CLUBCISO™
Powered by Telstra Purple

The ClubCISO Information Security Maturity Report 2020

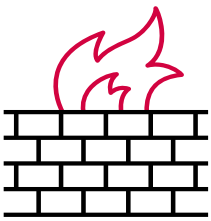
Full Survey Results

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

Who should read this report?

This report will be of interest to those that manage or are responsible for information 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

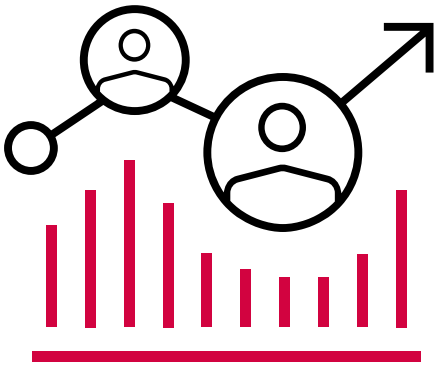
Highlight priorities for investment or areas for divestment

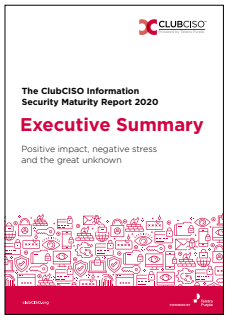
Drive process change to better protect your organisation

How was the data gathered?

This is ClubCISO's seventh annual report on information security maturity. It has been independently produced based on a survey of information security leaders working in public and private sector organisations globally. Responses were gathered anonymously in March 2020 via an online questionnaire, augmented by a live web-based discussion.

100 information security leaders took part, representing a range of business types. See the Demographics section for a full breakdown.





Click to download a copy of the Executive Summary of this year's survey, which features commentary on the discussion at the Live Vote event along with notable headlines from this year's results data.

All content © ClubCISO 2020. All information contained in this document may be freely referenced, citing as source: ClubCISO Information Security Maturity Report 2020.

Commentary

Vote results

Setting the scene

Role of the CISO

Wider security ecosystem

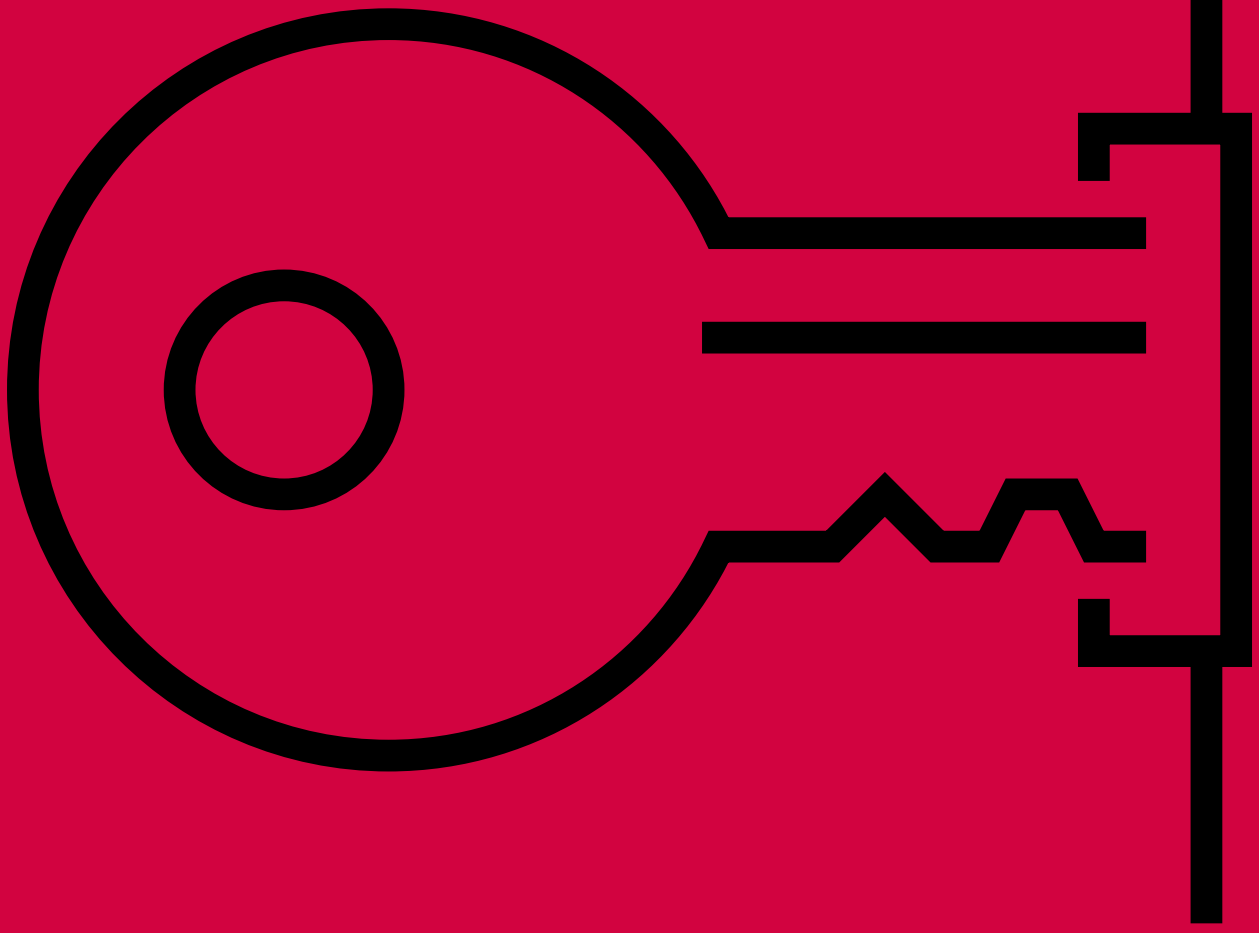
Hot topics

Wrapup

Demographics

Key findings

Commentary from the ClubCISO advisory board



POWERED BY Telstra Purple

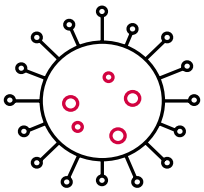
Cyber resilience moves up the agenda

CISOs are now taking a more proactive role when it comes to key material risks. **Over two-thirds of CISOs see cyber resilience as a major 'hot topic' for them**, just behind security culture. Cyber resilience is about ensuring that an organisation can continue in the face of adversity, which is quite different to traditional cyber security methods focused on protecting its 'crown jewels'.

Herein lies a story. **Well under half our CISOs told us their organisations weren't really prepared to withstand unforeseen circumstances**, although encouragingly **over three-quarters thought their security capabilities held up well when Covid-19 hit**. This, the biggest 'real' test of resilience ClubCISO members have seen outside of a cyber-attack scenarios, showed how quickly organisations were able to respond on the fly despite **many boards being largely focused on compliance or prevention over response capability.**

As illustrations of the security challenges our CISOs faced, there was a rush into remote working with minimal planning, and one member organisation reported internal phishing test clicks had jumped from 12% to 40% (with 30% actually entering credentials) as people tried to stay informed about Covid-19. Our voting spanned the period when the UK went into lockdown on 20th March, and several CISOs made the point that we should ask how well things actually held up again at a later date.

There's an underlying trend that **our organisations' security postures are generally improving year on year,** but the numbers there could be still be better. Even when we think our businesses coped well with the Covid-19 crisis there's no room for complacency. It's clear how important good culture basics are to maintaining good cyber resilience, and when it's all over there'll be initiatives spun up to reinforce improved cyber resilience complemented with robust business continuity planning to maintain customer service outcomes.



77%
of CISOs
agree their existing security capabilities held up well against Covid-19

Click to see full result.

Cyber resilience
is the second-hottest topic on CISOs' radars

Click to see full result.

Stephen Khan

Stephen is a member of the ClubCISO advisory board, Chairman of White Hat Ball for Childline, and is Head of Technology and Cyber Security Risk at HSBC.

www.linkedin.com/in/stephenskhan/

POWERED BY Telstra Purple

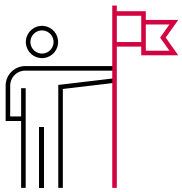
Creating better security cultures

As in previous ClubCISO surveys, **security culture remains the No. 1 topic for nearly three-quarters of CISOs. We're good at awareness training** and have actually moved on to a point where **we're carrying out a wide range of activities and other little nudges to foster better culture** which is really encouraging.

But the picture's not all rosy. There's been no significant change between the biggest causes of material cyber security incidents since last year, with **non-malicious insider and cybercriminal activity both occurring in more than 40% of organisations.** A similar number report that **organisational culture is a blocker to achieving security objectives,** and a **significant proportion still experience a blame culture around security incidents.** Such incidents are being driven underground because **fewer than half have a proactive 'no-blame' policy around reporting.**

So while **almost everyone says they're working to establish a good security culture, hardly anyone's at 'best practice' stage and a handful haven't even started addressing 'worrying' shortcomings.** What's more, **fewer than one-half believe their organisations have positive security cultures.** That figure's hardly changed since last year, so there's still a long way to go.

Board mentalities have traditionally seen security as a technology problem that can be 'fixed', while in contrast culture is a historically ill-defined, nebulous topic that's harder to get budget for. Demonstrating return on investment is fundamental. Think about the culture you want, map it to behaviours, and put metrics in place to measure progress. Because everything else depends on a foundation of a strong – and positive – security culture.



60%
of CISOs
say security culture is a worry or should be better

Click to see full result.

73%
of CISOs
say security culture is their No. 1 hot topic (up from 64% 2019)

Click to see full result.

Jessica Barker

Jess chairs ClubCISO and is co-CEO and Co-Founder of Cygenta, leading Socio-Technical work.

www.linkedin.com/in/jessica-barker/

Future strategic operating models

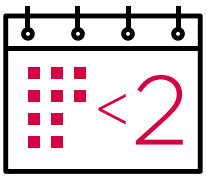
More than one-third of CISOs don't think their boards see information security as important as they do. We struggle to get security alignment with many areas of the business such as HR, legal, IT and innovation teams. And our CISOs tell us **maturity of processes for measuring and managing supply chain risk have grown worse.**

To address issues like these **most organisations have now adopted a 'future state' or 'target operating model (TOM)' approach to building a more robust security posture. Only a handful are not considering at TOM at all and one-tenth are already seeing benefits.**

A TOM is a robust way of sharing a security's strategic direction across the business. It makes sure everyone from the board downward is pulling in the same direction. In organisations where there might be disparate security teams, either globally or organisationally, this is vital. Individuals also understand the security context in which they operate, making the TOM a great tool for driving better security culture too.

With such clear benefits, it's a puzzle why so many organisations are making such slow progress with their TOMs. One factor could be the **short tenure cycles of most CISOs.** Another could simply be **insufficient staff.** The biggest obstacle of all could even be **reporting lines.** Well **over half of CISOs report into IT,** but a similar number think **they could do their jobs more effectively if they reported into the main board or audit/risk committee.**

Whatever you call it – a TOM, a strategic security operating model, or whatever – the one thing all CISOs have in common is a desire to improve security maturity. We need to find ever more creative and flexible ways to reach that goal.



80%

have been in role for under two years

Click to see full result.

47%

of CISOs

rate maturity of their cloud security strategies below the median

Click to see full result.

