Global Snapshot: The CISO in 2020

MARLIN HAWK

Executive Summary

The world of cybersecurity is constantly evolving, as is the nature of how businesses morph and adapt. The regulatory environment is also changing. Only in 2018 were GDPR laws introduced in Europe to better protect citizens from data breaches suffered by large businesses.

Because of this, cybersecurity is now in the mainstream. It is as much a societal issue as it is an enterprise one. Whether it's the credit card details of shoppers being leaked online, passport details stolen from airlines, or the intimate details of a private conversation with friends, the dangers of cybercrime now face everyone.

Business leaders have been attempting to work out how best to respond to this transformative threat and, most importantly, whose responsibility it should be. The constant cyber threat has completely changed the way boards around the world approach risk, and it's an issue that every business leadership team has had to respond to.

The broad world of "IT" typically falls under the control of a CTO or CIO. But, information security is so much more than a technical issue; it blends risk, people and data management, along with technical knowledge. Add to that the need for a strategic vision, and knowledge of the threat landscape, and the requirement is specific. This is where the CISO comes in.

But who is driving this change? Senior stakeholders widely realise the growing need for a CISO; whether through previous experience, because increased security is demanded by company strategy, or simply because they feel it's the right thing to do in the face of the threat landscape. Whatever the reason, the fact is that it's no longer simply the large global corporations that are deploying senior cybersecurity professionals to oversee their data security, given that criminals are attacking businesses in a much more indiscriminate way.

At Marlin Hawk, we work with some of the biggest businesses in the world. We identify and place the best cybersecurity talent at some of the world's best-known organisations. We work with many of the top global CISOs, a number of whom we spoke to while conducting this research.

However, we wanted to maintain a holistic view of the market, ensuring we include the CISOs who could be considered rising stars; CISOs who are sitting at a regional level, or those who may be a few rungs below board level, but still have responsibility for their organisation's cyber defences. Conducting the research in this way gives us more accurate market context, and allows us to track how the role is evolving.

This report is intended to shine a light on CISOs of all seniority levels around the world to holistically identify trends and patterns in the role, in a bid to locate where CISOs come from, what their worries are, how their role is evolving and what the talent market looks like.

Methodology

The data this research paper references is a combination of Marlin Hawk internal data and Vanson Bourne research, which took the input of 500 CISO (or equivalent) executives employed at businesses with 500 or more employees. This comprises 100 businesses in the UK, 150 in the US, and 50 each in Ireland, Netherlands, Switzerland, Hong Kong and Singapore.

Marlin Hawk is a global executive search firm founded in 2003, specialising initially in operations and technology before diversifying to encompass the majority of C-suite positions across a variety of industries. However, O&T remains to this day an area of expertise for the firm and, by extension, the rise of the CISO has been well mapped by the organisation. Its network is extensive, and amongst its contacts and placements it counts many of the world's leading CISOs at tier one, blue chip companies. By extension its market intelligence and data is far-reaching and diverse, encompassing multiple sectors and multiple geographies.

The objective was to collect and analyse a large enough dataset to make valid conclusions into the background, behaviours and mindset of those making cybersecurity decisions at large organisations.

This paper also includes qualitative research gathered by Marlin Hawk from interviews with CISOs working in APAC, Europe and the US.

Input from 500 CISO or equivalent executives employed at businesses with 500 or more employees.

CISO Demographics

Perhaps unsurprisingly, like many other senior leadership roles, CISOs are mainly male. But that's not to say that it's not a dynamic and evolving role.

The majority of CISOs appear, on average, younger than other senior business leaders, with 73% under the age of 45. Furthermore, 42% of female CISOs are under 35 years old; something that is quite surprising, but also encouraging. Diversity is becoming such an issue at businesses of all sizes, and it's possible we're seeing senior leaders take a chance on younger talent, in a bid to encourage diversity of thought and experience.

The gender pay parity is also encouraging. Globally, male CISOs earn an average of £0.53m, while female CISOs earn marginally more, with the average compensation being £0.55m. Given the desire for a greater diversification of talent across all C-suite roles, it is unsurprising that female CISOs are in high demand. Considering the scarcity of women who decide to pursue a career in information security – it therefore follows that organisations are willing to pay more for diverse talent.

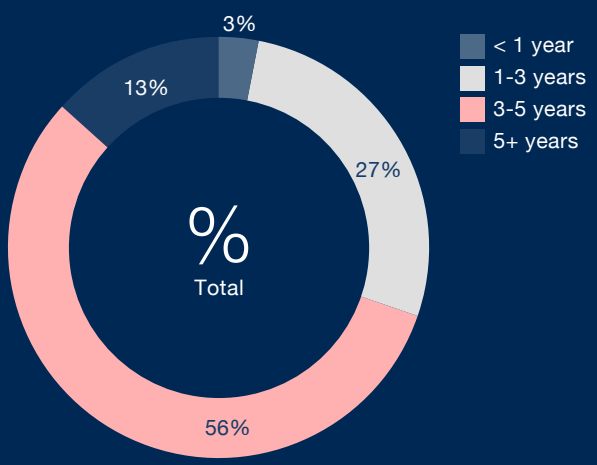
However, CISOs working at the largest organisations (and those under the greatest perceived threat) can be paid much more than their peers across the broader FTSE 500. Marlin Hawk data gathered from blue chip organisations revealed that their CISOs were paid on average £0.795m, whilst the highest earners interviewed were remunerated as much as £2.1m. Geography can also significantly affect a CISO's earning potential. In North America, CISOs are awarded an average of £0.87m, whilst in Africa the average total compensation is £0.65m. This is likely due to the number of large global organisations present in each location, and therefore the competition for strong CISOs across all industries.

