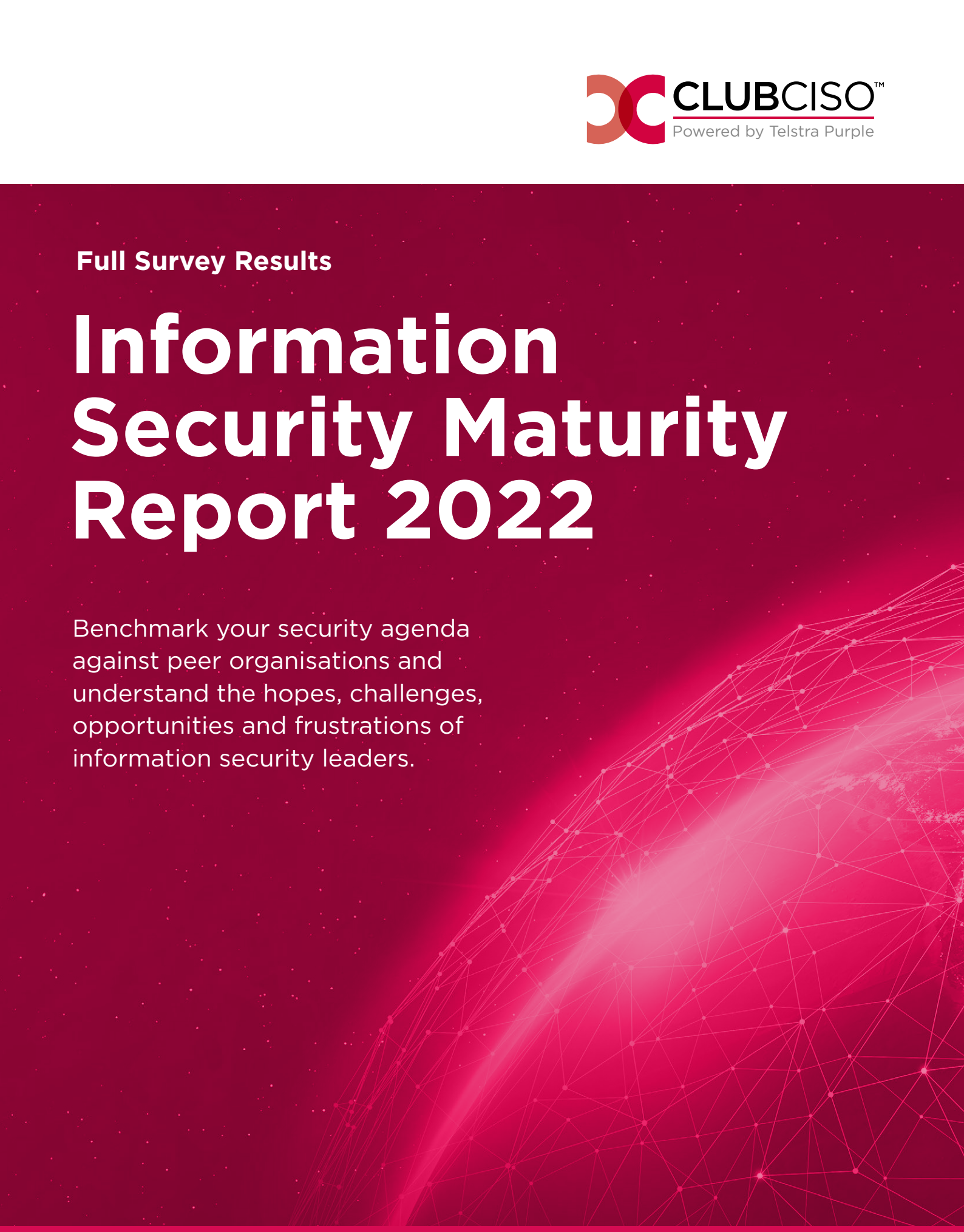
CLUBCISO™
Powered by Telstra Purple

Full Survey Results

Information Security Maturity Report 2022

Benchmark your security agenda against peer organisations and understand the hopes, challenges, opportunities and frustrations of information security leaders.



clubciso.org

POWERED BY Telstra Purple

Who should read this report?

This report will be of interest to those who manage or are responsible for information security within their organisations, and also for 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

How was the data gathered?

This is the ninth annual report on information security maturity produced by ClubCISO powered by Telstra Purple. It has been produced from an online survey, in March 2022, of 108 information security leader members working in public and private sector organisations globally (**see Demographics in the Results section for more detail)**. The results were discussed and interpreted by members during a live event on 23 March 2022 to create the analysis contained in this report.

Back to main contents page

Commentary

Survey questions

Back to main contents page

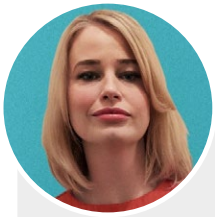
A fundamental shift in security culture

Last year we wondered if CISOs would slip back into the shadows following the changes forced on organisations by the pandemic. Instead, **we've improved our influence**, and finally **succeeded in gaining the critical leadership endorsement we needed to effect permanent change**. This fundamental shift in culture has had a measurable knock-on effect, with a **significant fall in material breaches** being one of the most positive results.

Why is this all happening now? For nearly half the organisations represented in the survey, the enforced **transformation to remote/hybrid working had a materially positive effect on attitudes to security**. At our event discussing the survey results, our CISOs made it clear that not only had **organisations put pressure on us to help them be more secure, but that employees had requested more security engagement**. Suddenly the floodgates were open, and we've been only too ready as a profession to capitalise on these demands.

But even if organisations are doing more, the fact that **three-quarters of CISOs don't think the challenges in our industry are getting any easier** is a salutary reminder that security is a continual journey, not a destination in itself. **Insufficient staff and speed of business change are our biggest concerns when it comes to ability to deliver**. The huge acceleration in business change has come at a time when many more CISOs are on the cusp of being able to lead the charge and to influence that change, and in discussion members suggested that **the few CISOs who lost influence early in the pandemic were those who struggled to react fast enough**.

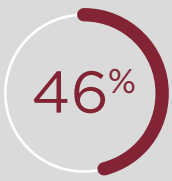
When we started this annual survey back in 2014 even basic 'security awareness' was a big problem. Since then **good security culture has become the norm for many organisations**. CISOs are increasingly seen as business enablers, and it's encouraging that so **few organisations now neglect to measure the value added by their CISOs**.



Jessica Barker

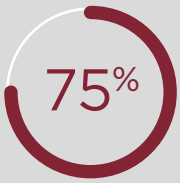
Jess is a past chair of ClubCISO and is co-CEO and Co-Founder at Cygenta.

www.linkedin.com/in/jessica-barker



of CISOs have extended influence in their organisations since COVID-19 hit

Click to see full result



of CISOs report positive or no material change in attitudes to security from increased remote/hybrid working

Click to see full result

Reinventing security technologies

There are no big surprises about most of the main hot topics on our radars this year, but we're starting to see **much more interest in subjects like security target operating models (TOMs), digital transformation and Internet of Things (IoT)**. These are reflected in our investment priorities which show a clear **appetite for more tools around governance, risk and compliance (GRC), identity and access management (IDAM) and even security incident and event management (SIEM)**.

Regarding the tactics we're employing to accelerate cyber-security in the wake of the pandemic, it's interesting that **over half of us are focused on policies, governance and frameworks [Q16], and that the number of organisations actively working on third party (i.e. supply chain) management has nearly doubled compared with last year**.

What seems to be happening is that the pandemic alerted many organisations to the fact that their core security fundamentals were no longer fit for purpose.