Manoj Bhatt

Manoj is an advisory board member of ClubCISO and leads the Cyber Security Advisory and Consulting team across Telstra Purple EMEA, championing cyber security as an enabler for digital transformation.

www.linkedin.com/in/manoj-bhatt/

POWERED BY Telstra Purple

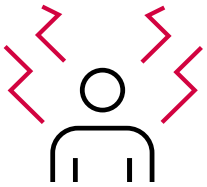
Caring for the security team

Last year we gave a lot of attention to how stress affects the CISO **(it's not really getting much better)**, but this year we looked at the wider team too. After all if there is a security incident then it's not just the CISO that feels the brunt of it. CISOs really feel for their teams as they are their main support structure. **42% say stress affects their teams, and 7% recognise it's unbearable for some team members.** With figures like that it's perhaps surprising that only **one-third of CISOs are struggling with retention.** Is that just down to the discipline we work in?

It's obvious **the concern most affecting CISOs' ability to deliver against their objectives remains insufficient staff. Over half of our CISOs are frequently having difficulties with recruitment**, with a lot of blame going on recruitment processes and lack of understanding from HR about what is required from roles and candidates. Some members pointed out that CISOs can lead change and this problem is in our gift to fix. There's a notable **improvement in the number of apprentices and security graduates coming through.**

To counter threats, CISOs recognise their security teams need to be as diverse as possible. Although their **teams aren't really diverse yet,** it appears **hiring policies are evolving well to make them more inclusive in future.** We don't just need to avoid unconscious bias in recruitment, but look beyond our own organisations. For example, one CISO told us they'd had recently chosen a security supplier because of "its commendable hiring policy".

In gender diversity though there's certainly a lot of ground to make up. Despite the admirable work being done by ClubCISO members through education and training, the more senior the security role the fewer the number of women applying. Some members tell us they'd consider a positive discrimination recruitment policy if only there was a diversity of candidates to make it worthwhile.



42%
of CISOs
believe the stress their teams are under affects performance

Click to see full result.

71%
of CISOs
think their hiring policies could be more diverse and inclusive

Click to see full result.

Debbie Saffer

Debbie is a ClubCISO advisory board member and Global Deputy CISO at Cushman & Wakefield.

www.linkedin.com/in/deborahsaffer/

Back to main contents page

Inside the mind of the CISO

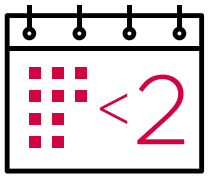
Security budgets are continuing to increase (albeit at a slower pace than we've seen in previous years), and a good CISO should be able to influence security posture and culture regardless of reporting lines **(a healthy proportion don't think it matters where they report into)**. These are good reasons to be optimistic.

But, as last year, **the stress of the job is increasing. Nearly one-quarter remain frustrated with their organisations' approach to security.** Others cite factors such as lack of resources and support, and still not seeing eye-to-eye with senior leadership. **Most CISOs typically move on within a couple of years in role.**

Dig a little deeper and you realise the main reason most CISOs leave their roles so quickly are simply **career progression and furthering their careers.** Typical comments are "I want to build things, not run them," and "I like seeing things take flight." Of course, it doesn't always work out that way. One CISO told us: "I changed companies because my employer wasn't taking security seriously enough, only to find my new organisation only pretended to be serious about it for the duration of my interview!"

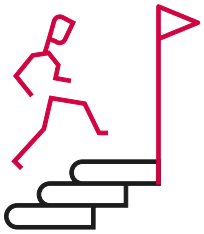
And unfortunately **this year we love our jobs a bit less.** Perhaps it's just that we're not feeling so optimistic in general right now. When we get back to BAU there'll be plenty of projects to make sure things are as they should be, and to make those hastily-deployed remote working solutions more robust.

The great news is that throughout the Covid-19 pandemic, ClubCISO members worked together to help shore up security for everyone. At times like these such communities are invaluable, enabling members to support each other at a time where professional and personal pressures combine to place even more strain on the security community.



60%
of CISOs
have been in role for under two years

Click to see full result.



55%
of CISOs
move on because they want new challenges and career progression

Click to see full result.

Paul Watts

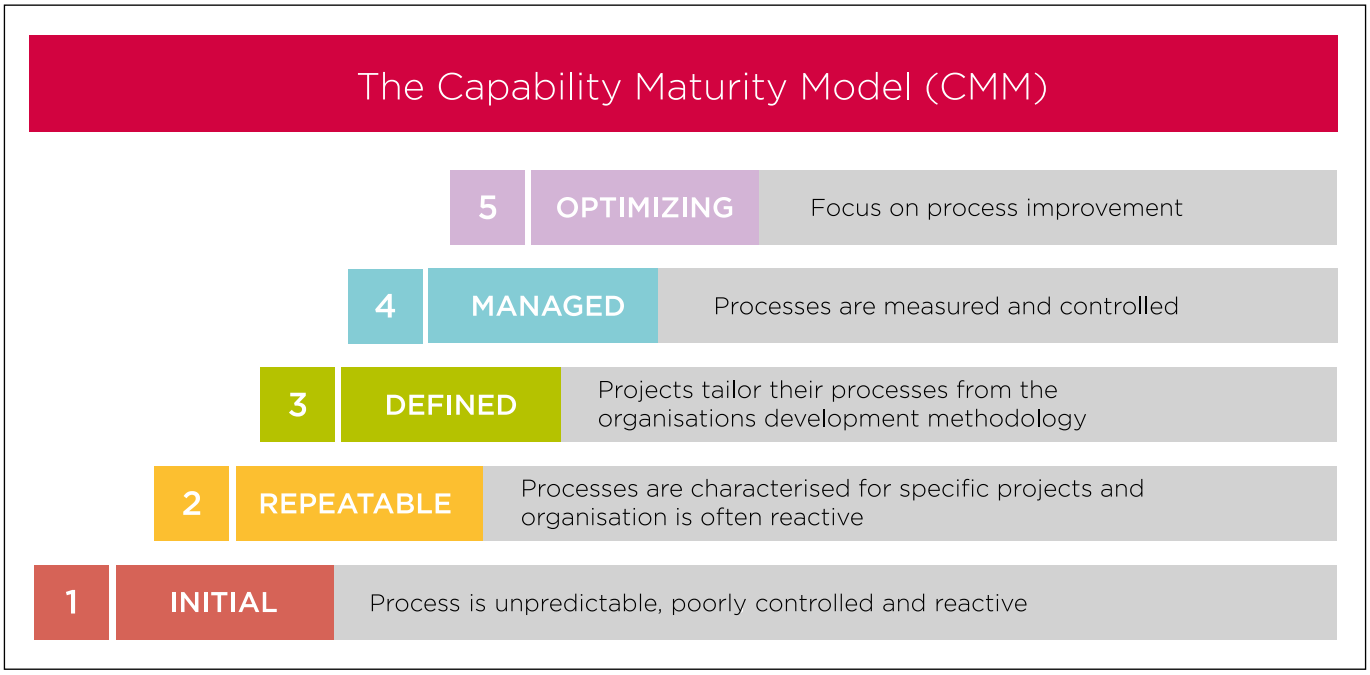
Paul is an advisory board member of ClubCISO and is CISO at Kantar.

www.linkedin.com/in/paulewatts/

POWERED BY Telstra Purple

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.

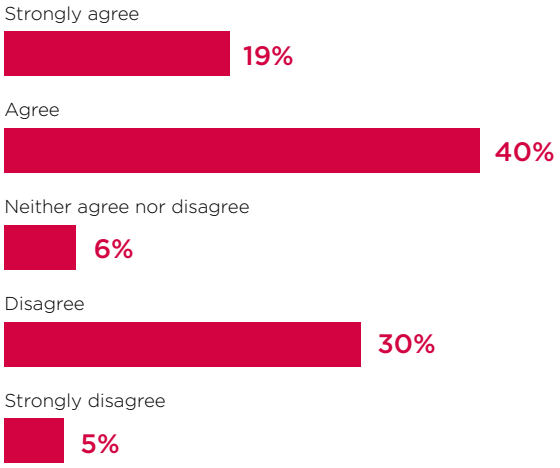


POWERED BY Telstra Purple

Setting the scene

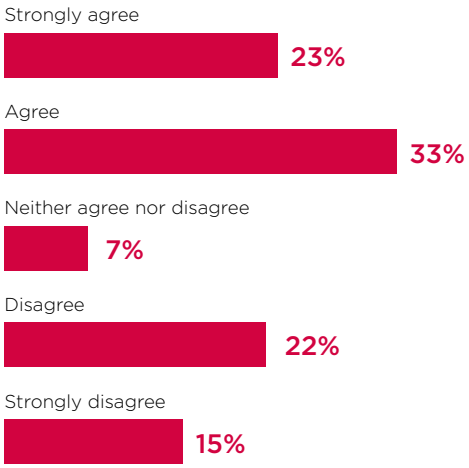
POWERED BY Telstra Purple

1. My organisation views information security as being as important as I do...



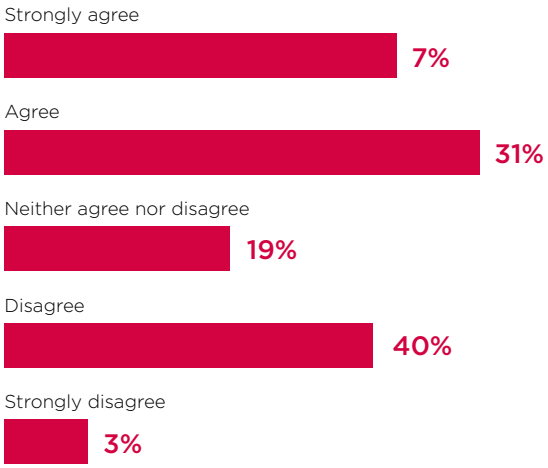
> 59% seem well-aligned with their businesses, but many don't agree that their organisations see security as important as they do.

2. ...and I'm OK with that



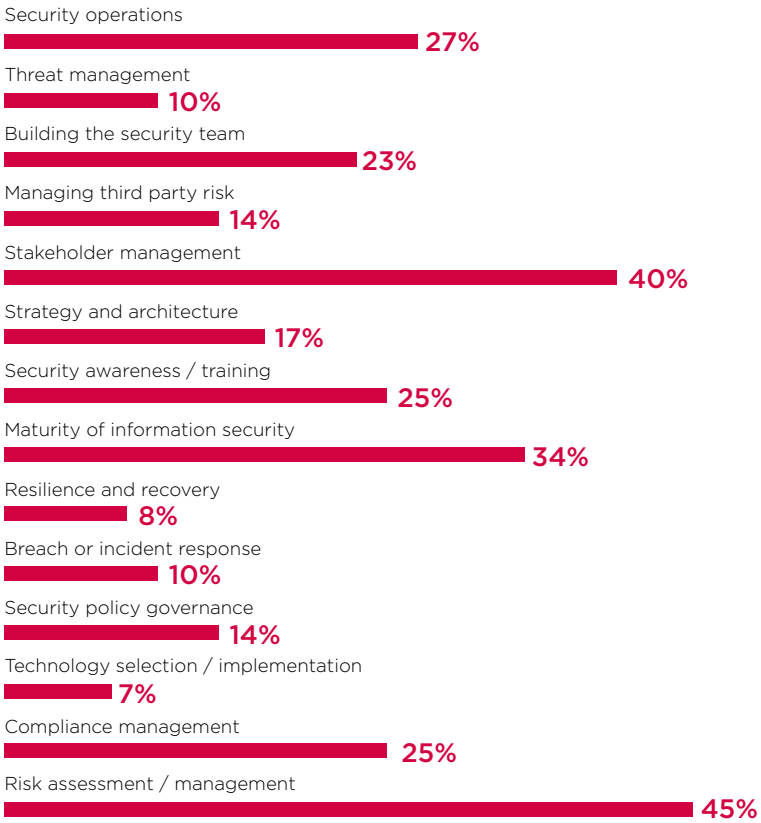
> Close analysis of the figures shows a clear correlation with the answers individual members gave to Q1. CISOs' frustrations are voiced in later questions about reasons for leaving (Q13), obstacles to success (Q14) and stress (Q15/16).

