CLUBCISO™
Powered by Telstra Purple

Information Security Maturity Report 2021

Executive Summary

The year the CISO led from the front

clubciso.org

POWERED BY Telstra Purple

Foreword

2020-2021 was ClubCISO's year. We have grown rapidly and now have over 500 members who are CISOs or security leaders in their organisations.

Membership has grown 56% over the past 12 months, with 28% of our members now based internationally.

Most importantly, we are a community run by CISOs for CISOs. Our growth and the record engagement with this year's Information Security Report shows that we are truly an organic and supportive community. We regularly see members swapping thoughts on immediate and long-term challenges and best practice in a safe and open environment, and it was heartening to have a record 158 CISOs involved in generating the insights you will read here.

Our annual survey is a benchmark for understanding the things that really matter in the profession. This year, sees our biggest survey ever, covering topics ranging from material breaches and risks to security culture, board relationships and stress. And it makes for very interesting and important reading.

As always, our aim is to learn together and move the CISO role forwards. Our members aren't just security practitioners and leaders of security teams, they are defining what it means to be a security leader. Thank you to all our members for their involvement.

The results and discussion will be published as a full report with commentary from the ClubCISO board at **www.clubciso.org.**

Contents

Introduction

Tom Berry
Advisory Board, ClubCISO

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

“There is a strong realisation that what we are going to do in the future is not what we’ve done in the past.”

This quote from a CISO at the live results presentation and discussion in March struck a chord with many of us. 2020 and 2021 have been monumental years for the way organisations structure themselves, communicate and protect information. The past few months also represent a significant shift upwards in the strategic importance of the CISO.

From a pure security angle, major breaches such as SolarWinds thrust the CISO back into the limelight – as they led efforts to protect, recover and keep their businesses in business. But, this time, the positivity around security feels more permanent and important than just another breach. As one attendee at the results presentation said: *“Security has honeymoons; everyone loves you immediately after an incident. COVID-19 may have changed this.”*

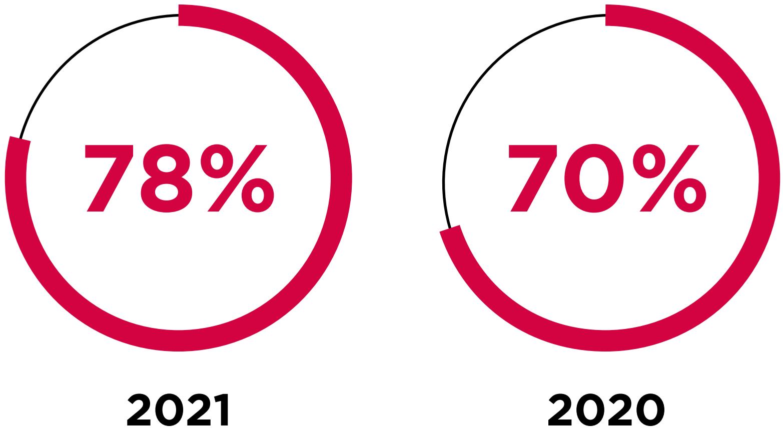
The key factor here is resilience and the CISOs that have built it. CISOs and their security teams have been putting in place best practice and incremental innovation for years, and that platform of good security stuff has shone through as the world of work changes.

However, it’s not all plain sailing and back slapping. It’s clear that the CISO role is still developing. The survey results show that CISOs are getting a seat at the top table, but they are still worried about developing their business skills. They are also making huge progress in fostering better security cultures, but they are still working out the best ways to stop breaches by non-malicious insiders (AKA real people just trying to do their jobs). Yes, cloud rollout has been accelerated, but security concerns still remain. And, above all, CISOs are facing more and more stress, while leading teams who are starting to fray at the edges.

This past year has told us that CISOs and the wider security function are making a tremendously important impact. They just need to maintain momentum, while ensuring their jobs are still enjoyable and their people are still motivated. With a fair wind, everything points in a positive direction – and long may it continue.