73% of CISOs are under the age of 45. Furthermore, 42% of female CISOs are under 35

Typically, CISOs working within multinational organisations receive even higher compensation for laborious work to counter threats across multiple time zones and heightened responsibility in keeping company data secure in locations around the world. In fact, according to Marlin Hawk data collected in 2019, salaries regularly reach heights of over $2m in sectors like financial services, especially in Switzerland and the US.

Globally, CISOs have spent an average of four years in their current role. In the UK and Ireland, only 10% of CISOs stay for longer than five years, compared to 22% in the US, and 14% in APAC.

How long have you been in your current position?



For full data set, please see: Appendix 1

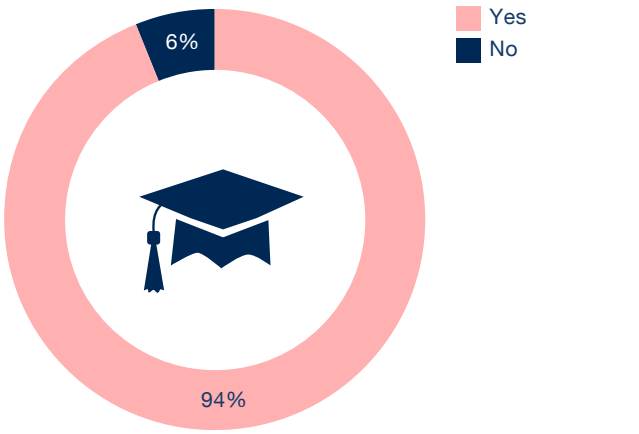
MARLIN HAWK

Education and Experience

The job market as a whole is seeing changes in attitude towards academic qualifications but, for senior cybersecurity professionals, having a degree is still commonplace for the majority (94%).

Moreover, of those who have a degree-level qualification, most (84%) still take the traditional route of studying computer science or similar. Interestingly, in the UK, there appears to be more educational diversity than in other markets. Only 76% of CISOs in the UK and Ireland have a CompSci degree, compared to the US and APAC (both 89%). More than nine-in-ten have a science degree (or similar) but, perhaps most unusually, one-in-fourteen (7%) have a design or architecture degree. Given the importance of understanding complex networks and IT architecture, we may see an emergence of design-led CISOs in the future.

Do you have a degree level qualification obtained from a university?



For full data set, please see: Appendix 2

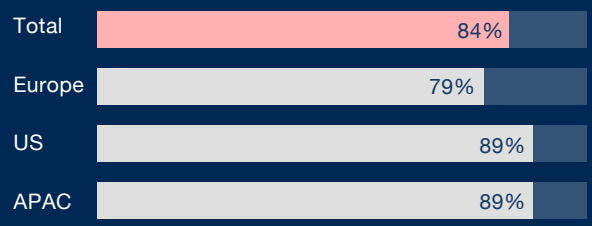
"The role of the CISO is becoming increasingly crucial in a much quicker timeframe than we anticipated. There may be a few universities currently with really relevant courses in this domain but there are maybe hundreds or thousands more which, although they offer IT courses, don't yet offer a targeted cybersecurity curriculum. This is one of the reasons why the senior talent pool is not that large."

Beate Zwijnenberg is the CISO at ING in Amsterdam

What did you study?

84%

still take the traditional route of studying computer science or similar.



For full data set, please see: Appendix 3

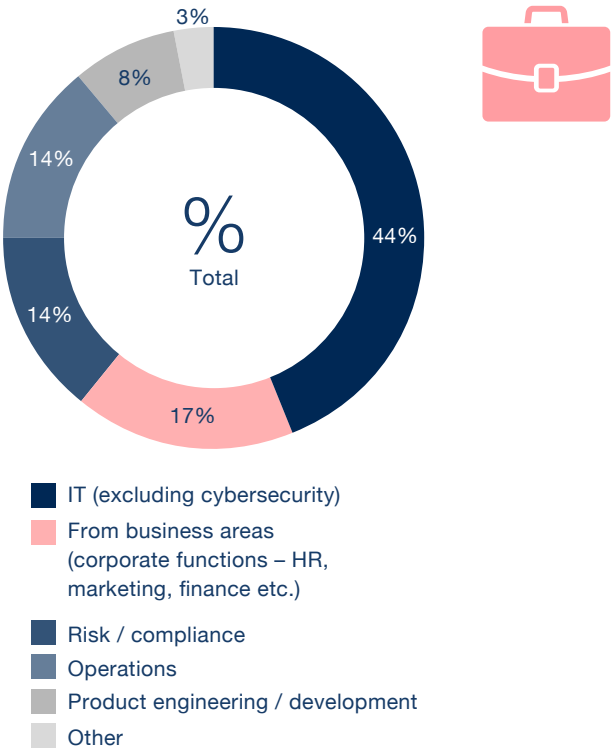
MARLIN HAWK

The older generation of CISOs (between the ages of 55-64) are the least likely to hold a degree of any kind (63%). This is likely due to generational differences, and that computer science wasn't a popular degree at the time they were studying, let alone the fact that cybersecurity (and computing in general) was still in its infancy. These more tenured CISOs are likely to have stood out within an organisation's IT team as the people most qualified to fill the role internally.

