CLUBCISO™
Powered by Telstra Purple

Information Security Maturity Report 2022

# Executive Summary

clubciso.org

POWERED BY Telstra Purple

# Foreword

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 600 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.

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

Click here to see the full survey results

# Introduction

**"There has been a hugely positive shift, post-pandemic. Not only did we get listened to during the eye of the storm, but we're still being valued in its wake, and driving business change far more as a result."**

CISOs have cemented their positions in the inner circle. Whether it would have happened regardless of the pandemic is up for debate. Whether it would have happened as quickly is hugely doubtful. But the important takeaway from the past year, is that CISOs are now being seen not just as a valuable asset, but as a business driver and solver of challenges.

It's been a rather uplifting turn of events, where the CISO and their community has matured in order to take on the difficulties of the past two years, while organisational attitudes towards the CISO have transformed in tandem. From diverse recruitment strategies to the consolidation of suppliers, from cloud adoption and migration to a stronger recognition of the link between leadership and the CISO; the picture is altogether encouraging.

There are a few key signifiers of this overarching cultural shift. Material breaches have fallen by double, year on year, as a leading indicator. Meanwhile, budgets are increasing and investments are continuing to be prioritised across the breadth of security processes with CISOs beginning to demand more control over this spend.

When it comes to team-building, CISOs are implementing higher levels of diversity in terms of both personnel, and technical background; something that the industry has been championing for many years and which is finally coming into fruition. And while individual mentorship and care around mental health still leaves room for improvement, the general approach to department development offers reason for optimism.

Inevitably, the rise of hybrid and remote working has driven a lot of the positive feeling that now exists between organisations and CISOs. The next frontier seems to be ensuring that both sides of the relationship continue to sing from the same hymn sheet.

Risk management continues to be an area of focus, not just within the mind of CISO but at a board level also. The key difference being that the boardroom still prioritises the end destination of resilience and compliancy – more than a third of respondents felt boards were most focused on regulatory compliance when it came to cyber security- while those on the ground would prefer to start by dissecting the journey to better understand blind spots and evaluate existing processes.

For every box ticked, there is still a mission to accomplish – for example, the reduction of material incident reports is slightly offset by a concern that most remaining incidents occur via non-malicious insiders and social engineering.

However, the overall relationship between the CISO and organisation is heading in the right direction. The next step is to perfect all the stages required to achieve that new dynamic.

**Stephen Khan**
Chairman of ClubCISO
Advisory Board

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

# A fundamental shift in security culture

A quick eight-year rewind to 2014 highlights how far organisations have come regarding their approach to security. We've seen a shift in the form of investments, intent and prioritisation. But the best overarching term to define these actions is 'culture'.

Over this period, CISOs have evolved to be seen more as business enablers, and it has been encouraging to see how few organisations now neglect to measure the role's ultimate company value.

**In fact, only 20% now disagree that CISOs are gauged from a business value perspective.**

Even more reassuringly, the CISO influence has been elevated further compared to last year's figures, with 46% reporting a stronger organisational impact since COVID-19.

A final metric for positivity comes from the senior leadership level, with 50% of CISOs noting a proactive 'no blame policy'. This signifies a 23% increase on 2021's figures and a stronger level of understanding of CISO responsibilities. The CISO is not considered the scapegoat according to the numbers and incidents are seen as an organisational problem rather than just one belonging to the CISO.

The transformation to remote and hybrid working has undoubtedly catalysed this culture shift. CISOs have had one of the clearest opportunities to demonstrate their value, but three-quarters of CISOs still believe that general industry challenges aren't getting any easier. Insufficient staff and the sheer speed of business transformation have made positive outcomes more difficult to deliver. **It's perhaps unsurprising, therefore, that business leaders are finally realising the worth of their previously-undervalued white knights.**

Amid a greater understanding of a CISOs true business value, they will now be looked upon to lead the charge, and influence decisions that can help businesses keep ahead of this rapidly changing industry climate.

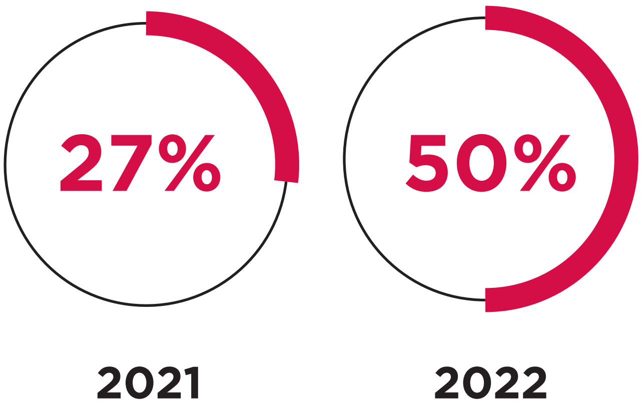
**What CISOs are saying:**

**"Organisations have put pressure on us to help them be more secure, and employees have requested more security engagement. Suddenly the floodgates have opened and we've been only too ready as a profession to capitalise on these demands."**

## Section 1: Culture

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

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.**



43%
Speed of business

25%
Culture of organisation

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

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.