I love my job

Percentage of CISOs who say they love their job:



The top three areas where CISOs have driven measurable improvements over the last 12 months

2021

Security Operations

Security awareness and training

Managing third party risk

2020

Security awareness and training

Risk assessment and management

Building the security team

Click here to see the full survey results

Section 1: What has actually changed?

When the going gets tough, look to the CISO

On one hand, not much has changed. Budgets are still on the increase, good people are still hard to find and too many CISOs are still being negatively affected by stress.

However, CISOs should also congratulate themselves on just how stable their businesses and organisations are given the year we've had.

The fact that 88% of CISOs said their existing security infrastructure held up well in the face of COVID is a great testament to systems they have put in place and the rigour that security teams have brought to cloud deployments and promoting security awareness.

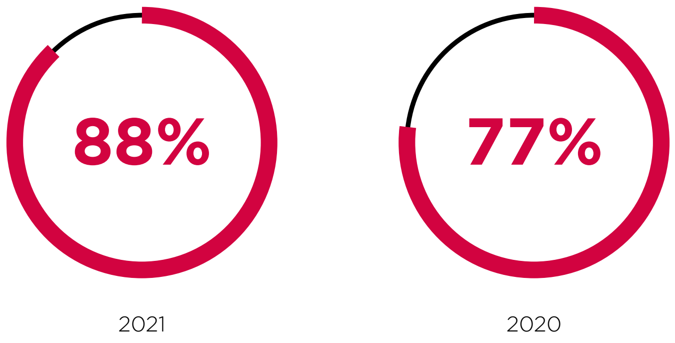
Of course, COVID and security are not the same thing. But the two needs have blurred this year, and the CISO and their team have been at the heart of it.

There's still work to be done. Working from home and access to remote systems has meant a greater need for endpoint protection, as well as greater risk through phishing attacks. As one CISO said, it's all about putting in place the right culture to allow people to understand and report their mistakes. *"Social engineering is in our nature, we are human beings, these things happen. Most people make mistakes because they are busy."*

> **"**
>
> ***What CISOs say:***
>
> *COVID-19 has given us time to do things that would otherwise have been more difficult with people in the office.*
>
> *Decision making has been quicker than it used to be. With less politics things have moved on.*
>
> *Cloud was a thing everybody was afraid of but the pandemic has forced organisations to embrace it.*
>
> **"**

CISOs should be rightly proud that every year their organisations become safer, and their people become better equipped to avoid and react to risk.

Our existing security capabilities coped well with the impact of COVID-19



The top three hot topics on the CISO's radar in 2020 and 2021

Security culture

Cloud Security

Cyber resilience

The top three tactics CISOs had to accelerate in response to COVID-19*

50% Endpoint protection

47% Security awareness programme

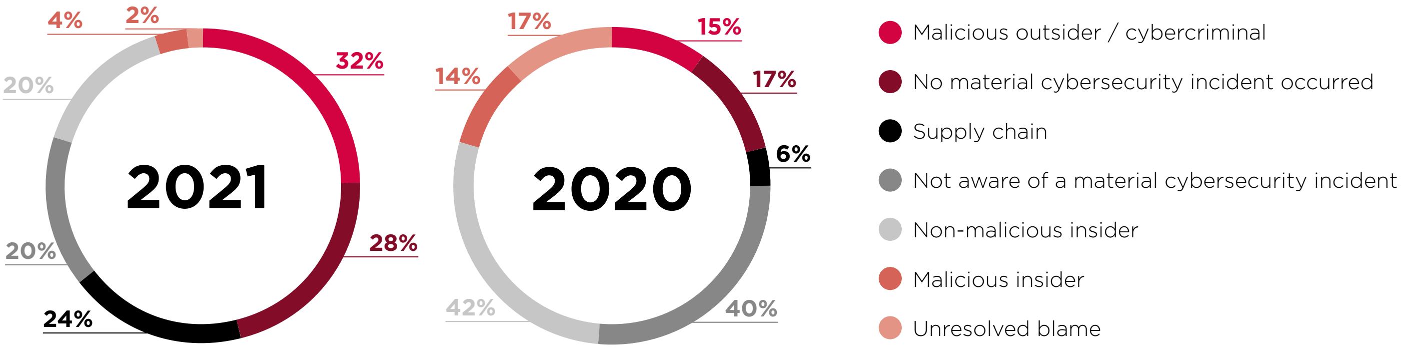
40% Enabling remote access

*16% of CISOs say they didn't have to change anything

Our organisations' security postures were improved or unchanged by COVID-19

69%

What activities led to a material cyber security incident in the past 12 months? (select all that apply)



Click here to see the full survey results

POWERED BY Telstra Purple

Section 2: What have you changed?

