


Information Security Maturity Report 2018: Executive Summary



Are you in
step with
your peers?

The fifth annual ClubCISO Maturity Survey marks an important moment in time for the CISO: high-profile data breaches have peppered the news; budgets for cyber security continue to increase; security has a greater board-level profile; and dare we mention GDPR?

This year's annual survey of CISOs was, therefore, the moment when we might have expected security maturity and readiness to be at an all time high.

Not so.

Tom Berry

CEO, Chameleon and ClubCISO
Advisory Board member

Likewise, we might have expected CISOs to want to step out from the shadow of the CIO, or for security strategy to move from prevention to recovery.

But that is far from clear cut.

Don't be too hasty in drawing your conclusions, however. The results don't mean the CISO is any less important or any less effective. In fact, the survey and discussion on the evening demonstrate just how far the role has come and just how widespread the impact of cyber security on the business. **If anything, the CISO leading role in uncovering risks in their organisations is causing a more thorough and - perhaps - more honest assessment of the security credentials of big business and their supply chains.** There are no quick fixes, but the CISO has to be at the heart of the ongoing evolution in security posture.





...what's on the mind of the CISO?




Among the **top three priorities for CISOs in 2018** were the perennial issues of risk assessment and maturity of information security. This year, **stakeholder management made the top three for the first time**, pointing to the growing importance of people outside of the security function in **creating, preventing and communicating risks**. When asked about the areas where CISOs had made a

measurable difference in the past year, **maturity of information security leads the way**. This is important, as maturity and awareness may be higher - and improvements are being made - but the **security issues seem to be growing** the more that CISOs look under the bonnet of their organisations. CISOs are doing an admirable job, but can they keep pace?

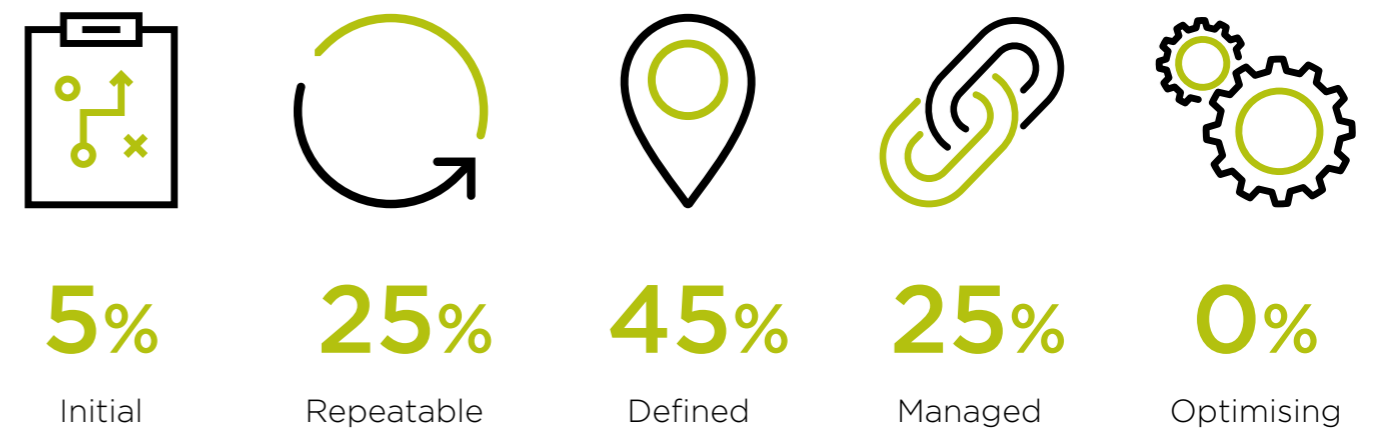
CISOs top responsibilities

-  Risk assessment and management
-  Maturity of information security
-  Stakeholder management

CISOs top measurable improvements in past 12 months

-  Maturity of information security
-  Breach and incident response
-  Risk assessment / Building the security team

Rate your organisation's security posture: (against Capability Maturity Model criteria)