And our spending patterns confirm that **compared with last year two-thirds of security budgets have increased (and they've gone up by more than 50% for one-fifth of us)**. Incidentally, we largely think **we as CISOs should carry most of the security technology cost centre**, not other parts of the organisation.

The **clear 'dash for cloud'** (influenced by many ClubCISO member organisations having started up with a 'cloud only' strategy and that game-changing new cloud security tools are coming onstream all the time) has been a further factor in re-assessing technology investment strategies. In reality cloud is a huge opportunity to be more secure, but as it constantly re-invents itself **cloud security maturity itself continues to elude us**.

As AI becomes more prevalent, **automation is enhancing both in-house and outsourcing capability**, and for more than 10% of us it is **starting to reduce our reliance on outsourcing**. Perhaps organisations are now getting more third party value from strategic security advisors than from managed service providers. It'll be fascinating to see if this develops into a clear trend.

Manoj Bhatt

Manoj is an advisory board member of ClubCISO and leads the Cyber Security Advisory and Consulting team for Telstra Purple in EMEA.

www.linkedin.com/in/manoj-bhatt

of CISOs say their organisations have increased their information security budget compared with last year

Click to see full result [Q17].

of CISOs have accelerated their cyber-security tactics in the last year

Click to see full result [Q16].

Back to main contents page

Driving conversations around risk

Our overall security postures are much better this year and our organisational risk management positions are generally encouraging. However, fewer than half our boards appear to be focused on anything more than compliance or maintaining parity with peers. ClubCISO members suggest that boards are conveying the importance of maintaining operational business outcomes, and may not always offer directional guidance on risk appetite through practical measures to manage that risk beyond maintaining security and resilience – hence the high emphasis on 'internal compliance'.

The truth is that not everyone defines risk appetite in the same way, and that is perhaps why we need better ways to focus conversations on maturity supported by relevant detail. A great example is that the pandemic shone a spotlight on the huge number of blind spots in our supply chains. So while we're actively doing more to improve third party security, supply chain risk in general still remains immature.

Another area where we may fall foul is internal incidents. It's hugely encouraging that the number of CISOs reporting that no material incident occurred has nearly doubled year-on-year, but despite improvements in culture nearly one-third of material incidents are caused by non-malicious insiders and social engineering. We still need to focus our efforts here whilst maintaining capabilities around the perimeter and remote access. Improvements and understanding will require robust conversations with the business about trust and confidence. Our organisations want our help as they re-architect their operating models so we should be pushing at an open door, especially given their continual emphasis on driving digital business outcomes.

70% of us have cyber insurance, but if we are so confident we are able to meet key security objectives do we actually need it? Regulators might insist on insurance, but its value can be limited. Organisations need to understand the benefits offered, and address any gaps through other controls. ClubCISO members note that although policies cannot cover the actual cost of a breach they can be useful in providing post-breach assistance. Premiums are problematic and renegotiating reduced cover (e.g. 3-day versus 2-day outage) can help. We should still ask if that premium could be better spent on improving maturity across all security resilience capabilities.

Stephen Khan

Stephen is Chairman of ClubCISO. He is a cyber security and cyber risk executive, and currently Group CISO for a FTSE100 organisation in financial services. He is Chairman of the infosec industry's charity organisation, White Hat Ball.

www.linkedin.com/in/stephenskhan

of CISOs reported no material breaches occurred in past year

Click to see full result [Q26].

of organisations don't want or can't get cyber insurance

Click to see full result [Q30].

People and teams: a work in progress

Our jobs haven't got any more stressful since last year, **but attempts to manage that stress for ourselves and our teams are having negligible impact**. **Fewer than one-third of us appear to have access to specialist professional mental health support**, and the most **common tactics we use (such as flexible working, one-to-ones and social team activities)** are **part of our general support and retention strategies anyway**. So... How do we do better? How do we better manage stress within security teams?

There's much more positive news in how we are building teams. In order to broaden our skills and working styles, **nearly two-thirds of CISOs are actively seeking to recruit from diverse backgrounds**. There's also **a lot of emphasis on apprentices and building talent from within, and deliberately seeking out complementary skills outside traditional security backgrounds**. While most of our best recruits still come from technology or infosec, **there's been a healthy increase in those with risk management backgrounds, graduates, apprentices and other non-infosec sources this year**.

At our post-survey discussion event, ClubCISO members raised **concerns about an apparent drop-off in STEM uptake in schools, which could affect the next generation of infosec professionals**.

We love the industry and can find it hard to move on when we've built a great team. At the same time, **we often don't seem so enamoured with our particular jobs**. Perhaps when changing roles we need to do more to ensure the organisational culture and role expectations align with our own career goals.

Moving to a new organisation, we recognise the most important priority is driving stakeholder engagement, and similarly **exhibiting the right presence is a must when transitioning to a new CISO role**. When looking at a new role, especially when it is an organisation's first CISO or when they are going through a transformation, we must understand the end goal and culture they are trying to build. ClubCISO is investigating the establishment of a formal mentorship programme and in the meantime please keep reaching out to your peers and the advisory board. There's a lot we can learn from each other.

Kevin Fielder

Kevin is CISO at FNZ Group, a board advisor, NED and coach.

www.linkedin.com/in/kevinfielder

Only 11% think their organisations' actions to combat stress are having a lot of impact

Click to see full result [Q33].

We're loyal to our teams and our industry, but 16% of CISOs don't love their particular jobs

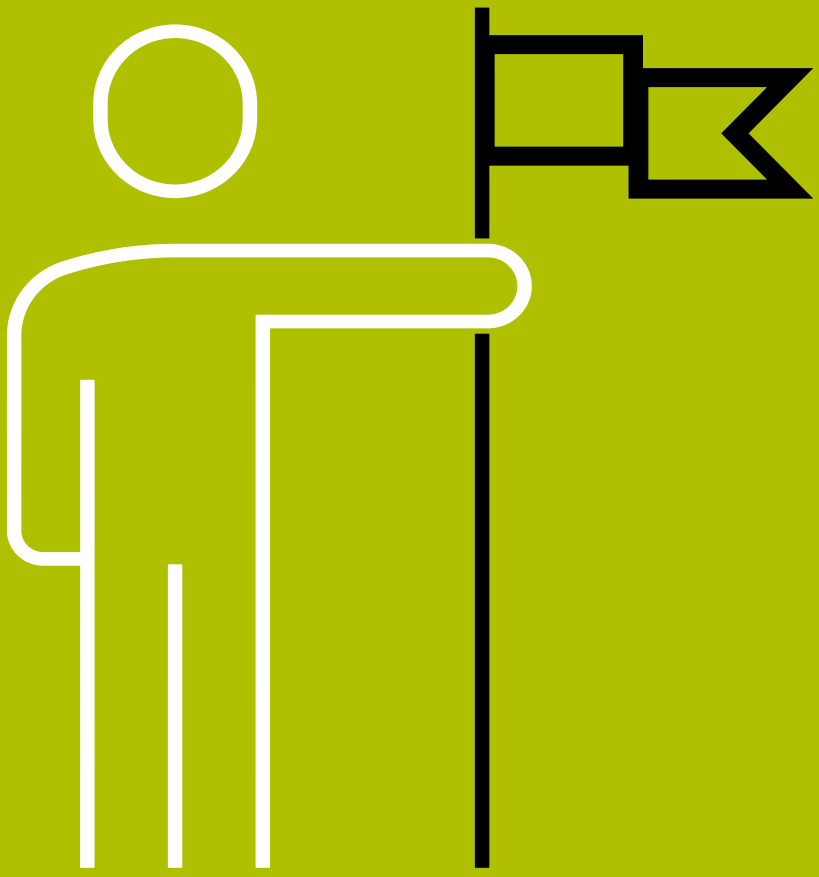
Click to see full result [Q38].