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

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.**

# Reinventing security technologies

**Compared with last year, two-thirds of security budgets have increased, and for one-fifth of the contingent this increase amounts to 50% or more.**

But where is this invigorated spend being targeted? Well, CISOs largely believe they should carry most of the security technology cost centre, and there are very clear topics on their radar that they want to own.

As many as 91% of CISOs have accelerated their cybersecurity tactics in the following target areas over the past year, and some of these may come as no surprise: security target operating models (TOMs), digital transformation and the Internet of Things (IoT). However, these are compounded by a greater appetite for more tools around governance, risk and compliance (GRC), identity and access management (IDAM) and even security incident and event management (SIEM).

Many of the latter concerns have been accelerated by the post-pandemic landscape, where a greater emphasis on policies, governance and frameworks has been brought to the fore. It alludes to a broader realisation that core security fundamentals were no longer fit for purpose, post-COVID. And, in turn, organisations are realising they need in-house fingers on the pulse when it comes to decision-making and service provision.

**The CISO represents that in-house reinventor of security technologies, aided by the role of AI and automation; and indeed by “a clear dash for cloud… which has been a further factor in reassessing technology investment strategies”.**

Cloud security maturity continues to elude the CISO as it has in previous years results, but this new era of security technology reinvention mirrors cloud’s profile perfectly, making it the ultimate focus as part of this technology transformation.

**What CISOs are saying:**

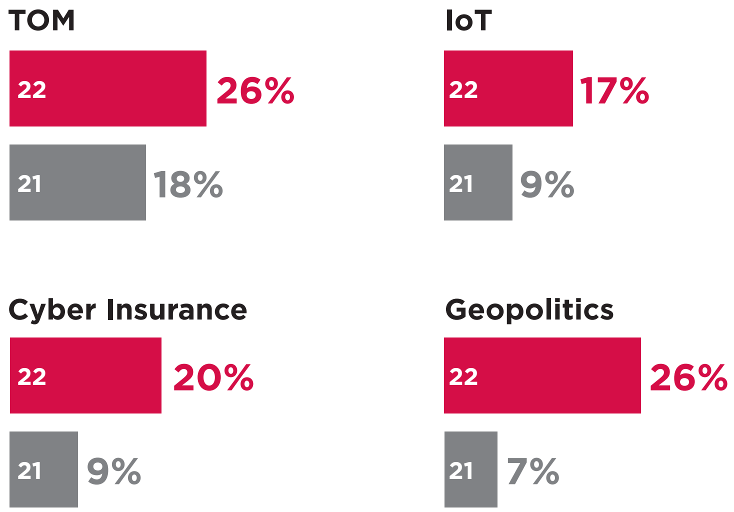
**“As AI becomes more prevalent, automation is enhancing both in-house and outsourcing capability, and for more than 10% of us it is starting to reduce our reliance on outsourcing. Perhaps organisations are now getting more third-party value from strategic security advisors than from managed service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

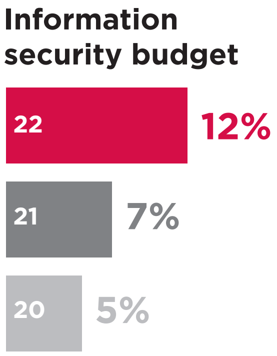
Click here to see the full survey results

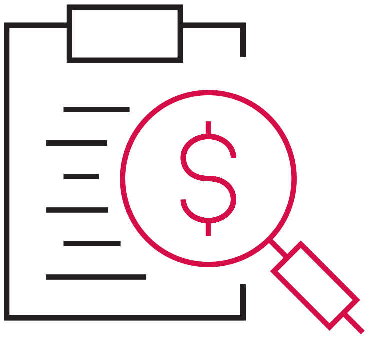
## Section 2: Technology

### Which of these hot topics are on your radar?

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%)**.







### Describe your organisation’s current information security budget relative to last year

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

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

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.

Click here to see the full survey results

Founded and Funded by Telstra Purple

# Driving conversations around risk

**Who decides what constitutes ‘risk’?**

Well, from a cybersecurity perspective, there is something of a disagreement playing out between the C-suite and CISOs, around this very question. For those sitting at the boardroom top table, the focus seems to be on high-level protectionism and overarching resilience. Notions of compliance, peer parity and end-goal business outcomes are all offered.

For those in the heart of battle, however, there is a stronger appetite for risk aversion as part of the journey, not just the destination. This comes in the form of directional guidance, practical measures and a reassessment of blind spots.

A frequent point of contention amid this slight conflict is the level of supply chain security – particularly given the number of prolific incidents reported in the media. In response, the number of organisations actively working on third-party (i.e., supply chain) management has nearly doubled compared with last year, according to our survey.

At first glance, the outlook is hugely encouraging – the number of CISOs reporting no material breaches, year on year, has almost **doubled to 68%.**

However, despite this signifier of cultural improvement, nearly one-third of material incidents that are still occurring, are a result of non-malicious insiders and social engineering.

**“We still need to focus our efforts here whilst maintaining capabilities around the perimeter and remote access,” cited a CISO in search of day-to-day process improvements, and not just end-goal resiliency.**

There continues to be disagreement around the value of cyber insurance too: 30% still don’t have cyber insurance.