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



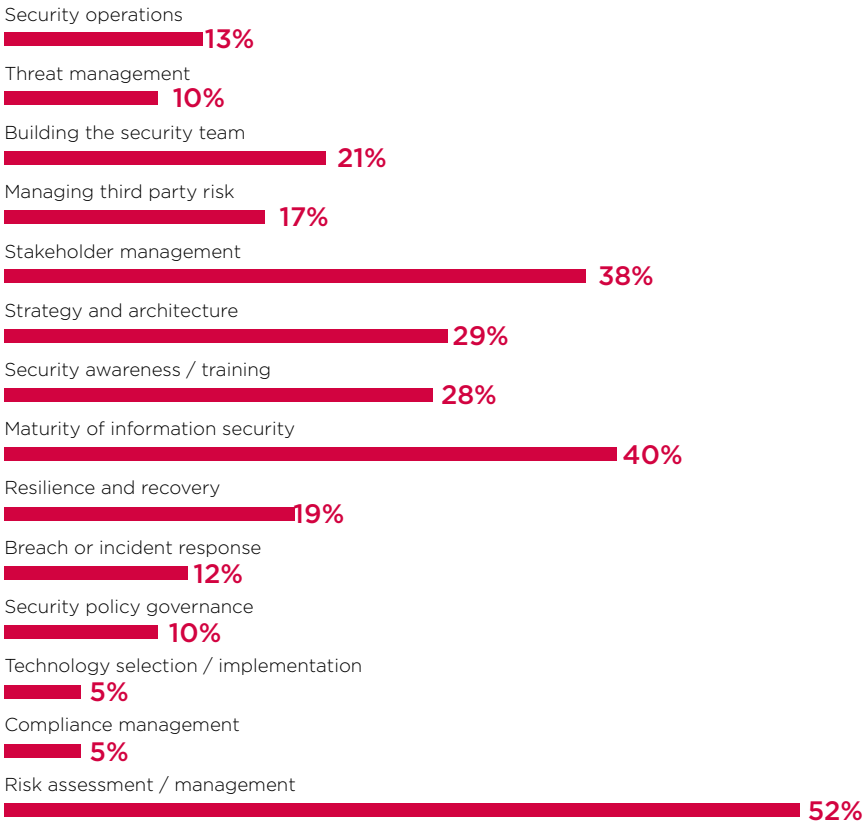
> This is a notable decline against our 2019 result, when 48% agreed their organisations could meet these objectives. This year that's down to 38%. Members suggested this is partly due to changes in the threat landscape, but also because 'Rumsfeldian unknown unknowns' were becoming more apparent as general maturity of security improves.

4. Which three of the following do you spend the most time and resource on?



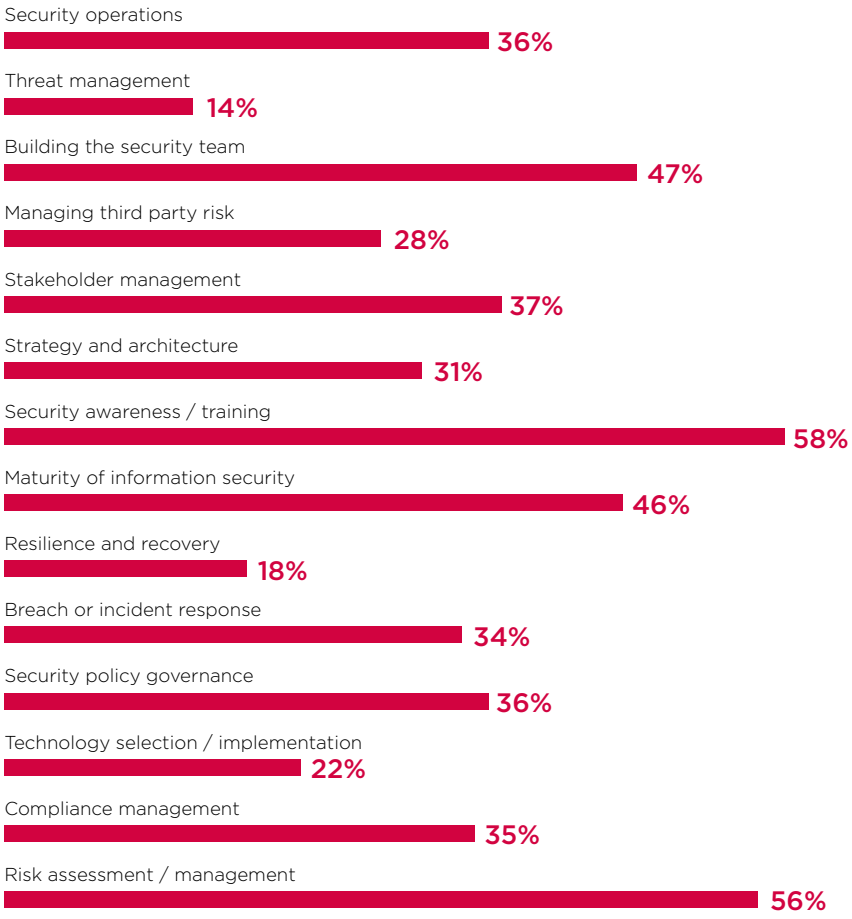
> This is moderately encouraging, as CISOs are not spending as much time on areas like tech selection / implementation (2019: 18%).

5. Which of the following do you think you should you be spending most time and resource on?

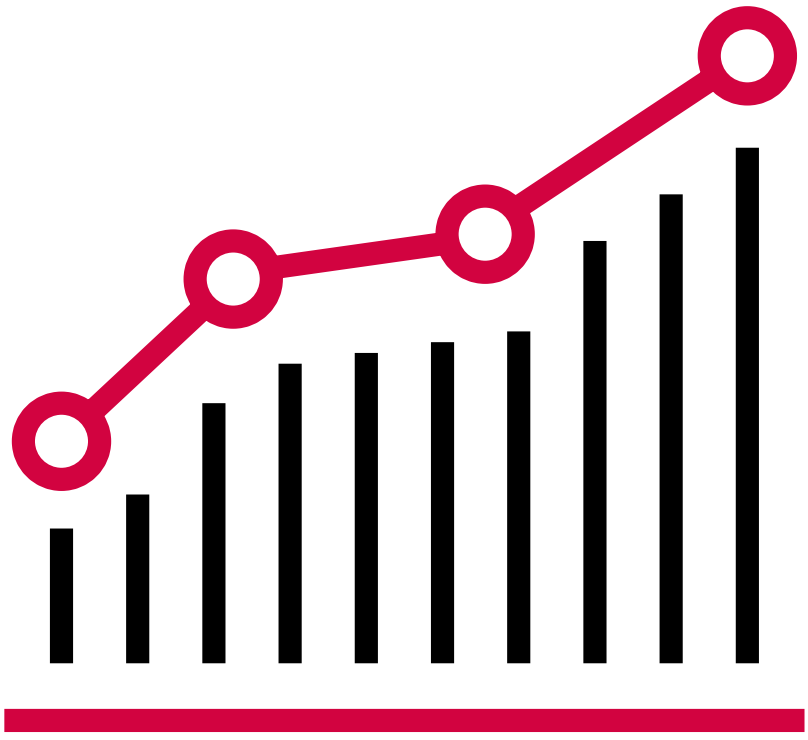


> Risk assessment, maturity of infosec and stakeholder management are the same top 3 as shown in Q4. CISOs are generally spending time and resource on the right things.

6. Indicate any areas in which you have driven measurable improvements over the past 12 months



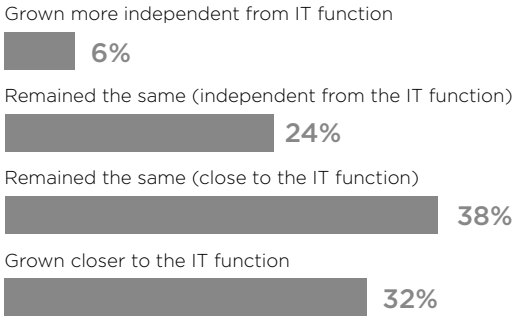
> Good progress across everything here, and note particularly the improvements in security awareness and training. We think the introduction of GDPR may have also been a factor. We look closer at human aspects of security later in the survey. This also seems an encouraging response around management of stakeholder expectations, as some board members are acquiring a better basic understanding of their security risk.



Role of the CISO

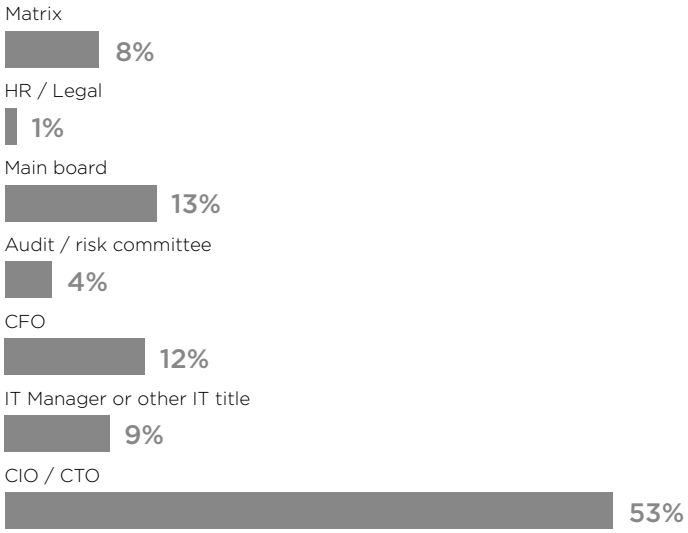
POWERED BY Telstra Purple

7. How has your working relationship with IT changed in the last 12 months?



"These figures have flipped back and forth over the years we've been doing this survey. This year we've grown closer to the IT function again. In smaller organisations, the roles of CIO and CISO are often combined."

8. Within your organisation, where does the information security function report currently?



"These figures are nearly identical to our 2019 survey. Some CISOs find working under the wing of the CIO provides better air cover and share of voice. Better the devil you know? Others point out that in many circumstances there's an inherent conflict of interest in the CISO reporting to the IT function."

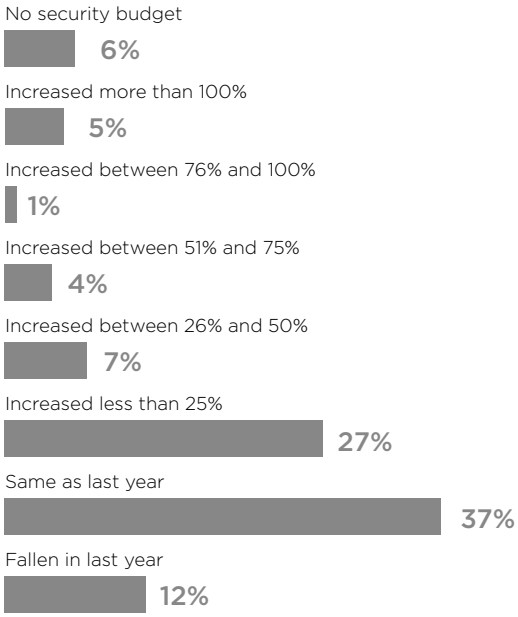
9. Where do you think you should report in order to perform your role to best effect?

