CLUBCISO™
Powered by Telstra Purple

Information Security Maturity Report 2019:
Executive Summary

clubCISO.org

POWERED BY Telstra Purple

2019: the year the CISO comes of age

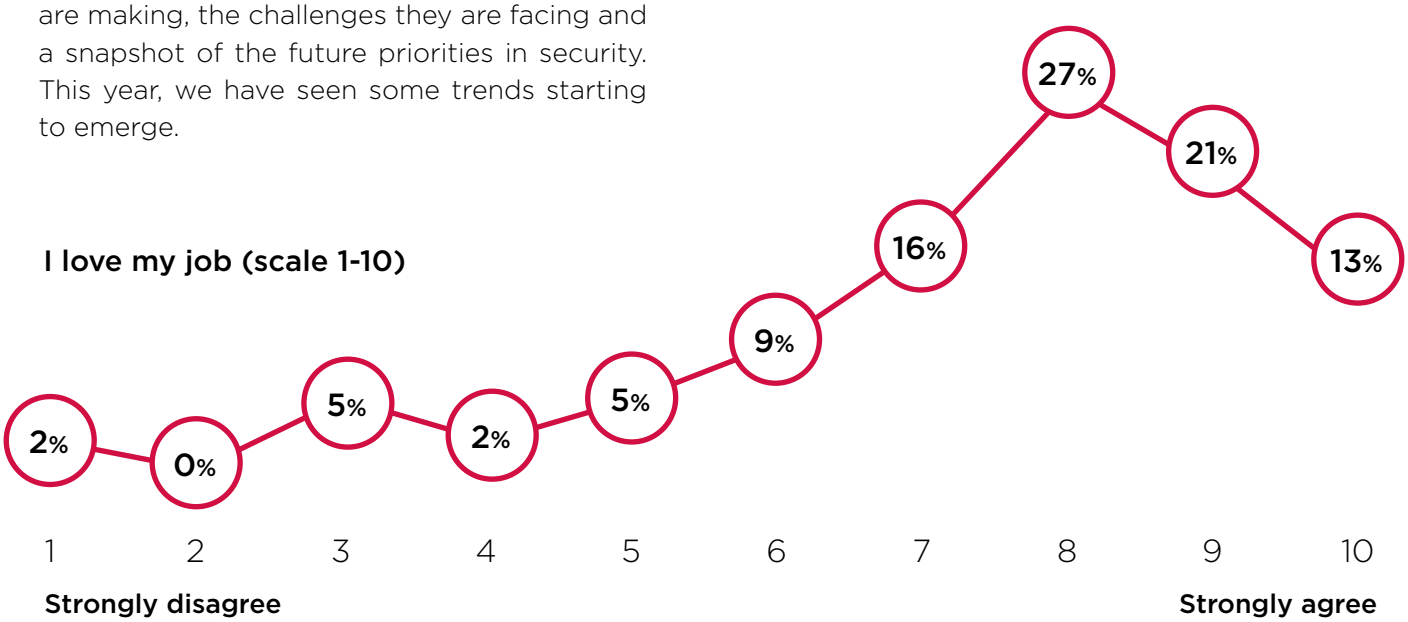
Tom Berry
CEO, Chameleon and ClubCISO
Advisory Board member

CISOs have always struggled slightly with their identity. After all, the function is a fairly young one and the growing pains of the role are starting to put stress — in more ways than one — on the most senior information security professional in business. Our 2019 live vote is always a very useful review of the impact CISOs are making, the challenges they are facing and a snapshot of the future priorities in security. This year, we have seen some trends starting to emerge.

Bigger budgets, bigger impact and bigger problems.