The Capability Maturity Model (CMM)

The CMM defines five maturity levels, and all questions which cite the five levels (initial, repeatable, defined, managed and optimizing) are using CMM definitions.

The Capability Maturity Model (CMM)	
5. OPTIMIZING	Focus on process improvement
4. MANAGED	Processes are measured and controlled
3. DEFINED	Projects tailor their processes from the organisations development methodology
2. REPEATABLE	Processes are characterised for specific projects and the organisation is often reactive
1. INITIAL	Process is unpredictable, poorly controlled and reactive

Back to main contents page

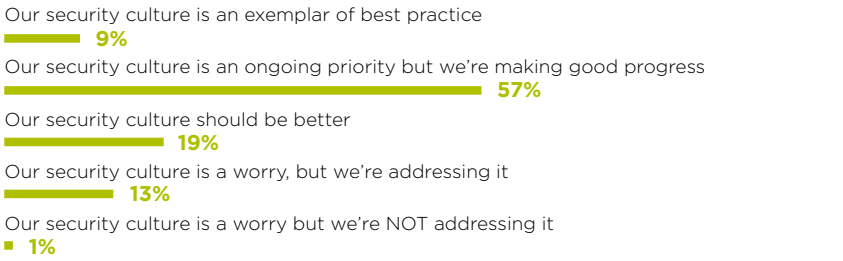


Culture

Back to main contents page

"This is marginal improvement on last year's result, which had shown substantial progress against 2020. 66% now report progress or best practice (2021: 61%, 2020: 39%). The concept of cyber security culture is no longer a novelty."

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

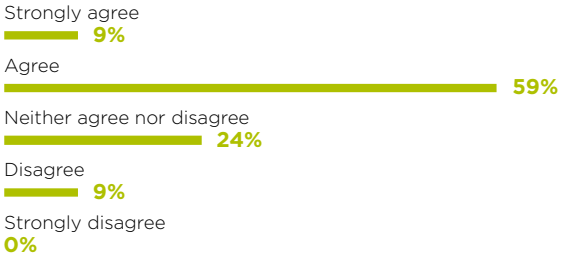


"These selections are slightly different from 2021. Leadership endorsement and simulated phishing weren't previously included, and their runaway effectiveness is obvious. An important shift in culture is indicated by 'proactive no blame policy', which we're delighted to see has nearly doubled from 27% in 2021 to 50% this year."

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

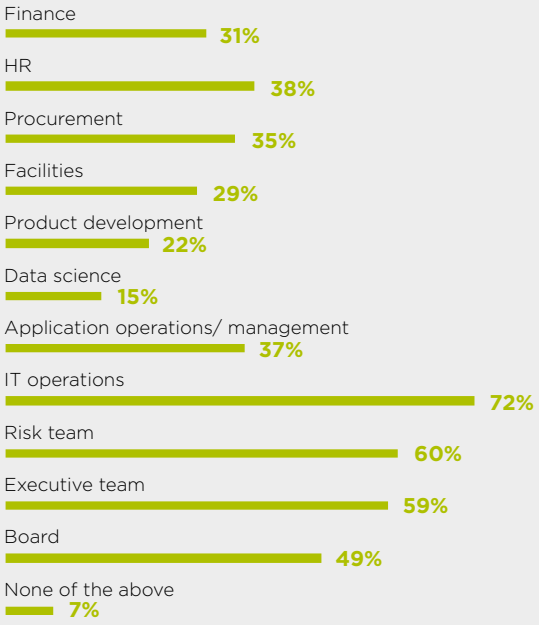
"Very little changed in the responses to this question in 2019 and 2020, but there was a huge shift last year and in 2022 the result is similar to that of 2021. For example, 'disagreements' fell from 22% in 2020 to 7% in 2021 and stand at 9% this year, which isn't a significant change in the last 12 months."

3. Taken as a whole, my organisation has a positive security culture



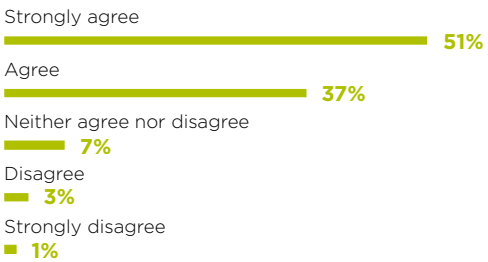
"This year we modified the options to include the exec and board. Most of the results are otherwise similar to 2021, except that product development shows a clear move in the right direction (2022: 22%, 2021: 16%). This suggests that in this critical area we are increasing our influence so that security gets baked in at the outset, which is very good news."

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



"You'd expect us to have faith in the way we add value (if anything this result shows we are a little more ambivalent than in 2021)."

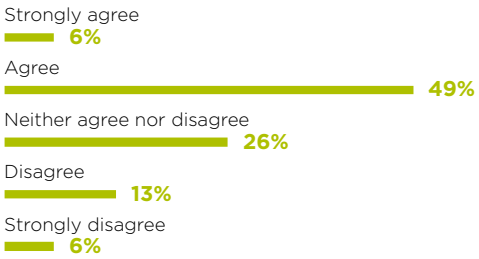
5. I believe I add value to the business



Back to main contents page

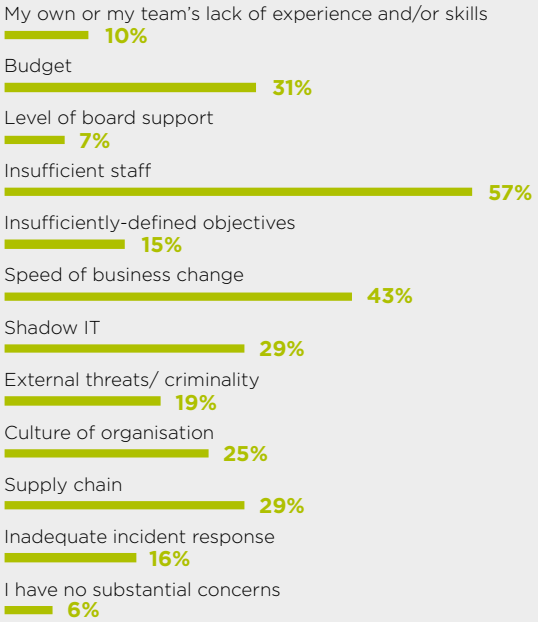
"Previously we've asked if the business believes we add value to it. This year we changed the question, to explore whether CISOs are actually measured as adding value. This is an encouraging response, and we'd like to dig deeper to find out what metrics are being commonly used."

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



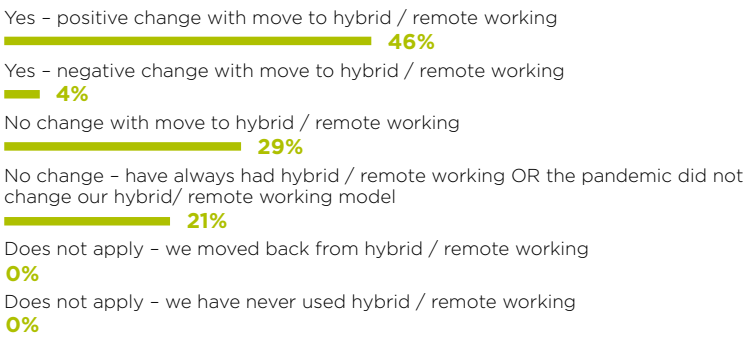
"Two clear movers here. Speed of business change has increased to 43% (2021: 32%), while culture of organisation has fallen to 25% (2021: 43%). This reinforces our view that there's been fundamental change as a result of changed working practices driven by the pandemic."