"Many CISOs want a reporting line to the board or, in particular, the Audit & Risk Committee (ARC). Some say the ARC provides better operational oversight, which is what really matters. If you're a good influencer perhaps it shouldn't matter where you report – which is reflected in the 13% who say exactly that.

There's no single reporting line model that suits all organisations."

POWERED BY Telstra Purple

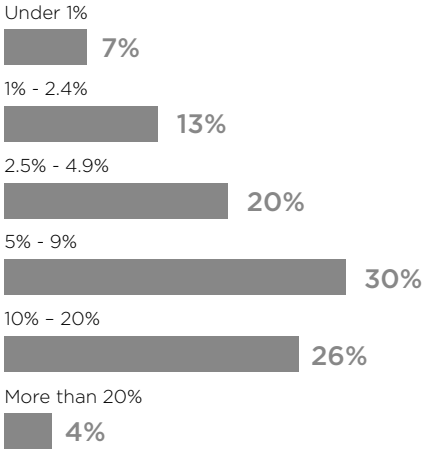
10. Describe your organisation's current information security budget



"Growth in security budgets is slowing compared with the last few years. Increases of up to 25% are broadly in line with 2019, but above 25% there have been far fewer increases. The proportion of budgets that have stayed the same has risen from 18% in 2019 to 37% now.

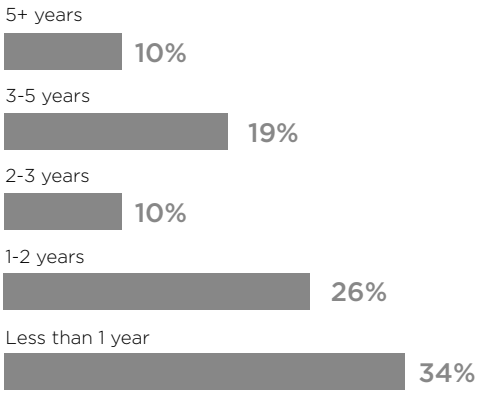
Some members even reported they were getting increased budgets but couldn't spend them because they couldn't get the resources (for example see Q14 citing insufficient staff and Q26 on difficulties attracting staff)."

11. What is security's budget expressed as a percentage of the overall IT budget?



"This is never an ideal measurement, but it's purely used as a comparative benchmark. As noted in Q8, remaining aligned with IT can give some CISOs a huge amount of influence over security budgets. There's been no significant shift in these figures since the 2019 survey."

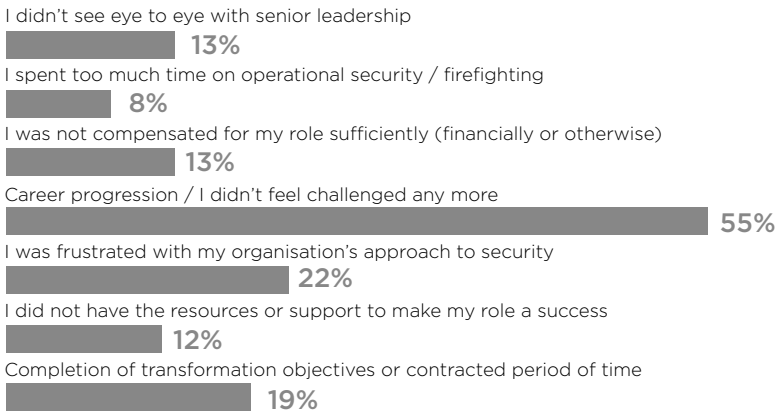
12. How long have you been in your current role?



"This result is almost identical to 2019, with 70% of CISOs being in role less than three years. If people were staying in role we'd have expected the '3-5 year' number to have increased; in fact, at 19%, it's identical to 2019.

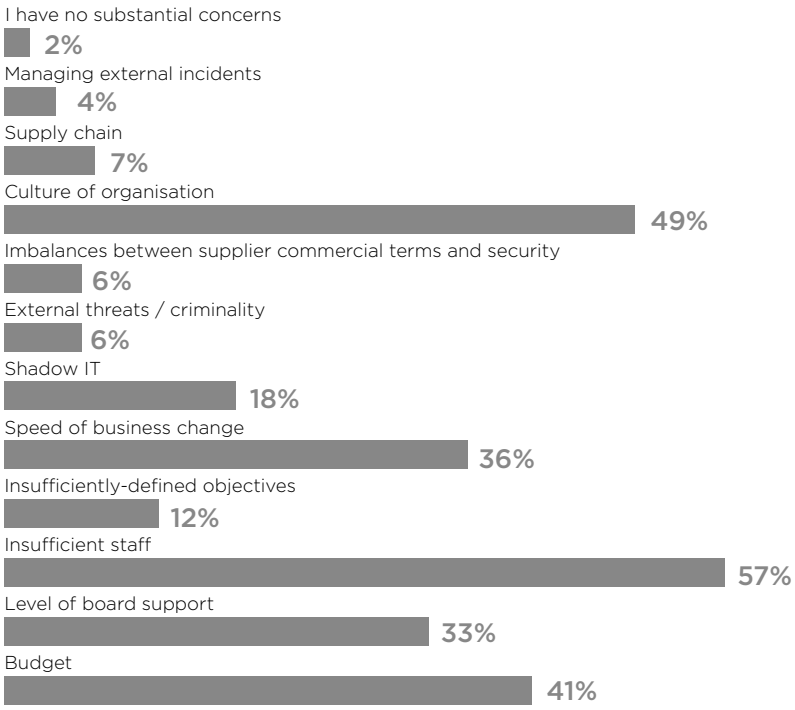
This year we've made the question more granular, and can see a high proportion haven't even made it to two years yet. The implication remains that CISOs don't stay in their roles long. There may even be a link to staff retention if these CISOs take their best people with them when they move on."

13. Why did you leave your last role?



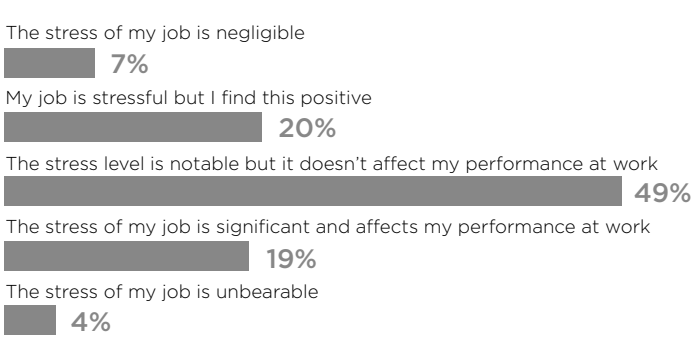
"CISOs need to feel challenged, and then it's typically on to the next gig. However, 22% move on because they are frustrated with their organisation's approach to security, which is in line with last year's result and reflects concerns highlighted in Q1 and Q2. Perhaps CISOs are maturing their skill sets faster than their organisations can keep up with them."

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



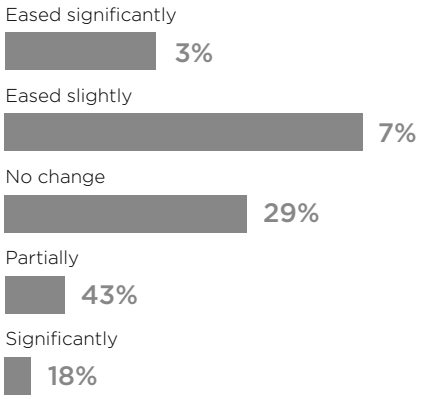
"These concerns are broadly similar to those we saw in 2019. There's clearly a staffing issue, and a budget one too (though as we saw in Q10, budget growth is slowing). The standout change though is that concern about level of board support has rocketed from 16% to 33%. That's worrying, and correlates with our findings on how seriously the organisation takes security in Q1."

15. How stressful is your job?



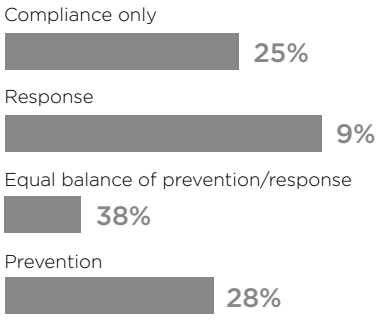
"We were alarmed by the level of stress felt by CISOs in the 2019 survey, and this has been partially blunted by the inclusion of a 'stressful but positive' option in this year's question. But still, your heart must go out to the 23% who are clearly struggling."

16. Has the stress level in your job got worse over the past 12 months?



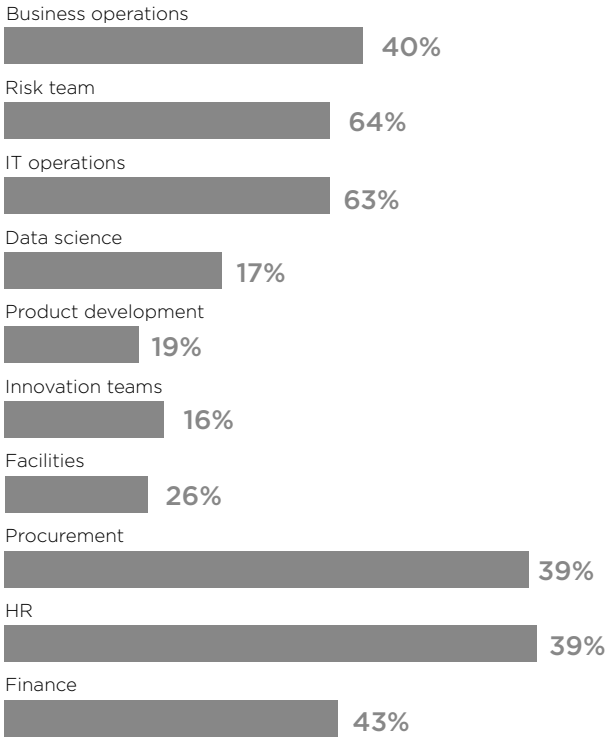
"The big takeaway from this chart compared with 2019 is that stress is still an issue, although there are signs of it easing slightly. Those suffering most talk about the lack of control they feel about being able to influence positive change."

17. Which of the following does your board prioritise with regard to information security?



"We've asked this question in various forms over the years, and included the 'balance of prevention/response' option this year. Look closely at the low figure for 'Response' though; are those the organisations that most struggled with Covid-19? The 'compliance only' figure is also concerning, although in some cases this could be due to organisations that have to complete forms when acting as suppliers."