Security culture and awareness is delivering real results

“We’re doing more of everything.”

This was a quote delivered by a CISO at the results presentation. But it’s ‘more’ in a predominately good way. CISOs are taking on more responsibility and are busier, but they have also demonstrated real tangible results and valuable improvements that make their organisations safer and better.

This year, 61% of CISOs say that their security culture exemplifies best practice or is improving significantly, while nearly 68% say their organisations have a positive security culture. Both of these represent a significant ongoing improvement which accounts for just how resilient their organisations have been when everything has been thrown at them.

Despite concerns about how we define culture and how we measure it, this is a striking move in the right direction. There is a great buzz around security culture whenever it comes up in ClubCISO conversations and there have also been encouraging reductions in blame cultures around security incidents.

> **_What CISOs say:_**
>
> _People need to feel safe reporting an incident, and for it to be quick and easy._
>
> _Our industry is maturing. We need to learn more about business culture and what works. Nothing to do with security._
>
> _The penny has finally dropped._

Most heartening, perhaps, is the improvement in the perception of security as a value-adding business function.

That represents real progress.

Click here to see the full survey results

Percentage of CISOs who say their security cultures are improving or exemplify best practice

61%

Percentage of CISOs who say security culture is a # 1 hot topic

56%

My organisation sees security as being as important as I do

77%
Agree

My organisation has a blame culture around security incidents

13%
17% in 2020

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

Agree
68%
45% in 2020

Disagree
6%
22% in 2020

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

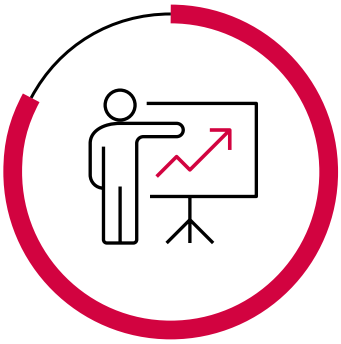
We are making progress or are delivering best practice

61%
39% in 2020

Our security culture is a worry

17%
29% in 2020

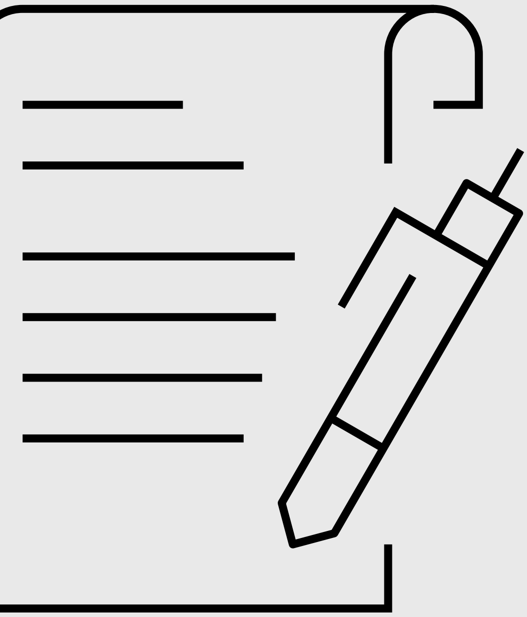
My organisation believes I add value



83%
Agree

Click here to see the full survey results

POWERED BY Telstra Purple



Section 3 - What will you change?

It's time to think about our own role and what comes next

While CISOs have made significant progress in improving the security culture and resilience of their organisations, perhaps it is time they turned their attention to their own role. This year, we asked CISOs about the ideal skills they need for their jobs, the skills they have and the skills they look for in their teams. And while business knowledge is nearly 3x as important as tech knowledge for a good CISO, only a minority of them say they have those skills.