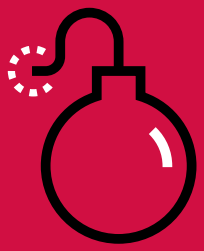
You might read this summary of findings and think that these teenage years of the CISO profession are marked by a tendency to see the gloomy side of things. But security professionals are nothing but pragmatists, and if something isn't quite right, they want to know why and interrogate the problem. Whether that is the ongoing risks of cloud, the ongoing frustrations with technology vendors or the wider culture of security, the need to identify and deal with bad stuff is what makes CISOs so good at their job. And, all in all, it's a job they love.

I love my job (scale 1-10)



Click here to see the full survey results

The top three areas CISOs spend most time and resources on:



Risk assessment and management

Stakeholder management

Security operations and maturity of security information

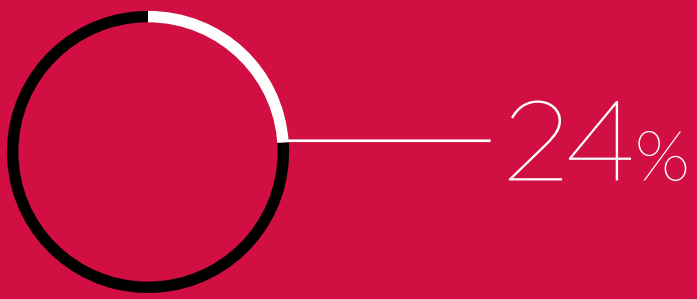
The top three areas where CISOs have driven measurable improvements in the past year:

Security policy governance

Risk assessment and management

Building the security team

The percentage of CISOs who have made measurable improvements in technology selection and implementation in the past year:



What CISOs say:

> When people ask me how big my security team is I say "not big enough", because my team should be 2,500 people, because that's the size of my entire company.

Click here to see the full survey results

CISO: a chief, but with a big or little 'c'?

CISOs are technically part of the "c-suite", the chiefs of the organisation. Well, it's there in the title, right? But there has never been a very clear, set path for CISOs to follow or metrics to measure their success and the value they bring. Stopping bad stuff from happening isn't as glamorous as making money or developing new products and services. However, we have seen a growing tendency in the past year for CISOs to become more integrated into their business. In 2018 we found that a quarter of CISO were not formally measured, which has dropped to 12% this year. We are also seeing some small shifts in terms of reporting lines. While most CISOs still report into the CIO, nearly a third of them have grown further away from the IT function in the past year and half say that reporting directly to their boards is their preference. As budgets continue to increase, the scrutiny CISOs will face will only continue to increase, so what can we do to ensure CISOs take a seat at the top table and turn that small "c" into a big one?

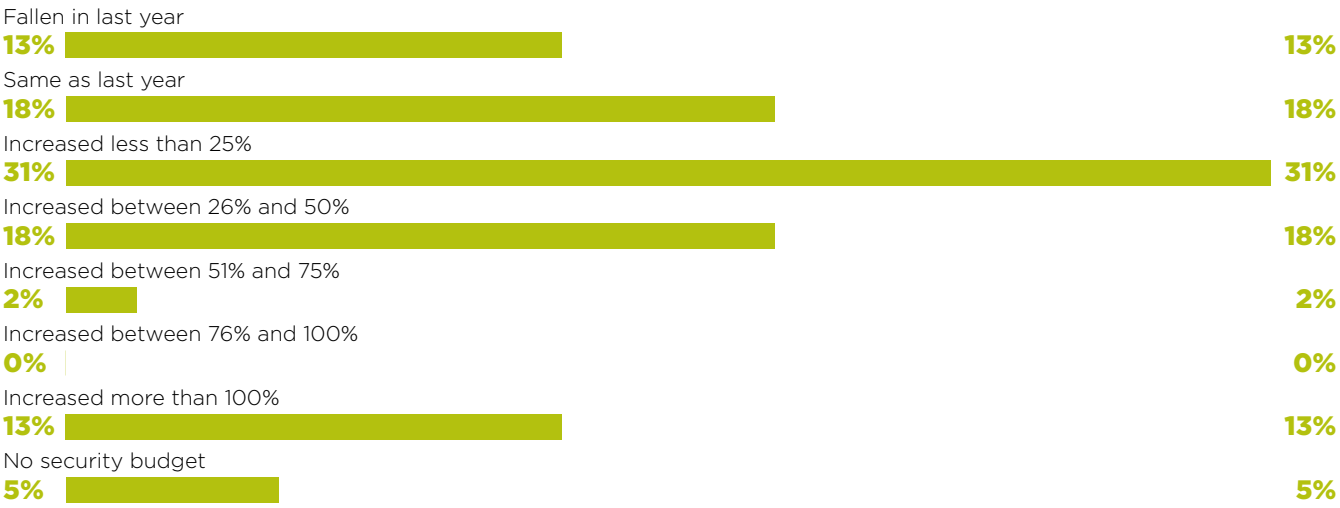
Percentage of CISOs whose performance is not formally measured by the business:

Click here to see the full survey results

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

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

Describe your organisation's current information security budget.



Click here to see the full survey results

A perfect storm is brewing in security

CISOs occupy a position as a voice of reason and considered thinking in the centre of a maelstrom. Security threats come in waves, the organisation is consistently under attack and businesses are continually transforming in an effort to stay competitive and relevant. The stress of the job shouldn't be underestimated, with 34% of CISOs saying the stress they feel in role is significant and affects performance. Nearly one-tenth say this stress is unbearable. It is any wonder that there is churn in the job? 35% of CISOs are new in role, partly because it is a candidates' market, but also because CISOs are often frustrated by their organisation's security culture, a lack of good people or because they don't see eye to eye with business leaders. Many CISOs are looking for a home; organisations that understand how tough their job is and make security a priority in an environment of constant threat. The world is moving quickly, but security has to be done properly.

What CISOs say:

> Do I stick my neck out or opt for a quiet life and, perhaps, have a longer tenure because of it? The nuclear option is to say exactly what I think and accept the consequences.

> I had too much of a purist's view and was too risk averse. That's what caused the stress. You have to realise that it is all about business problems and detach your emotions. State the facts and let the business make the big decisions.

> Apprentices are one solution, but who is going to train them and what do we teach them?

Click here to see the full survey results

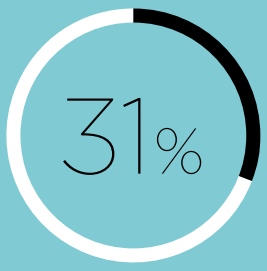
The three factors that have the biggest material negative impact on CISO performance

Lack of skilled staff

Culture of the organisation

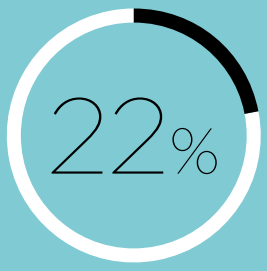
Speed of business change

Why did you leave your last job?



I felt I wasn't challenged

I was frustrated by my organisation's approach to security



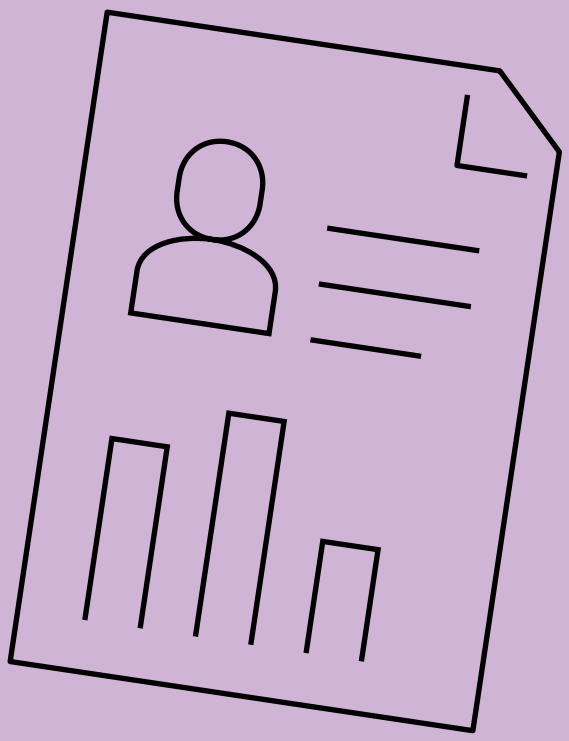
I didn't see eye to eye with senior leadership

How stressful is your job?

How has the stress level in your job changed in the last year?

Click here to see the full survey results

People, policy and partners



A positive security culture is very important for CISOs. If everyone is the first line of defence, then the risks of material breaches and incidents are greatly reduced. But the traditional, policy-led approach is problematic, with a shockingly large percentage of CISOs (over half of them) saying their organisation's security policies are largely ineffective or unenforceable. The picture across the supply chain isn't much better, with half of CISOs saying their ability to enforce security policies across their partner and supplier base is "repeatable" at best, according to standard maturity models. It is clear that, more and more, security culture is about communication and inclusion, not enforcement.

What CISOs say:

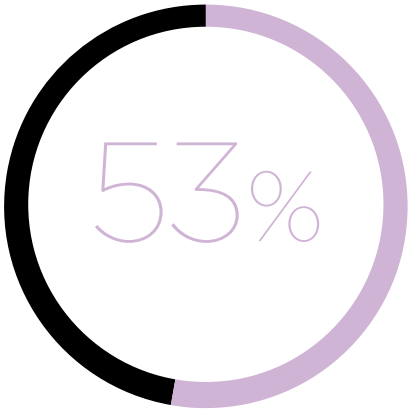
> We have lots of policies, but the problem is they are too often not understood or are largely unenforceable. We talk a lot about wanting a great security culture, so let's start with getting better at communicating.

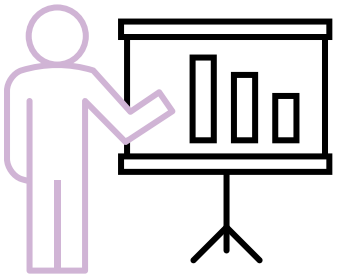
> It's not about young vs old. If you feel you can't communicate with millennials, then you probably can't communicate at all.

> We need to train and persuade, not enforce.

Click here to see the full survey results

Percentage of CISOs who think their policies are ineffective, dormant or don't affect day to day behaviours:





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

Optimising (highest maturity)
4%

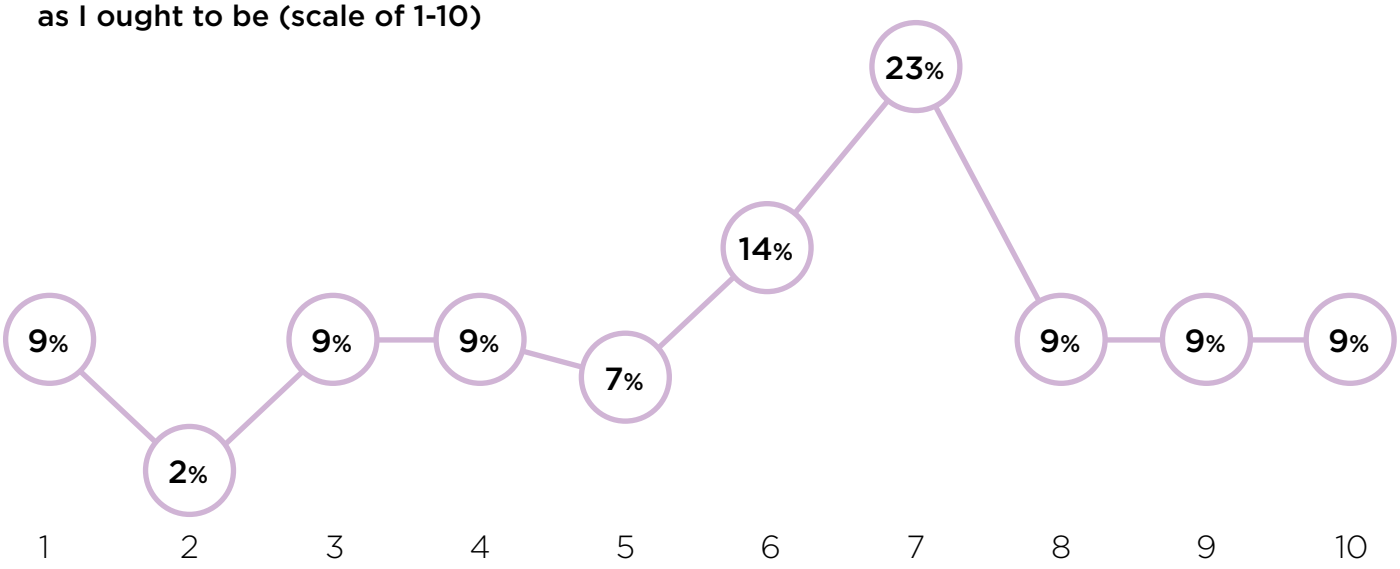
Managed
19%

Defined
34%

Repeatable
23%

Initial (lowest maturity)
21%

I feel as aligned with the business as I ought to be (scale of 1-10)

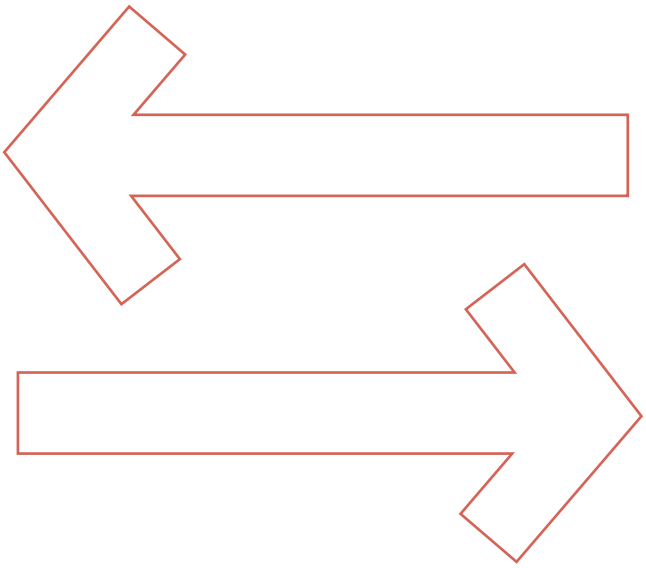


Strongly disagree **Strongly agree**

Click here to see the full survey results

To go forwards, sometimes we have to go backwards

In last year's results CISOs rated the maturity of their cloud security policies as low — for the first time since the survey began. While two points don't make a trend, we have seen another fall in cloud maturity in this year's results. However, just as before, CISOs don't necessarily see this fall in maturity as problematic. The pace of change in cloud is so rapid that CISOs understand they have to keep adapting and analysing their strategies. Cloud is a risk that will continue to offer challenges, but it is here to stay. One of the strengths of cloud is also its major weakness; when people have control over data, applications and devices, the chances of breaches are increased. After all, it isn't the technology that is necessarily the risk, but how people interact with it. Perhaps that is why non-malicious insider threats are almost on a par with cybercriminal activity when it comes to material incidents CISOs have experienced this year. Expect more discussion about zero-trust and what that means in the coming months. Oh, and one last word to the technology vendor community — many of you aren't helping yourselves because CISOs don't think you are helping them deal with issues, they just see you trying to sell stuff. Try listening more.



What CISOs say:

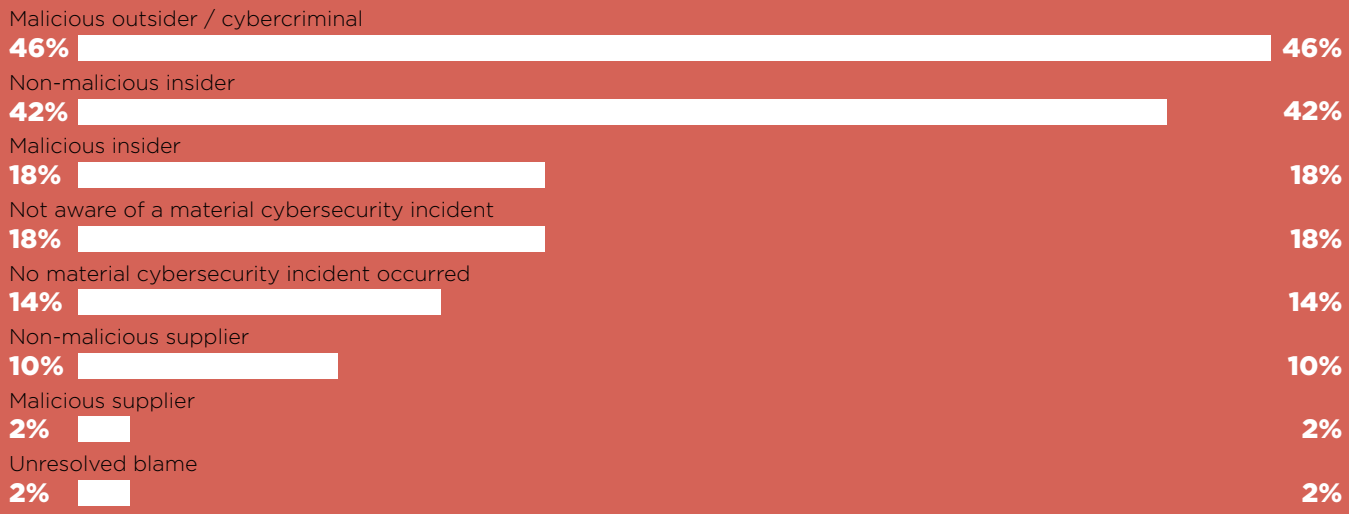
> Just because the numbers look bad means we actually understand it better.

> The cadence of cloud is so high that we have to reset the clock on cloud security quarterly.

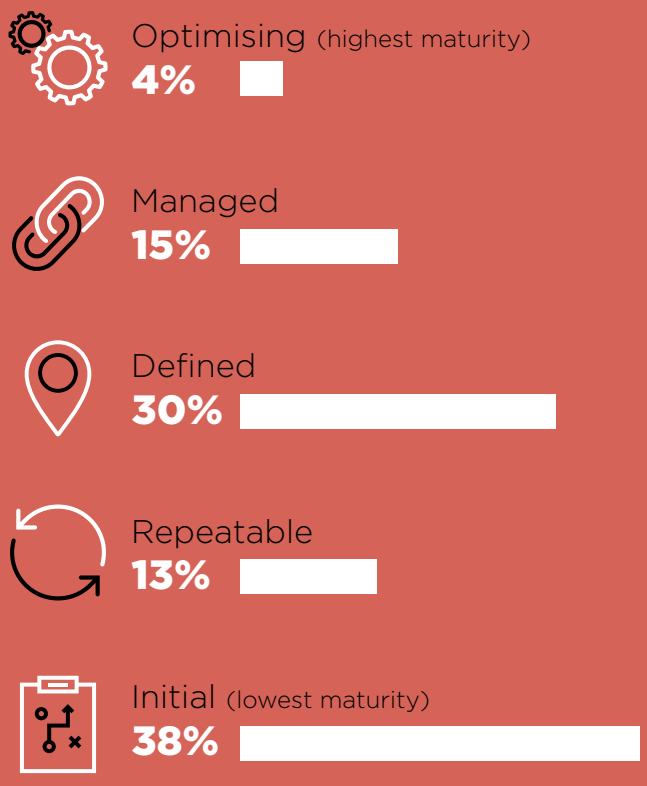
> My CEO told me that everything in information security is a compromise. At the time I wanted to punch him... but he might be right.

Click here to see the full survey results

What activities have led to a material cybersecurity incident in your organisation in the past 12 months?



Rate the maturity of your cloud security strategy



The top 3 hot topics on the CISO radar:

Net promoter score*: Would CISOs recommend their technology providers to friends or colleagues?

(0 is considered neutral. +50 is considered excellent.)

*NPS is calculated by subtracting the percentage of those who score 6 or below from the percentage of those who score 9 or 10

Click here to see the full survey results

Growing pains, but a growing sense of worth

This year, we got a warts and all view of the challenges CISOs face, but we also got a glimpse of how much value CISOs can bring to their organisations. Yes, they have a tendency to be purists, but they recognise the need to challenge this instinct and instead be open to compromise. Prevention and policies aren't working, so CISOs are finding new ways to influence and inspire better security cultures. CISOs are starting to take control over their own destinies — for the better and for the benefit of their organisations. Now they just need the technology industry, and senior business leaders, to support them and we will then see some major strides in making information security a driver of business value. As one CISO said:

> "We need to keep the story straight and take back some control. Marketers are always inventing new names for security threats, but we have FUD fatigue. Let's be active about what matters to us and wrest control back. We have to accelerate the journey as a community, stick together and choose one language to talk."

Click here to see the full survey results

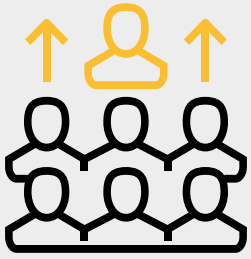
So what happens next?

Following the Live Vote, members of the ClubCISO Advisory Board held a planning session with new ClubCISO chair Dr Jess Barker on how we act on the results.

The board, comprising many prominent CISOs, decided that ClubCISO and its members should be focusing on three clear areas. For each of these, we are calling on ClubCISO members to join working groups to discuss, define and deliver our strategy.

Stress

Our goal is for ClubCISO members to provide support to each other, and for our group to use its outward influence to raise awareness of stress in the CISO role and encourage practical support and understanding from employers.



Broaden our influence

The CISO community is of huge importance to business continuity and success. We want to engage CISO members to fly the flag for the function. We want to use our influence to challenge the tech industry, lobby government and engage communities about the importance of the positive steps we can all take to be more secure.

Be a voice of reason

ClubCISO will drive conversations around "Hot Topics", both to our members and the wider community. We will aim to have sensible and grown-up discussion that separate fact from fiction and dispel the myths and hype in the industry.

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

Thank you.

Click here to see the full survey results

See the full results of the survey at...

club CISO.org

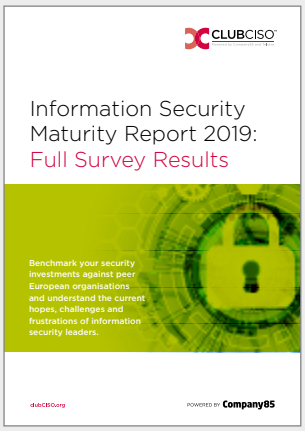
CLUBCISO™
Powered by Telstra Purple

These are just the headlines; now read the full results of the vote on four key areas for security in business:

- Setting the scene
- Role of the CISO
- Wider Security Ecosystem
- Hot Topics

Benchmark your organisation's security investments against the responses of peer businesses, identify clear trends across the UK information security landscape and read commentary on key observations about:

- Cloud
- Digital transformation
- Target operating model
- Business alignment
- People



Download your copy here

clubCISO.org

POWERED BY Telstra Purple

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 200 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 Telstra Purple

clubCISO.org

POWERED BY Telstra Purple