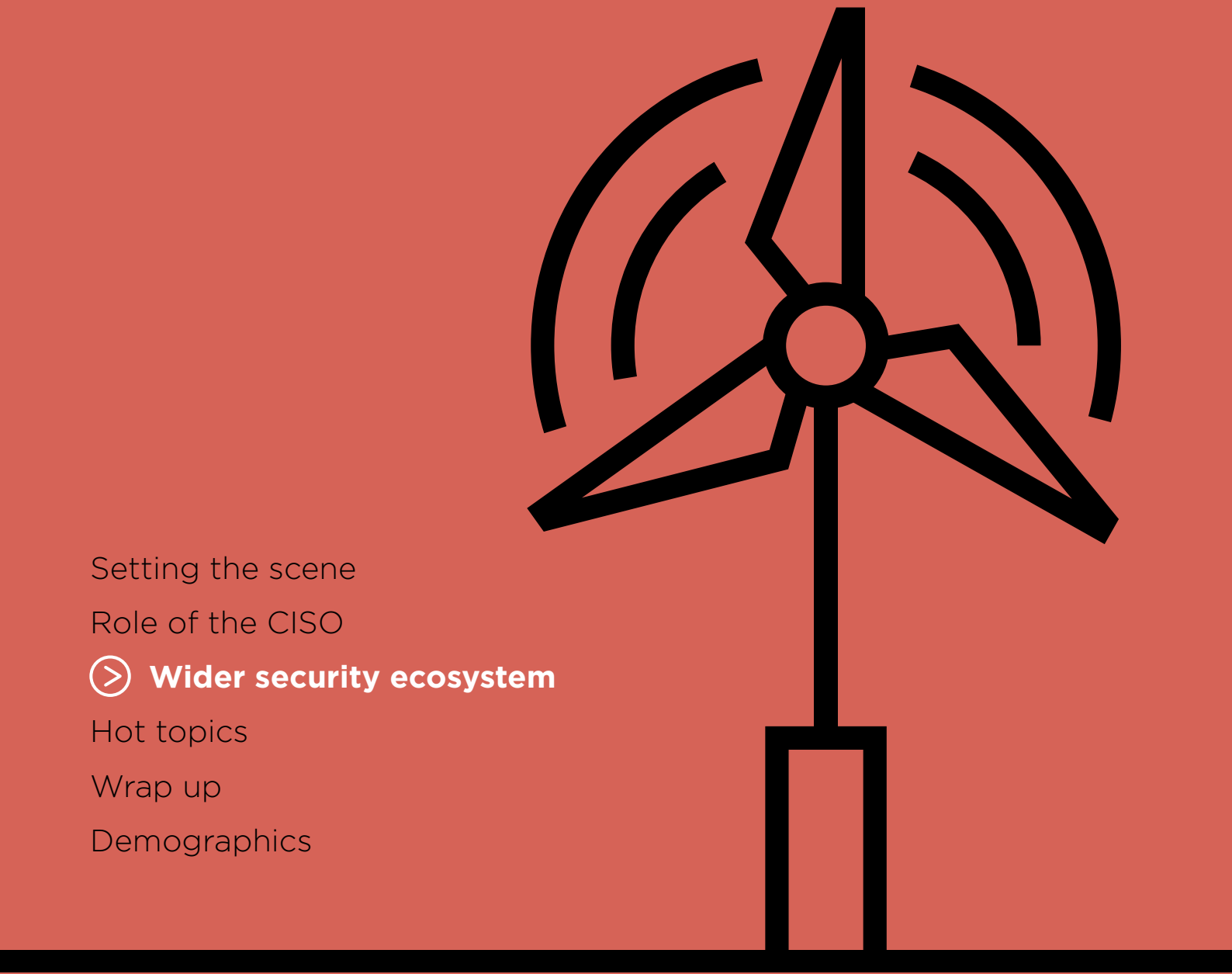
18. I am comfortable with how well security is aligned with these areas of my organisation right now



"The ideal answer to this chart should be 100% across the board. It's encouraging that areas like risk and IT operations score so highly, but it's worrying that our relationship with HR is often so fractious when security culture is such a big concern. We noted last year that speed of business change was an issue (it still is – see Q14), and this is reflected in our low alignment with innovation and product developers.

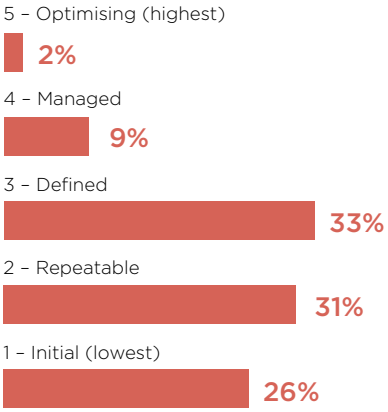
This topic sparked a lot of discussion at ClubCISO's 'Lockdown 1' open mic in November 2019 (we were ahead of the game when we came up with that title, weren't we?), and doubtless we'll return to it. Where resources allow, we need security champions and relationship managers from the security team to help embed good cultures."

Wider security ecosystem



POWERED BY Telstra Purple

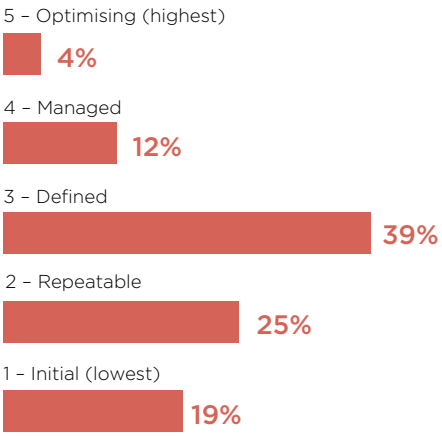
19. Rate the maturity of your process to measure and manage supply chain risk



In all the years we've asked this question supply chains have remained a big concern. This result is worse than last year, with 57% in the bottom two sectors of the CMM compared with 44% in 2019.

One member pointed out that a major issue is ensuring 'cultural compliance' throughout the supply chain, and this is something organisations are trying to work toward as part of their security operating models (Q33).

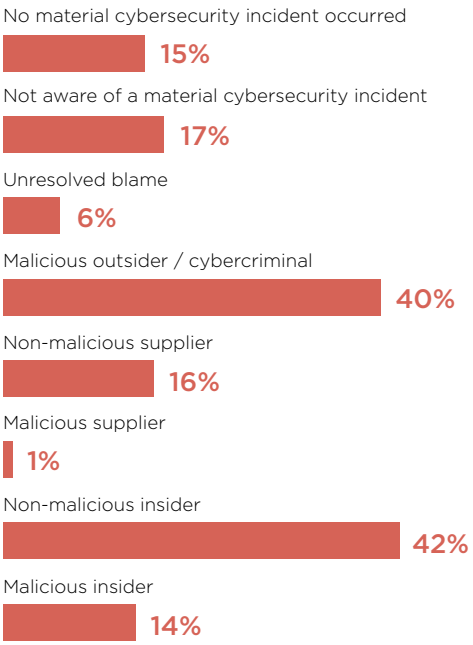
20. Rate the maturity of your organisation's overall risk management programme



The main shift this year has been a slight fall from managed (12% in 2020 vs. 20% in 2019) and a corresponding increase in defined (39% in 2020 vs. 30% in 2019). In discussion, our CISOs felt we were making progress with dedicated platforms rather than "tossing spreadsheets around", and what we'd discovered as a result had, for now, downgraded our expectations.

A perpetual gripe among CISOs is the hugely variable quality of the third party risk assessments they are asked to complete as suppliers.

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

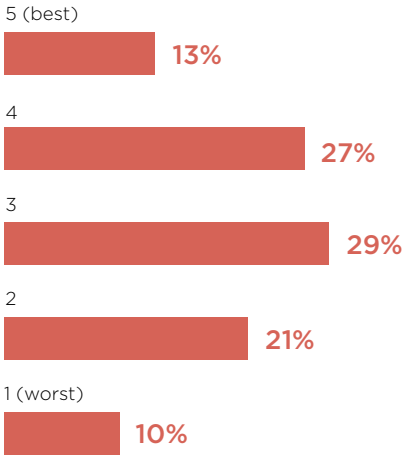


Unsurprisingly, as with 2019, malicious outsiders and non-malicious insiders remain the biggest threats. Some CISOs reported a rise in phishing test click rates as the Coronavirus pandemic hit, but this was too late to seriously affect our survey.

We believe the incidence of malicious insiders continues to be over-inflated by the media, and this survey shows a fall from 18% in 2019 to 14% in 2020. Nonetheless, with disruption caused by Covid-19 this will be an interesting statistic to look at in 2021.

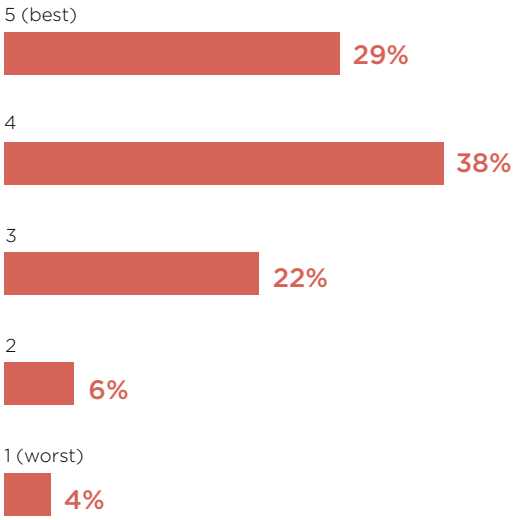
A point that came out in discussion was that in some cases there is a convergence of security going on, whereby physical and cyber security were being brought back together. We think this is being caused by developments such as the Internet of Things (IoT).

22. Be honest – on a scale of 1 to 5 how inclusive and diverse is your security team?



There's little doubt these figures should be better, but this was the first time we've asked this question and it gives us a benchmark to work from. When we talk about diversity and inclusivity we're examining all 'protected characteristics', including age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

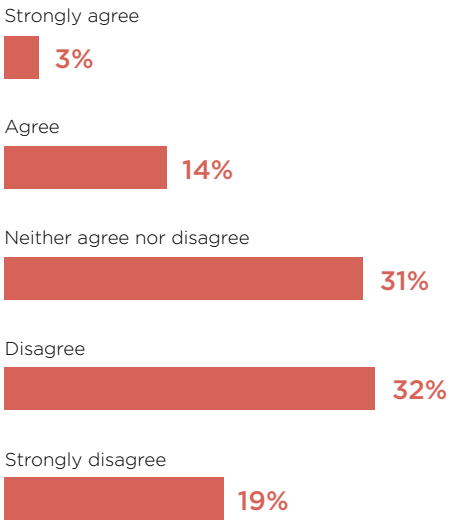
23. Be honest – on a scale of 1 to 5 how inclusive and diverse is your hiring policy?



The good news is that most organisations are proactively attempting to redress the balance. Proactively seeking neurodiversity, whereby the security team includes people who represent the diversity of human brains and minds, helps address the widest possible range of threats. And we're encouraging our suppliers and service providers to take the same view.

The bad news is that we're struggling to find appropriate candidates. For example, one CISO reported hiring 80% of all female applicants, but their team was still 70% male. CISOs are crying out for a more diverse range of applicants, and many are actively working to develop young talent.

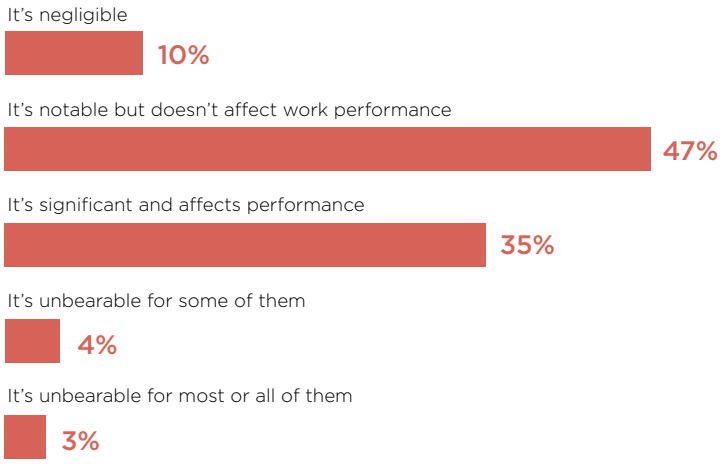
24. My organisation has a blame culture around security incidents



It's great that over half our CISOs are so confident, with 51% saying their organisations don't have a blame culture around security. In previous years, CISOs felt that they could be potential scapegoats when a cyber incident could take place.

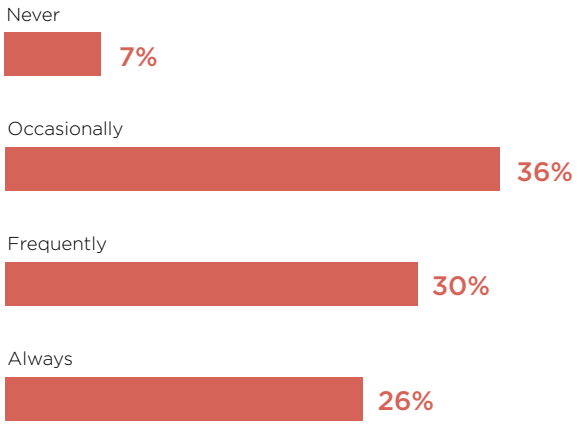
However, 17% openly say they do have a blame culture and 31% aren't sure. This paints a picture of security culture none of us wants to see in 2020. Incidents are still being driven underground and not reported and organisations are putting themselves at far more risk than they need to. This is reflected in Q30, where we see only 47% have a proactive 'report it' no-blame policy.

25. How stressed do you think your team feel?



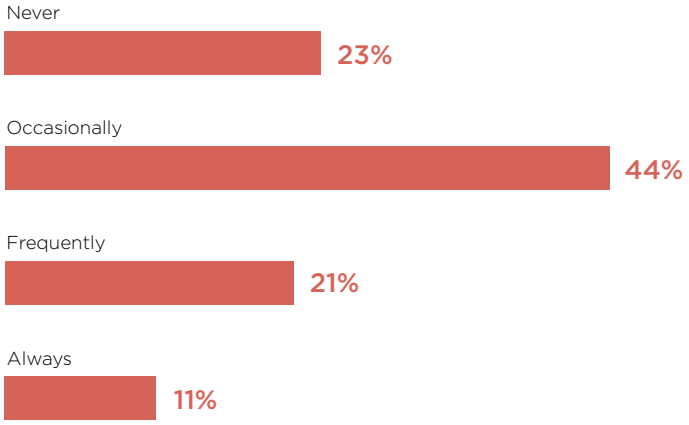
"This is the first time we've looked at team stress, and we can see detrimental stress is cascading down the team hierarchy in 42% of cases. We'd also question the 47% figure: how can CISOs be so assured that stress isn't affecting their team's work performance? More importantly, what are they doing to make things better? We'll look closely at this next year."

26. Are you having difficulty attracting good information security staff?



"56% of CISOs are having significant issues attracting good staff. The figure is down against 2019 (75%) but is still concerning. Does this mean that there are now more candidates available but that these candidates are not of sufficient skill and quality? Some CISOs say the biggest issue is that they only get in the recruitment process too late (highlighting again the friction that can sometimes occur between security and HR – see Q18). Where that's the case, the problem can be fixed."

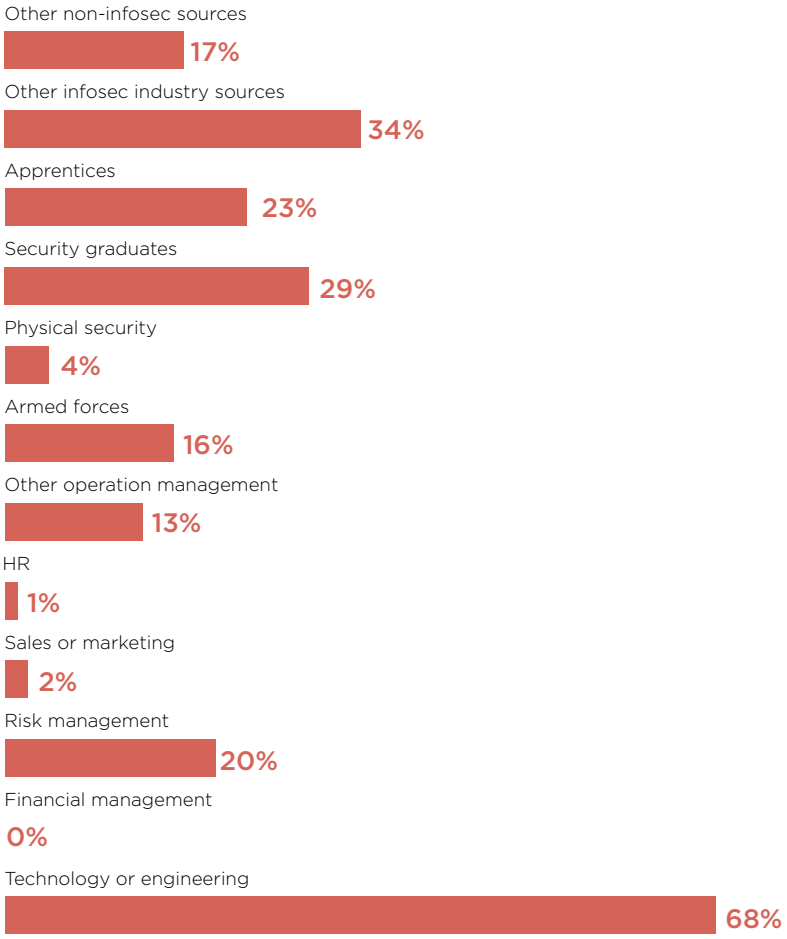
27. Are you having difficulty retaining good information security staff?



"There's no significant difference between these figures and 2019. It's good to know we're better at holding onto good people than we are at finding them. As with CISO retention (Q12) we need to make sure our teams remain challenged if we are to hold onto them."

POWERED BY Telstra Purple

28. Where are your best recruits coming from?

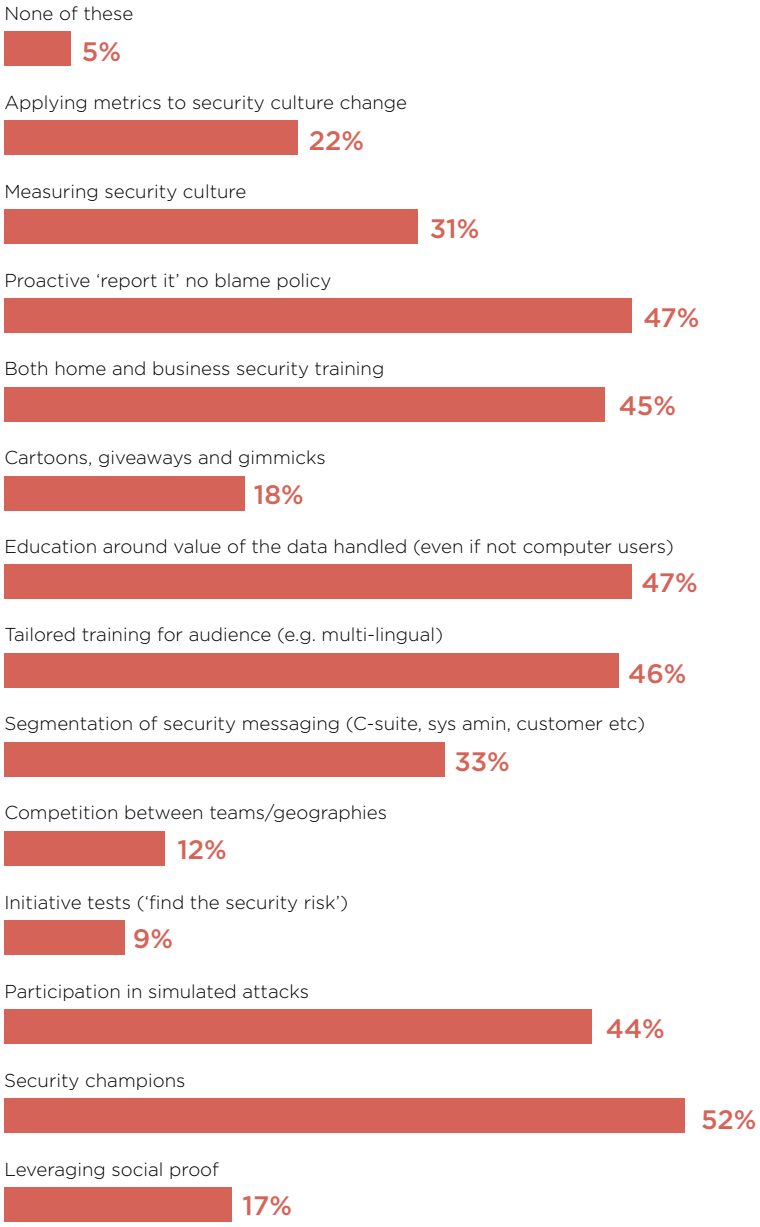


> This year we added 'other infosec industry sources' and 'other non-infosec industry sources'. Both threw up some interesting results. It's also good to see an increase in apprentices and security graduates.
>
> There's still a tech/engineering bias of course, but look at that financial management background figure of zero. As one CISO put it: "Finance are good at compliance – not security!"

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

> When we asked about, for example, hiring policies (Q23) the result was encouraging because it's documented and written down. But culture is less well-defined and more nebulous. Is that why 60% of our CISOs don't really think they're making good progress?
>
> Perhaps for some the concept of cyber security culture is relatively new and over the next few years this result may become more positive.

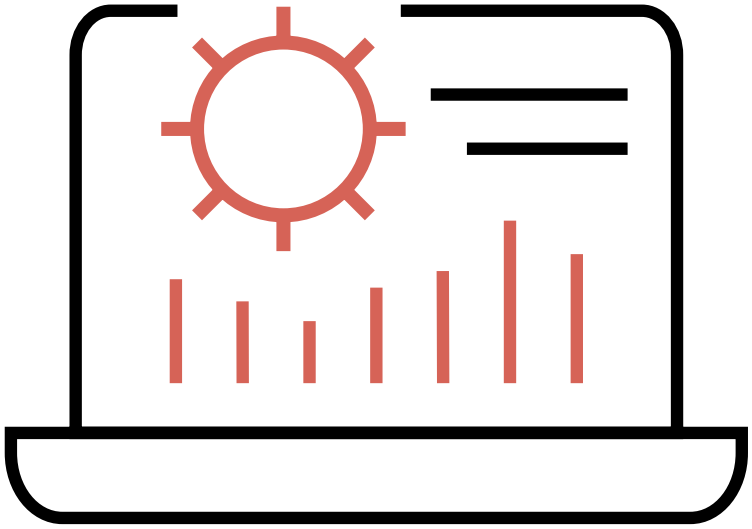
30. Which of the following are you currently doing to foster a better security culture within your organisation?