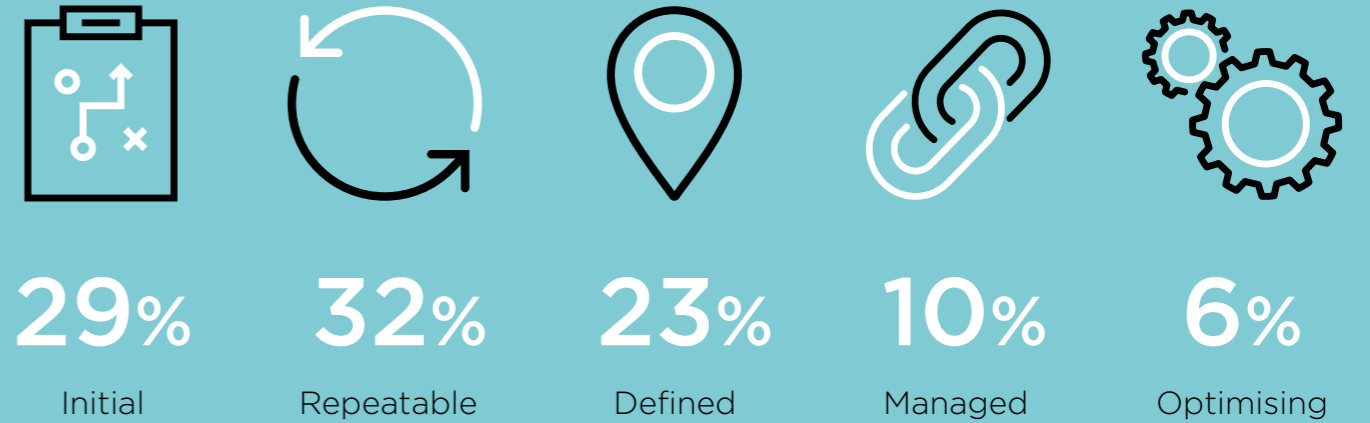


The more we look, the trickier it gets

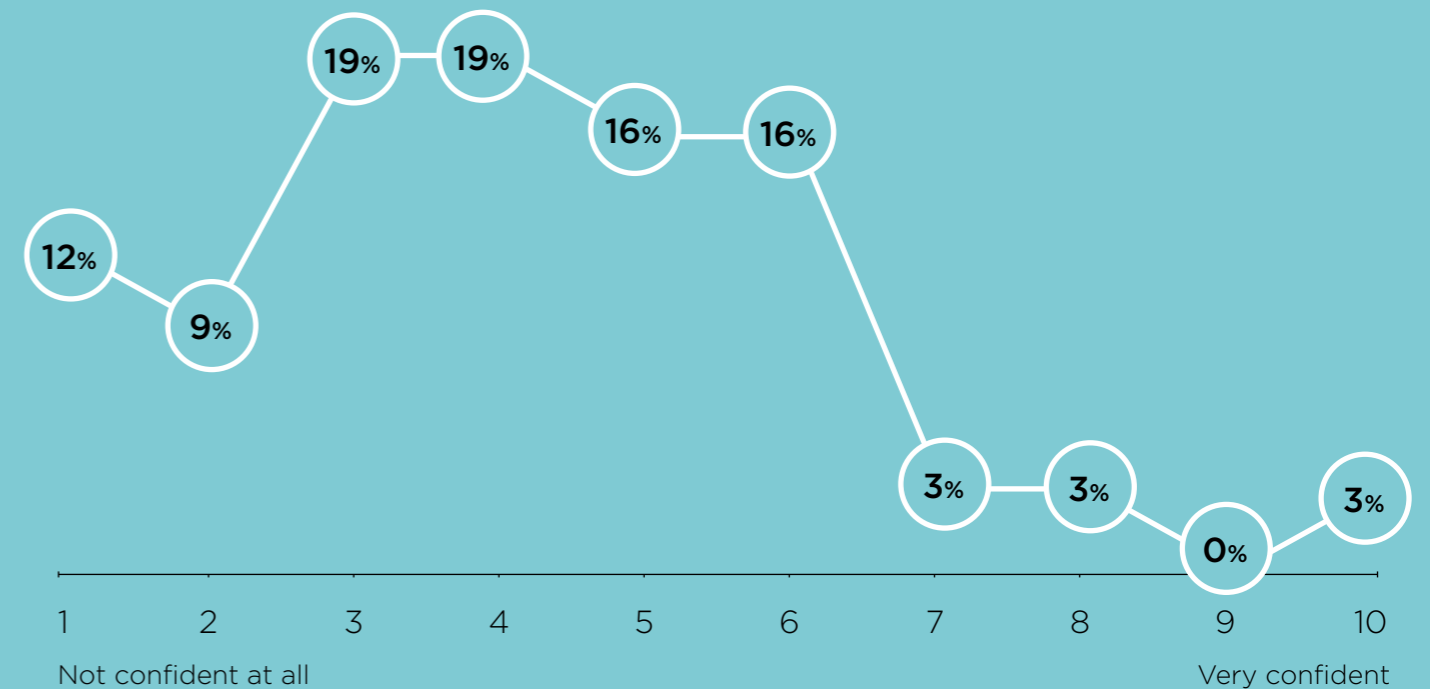
In 2017, CISOs were bullish about their cloud security strategy. In 2018, **72% of respondents said cloud security strategy is a hot topic for them**, but their confidence in the maturity of their strategy for cloud has actually fallen year on year. Why? During the discussion at the annual survey event, CISOs openly discussed how regulation, GDPR and wider focus on security issues had given them the mandate

to **explore the security risks their organisations face** outside the four walls of the office environment. Now the lid has been lifted, the **CISOs surveyed are uncovering some pretty major third party risks across their supply chain**. As was said on the night: “Is it really that the waters in which we swim are getting worse, or is it that we are getting more honest and aware of the issues the closer we look?”