Some CISOs at the results presentation said they are actively getting more involved in the business, and some said they are even asking for business training as a part of their personal development plans. It's true that CISOs are often self-critical by nature, but it's also positive that they want to continue to make the C in CISO as big as possible.

Part of it might be about letting go of the day to day. As one CISO said: *"We don't need to rely on spider sense. We don't have to have awareness of every single part of the process"*. However, as another CISO pointed out, too much management and leadership responsibility might become a distraction: *"Ten years ago we wanted the board to notice us. They have noticed us now. Be careful what you wish for."* Watch this space for how this plays out in the coming months.

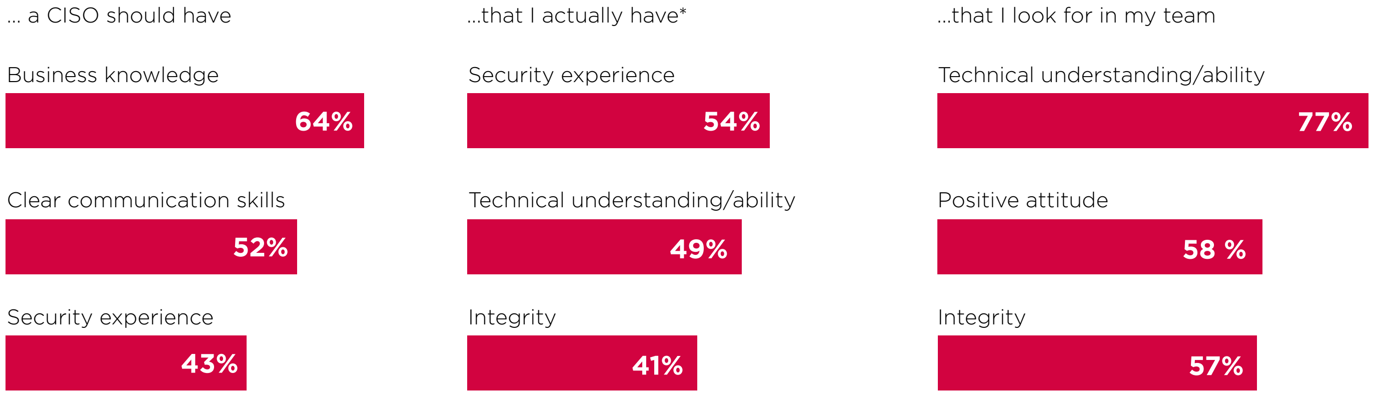
> “
>
> ***What CISOs say:***
>
> *Half of us think we are quite technical, but say we don't need those skills. It's the same thing every year: we need to get better at communication.*
>
> *We are not the awkward people in the corner now, we're the enablers*
>
> *I don't know what I'm talking about most of the time! But I have people in my team who do.*
>
> ”

Do you think your current role/ job function will exist in the same way in 2 years?

52% YES

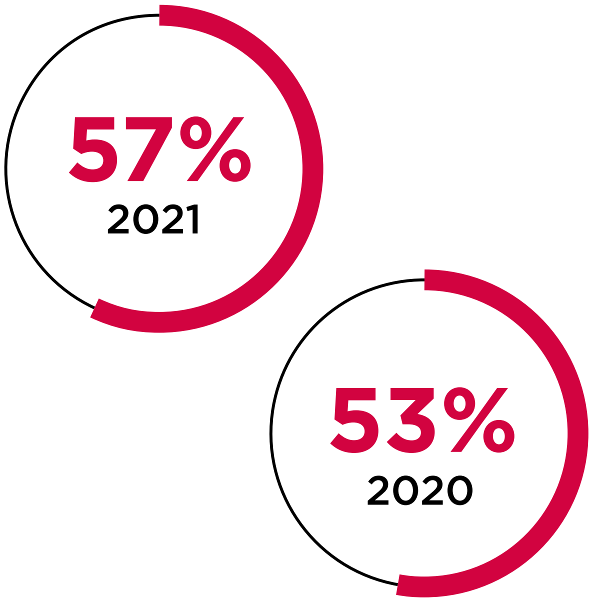
31% NO

What are the three most important skills...