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



"This result also makes the point that for many CISOs the pandemic brought positive change."

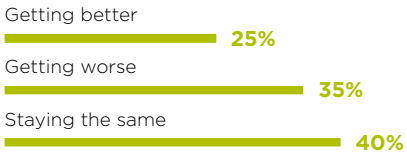
8. Has there been a material change in attitudes to security caused by a move to hybrid / remote working in the past year?



Back to main contents page

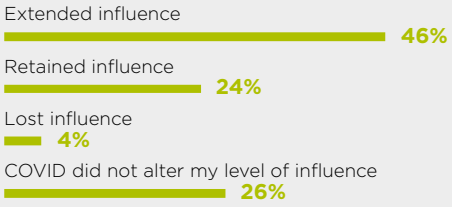
"This is a deliberately subjective question, and it's clear that there are swings and roundabouts. Challenges are marginally 'worse' inasmuch as they are now often different, new challenges."

9. Do you think that challenges across all sectors of the security industry are generally getting better, getting worse, or staying about the same?

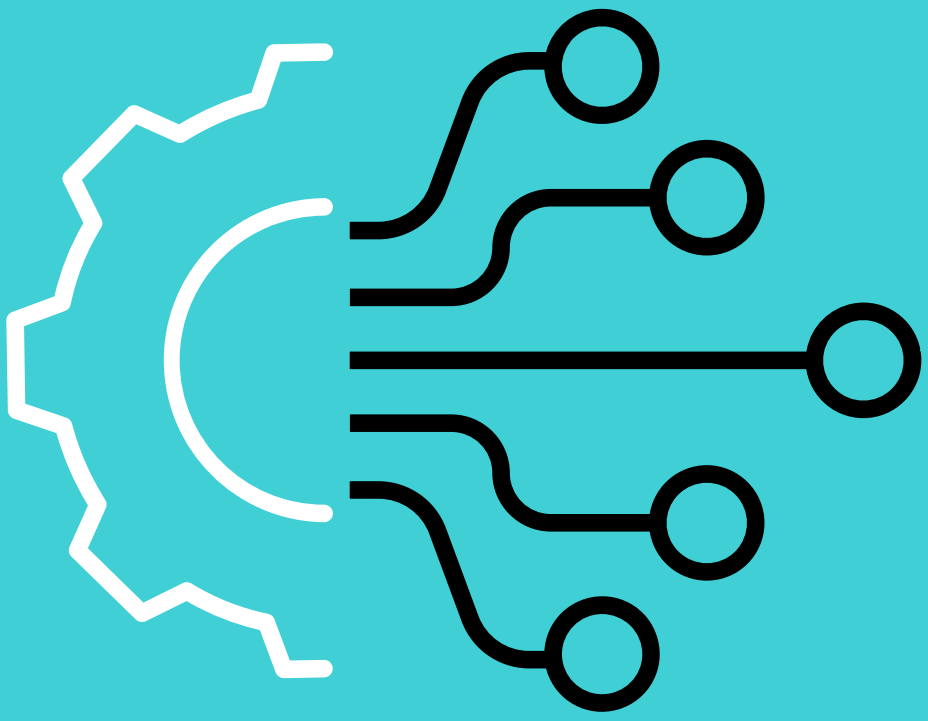


"Twelve months ago we were a year into the pandemic, and organisations were rapidly learning the importance of security culture to support new working models. We were concerned that our seemingly increased influence might have been a temporary blip and that our employers might fall back into old habits. Fortunately these fears appear to have been unfounded, and the lasting influence of the pandemic is that CISOs have retained or extended their influence."

10. Have you extended, retained or lost influence in your organisation since COVID hit?



Back to main contents page

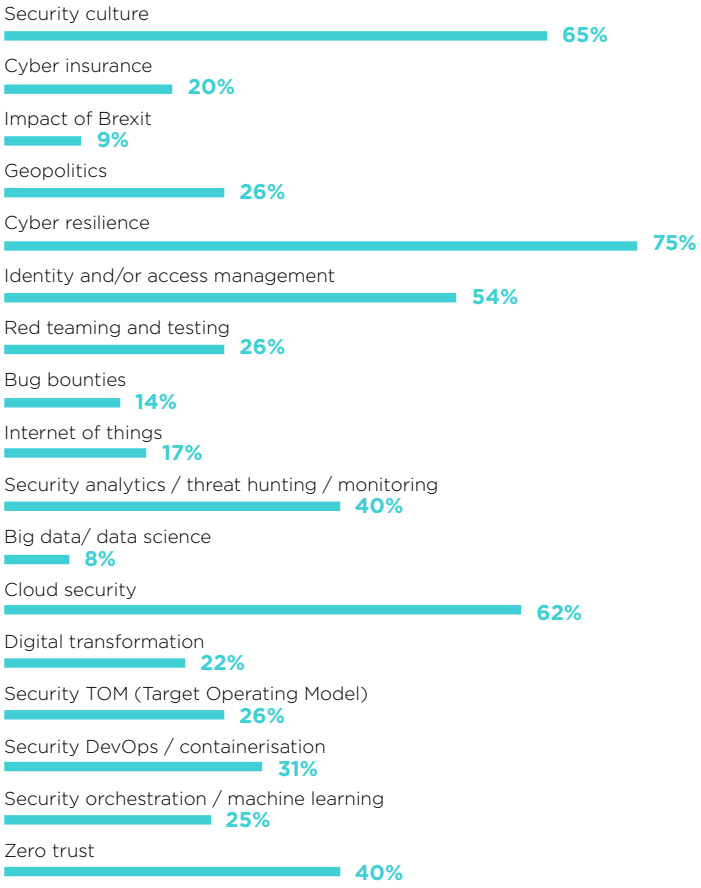


Technology

Back to main contents page

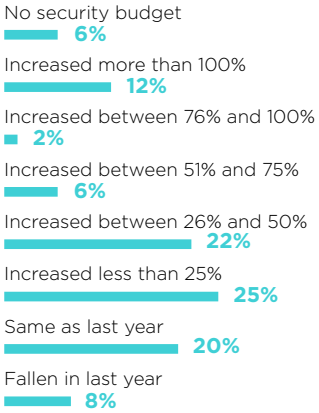
"The 'big four' hot topics – resilience, culture, cloud and IAM – remain the same, but there are notable increases in TOM (2022: 26%, 2021: 18%), IoT (2022: 17%, 2021: 9%), and cyber insurance (2022: 20%, 2021: 9%). Global events at the time of the survey helped drive an increase in geopolitics to 26% (2021: 7%)."

11. Which of these hot topics are on your radar?



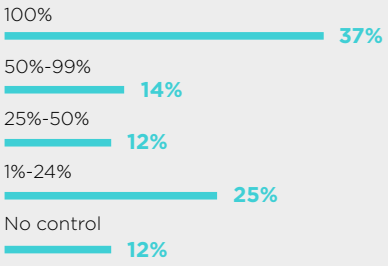
"Budgets have increased overall, and those seeing an increase of over 100% have risen to 12% (2021: 7%, 2020: 5%)."

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



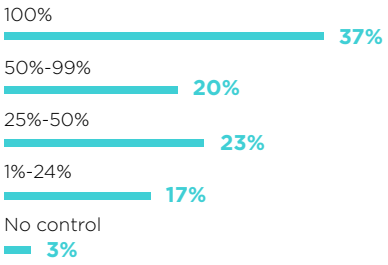
"There's been speculation that some CISOs are responsible for setting strategic direction but that in practice actual budget control is increasingly falling under IT or other areas of the business. This result suggests that is not the case."

13. What percentage of your organisation's security technology budget falls under your cost centre?



"Do CISOs actually want control of the budget? We wanted to test that idea too, and for most of us the answer is an emphatic yes."

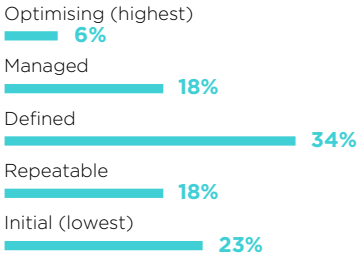
14. What percentage of your organisation's security technology budget should fall under your cost centre?



Back to main contents page

"We've asked this question every year since the first ClubCISO survey in 2014. Progress has been lumpy to say the least, and this year's result shows that 75% of us are still in one of the lowest three levels (2021: 79%). We're still running to keep up with the pace of cloud."

15. Rate the maturity of your cloud security strategy

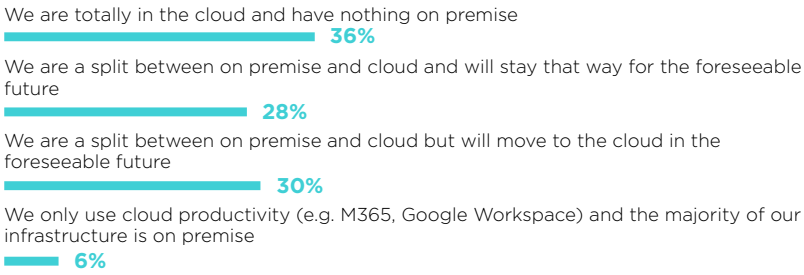


"We've rephrased this question as last year we asked which tactics were being accelerated in response to COVID-19, rather than post pandemic. We've clearly enabled nearly as much remote access as we need to (2022: 9%, 2021: 40%), but most of the other tactics listed have increased as the way we 'do security' has changed."

16. Which of the following tactics are you focusing on to accelerate your cyber security strategy post pandemic

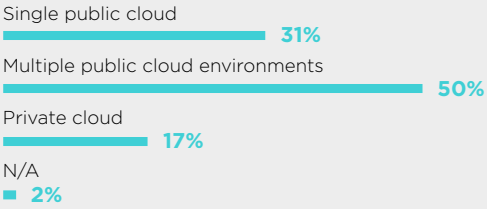
"Many ClubCISO member organisations are less than 10 years old and have never had an on-premise strategy, but of the others only 34% don't expect to move further into the cloud (and of those only 6% only use cloud for productivity tools rather than key services)."

17. How is cloud currently implemented in your organisation?



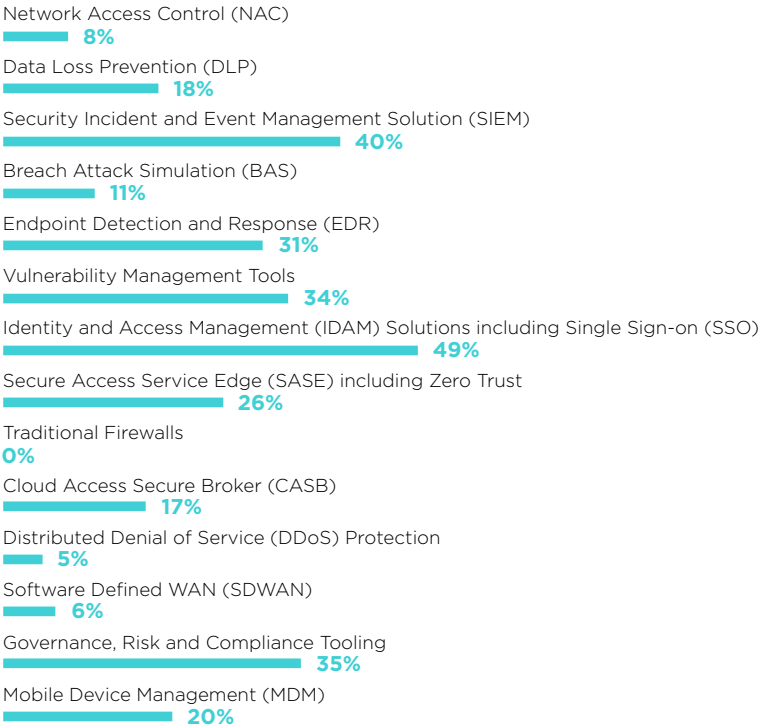
"There's a clear bias toward public cloud environments."

18. Describe your cloud environment



"IDAM/SSO and SIEM lead the pack, with DLP trailing and traditional firewalls not even registering. That says a lot about the changing nature of the workplace. Perhaps more interesting are the high scores for GRC and vulnerability management as we reinvigorate core security practices."

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



> We wanted to test the theory that automation is allowing organisations to bring services back in house rather than using managed service providers. While it's clear that AI is boosting capability across the board, any reduction in outsourcing this is causing is so far a trickle rather than a flood.

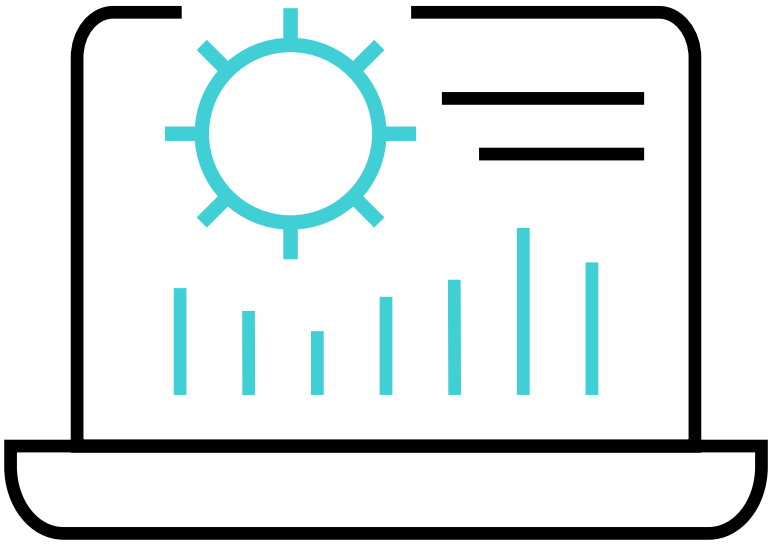
20. Is automation of security technologies changing the balance of insourcing v outsourcing for your organisation?

Yes – automation is reducing our reliance on outsourcing
11%

No – automation is, however, enhancing in-house capability
32%

No – automation is enhancing both in-house and outsourced capability
23%

No – there is no change between balance or capabilities of in-house and outsourced capability
34%



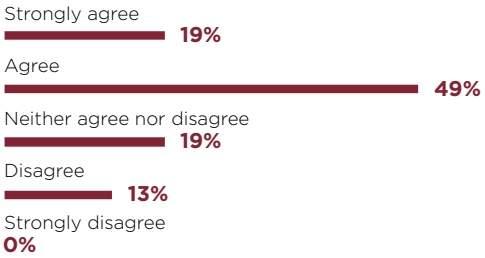
Back to main contents page

Risk

Back to main contents page

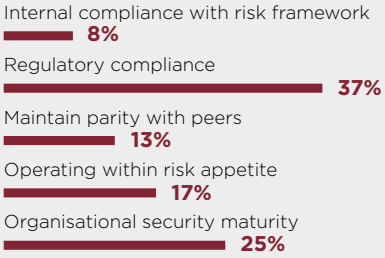
"It's great news – and hardly surprising given the other results in this survey – that we have even more confidence in being able to meet security objectives. The percentage of agree/ strongly agree is now 68% (2021: 53%, 2020: 38%)."

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



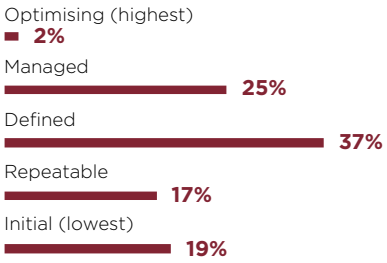
"Box-ticking and maintaining parity seem to be priorities for 58% of boards, although there's a debate to be had around whether internal compliance is actually the board's way of putting risk appetite into a tangible form."

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



"We're making a little headway with supply chain risk. Managed and optimising stand at 27% (2021: 23%, 2020: 11%)."

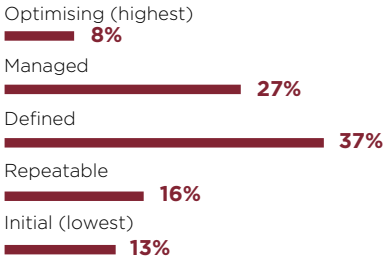
23. Rate the maturity of your process to measure, manage and assure supply chain risk



Back to main contents page

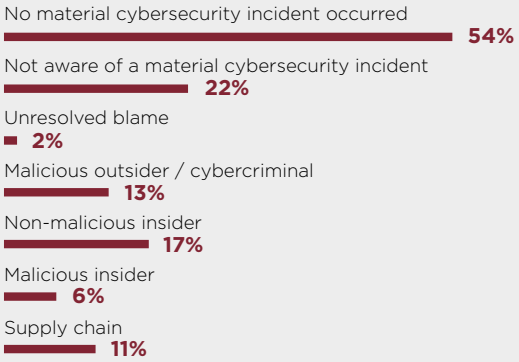
"Clear improvement trend. Managed and optimising stand at 35% (2021: 19%, 2020: 16%)."

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



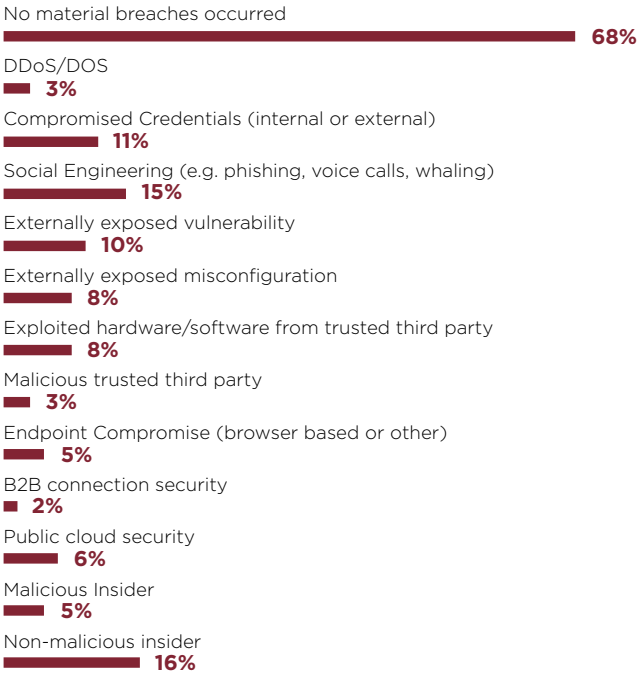
"The most obvious changes are that 'no material incident occurred' has nearly doubled to 54% (2021: 28%), and that 'malicious outsider' has nearly halved to 17% (2021: 32%). Those figures suggest a good pat on the back is in order, but we mustn't be too complacent. The risks from non-malicious insiders have hardly changed (2022: 17%, 2021: 20%), suggesting this is where much effort still needs to be focused."

25. What activities have led to a material cyber security incident in the past 12 months?



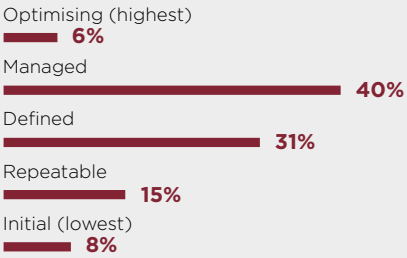
"Echoing the results of question 25, this result looks a little more deeply at how those breaches occurred. Improvements in culture and awareness have contributed to a notable drop in social engineering (2022: 15%, 2021: 32%)."

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



"This is probably the best result in the nine years we've been running this survey. The positive developments we've noted elsewhere have led to a managed/optimising result of 46% (2021: 27%, 2020: 20%)."

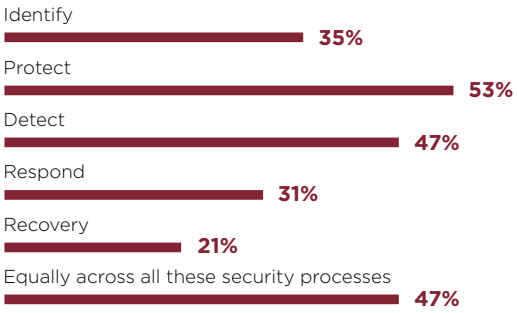
27. Rate your organisation's security posture



Back to main contents page

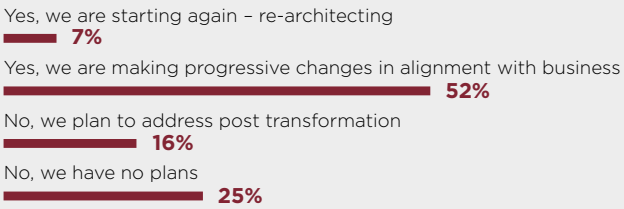
"These are the five categories of the NIST security framework, intended to all work concurrently and continuously to form a solid security foundation. It seems that we are prepared for both pre-and post-breach scenarios."

28. Where and how does your organisation direct investments to improve your security maturity and capability?



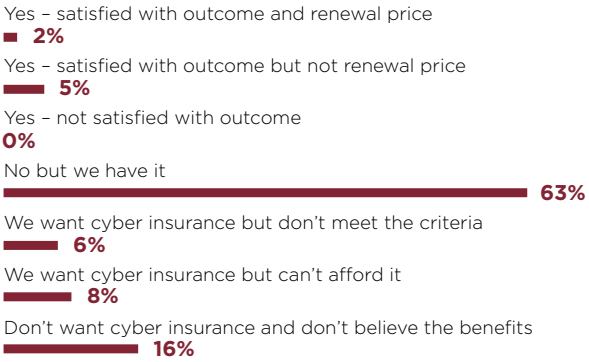
"We'd previously come across anecdotal evidence that organisations were reducing the number of security vendors they use, and these results bear that out. it's notable that only 25% have no plans to do so."

29. As your organisation adopts cloud are you reducing or consolidating your security vendors?



"As a topic, cyber insurance always excites much debate. It seems it's becoming more and more difficult to meet the criteria or premiums required, and those who have claimed are alarmed about how much the cost has subsequently increased. If you're not required to have insurance by your regulator, are there higher spending priorities that can make your organisation more cyber resilient?"