"This is essentially a non-exhaustive list of basic suggestions for building a better culture. It's encouraging so many people are at least doing something, but only 'security champions' has over 50% traction so far. It's concerning that 5% are doing 'none of these'.

It's good to see so much action going on across so many fronts though. Culture change takes years of little nudges. It's about engaging individuals, and there really do need to be behavioural measurements in place to track progress. Doing so will help drive future improvements when we ask Q29 again.

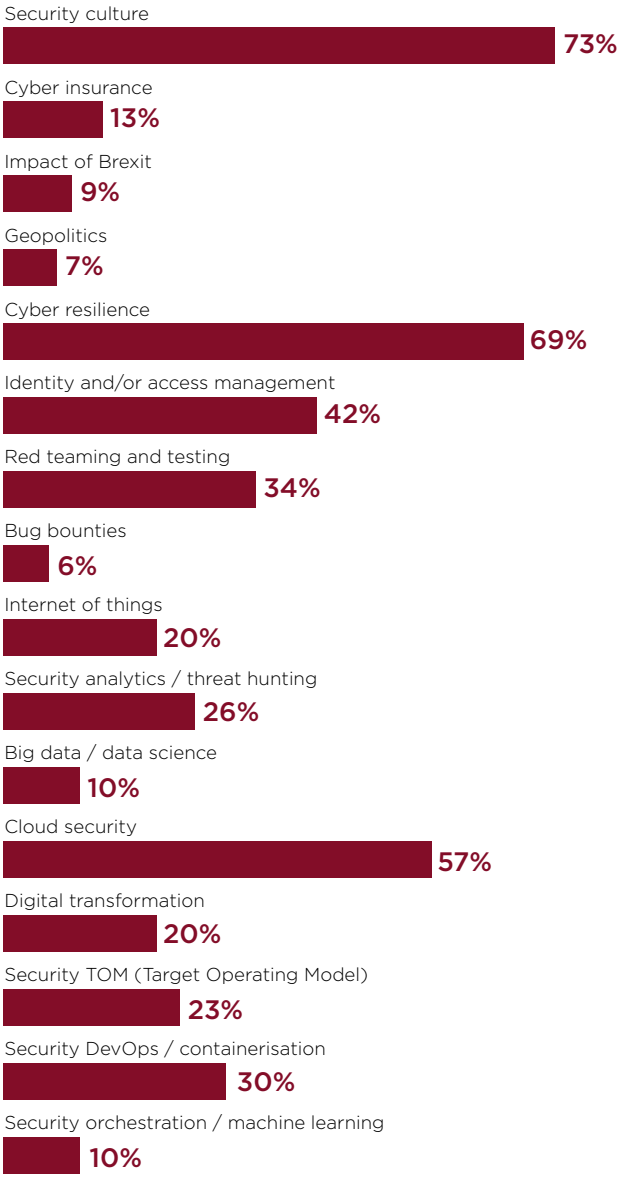
We've all seen gimmicky mouse mats, coasters and various other things in the past to boost security awareness, but may be a recognition that these methods don't actually change culture."



Hot topics

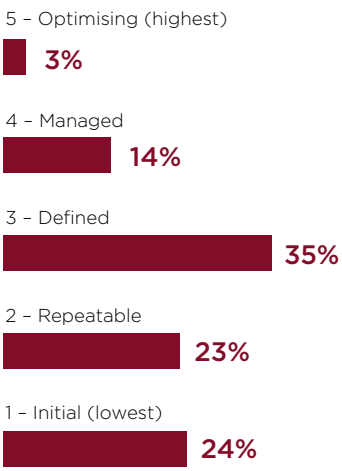
POWERED BY Telstra Purple

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



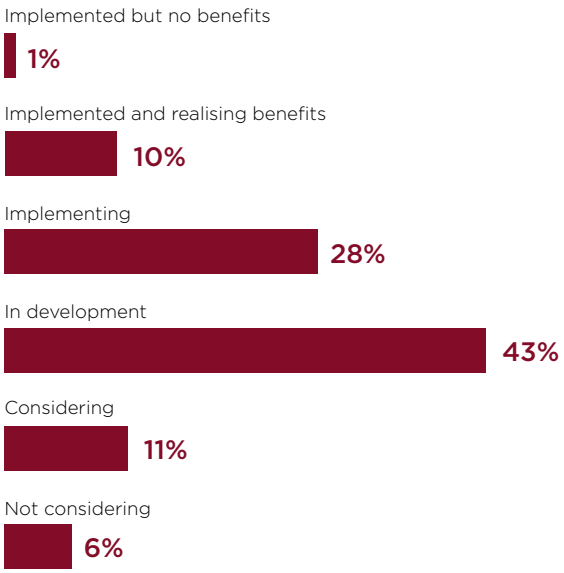
> It's little surprise to see security culture and cloud security yet again emerge as hot topics, but cyber resilience has made a big surge. And if anything is going to push security up the boardroom agenda in the wake of Covid-19 it's this. A resilient organisation is built on security and business continuity.

32. Rate the maturity of your cloud security strategy



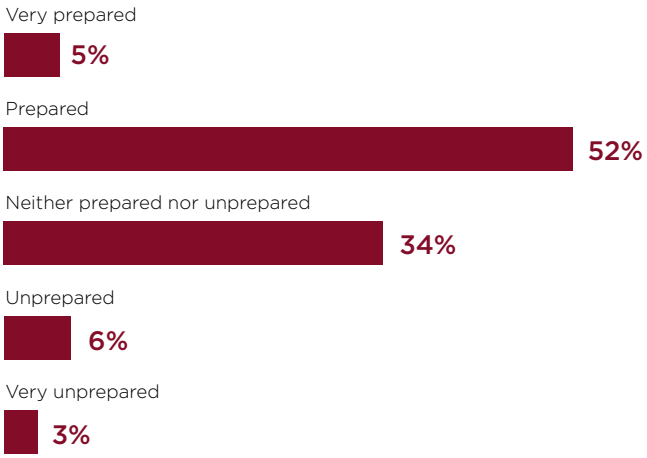
> This question has been asked in six previous annual ClubCISO surveys, and we're constantly surprised how slow progress is. This year there's been some positive movement in the lower tiers of the CMM, but there's no significant change in the two highest ones.
>
> Perhaps we're just seeing a gradual positive change. Use of cloud is constantly evolving; it changes a lot in a short space of time and we're always running to catch up to some extent. Some CISOs admit that security has actually been an impediment to cloud adoption before now. But if you do data security well, it shouldn't matter what platform – or cloud – you're running. It's now about securing your pipelines rather than your perimeters.

33. How far along your journey to building out your Security Operating Model are you?



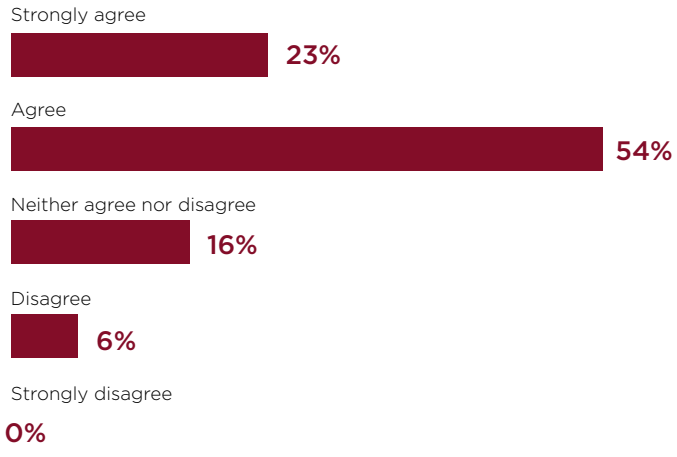
> Only 6% aren't considering a security operating model as the way to tie up security strategy across everywhere the business touches, and it's great that 10% are already seeing tangible benefits. Most organisations are only part way along the journey. Is the process more difficult than they expected? Is the short tenure of CISOs (Q12) having a detrimental effect?

34. How prepared is your organisation to withstand unforeseen circumstances (e.g. geopolitical threats)



> It's important to note we planned this question to examine resilience before Covid-19 hit, at a time when some organisations were revising their contingency planning to take account of international tensions. We think the answers to this question send out a semi-positive message.

35. Our existing security capabilities held up well when Covid-19 hit



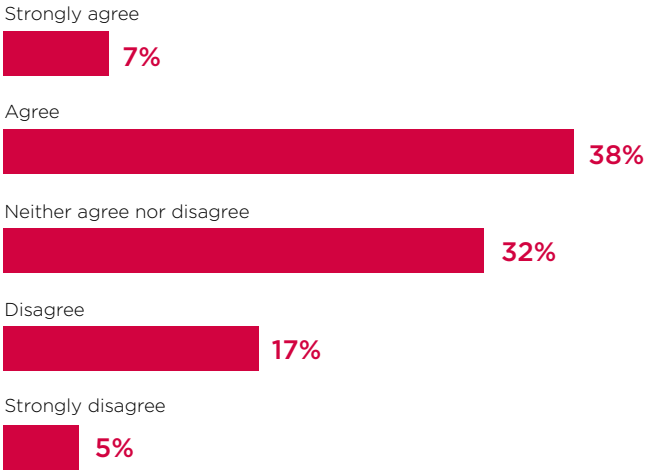
> A really positive development is how well-integrated with the business CISOs had to be in order to respond to Covid-19. When we were really tested our capabilities seem to have held up better than Q34 might have suggested. But it's possible we were asking this question too early in the crisis, and that we might get a more sober response when we test it again.

Back to main contents page

Wrap up

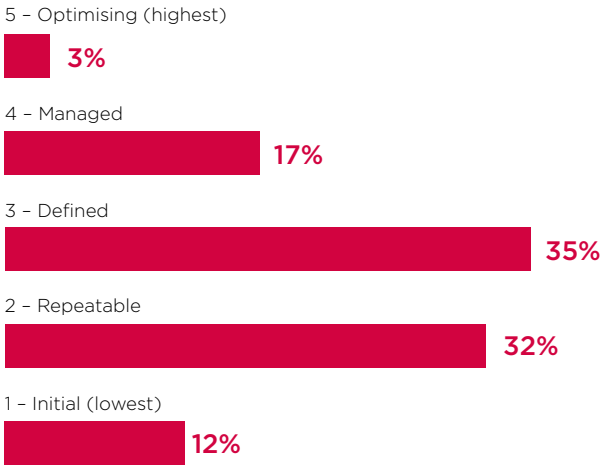
POWERED BY Telstra Purple

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



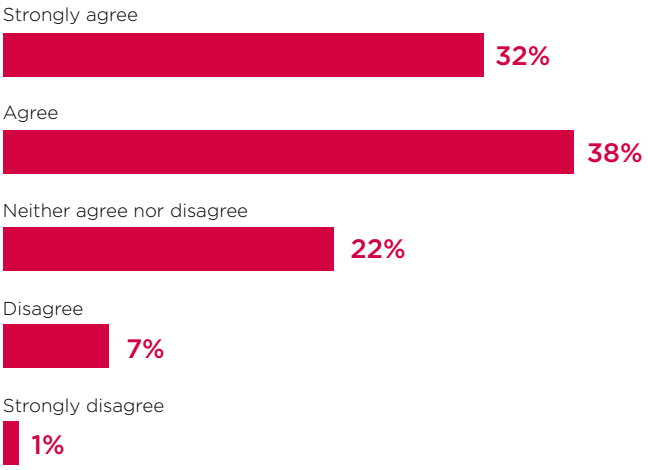
> Almost nothing has happened since we asked this question in 2019. The most encouraging statistic is that those who strongly disagree has fallen from 10% to 5%.

37. Rate your organisation's security posture



> There's been a definite improvement this year. The lowest two tiers have dropped from 57% to 44%, and we've even got 3% optimising (0% in 2019)..

38. I love my job



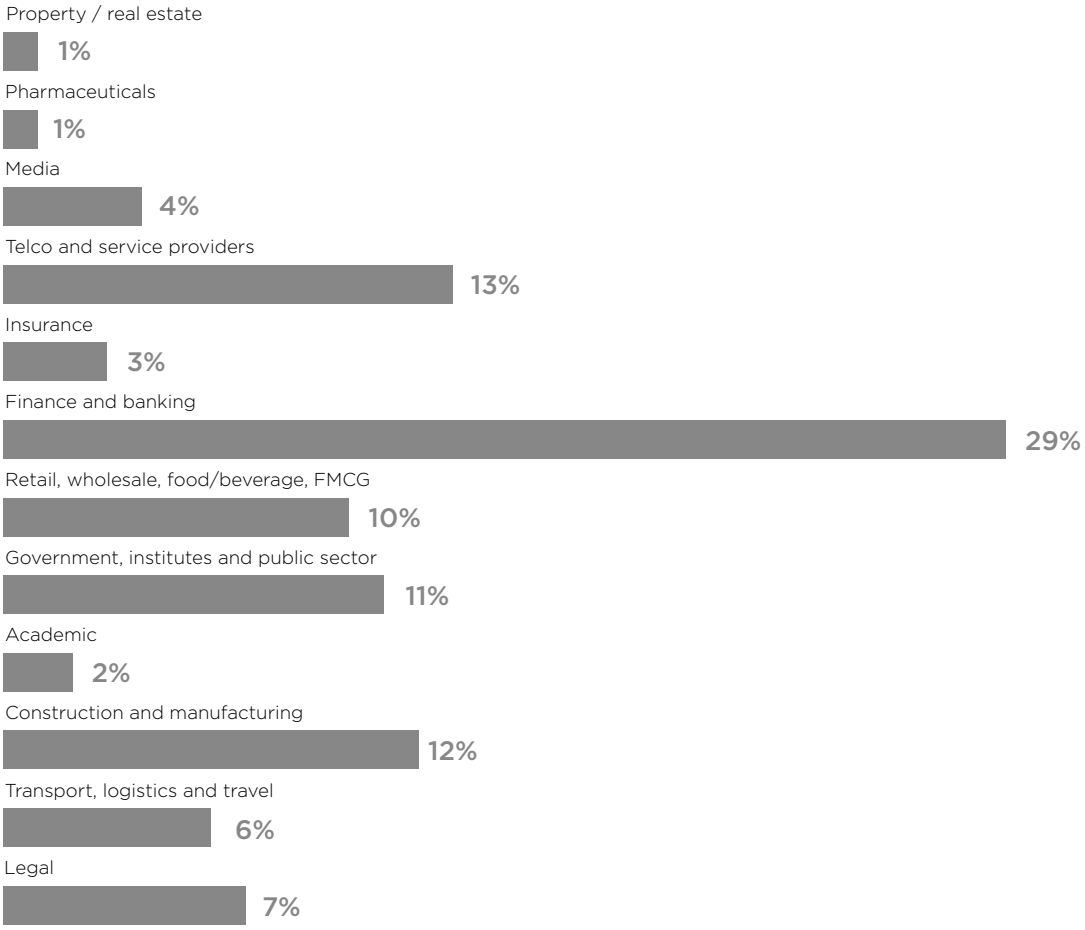
> We've loved our jobs more in the previous two years, so is it their organisations people don't love as much? Or that people are generally more overwhelmed and stretched? Perhaps Covid-19 circumstances have made this an exceptional result and perhaps that's why we just don't love our organisations as much as usual.
>
> Taking note of our stress results (Q15), as cyber security becomes more prevalent and integrated within the business our jobs are going to be more and more challenging.

Demographics

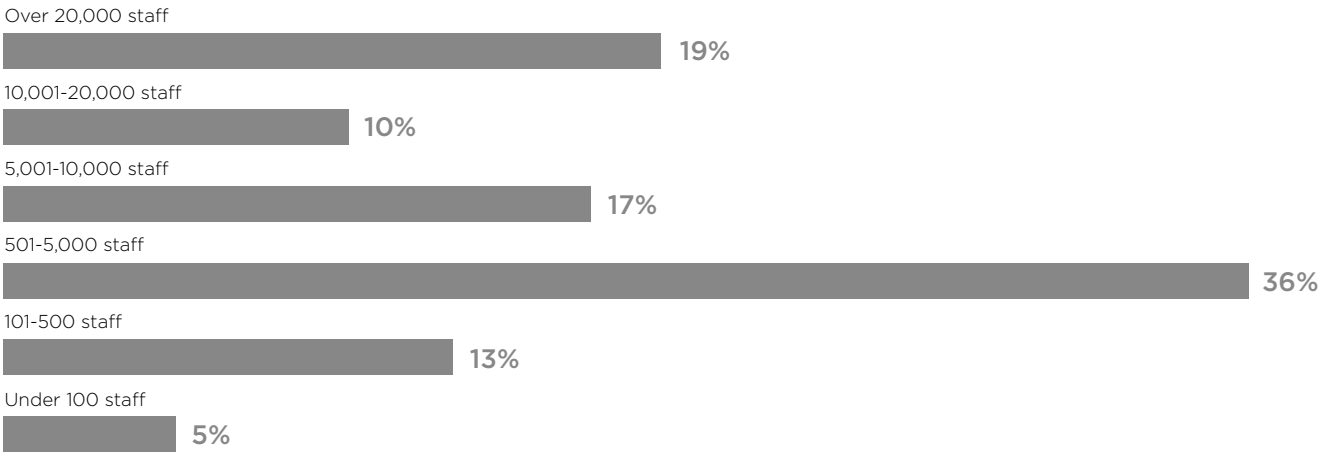
POWERED BY Telstra Purple

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

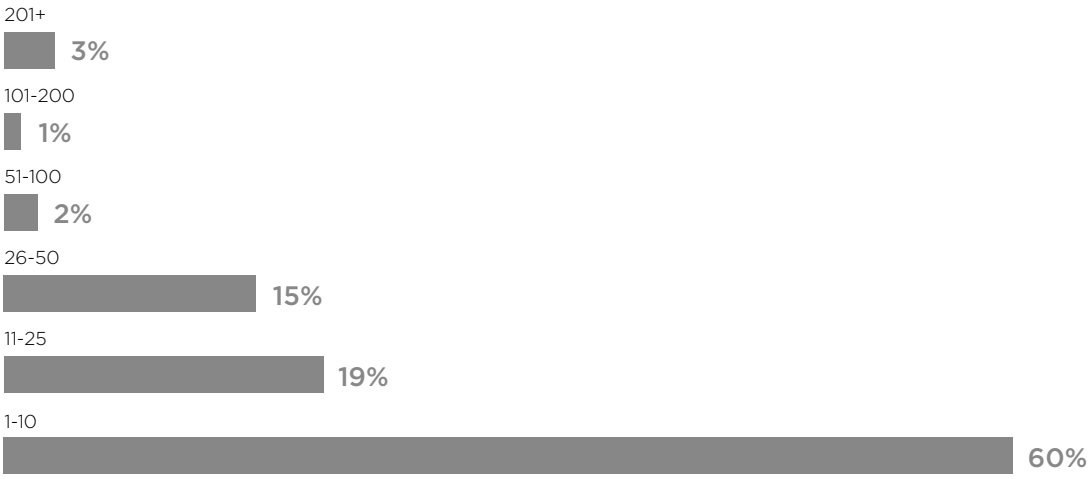
i - Indicate the industry sector that most closely matches yours



ii - Indicate the size of your business

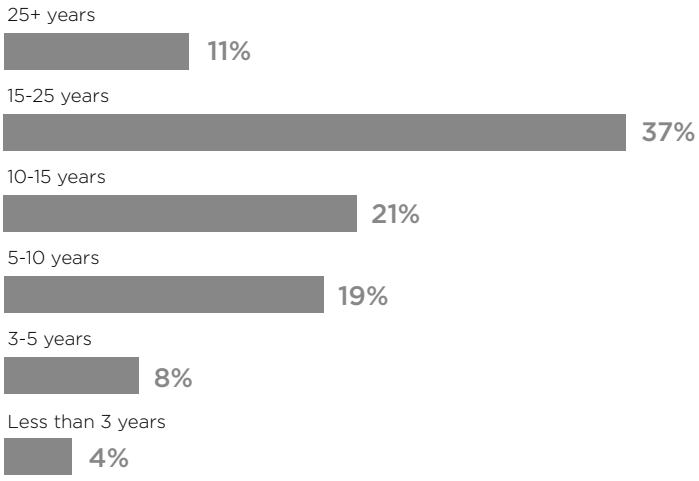


iii - Indicate the size of your security team



iv – Where is your company headquartered?

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



So what happens next?

Following the Live Vote, 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 board, composed of many prominent CISOs, will agree and communicate a clear path for the profession to take in 2020, 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 350 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.

Live vote hosts and ClubCISO advisory board

Event hosts on 25 March 2020

Jessica Barker

Jess chairs ClubCISO and is co-CEO and Co-Founder of Cygenta, leading Socio-Technical work.

www.linkedin.com/in/jessica-barker/

Tom Berry

Tom is an advisory board member of ClubCISO and chair and co-owner of Chameleon. He is also a business teacher at Sutton Grammar School.

www.linkedin.com/in/tomberry/

Manoj Bhatt

Manoj is an advisory board member of ClubCISO and leads the Cyber Security Advisory and Consulting team across Telstra Purple EMEA, championing cyber security as an enabler for digital transformation.

www.linkedin.com/in/manoj-bhatt/

Marc Lueck

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

www.linkedin.com/in/marclueck/

Other members of the ClubCISO Advisory Board

Chris Leather

Chris is Global Director of IT Risk & Security at Clifford Chance LLP.

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

Clive Room

Clive 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/clive-room-912835127/

Debbie Saffer

Debbie is Head of EMEA Info Security and Risk Management at Cushman & Wakefield.

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

John Meakin

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

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

James Thornton

James is VP & Regional Information Security Officer - EMEA at Chubb.

https://www.linkedin.com/in/james-thornton-5267652/

Kevin Fielder

Kevin is CISO at Just Eat, a board advisor, and keynote speaker.

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

Paul Watts

Paul is CISO at Kantar.

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

Stephen Khan

Stephen is Head of Technology and Cyber Security Risk at HSBC.

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

CLUBCISO™
Powered by Telstra Purple

About ClubCISO

ClubCISO is a private members forum for European 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 350 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.

About Telstra Purple

A team of 1500 technology experts across the globe specialising in network, cloud, security, collaboration, mobility, software, data and analytics, and design.
Built on a foundation of acquisitions we are a powerhouse of demonstrable experience and expertise. We're committed to collaboration. We bring the best people across our organisation together with yours to design, build and deliver outcome-based solutions. We've built strong partnerships with industry leaders including Microsoft, AWS & Cisco but always deliver purpose-built solutions, with people at the centre.

Join the conversation:

ClubCISO @ClubCISO TelstraPurple @TelstraPurple