At the moment, relevant policies require almost perfect security postures and coverage is provided at eye-watering premiums. In an ever-evolving threat landscape, will policy ever be fully relevant and all-ecompasing? Or will there always be gaps?

The current hope among CISOs is that these premiums might instead be spent on improving risk maturity with a process- (not protection-) driven mindset, in the near future.

**“If we are so confident that we are able to meet key security objectives, do we actually need it?”**

**What CISOs are saying:**

**“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. For example, 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.”**

## Section 2: Risk

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

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%).**

**68%**

**54%**

No material incident occurred

**17%**

Malicious outsider

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

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.

### Through what vectors did a material breach occur in your organisation 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%).**

### Rate your organisation’s security posture

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%)**.

# People and teams: a work in progress

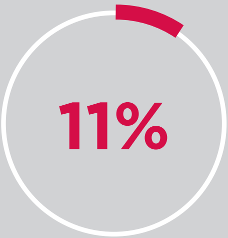
There's good and bad news when it comes to the development and care of our human resource.

'Good' can largely be assigned to the 'teams' column, with the industry seemingly breaking out of its norms and broadening the way in which it builds departments.

**Nearly two-thirds of CISOs are actively seeking to recruit from diverse backgrounds, while there is also now a greater emphasis on building talent from within.**

The technical backgrounds of new recruits also point to a change of approach, with skills outside of traditional security being explored. Think, risk management, fresh graduates, non-infosec personnel, and apprentices. An apparent drop-off in STEM uptake in schools could affect future crops of infosec professionals, so diversifying the resource pool now makes perfect sense.

Getting the right people – or team of people – through the door is one thing. Providing a productive and encouraging environment for each individual is a tougher nut to crack. Alarmingly, only 11% of CISOs believe their organisations' actions to combat stress are having a notable impact. Common tactics to try and alleviate mental health strains are already commonplace strategies to attract and retain staff, such as flexible working, social events, etc.



It's not all positive on the HR front, however.

Failing to address individual needs or to offer tailored support isn't ideal considering the pressure being placed on CISOs and their teams at this transformative time. For the CISO's part, they seem to acknowledge how important it is to exhibit the right presence and to adhere to their employer's goals and ambitions moving forward.

The hope now is that this loyalty is returned in the shape of personalised support and mentorship, to solidify a new relationship dynamic.

**What CISOs are saying:**

**"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."**

## Section 4: People

### How are you addressing stress for yourself and your team?

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

Flexible working

One-to-ones

Social team activities

Building a team

Security culture

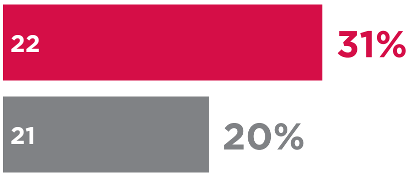
### What should be the CISO's role in recruiting and attracting team members?

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

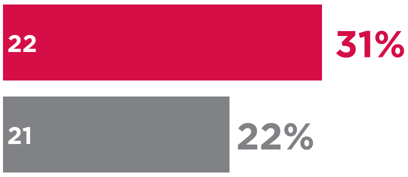
### Where are your best recruits coming from?

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%).

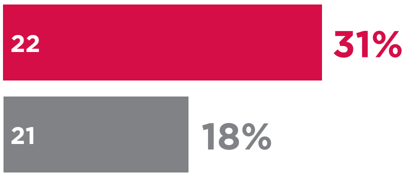
**Non-infosec**



**Security graduates**



**Apprentices**



## Conclusion

# The ClubCISO community is at the top table, and ready to make an impact

Not only has there been a cultural shift over the past year, but there has been a focus shift.

Security controls dominated CISO conversations in 2021, but we're seeing that focus drift towards aspects of identity and access management (IDAM), and governance, risk and compliance (GRC) – in part encouraged by the tighter synergy with boardroom priorities.

Already, we're seeing the fruits of these efforts, in the form of fewer security incidents, which validates the emphasis on changing tactics post-pandemic. Awareness, monitoring, governance, third party involvement, organisational maturity and team enhancement are all moving up the priority agenda ranking list.

Naturally, there continues to be areas to work on. From a technical standpoint, the cloud still remains elusive to the CISO contingent. Despite an increase in migrations, understanding of how best to leverage its capabilities remains limited.

More culturally, despite a more ingrained understanding of how best to utilise the CISO and their teams, individual wellbeing hasn't quite progressed at the same rate. Too frequently, techniques to help alleviate stress or address mental health strains are simply an over-spill from general teambuilding exercises or attraction/retention techniques.

Amid a new, refreshing, emboldened perspective of the CISO, individual care can't be overlooked, and perhaps represents the next frontier to be addressed as we look to 2023 and beyond.

CLUBCISO™
Powered by Telstra Purple

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.

## 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:

| | |
|---|---|
| in ClubCISO | in TelstraPurple |
| @ClubCISO | @TelstraPurple |
| clubciso.org | telstrapurple.co.uk |

Click here to see the full survey results