30. Has your organisation ever claimed on cyber insurance?



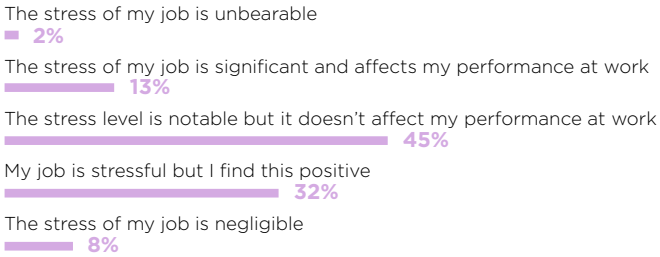
Back to main contents page

People

Back to main contents page

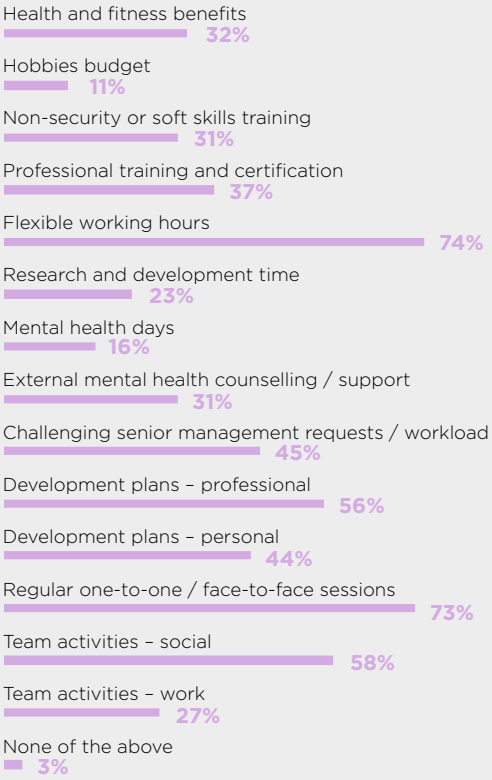
"If anything, the stress of our jobs has generally eased. Unbearable/significant now stands at 15% (2021: 22%, 2020: 23%)."

31. How stressful is your job?



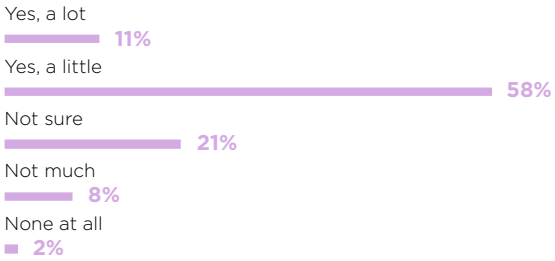
"Flexible working, one-to-ones and social team activities feature strongly."

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



"But the tactics we're using to manage stress for ourselves and our teams don't seem to be having a huge impact. Only 31% have external mental health support. Is this enough?"

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

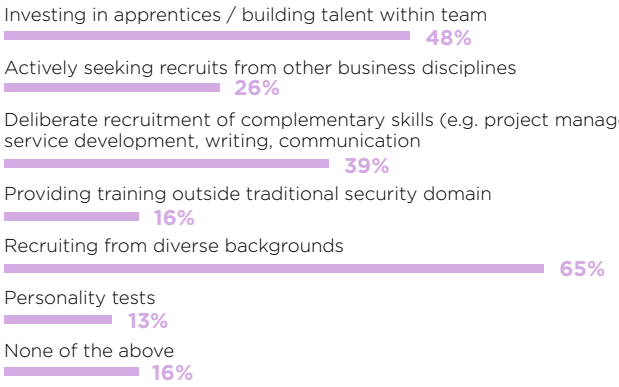


"In fact the tactics we use to 'address stress' are those we use in any case to support and retain our teams."

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

"65% of us are recruiting from diverse backgrounds, and we're investing in more home-grown talent, apprentices, and stars from other disciplines. This is all great news. Only 16% aren't doing anything proactive to enhance their team's skills and working styles."

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

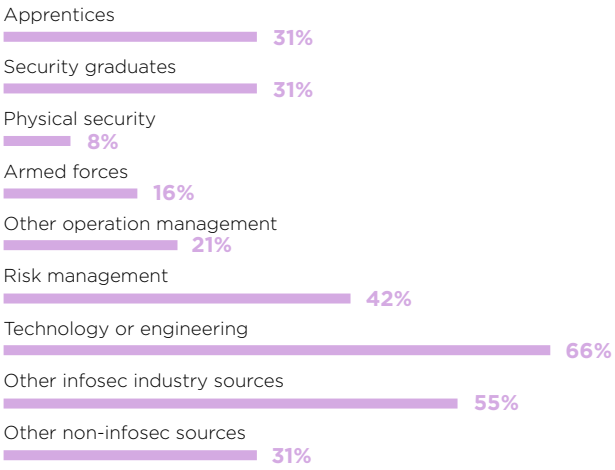


"Very high scores for 'building a team others want to join' and 'championing positive security culture'."

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

"Technology and infosec are still where the best recruits come from, but there are notable increases in non-infosec (2022: 31%, 2021: 20%), security graduates (2022: 31%, 2021: 22%) and apprentices (2022: 31%, 2021: 18%)."

37. Where are your best recruits coming from?



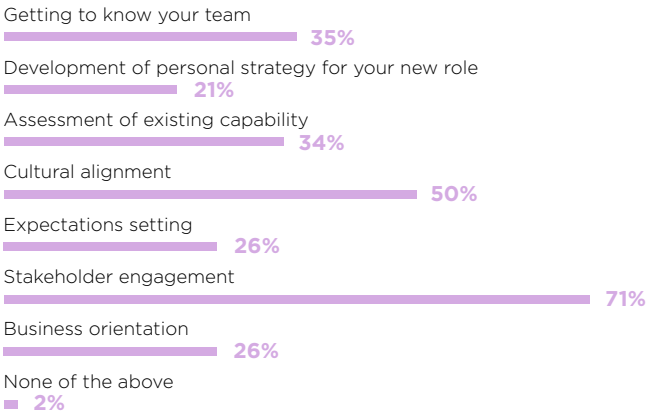
"CISOs are staying in their roles for all the right reasons, but it's notable that only 16% of us love 'this particular job'."

38. What keeps you in your current role?

Back to main contents page

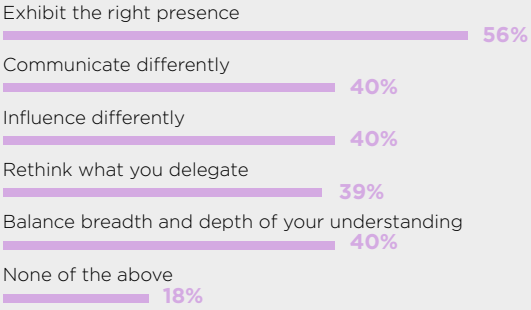
"Stakeholder engagement and cultural alignment are way ahead of setting expectations and business orientation when moving to a new role."

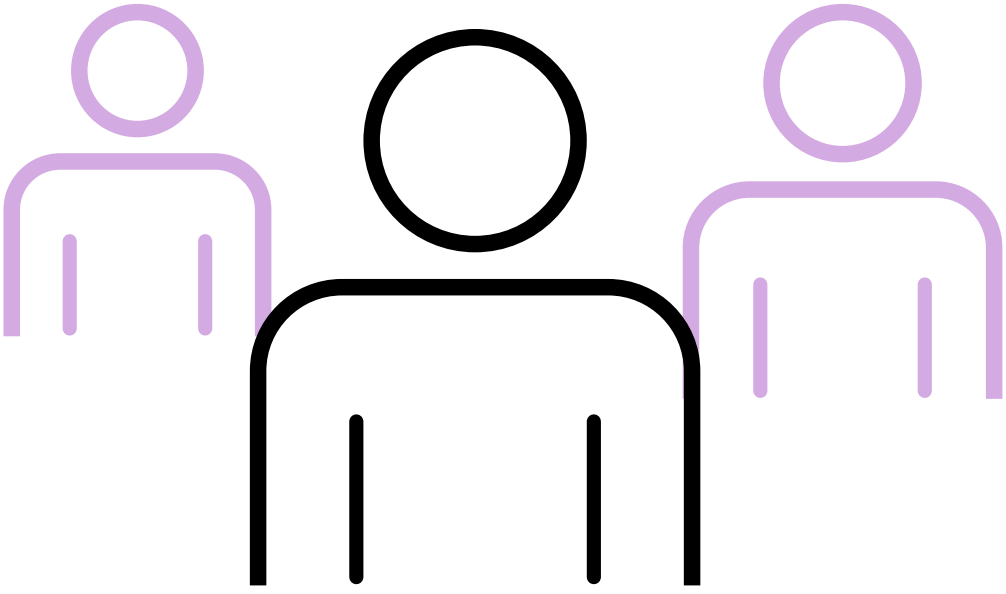
39. If moving to a new organisation what would be your top three priorities?