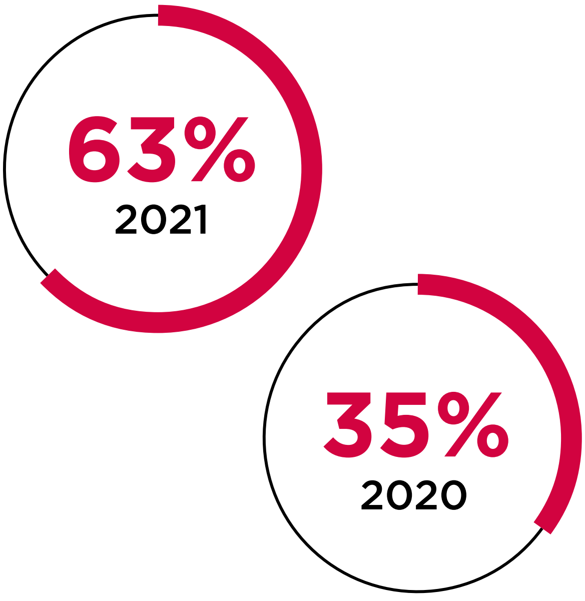


*Only 25% and 33% of CISOs say they have business knowledge and clear communication skills respectively

The percentage of CISOs who report into IT



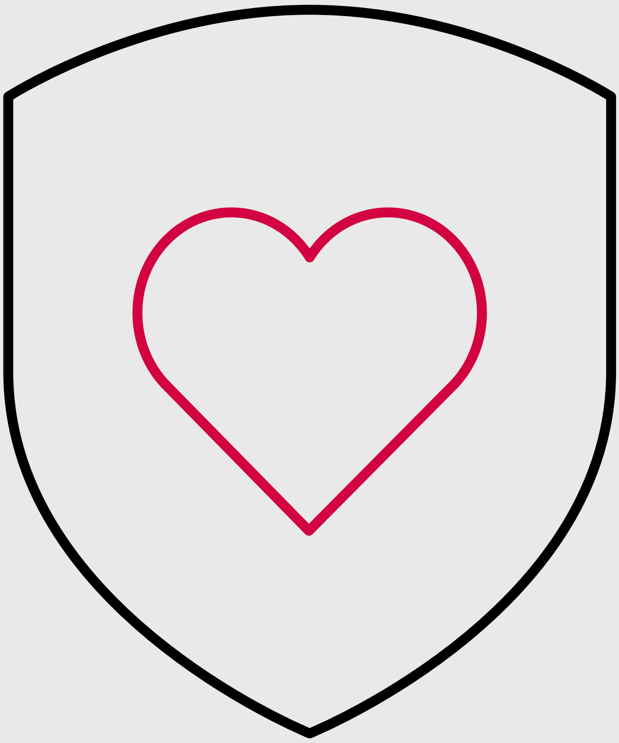
The percentage who think they should report into the main board



Click here to see the full survey results

Section 4 - How do we feel about everything?

Resilience must never come at the expense of mental health



Resilience has been a defining theme for CISOs and ClubCISO over the last two years. However, whether it is in dealing with new threats, keeping up with the pace of transformation or dealing with the increasing stress and workload of the role, the suck-it-up mentality is no longer enough if people's personal lives and mental health are at risk.

Stress is a big problem, and it has been increasing year-on-year as we have conducted the ClubCISO surveys.

> ***What CISOs say:***
>
> *It often feels like we're self-critical by nature, but there have been some really positive changes in the way security is viewed by the business.*
>
> *The openness of the ClubCISO membership to discuss their personal and team challenges has been one of the most important steps forward in us taking a stand and opening up.*

In 2021, interfunctional relationships and lack of team skills are the main contributors to CISOs stress, but cultural factors still play a large part in burnout. Most worrying is the continuing problem of stress among more junior security staff.