How do CISOs rate the maturity of their cloud security strategy? (against Capability Maturity Model criteria)



How confident are CISOs that they can enforce their security policies with third-party suppliers?



The path of least resistance has the most effect

There is always a healthy debate about the independence of information security. One argument is that CISOs and their teams should exist separately from IT to avoid any conflict of interest – and **60% of CISOs are seeing their function grow more independent from IT in the past year.** However, there is also an argument that **reporting into the CIO is the most effective way to get things done** and have a champion for security on the board who speaks the CISO’s language. In fact, 80% of CISOs surveyed still report into the CIO, and, despite

some concerns in the room that IT sometimes defends its own territory, it was largely thought to be better to have IT on-side. **And while IT budgets are falling, security budgets are rising rapidly,** so having those budgets aligned was also thought to be largely sensible, especially as one CISO commented: “I’m worried that one of the biggest risks is that due to budget cuts at IT level, the infrastructure won’t be in place to fulfil my strategy – even though I have more budget in security.”

Has information security become more or less independent from IT in the last 12 months?



How has your organisation’s information security budget changed in the last 12 months?





Carrot or stick?

Regulators under the spotlight

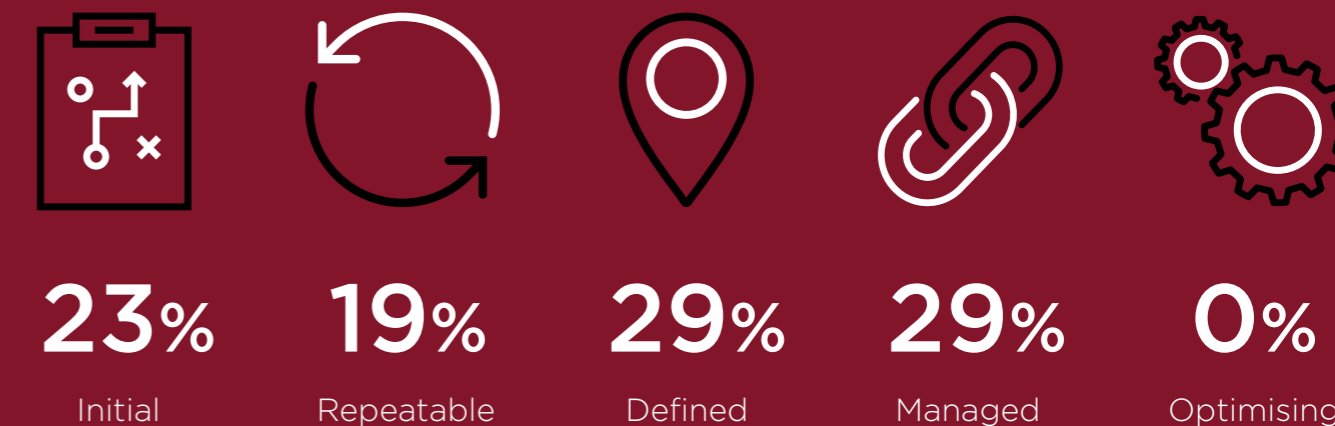
Never has there been so much talk about regulators at a ClubCISO event. **The arrival of GDPR and the risk of heavy fines has sharpened the mind, naturally.** But, this year's discussion was also fascinating in that the CISOs leading the debate were not just those in the most regulated industries, such as financial services. In general, CISOs felt it **unlikely that regulators will be keen to make examples of businesses under GDPR**, but will instead act more supportingly to improve standards across the board. The help may be needed as CISOs were very honest in their assessment of GDPR readiness, with **over half of them saying their systems, process and policies are repeatable at best and initial at worst.**

[Click here to see the full survey results](#)

Percentage of CISOs who say GDPR is one of their top five hot topics today



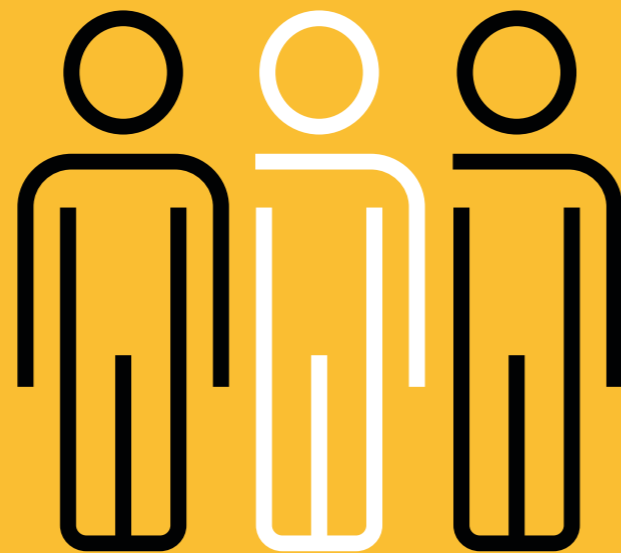
How do CISOs rate their organisation's readiness for GDPR? (against Capability Maturity Model criteria)