"It's interesting to see how important exhibiting the right presence is for someone transitioning into a new CISO role."

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





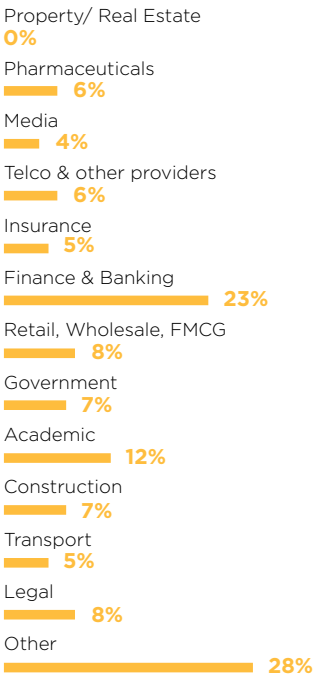
Demographics

Back to main contents page

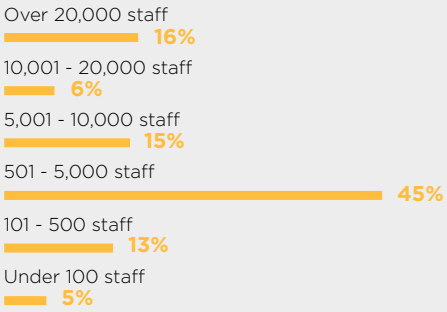
Demographics

This information is provided to illustrate the profiles of those who took part in the survey.

i - Indicate the industry sector that most closely matches yours

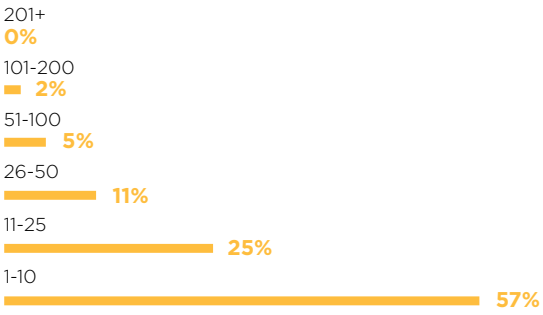


ii - Indicate the size of your business

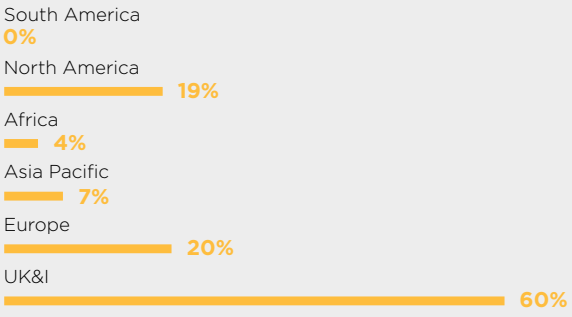


Back to main contents page

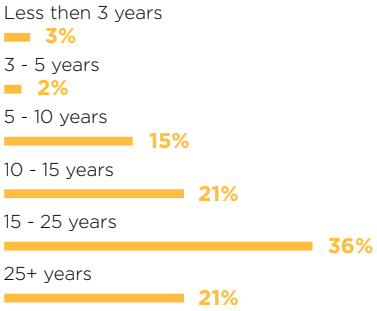
iii - Indicate the size of your security team



iv – Where is your HQ?

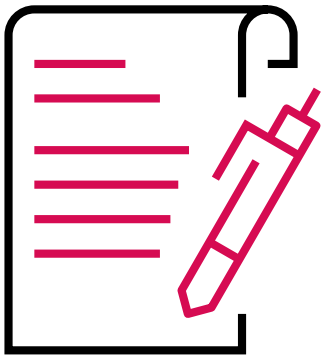


v – How long have you worked in the infosec industry?



Back to main contents page

So what happens next?



Members of the ClubCISO Advisory Board will hold a planning session on how we act on the results and shape the community's strategy for the coming year.

The AB, comprised of a number of prominent CISOs, will agree and communicate a clear path for the profession to take in 2022, while providing ongoing support and networking opportunities for CISOs to share experiences, concerns and opportunities.

ClubCISO operates to fulfil to three clear aims:

We are a **community of peers,** working together to help **shape the future of the profession.**

We are a non-commercial organisation with over 650 members helping to **define, support** and **promote** the **critical role** and **value** of information security leaders in business and society.

ClubCISO provides a forum in which security leaders can **build their network,** be involved in **proactive discussion, solve problems** and **create practical guidance that moves the industry forward.**

We are always seeking new ClubCISO members to help us reach our goals. If you have an interest in participating in the development of specific working groups, please contact team@clubciso.org to register your interest.

Back to main contents page

Live vote hosts and ClubCISO advisory board

Event hosts on 23 March 2022

Stephen Khan

Stephen is Chairman of ClubCISO. He is a cyber security and cyber risk executive, and currently Group CISO for a FTSE100 organisation in financial services. He is Chairman of the infosec industry's charity organisation, White Hat Ball.

https://www.linkedin.com/in/stephenskhan

Dr Jessica Barker

Jess is a past chair of ClubCISO and is co-CEO and Co-Founder at Cygenta.

www.linkedin.com/in/jessica-barker

Manoj Bhatt

Manoj is an advisory board member of ClubCISO and leads the Cyber Security Advisory and Consulting team for Telstra Purple in EMEA.

www.linkedin.com/in/manoj-bhatt

Kevin Fielder

Kevin is CISO at FNZ Group, a board advisor, NED and coach.

https://www.linkedin.com/in/kevinfielder

Marc Lueck

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

https://uk.linkedin.com/in/marclueck

John Meakin

John is a CISO and cyber security advisor who has worked with organisations including Burberry and GSK.

https://www.linkedin.com/in/john-meakin-52ba2

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.

https://www.linkedin.com/in/john-meakin-52ba2/

Paul Watts

Paul is distinguished analyst at the ISF Information Security Forum.

https://www.linkedin.com/in/paulewatts

Tom Berry

Special thanks to Tom, who retired from the advisory board following the 2022 results event. Tom has been a mainstay of ClubCISO for a number of years, helping to challenge our assumptions and to bring new perspectives to our profession. He is a non-executive director and board advisor, and a business teacher at Sutton Grammar School. He would welcome you staying in touch.

https://www.linkedin.com/in/tomberry

Debbie Saffer

Debbie is Global Deputy CISO at Cushman & Wakefield and an Advisory Board Member at UK&I CISO Alliance.

https://www.linkedin.com/in/deborahsaffer

Back to main contents page

CLUBCISO™
Powered by Telstra Purple

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.

Telstra Purple

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.

www.telstrapurple.co.uk

If you would like to discuss any of these topics with a Senior Security Consultant from Purple then reach out to Lizzie to arrange a free of charge clinic session (only available to members).

Elizabeth Hodges
ClubCISO Liaison
elizabeth.hodges@team.telstra.com

Join the conversation:

ClubCISO
TelstraPurple
@ClubCISO
@TelstraPurple
clubciso.org
telstrapurple.co.uk