This is the one area where CISOs and the ClubCISO community need to open up and discuss better ways of working together. After all, the progress we have made as a profession shouldn't come at the expense of our happiness and effectiveness.

The stress of my job affects my performance or is unbearable

22%

23% in 2020

The stress of my job has become worse over the last 12 months

64%

61% in 2020

The stress my team faces negatively affects their performance

36%

42% in 2020

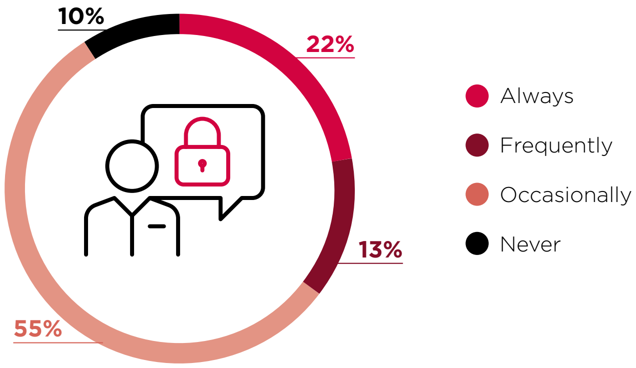
The top three contributors to CISO’s stress levels:

Lack of the right skills in the security team

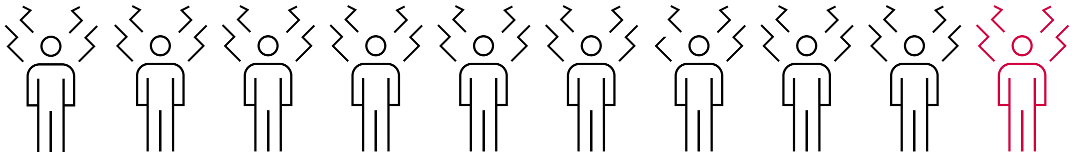
Inter-functional relationships

Challenging stakeholder requirements

Are you having trouble attracting good security staff?



Percentage of CISOs who leave their roles because of the effect on mental health



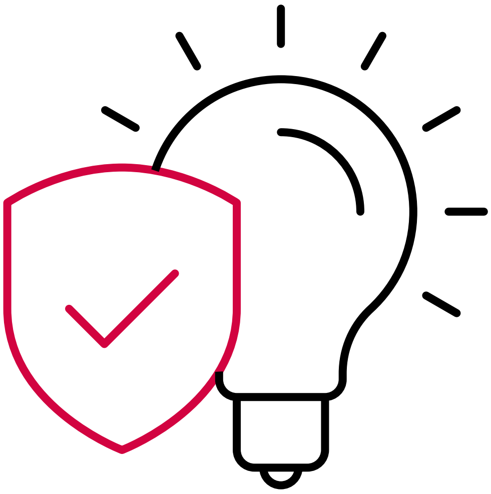
10%

Conclusion

The ClubCISO community is shaping the future of the security function

This year's CISO engagement in the Information Maturity Survey has shown just how far we have come, as well as the important role that ClubCISO has played in giving the security profession a voice and community. ClubCISO addresses real problems for real people. It is not an academic community or a training body. Our members are right at the coal face of security leadership.

Our community has the potential to become a one-stop shop for CISOs internationally. We don't only invest in CISOs as individuals, but we also give them the opportunity to glean better intelligence, better access to thought leadership and a truly international network of best practice to draw on.



The next step we must take is in empowering the community by asking what they want to see from the group. After all, it's all about how the members shape the industry. We have something really special here and want to make sure that CISOs remain at the heart of it.

Finally, we can't wait to all be back together again in person. As one CISO told us: *"When we get back together it would be great to give everybody a big hug!"*

If you like that sort of thing, of course. Stay safe and see you soon.

About ClubCISO

ClubCISO is a global private members forum for 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 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. ClubCISO is powered by Telstra Purple

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.

About ClubCISO

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

About Telstra Purple

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

Join the conversation:

ClubCISO

@ClubCISO

clubciso.org

TelstraPurple

@TelstraPurple

telstrapurple.co.uk