Despite prevalence amongst the older demographic of respondents, the research suggests that the trend of picking front-runners from the IT team is changing. In fact, a surprisingly low number of CISOs who have not always worked in information security have come from the IT department (excluding cybersecurity), with fewer than half (44%) working there before transitioning to security. Indeed, nearly one-in-five (17%) have come from other business management areas, including HR, marketing and finance. Moreover, we are seeing career CISOs; 50% of CISOs globally have always had an interest in cybersecurity, and this number decreases for older CISOs.

Interestingly, despite a CISO's role being so closely linked to risk and compliance, only 14% of those who have not always worked in information security come from this area of the business. It's particularly low in the US (6%) but is slightly higher in the UK & Ireland at 17%.

Which business unit did you come from?



For full data set, please see: Appendix 5

"One of my favourite interview questions which I ask people is, 'what do you think comes first; security or compliance?' I come from a compliance background and I had to learn what controls needed to be put in place to meet regulations and then how to build security based on those controls. So I'm completely backwards to most security people – with my background I would always say that compliance comes first. But for someone that grew out of the hacker world or, for instance, deep tech, they would always say security comes before compliance."

Steve Kinman is the CISO at Zalando in Berlin

However, in APAC, a third (33%) of CISOs come from a risk and/or compliance role. This may be for a number of reasons, including a more limited talent pool, and a focus on regulated businesses where risk management is paramount.

While half of CISOs entered the role because they've always had an interest in cybersecurity, 29% do it because they want to be at the forefront of one of the biggest business growth areas. Given the dynamic nature of the threat landscape, it's no wonder that the role is growing in response, and that we're seeing a lot of movement between industries as businesses globally look to stay ahead of the curve.

Cross-Industry Moves

Cross-industry hires bring both pros and cons. Professionals new to an industry can bring diversity of thought and fresh perspectives, however they may lack the granular knowledge acquired by veterans of industry.

Cybersecurity is somewhat of an outlier when it comes to cross-industry moves. Some would argue that the pervasive cyber threat is present no matter what the industry, but others state that the attacks a bank may face have different nuances to an energy business.

Last year, Marlin Hawk placed a group CISO at a leading multinational investment bank. The candidate possessed a varied background, having started his career at a Big Four accounting firm before moving across sectors including gaming and utilities. His diverse experience made him an attractive option for the company, which desired a CISO who had witnessed and handled a variety of threats and who would therefore be capable of taking on new challenges.

Just under a third (29%) of all CISOs have moved across industries. It's particularly prevalent in the UK and Ireland, as 37% of CISOs have moved across industry, compared to 18% in the US, and 16% in APAC. This may be due to a number of factors. For example, in the UK, having a CompSci degree is less desirable than in other markets. Given that businesses are looking for CISOs with diverse qualifications, it makes sense that these same businesses would welcome CISOs that have different professional backgrounds.

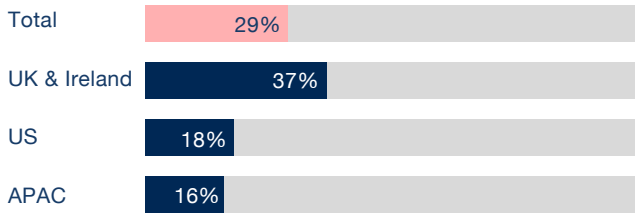
Around the world, consumer services (businesses like Spotify, Netflix and Uber) have acquired the most diverse CISOs, with 60% coming from other industries. Meanwhile, energy, oil and gas organisations have the least movement, with 87% having stayed within the industry for their whole career. This is likely because of heavy regulations, which require specialist knowledge. IT and telecoms businesses have a similarly low rate of attrition; 84% have remained in the industry.

Indeed, digging deeper into the data, we can see that those CISOs working in energy, oil and gas that have moved across industries have either come from IT and telecoms, construction, or professional services; other industries familiar with deep regulatory environments.

Other industries have a much more rounded CISO. Interestingly, CISOs working in the financial services – another highly regulated industry – appear to have a mixed background, with experience in IT, manufacturing, and public sector businesses, among others. This could be because the financial industry is undergoing its own transformation. With the growth of neobanks and challenger brands, traditional institutions are having to think outside the box, and this is extending to leadership teams. Hiring from across industry brings diversity of thought, and in the shifting financial landscape, this is important. It will be interesting therefore to see if the oil and gas industry follows suit, as digital begins to disrupt an otherwise very traditional sector and exposes it to new threats and challenges.

29%

of all CISOs have moved across industries

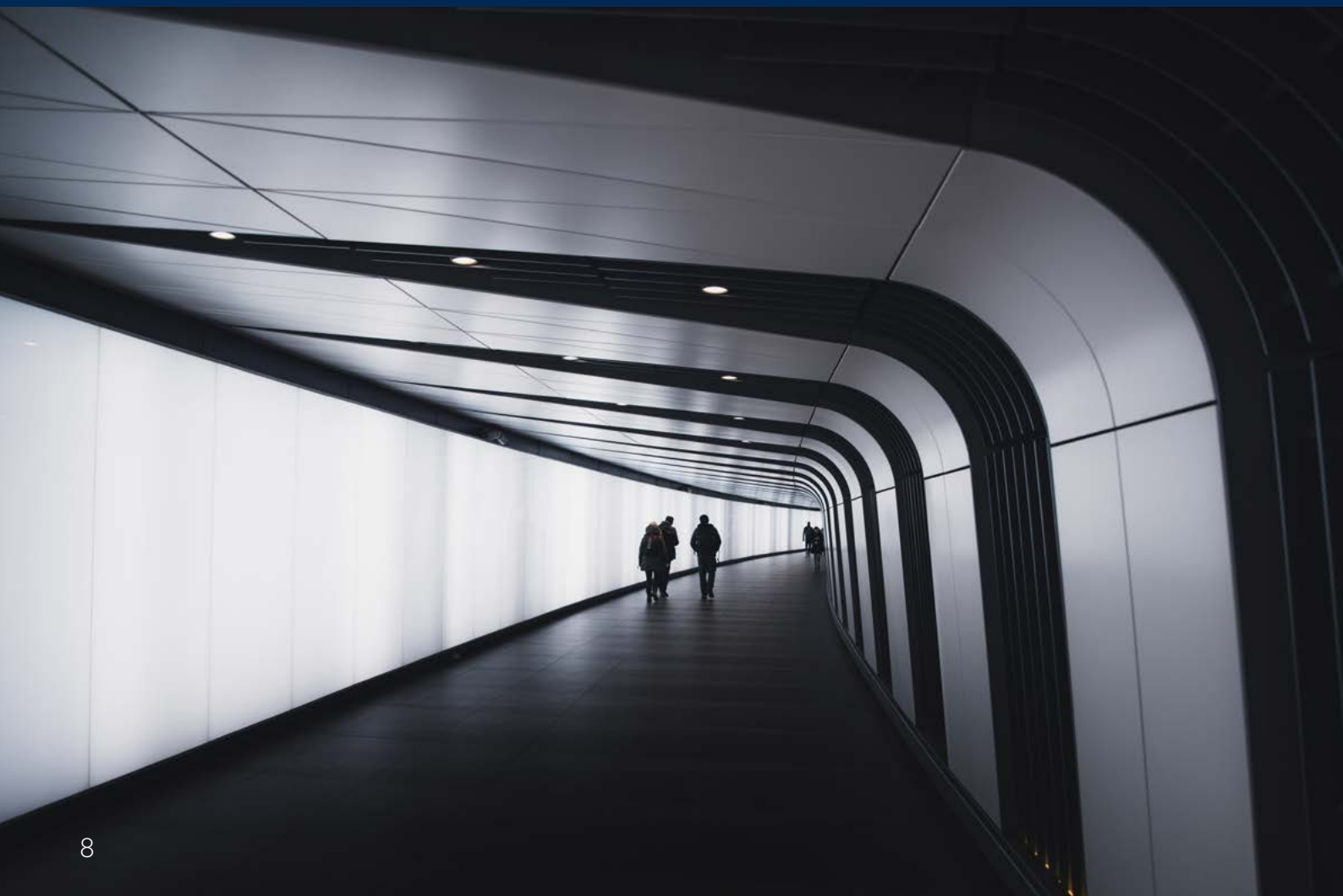


For full data set, please see: Appendix 7

“My background is predominantly finance and I think the governance processes in banks, in some instances, are crippling when it comes to allowing organisations to move quickly. And you see that between the big banks versus the challenger banks and the startups; there’s a huge degree of difference in how budgets and how approval authorities are done amongst those organisations.

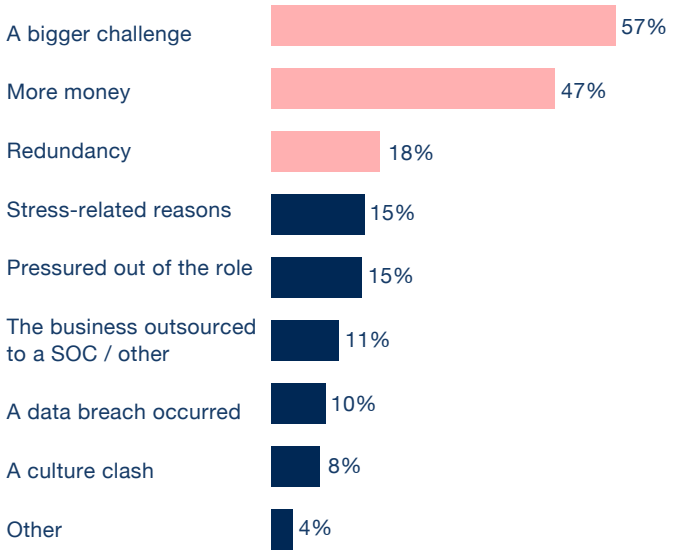
“Because of such a variance in working environments, some CISOs might look to move cross-industry but others who have worked in security for a period of time may want to move on to other specialisms. This is a new and emerging conversation and there’s different tracks from my perspective; there’s the risk or wider technology tracks open to CISO professionals. The question is which one of those will enable you to keep progressing further if you want to become the next COO or even the CEO.”

Ashish Surti is the CISO at Colt in London



The motivations for moving also vary around the world. For example, in the US, CISOs are more incentivised by money (70%) than the UK (47%), whereas CISOs based in the UK and Ireland would rather move because of the lure of a greater challenge (64%). This is likely a cultural difference; compensation in the US is higher across the board than in other countries, so CISOs know that they can attract a higher salary.

Why did you move?



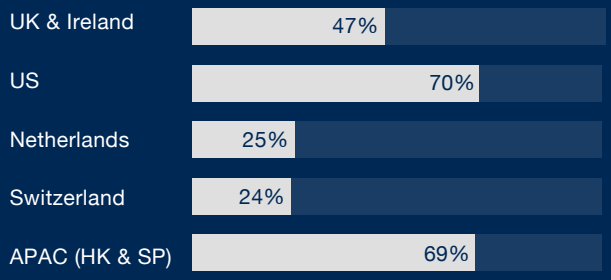
For full data set, please see: Appendix 8

70%

in the US, CISOs are more incentivised by money (70%), compared to

47%

in the UK



For full data set, please see: Appendix 8

The Role of the CISO

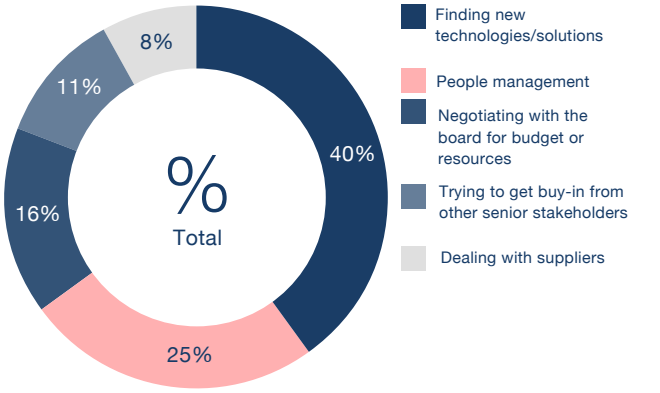
According to our research, respondents claim to only spend 50% of their time actively defending their businesses, while the rest of the time is split among other related responsibilities.

Globally, finding new technologies (40%) and people management (25%) take up the most time. In the UK, people management jumps up to 40% – compared with 33% in the US, and 9% in APAC. Given the demand for technology and cybersecurity talent globally, UK CISOs may be concerned that the lure of working on the US's West Coast – a market where salaries are typically higher – may attract their best talent. Therefore they may be working hard to ensure they keep their best people.

The lack of time spent on people management is indicative of the evolving role of the CISO and further proof that, in terms of business leadership, the role is somewhat ill-defined.

People management should take up much of the time of any senior business leader and, in fact, the actual protection of the business on a cyber front should be down to the CISO's team.

What takes up most time:



For full data set, please see: Appendix 9

"People management is more than growing leaders by sending them to training sessions to watch PowerPoint presentations. Having worked my way up the corporate structure, I find the most effective way is to nominate people to work on hard projects, be frustrated and at the end, be better for it.

"The other aspect of people management is organisational. We have thousands of systems and application development managers checking boxes saying they've gone through the litany of update checklists but, occasionally, somebody will fail to update something and it creates a gap in our security. So there's the human element that always comes up against the odds."

Kevin Meehan is the former CISO of Boeing

It may be that the profile of the CISO is changing, and other business leaders need to recognise this. The CISO role needs to blend technical knowledge with strategic leadership, and boards must consider this when hiring their CISO.

The next generation of CISOs we're beginning to see move through the ranks are altogether different; they are technically able, while also ambitious leaders. If the CISO role is to become truly strategic, or even elevated to a board level, these are the types of people who need to move into the role to shape it.

However, the CISO job market is a tough place to operate at present.

The Current Market

Around the world, 85% of senior cybersecurity professionals are either actively looking for a new role, or would consider one if approached.

It varies geographically as well; only 7% of US CISOs aren't actively looking or willing to consider a move, compared to 11% in APAC and 16% in UK and Ireland.

85%

of senior cybersecurity professionals are either actively looking for a new role, or would consider one if approached.

For full data set, please see: Appendix 11

There's a danger of a brain drain in the public sector. More than a quarter (26%) of public sector CISOs are actively pursuing new roles; over half of those (52%) want a new challenge, while 37% want better compensation. Of course, public sector roles are always going to be limited by the funds they have available, and they simply can't compete with the deep pockets of private businesses. That said, it's unusual that they are looking for a new challenge. From a threat perspective, public sector businesses may be at most risk, given the public data they typically hold.

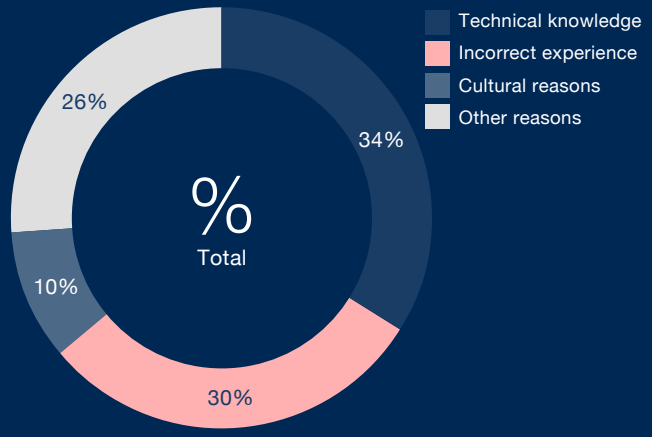
The CISO's willingness to move on is at odds with their own recruitment efforts, as 66% say they are struggling to recruit senior talent. The main reason given is that candidates lack the right level of technical knowledge (34%), don't have the right experience (30%) or simply aren't the right fit culturally (10%).

CISOs in APAC struggle more than others, with 91% saying they find it difficult to find the right talent, compared to 61% in the UK and 54% in the US. This may again come down to local candidates; if a business in APAC is demanding a candidate that is fluent in English and Cantonese, they are immediately cutting out large swathes of the market.

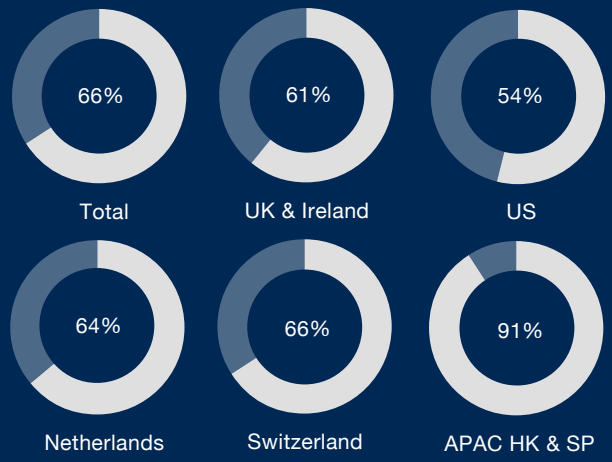
66%

say they are struggling to recruit senior talent

Do you struggle to recruit?



For full data set, please see: Appendix 11



For full data set, please see: Appendix 12

"It is certainly my experience that there is a shortage of talent globally, but also specifically here in Hong Kong. The maturity of cybersecurity and how it is viewed by businesses in Asia is probably not at the same level as in Europe or North America. For many years there has been no cultural obsession with cybersecurity, meaning that the teams historically have not been well-resourced or employed as many people. I don't think cybersecurity has really been given the prominence that it deserves in Asian companies. And that, fundamentally, is the reason there is a limited talent pool of qualified people."

David Gracey is the CISO at CLP Power in Hong Kong

Given the number of professionals who want to move, it seems strange that CISOs struggle to recruit. There appears to be a plethora of willing senior cybersecurity professionals out there, but CISOs feel that they simply aren't the right fit. It may well be that experienced cybersecurity professionals are viewed as either too technical, or too strategic, and not a strong enough blend of the two to be a potential cybersecurity leader. Therefore, companies are looking for younger talent that they believe have the potential to do both as they develop.

Moreover, they're not optimistic; 62% of CISOs worldwide think it's going to get harder to recruit over the next five years.

It becomes even more of a paradox when you consider that fewer than one-in-ten CISOs named recruitment as the biggest worry for them. Given the growing role of cybersecurity, and the importance of maintaining a secure posture, you would think this would rank higher. Indeed, only securing board buy-in ranked lower in their list of worries (4%).

62%

of CISOs worldwide think it's going to get harder to recruit over the next five years

Part of the issue may be that, unlike other senior business roles, the progression path of the senior cybersecurity professional or CISO is not clear. Fewer than half (40%) have ambitions of being a CEO, which makes sense as it's not a natural progression. The CISO role is specialist, and given the requirement to blend both technical knowledge and strategy, it wouldn't make sense for a CISO to put their technical expertise to one side in order to lead a business. But, given the continued growth of the cyber threat, we may see CEOs in the future be given some level of cybersecurity training, or indeed, bring the CISO closer to the top.

40%

Fewer than half have ambitions of being a CEO

The CISO in 2020

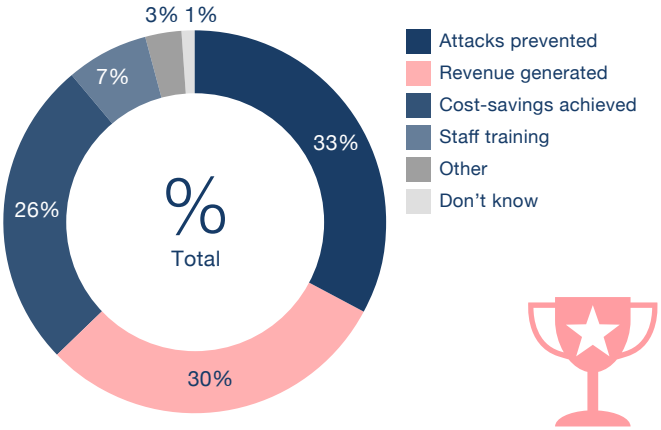
CISOs are in tune with the impact that both cybersecurity successes and failures can have on their businesses. Indeed, 61% believe that innovation within their organisations will be stifled due to security concerns. This makes their role increasingly important from a strategic standpoint, and will help them attach value to their role.

At present, the primary KPI for the modern CISO is attacks prevented (33%). The majority of CISOs globally agree with this (77%), which makes sense, given that evolving threats remain the number one concern for them. But, as the focus turns to talent and people management, and the role becomes more about strategic leadership, it is likely we'll see this change.

61%

believe that innovation within their organisations will be stifled due to security concerns

How is success measured at your organisation?



For full data set, please see: Appendix 13

However, with data protection remaining on the agenda for both businesses and consumers, risk will continue to be a primary concern for business leaders. Taking into account the CISO's natural predisposition for data protection, and the way it's intrinsically linked with cybersecurity, it's likely that this will soon become part of the CISO's remit too. In terms of progression, we may even see CISOs move into the role of Chief Risk Officer or CIO, with the latter taking cybersecurity into account when creating strategic plans for their organisation's IT infrastructure.

With heightened awareness around data protection and the looming worry of a lack of innovation, it's probable that in 2020 we'll see this start to happen, as board directors attempt to work out how to value these senior cybersecurity professionals. Indeed, we may even see the CISO's role begin to be subsumed into other areas of organisations, especially as the younger generation of cybersecurity professionals continue to emerge with a blend of technical abilities and strategic thinking. These younger people may use their skills to take ownership of the cyber defensive posture, but also to inform their organisation's overall IT strategy.

“We’re going to need solutions that can help the humans get away from more of the routine problem-solving and take it off of their plate so that they can work on the more difficult tasks. I think in the future you’ll see the security operators essentially have an AI or advanced computing partner so that you get both the human who can think through the new and interesting problem in the way that they typically do, and the partner that can run at machine speed to address the things that the human can do but are mundane and time-consuming.”

Ron Green is the CISO at Mastercard in St Louis, MO

One thing is for certain; 2020 is going to be an important year for the world of cybersecurity and those working within it. The threats will continue to evolve, as will those whose job it is to counter them.

To learn more about the experiences of the modern CISO, please visit our website to read full interviews with cybersecurity professionals from a range of different organisations – *Mastercard*, *ING*, and *Boeing*.

Data Tables

Appendix 1: How long have you been in your current position?

	Total	Europe	US	APAC (Hong Kong and Singapore)
Less than a year	3.20%	5.60%	0.67%	1.00%
1-3 years	27.20%	34.00%	20.67%	20.00%
3-5 years	56.40%	52.80%	56.67%	65.00%
5+ years	13.20%	7.60%	22.00%	14.00%
Average (years)	4	4	5	4
Base	500	250	150	100

Appendix 2: Do you have a degree level qualification obtained from a university?

	Total	Europe	US	APAC (Hong Kong and Singapore)
Yes	94.00%	88.40%	99.33%	100.00%
No	6.00%	11.60%	0.67%	0.00%
Don’t know	0.00%	0.00%	0.00%	0.00%
Base	500	250	150	100
Average (years)	4	4	5	4
Base	500	250	150	100

Data Tables

Appendix 3: What did you study?

	Total	Europe	US	APAC (Hong Kong and Singapore)
Computer science / similar	84.47%	79.19%	89.26%	89.00%
Maths / science / similar	6.81%	11.31%	2.68%	3.00%
Design / Architecture / Engineering / similar	6.60%	5.43%	7.38%	8.00%
English / Arts / similar	1.49%	3.17%	0.00%	0.00%
Other	0.64%	0.90%	0.67%	0.00%
Base	470	221	149	100

*Base total reflects number of respondents who answered 'yes' to having a degree level qualification

Appendix 4: Do you have a degree level qualification obtained from a university?

	Total	18-24	25-34	35-44	45-54	55-64
Yes	94.00%	72.73%	98.47%	96.43%	92.73%	62.50%
No	6.00%	27.27%	1.53%	3.57%	7.27%	37.50%
Don't know	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Base	500	11	131	224	110	24

Data Tables

Appendix 5: Which business unit did you come from?

	Total	UK & Ireland	US	Netherlands	Switzerland	APAC (Hong Kong & Singapore)
IT (excluding cybersecurity)	44.14%	35.85%	47.06%	57.14%	47.06%	66.67%
From business areas (corporate functions – HR, marketing, finance etc.)	17.12%	28.30%	17.65%	4.76%	0.00%	0.00%
Risk / compliance	14.41%	16.98%	5.88%	14.29%	11.76%	33.33%
Operations	13.51%	9.43%	17.65%	14.29%	23.53%	0.00%
Product engineering / development	8.11%	5.66%	5.88%	9.52%	17.65%	0.00%
Other	2.70%	3.77%	5.88%	0.00%	0.00%	0.00%
Base	111	53	17	21	17	3

*Base total reflects number of respondents who answered 'no' to always working in the field of information security

Appendix 6: Why did you want to be a senior IT security professional?

	Total	UK & Ireland	US	Netherlands	Switzerland	APAC (Hong Kong & Singapore)
I have always had an interest in cybersecurity	50.00%	48.00%	52.67%	46.00%	38.00%	57.00%
To be at the forefront of one of the biggest growth areas	29.40%	29.33%	38.67%	20.00%	16.00%	27.00%
No particular reason, I naturally progressed into the role	12.60%	16.00%	4.67%	18.00%	24.00%	11.00%
I wanted to be on a board	8.00%	6.67%	4.00%	16.00%	22.00%	5.00%
Base	500	150	150	50	50	100
Other	2.70%	3.77%	5.88%	0.00%	0.00%	0.00%
Base	111	53	17	21	17	3

Data Tables

Appendix 7: Have you always worked in the same sector?

	Total	UK & Ireland	US	Netherlands	Switzerland	APAC (Hong Kong & Singapore)
Yes	71.40%	63.33%	82.00%	60.00%	50.00%	84.00%
No	28.60%	36.67%	18.00%	40.00%	50.00%	16.00%
Don't know	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Base	500	150	150	50	50	100

Appendix 8: Why did you move role?

	Total	UK & Ireland	US	Netherlands	Switzerland	APAC (Hong Kong & Singapore)
A bigger challenge	56.64%	63.64%	62.96%	65.00%	40.00%	37.50%
More money	46.85%	47.27%	70.37%	25.00%	24.00%	68.75%
Redundancy	18.18%	10.91%	18.52%	25.00%	28.00%	18.75%
Stress-related reasons	15.38%	12.73%	14.81%	10.00%	16.00%	31.25%
Pressured out of the role	14.69%	10.91%	7.41%	20.00%	28.00%	12.50%

*Base total reflects number of respondents who answered 'no' to not always working in the same business sector

Data Tables

Appendix 9: What takes up most time in your role?

	Total	UK & Ireland	US	Netherlands	Switzerland	APAC (Hong Kong & Singapore)
Finding new technologies/ solutions	40.08%	29.76%	36.54%	40.74%	44.44%	59.57%
People management	24.89%	36.90%	32.69%	11.11%	14.81%	8.51%
Negotiating with the board for budget or resources	16.03%	15.48%	19.23%	18.52%	18.52%	10.64%
Trying to get buy-in from other senior stakeholders	10.55%	10.71%	11.54%	3.70%	14.81%	10.64%
Dealing with suppliers	8.44%	7.14%	0.00%	25.93%	7.41%	10.64%
Other	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Base	237	84	52	27	27	47

*Base total reflects number of respondents who answered 'yes' to spending less time than they'd like protecting the business

Appendix 10: Are you looking for a new role?

	Total	UK & Ireland	US	Netherlands	Switzerland	APAC (Hong Kong & Singapore)
I'm actively looking for a new role	24.20%	20.00%	17.33%	30.00%	36.00%	32.00%
I'm not actively looking, but would consider a new role if I was approached	61.00%	63.33%	74.67%	44.00%	40.00%	56.00%
I'm not actively looking and would not consider a new role if I was approached	14.00%	16.00%	7.33%	24.00%	24.00%	11.00%
Don't know	0.80%	0.67%	0.67%	2.00%	0.00%	1.00%
Base	500	150	150	50	50	100

Data Tables

Appendix 11: Do you struggle to recruit?

	Total	UK & Ireland	US	Netherlands	Switzerland	APAC (Hong Kong & Singapore)
Yes	65.80%	61.33%	54.00%	64.00%	66.00%	91.00%
No	33.80%	37.33%	46.00%	36.00%	34.00%	9.00%
Don't know	0.40%	1.33%	0.00%	0.00%	0.00%	0.00%
Base	500	150	150	50	50	100

Appendix 12: What do you struggle with most when hiring senior leaders?

	Total	UK & Ireland	US	Netherlands	Switzerland	APAC (Hong Kong & Singapore)
Finding the right level of technical knowledge	34.35%	39.13%	41.98%	15.63%	21.21%	34.07%
Finding the right experience	30.09%	26.09%	28.40%	34.38%	24.24%	36.26%
Finding the right cultural fit	10.33%	9.78%	7.41%	21.88%	6.06%	10.99%
Finding the right level of compensation	9.73%	6.52%	11.11%	12.50%	21.21%	6.59%
Finding the right level of seniority	8.81%	10.87%	6.17%	6.25%	18.18%	6.59%
Finding diverse candidates	6.38%	6.52%	4.94%	9.38%	9.09%	5.49%
Other	0.30%	1.09%	0.00%	0.00%	0.00%	0.00%
Don't know	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Base	329	92	81	32	33	91

*Base total reflects number of respondents who answered 'yes' to struggling to recruit talent in the current market

Data Tables

Appendix 13: How is success measured at your organisation?

	Total	UK & Ireland	US	Netherlands	Switzerland	APAC (Hong Kong & Singapore)
Attacks prevented	33.40%	40.00%	32.00%	24.00%	54.00%	20.00%
Revenue generated	29.60%	26.67%	30.67%	30.00%	10.00%	42.00%
Cost-savings achieved	26.20%	18.00%	31.33%	24.00%	22.00%	34.00%
Staff training	7.00%	12.00%	2.67%	12.00%	8.00%	3.00%
Other	2.80%	1.33%	2.00%	10.00%	6.00%	1.00%
Don't know	1.00%	2.00%	1.33%	0.00%	0.00%	0.00%
Base	500	150	150	50	50	100

MARLIN HAWK