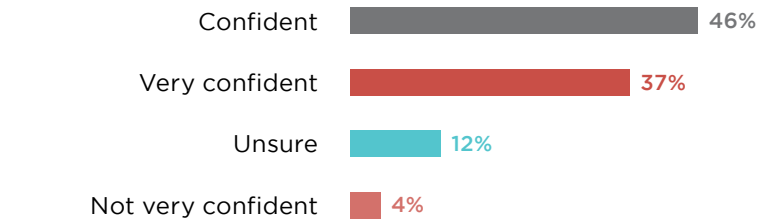
Click here to see full survey results

Q43. What should be the CISO's role in recruiting and attracting team members?

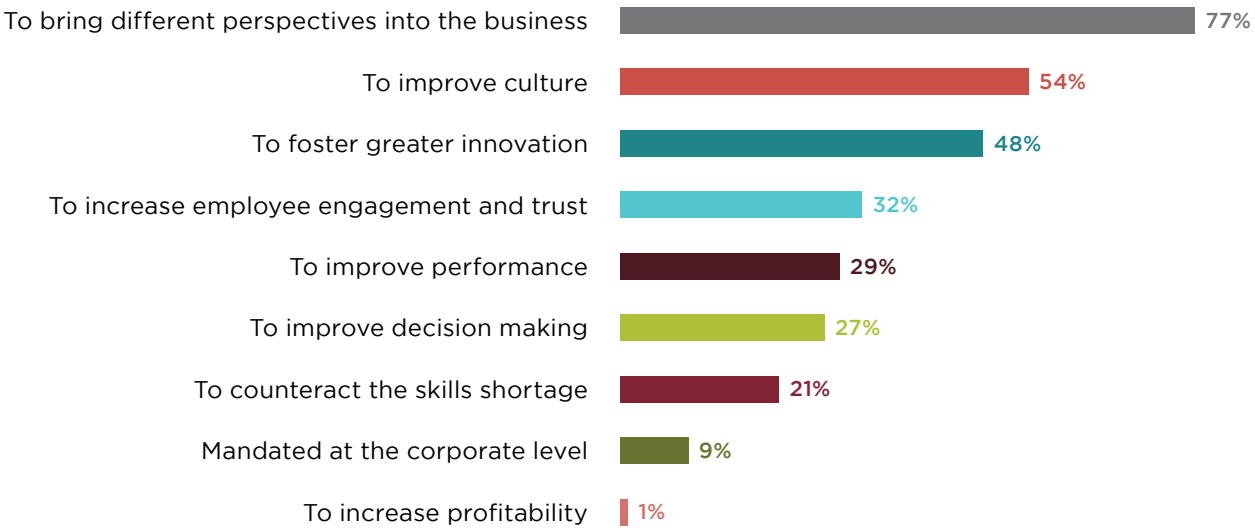
Q44. Where are your best recruits coming from?



Q46. How confident are you that you organisation has a strategy in place to offer equality of opportunities for candidates?



Q47. Why is it important to build diverse teams?

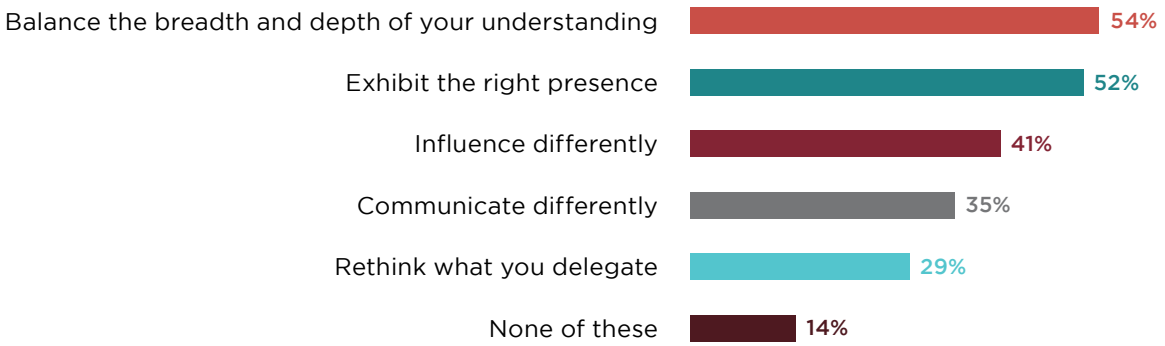


Q48. What non-traditional skills are you looking for in prospective candidates?

Q49. What keeps you in your current role?

Q50. If moving to a new organisation what would be your top three priorities?

Q51. If transitioning to a new CISO role within an existing organisation what would be your top three priorities?



Telstra Purple perspective on the findings

The ClubCISO report is becoming an invaluable tool for us and the wider community to benchmark the maturity of the global security industry and compare real CISOs' perspectives against common narratives within the space. At times it can provide substantial evidence of these, as is the case for the talent squeeze across the security industry - and indeed, the wider technology ecosystem. At other times, the report can challenge widely-held beliefs, as is perhaps the case with the reduction in material cyber events and breaches that has been evident in the last two editions of the report.

That is not to say that companies should become complacent regarding their security. We are continuing to see a rapid evolution of the threat landscape, which was cited as the leading reason why budgets have increased this year. Threats like ransomware and social engineering continue to develop and mature, and wider trends such as cloud migration and third-party supply chain growth mean the ground that CISOs and their teams need to cover is continuously expanding. As these new threats continue to grow, locking down known threats and keeping day-to-day solutions such as the SOC and SIEM functioning as they should will remain critical.

The current economic situation is exasperating many of these issues. The pandemic and conflict in Ukraine have compounded supply chain assurance challenges and the latter spearheads an emerging issue of nation-state attacks threatening the public and private sectors. Worldwide economic uncertainty also complicates CISOs' core mandate of improving security culture, particularly when their biggest pain point is a lack of resources like insufficient staffing. Tackling the skills shortage and confronting issues like diversity is not always as easy as it seems, but the benefits of bringing unique perspectives and viewpoints into the cyber workforce cannot be understated.

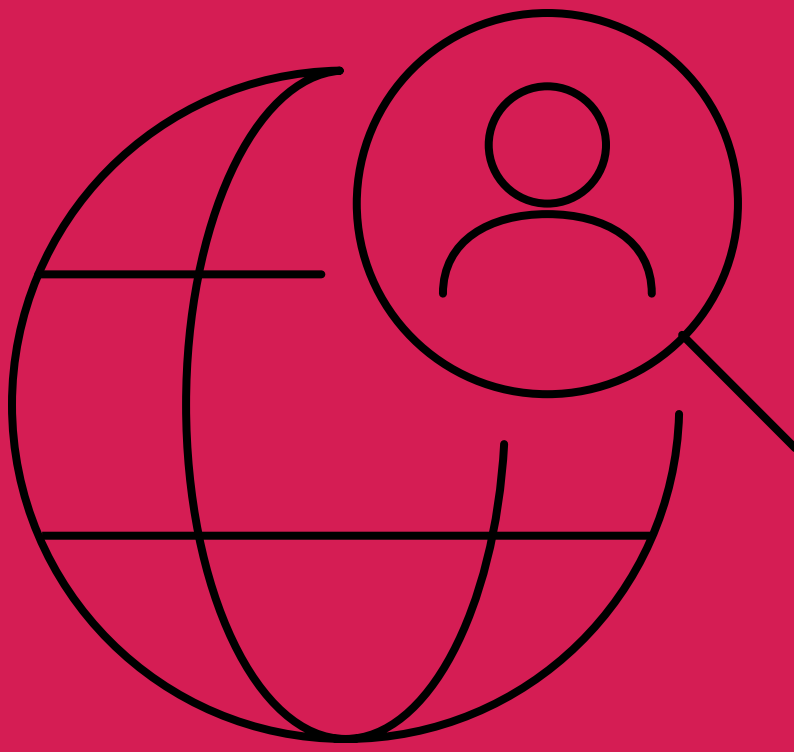
Despite the dark clouds of the past year, we've seen remarkable resilience from the security industry. Clearly, the dedication and innovation of CISOs around the world is helping identify and respond to risks, and ultimately drive process and culture changes to help protect their organisations. From what we've seen from how critical CISOs are of their own security posture, it seems they will not be resting on their laurels and will continue to drive change and improvements, within their organisations, and the industry at large. For the C-suite, the value of cyber security in enabling innovation has never been clearer. Links between security and business transformation are well established and its impact on the business as a whole is the reason why cyber security is quickly rising up the corporate agenda.

This is why initiatives like ClubCISO are so important. The security industry is far stronger working together and collaborating to meet a common challenge. ClubCISO provides a forum in which security leaders can build their network, be involved in a proactive discussion, solve problems and create practical guidance that moves the industry forward.

Rob Robinson
Head of Telstra Purple
EMEA

Connect on LinkedIn

Click here to see full survey results



Get in touch

If you are a ClubCISO member and would like to explore your security challenges, Telstra Purple offers an exploratory workshop to help you address any pain points in your strategy or meet your professional objectives.

If any of the findings resonate with you and you would like to explore further, contact our team at **team@clubciso.org**

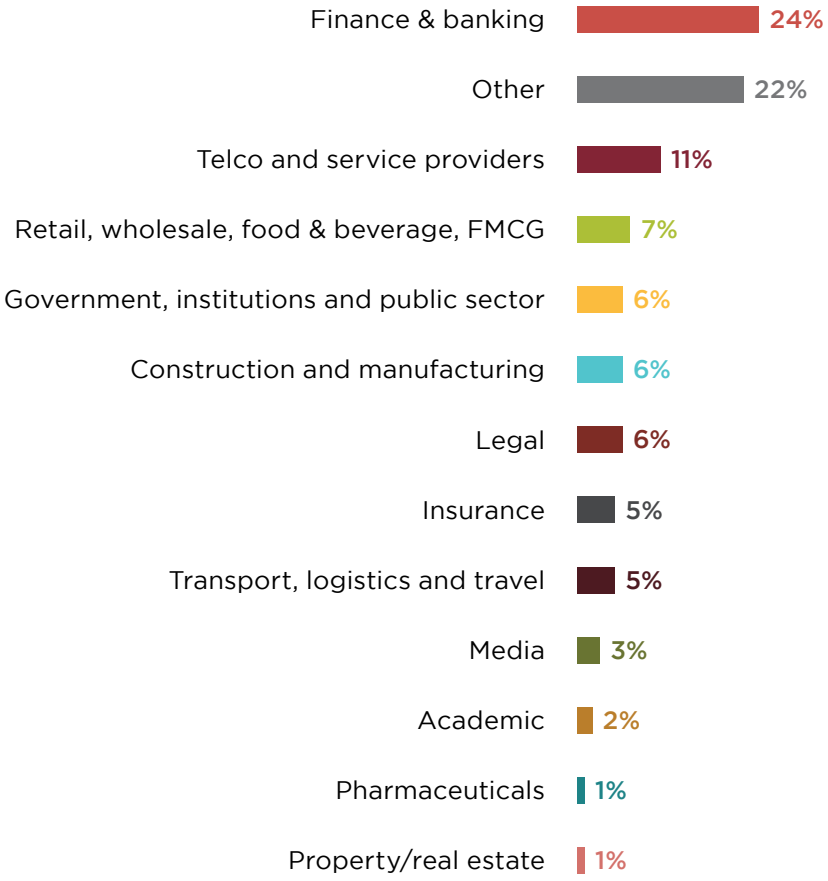
Ask an Expert

Click here to see full survey results

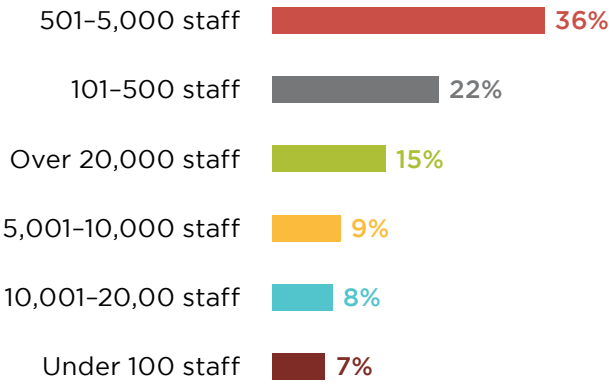
Founded and Funded by Telstra Purple

Demographics

Q1. Indicate the industry sector that most closely matches yours



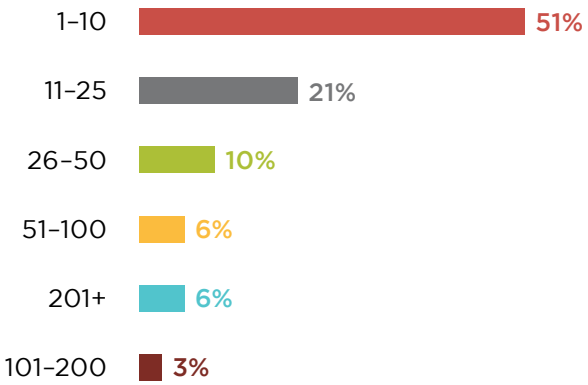
Q2. Indicate the size of your business



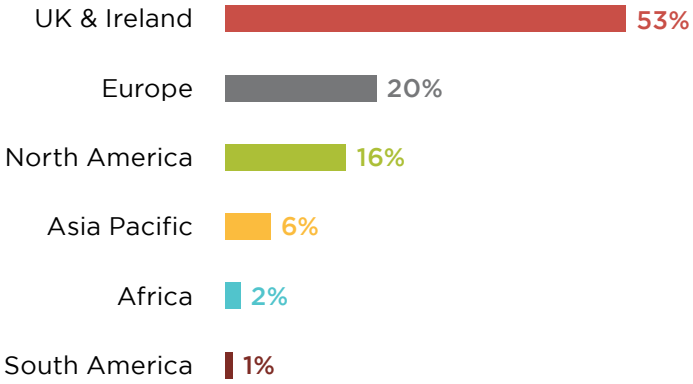
Click here to see full survey results

Founded and Funded by Telstra Purple

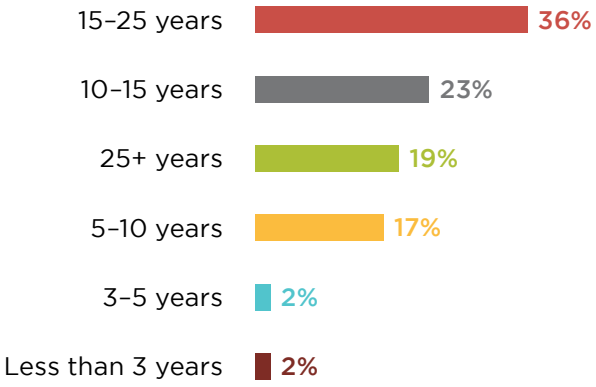
Q3. Indicate the size of your security team



Q4. Where is your HQ?



Q5. How long have you worked in the infosec industry?



Methodology

This is the tenth edition of the annual ClubCISO Information Security Maturity Report - a survey produced by ClubCISO, a global members forum of over 800 security leaders focussed on the challenges, opportunities and focus of today's information security leaders. The 2023 survey features its largest pool of respondents since it began a decade ago. This report features the full list of findings from this year's survey as well as analysis and commentary on its main themes and trends. The Information Security Maturity Report is produced by ClubCISO, a global private members forum for information security leaders powered by Telstra Purple.

The contents of this report and all data points were produced from an online survey, in March 2023, of global CISOs across the public and private sectors, including finance & banking, government institutions, media, transport and logistics and many others (see the Demographics section for a full breakdown). The results were discussed and interpreted by members during a live event on 23rd March 2023 to create the analysis contained in this report.

This report will be of interest to those who manage or are responsible for information security within their organisations or those involved in managing risk as board members and on audit and risk committees. It is also relevant to business leaders in organisations that don't have a defined CISO role.

Benchmarking the maturity of your business's security posture can:

Help identify potentially damaging risks

Highlight priorities for investment or areas for divestment

Drive process change to better protect your organisation

Click here to see full survey results

ClubCISO Advisory Board

Stephen Khan
Stephen is the Chairman of ClubCISO. He is a cyber security and cyber risk executive, and currently Group CISO for Hargreaves Lansdown.

Connect on LinkedIn

Marc Lueck
Marc is a former chair of ClubCISO and is CISO EMEA at Zscaler.

Connect on LinkedIn

Dr. Jessica Barker
Jess is a past chair of ClubCISO and is Co-CEO and Co-Founder at Cygenta.

Connect on LinkedIn

Clive Room
Clive was MC on the event night. He is Director of Conferences at Pulse Conferences and is a committee member and former chairman of the industry's White Hat charity.

Connect on LinkedIn

Manoj Bhatt
Manoj is an Advisory Board Member of ClubCISO and Founder of Cyberhas.

Connect on LinkedIn

Paul Watts
Paul is distinguished analyst at the ISF Information Security Forum.

Connect on LinkedIn

Kevin Fielder
Kevin is CISO at Mettle, a board advisor, NED, and coach.

Connect on LinkedIn

Deborah Saffer
Debbie is the Director of Information Security at Liberty Specialty Markets and an Advisory Board Member at UK&I CISO Alliance.

Connect on LinkedIn

About ClubCISO

ClubCISO is a global community of 'in role' information security leaders working in public and private sector organisations. We are a community of peers, working together to help shape the future of the profession. We are a non-commercial organisation with over 500 members helping to define, support and promote the critical role and value of information security in business and society. Through ClubCISO, members can build their networks, support and coach their peers, solve problems, and create practical guidance that moves the industry forward.

About Telstra Purple

Telstra Purple is an International technology services business, bringing together Telstra Enterprise's business technology services capabilities and a number of its acquired companies, focused on outcome-based, transformative tech solutions. The company's broad capability consists of over 1,500 certified experts in network, security, cloud, collaboration, mobility, software, data and analytics, and design. Diverse by design, its differences bring a radically open-minded approach to every idea, process and solution.

Join the conversation

ClubCISO

@ClubCISO

Clubciso.org

TelstraPurple

@TelstraPurple

Telstrapurple.co.uk

Click here to see full survey results

Founded and Funded by Telstra Purple