[Click here to see the full survey results](#)

It's all about people

For the first year, **almost all respondents say they have suffered a material data breach of some kind in the last 12 months** - whether malicious or not. Human behaviour is a common factor across breaches and it is almost inevitable in a flexible and fragmented working environment that data is always at risk. Perhaps this is why **three quarters of CISOs say that security awareness throughout their organisations is an important hot topic** for the coming year. Other people issues discussed included procurement, who in some instances remove security elements to tenders and contracts at negotiation stage to reduce costs. Some CISOs in the room stated that their **carefully**



thought out plans, baking security by design into projects from the outset, are regularly removed without their knowledge. Once again, stakeholder management - from the board down and throughout the organisation - is going to be critical in 2018.

CISOs' top hot topics



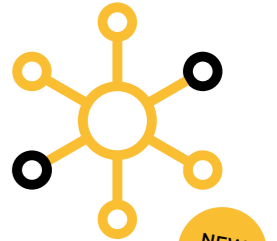
Security awareness



GDPR

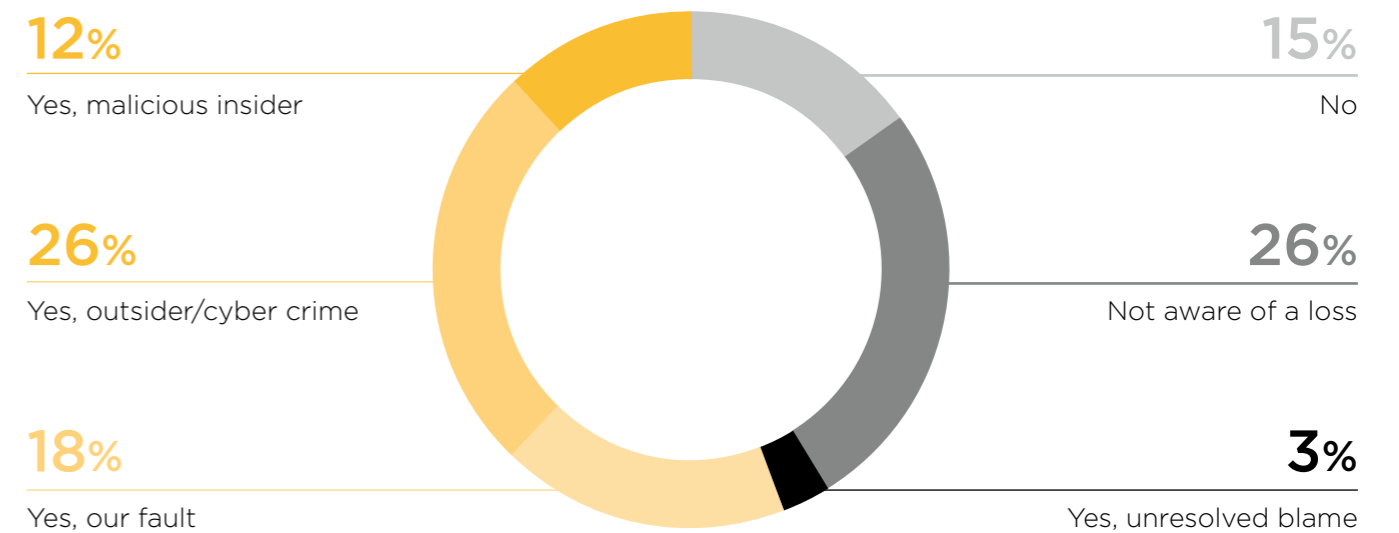


Cloud security strategy



Digital Transformation

Has your organisation suffered a material data loss incident in the last 12 months?

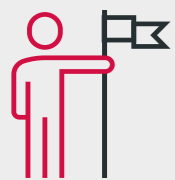


See the full results of the survey at...

**club
CISO.org**



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



Role of the CISO



Board Perspective



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

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 Company85

Company85 is a non-aligned IT services firm which leads change, strips out cost and safeguards information. We have been at the forefront of infrastructure innovation for over 25 years and are now part of the Telstra group.

Headquartered in London, we provide security, cloud, data centre, workspace and network services to some of the biggest global organisations in the public and private sectors across the UK and the world.

Our security professionals help organisations define strategy, understand threats, align security and business objectives, and educate users on safe practice.

Join the conversation:

