



MARLIN HAWK

Global Snapshot: The CISO in 2024



Executive Summary

The global threat landscape has been reshaped in the past year with growing international instability, between China and the US, Russia's existential threat to global security, the outbreak of war in the Middle East, and the meteoric rise of Generative Artificial Intelligence (GenAI). In 2024, the Chief Information Security Officer (CISO) will play an increasingly pivotal role in helping the organizations they serve navigate the complex set of security risks associated with doing business in today's marketplace.

Drawing on proprietary data from [Fortune Global 500](#) organizations, interviews with leading CISOs across the US, Europe, and Asia, and leveraging our strategic intelligence capabilities, this fourth annual CISO study explores the dynamic landscape of cybersecurity leadership, aligning with our decade-long commitment to tracking this function's evolution.

CISOs have transitioned from technical specialists to integral business leaders, honing their skills of influencing, storytelling and translating cybersecurity issues into a language more aligned to broader business risk. CISOs are spending more time with their board members, executive leadership and broader business leaders, addressing cyber threats as a top organizational risk. The traditional reporting line of CISOs into technology leaders is being challenged, with CISOs increasingly aligned with other functions focused on risk such as operations, finance, legal, or directly with the CEO.

There continues to be high turnover in the CISO seat attributable to challenges around the pressure on top-level talent: budgeting and resources, the level of board exposure and executive support, burnout, the growing issue of personal liability, and a multitude of regulatory changes, to list a few. Artificial Intelligence (AI) is reshaping the cybersecurity space and CISOs are creating sophisticated strategies for AI implementation in order to keep their organizations secure in the face of increasingly advanced attacks from outside actors leveraging this technological leap. As CISOs become more integrated with business areas such as data, privacy, product, fraud, anti-crime, and infrastructure, their experience, knowledge, and expertise becomes evermore invaluable.

Our 2024 report addresses CISO tenure, succession planning and strategic hiring, and diversity, equity, and inclusion against a backdrop of the following research findings of the Fortune Global 500 CISOs:

- 51% of CISOs were hired externally into their current role
- 46% of CISOs have spent less than 24 months in their current role
- 18% of CISOs are (perceived to be) gender diverse
- 26% of CISOs are (perceived to be) ethnically diverse

Methodology

This research paper references Marlin Hawk proprietary data, which analyzed the CISOs of the Fortune Global 500; in 2022, these 500 organizations recorded aggregate revenues of \$41 trillion. Since 2020, it has been our commitment to track the evolving role of the CISO over a decade period, with this year's report marking our fourth annual CISO study. For this year's research, we opted to align our CISO analysis with the globally-recognized Fortune Global 500 index. Going forward, we will continue to track the Fortune Global 500 and provide year-on-year analysis of CISOs leading the cybersecurity agenda at these organizations.

Marlin Hawk is a global executive search and leadership advisory firm. We aspire to be the boutique partner of choice at the forefront of transformational change and of placing the most positively disruptive talent into ambitious and forward-thinking organizations. Our expertise today is far-reaching across functions, sectors, and geographies; our history is rooted in the technology office. The cybersecurity function has been extensively mapped and

researched through our world-class strategic intelligence capabilities and cybersecurity search mandates. Our professional network spans leading subject matter experts and decision makers for the CISO function.

The objective of our research is to collect and analyze a large enough dataset to draw valid conclusions about the background and behaviours of those making cybersecurity decisions at large organizations. This paper also includes qualitative research gathered by Marlin Hawk from interviews with CISOs working in the US, Europe, and Asia Pacific.

Marlin Hawk analyzed the profiles of the Fortune Global 500 CISO executives to understand the changing dynamics in this critical leadership position.

Evolving Responsibilities

Today's CISO operates amid greater challenges to organizational resiliency than ever before; challenges such as: an expanding attack surface, nation state attacks, and constraints to budgets and resources. As a result, CISOs have moved from technical, domain experts towards business leaders focused on enterprise-wide risk mitigation.

With increased visibility and exposure of the CISO across the organization comes greater responsibility. How exactly the CISO's responsibilities have evolved is dependent on the size of the organization, the regulation level of the industry they operate in, and what other functional areas make sense to consume into their remit because of the company's business model.

The CISO of a financial services organization will likely be dedicating more than half their time to external (regulators) and internal (board, executive leadership and business line leadership) stakeholder management. They may also be taking on responsibility for anti-crime units within the organization, where cybersecurity converges with fraud, financial crime, and data management. In non-regulated industries, we are seeing CISOs take on responsibility for areas of technology such as infrastructure. As the CISO moves from more of a specialist to a generalist, their direct reports and team at large become increasingly specialized in their expertise.

“It is the responsibility of today’s CISO to move from a specialized view on cybersecurity to a broad, generalist view across the business. What will evolve within the CISO’s team, are more specialized leaders reporting into the CISO who know more about their specialty than the CISO does. It’s then on the CISO to see across that specialist knowledge with a general overview of the business and that is a newer skill set than we are used to.”

Jason Mallinder is a Client Partner, EMEA at ISTARI and formerly the Chief Information Security Officer at Credit Suisse

An organization's cybersecurity vendor strategy is one area of increasing complexity within the evolving role of the CISO. The vendor landscape grew to a [\\$7.8 billion industry in 2023](#) with key dominant players - for example, Palo Alto Networks owns more than a quarter of market share - as well as a large number of niche operators.

This can lead to an organization's vendor strategy being multiple layers deep. If a company is undergoing significant M&A, ensuring integration of third-party vendors on both sides of the transaction will be a core aspect of the CISO's role. It will also be under the scrutiny of the organization's board and leadership team.

“The evolution of cybersecurity needs to continually move past security for compliance and security's sake, and move further towards supporting the organization to make business-based management decisions with the view to reducing risk. An example of this is an organization's third-party strategy where requiring vendors to adhere to one-size-fits-all assessments doesn't necessarily translate into reducing risk, as seen through all vendor breaches. Moving away from such box-ticking exercises towards understanding how to assess the supply chain at scale is one area where we will see a shift in the role of the CISO.”

Jenny Menna is the Chief Security Officer at Sallie Mae

“CISOs can ask for investment in a strategic way, which is to balance the cost of the risk versus the cost of investing to reduce the risk. Taking risks is the cost of doing business because without taking risks you cannot grow. As a CISO, it's critical to hone your storytelling craft and know the right people to share that story with to have influence. There is power in the intersection of good data, good storytelling and influence that ensures you secure your company with acceptable risks while also allowing it to grow.”

Aimee Cardwell is the former Chief Information Security Officer at UnitedHealth Group

CISOs are now key contributors to boardroom discussions and frequently sit on the executive leadership. How focused the leadership team is on cybersecurity, and the organization's overall risk appetite, are determining factors for how the CISO's exposure to the C-Suite has grown.

Speaking the language of revenue generation, brand reputation, and customer satisfaction has become a prerequisite for effective communication and a skillset all CISOs must now have, or be developing. For example, when it comes to being successful in securing the investments needed for cybersecurity, the risks related to not investing need to be put into plain business terminology. The ability to weave compelling narratives around business risk becomes pivotal in capturing the attention of the organization's leadership, prompting a constructive dialogue on necessary fixes to maintain a secure posture.



Boardroom Representation

Cyber threats rank prominently in the context of modern-day risks faced by any organization. As the board is instated as a governing entity to guide the strategic direction of its organization and manage risk, it is no surprise cybersecurity is now increasingly top of the agenda. The growing interest of boards in understanding cybersecurity reflects the recognition of its existential threat to businesses in the digital age.

The role of the CISO at the board level within their own organization is to provide a strategic perspective on top organizational risks, and to translate complex cybersecurity information into a language understandable by the board. The CISO is there to bridge the gap between technical intricacies and strategic business decisions, ensuring the cybersecurity narrative is accurately delivered, and individual and organizational protection is maintained.

“How can you get the attention of the CEO? Fear tactics may work once or twice, but not in the long run. It’s best to show numbers and probabilities backed by research and evidence. When describing a cyber risk, it’s more impactful to emphasize the probability of an event negatively impacting business operations. Qualitative metrics, based on opinions and experience, can be limited to one’s career. The CEO needs quantitative data to make informed decisions when investing in cybersecurity resources. With quantitative data, the CEO and their team can make informed decisions based on facts, rather than fear.”

Brenton McKinney is a Partner at Fortium Partners

There are skills all CISOs need to develop to be able to be effective at the board level such as storytelling, influencing, and radical transparency. However, appointing a cybersecurity expert to the board, or relying too heavily on the CISO within the organization itself, will not alone solve risks faced by businesses today. Board members need to be well versed and appropriately educated on cybersecurity threats and their possible implications. Everyone on the board needs to speak the language of business risk when it comes to cybersecurity.

Finally, there is the matter of legal considerations and personal liability for board members, and the CISO, in the face of a breach. In May 2023, former Uber CISO, Joe Sullivan, was sentenced to three years probation and a substantial fine for the 2016 data breach. In October 2023, the SEC charged SolarWinds and its CISO, Tim Brown, for fraud and internal control failures relating to allegedly known cybersecurity risks and vulnerabilities. These cases of executive and board liability are adding to the feeling within the CISO community that the role itself is now overexposed, with too much responsibility and, too often, not enough control over decision-making.

“When a CFO sits on the board of an organization, and they’re responsible for managing all the financials, it doesn’t mean that everybody else who sits on the board doesn’t need to understand financials. Everybody around that board table, many of which will never have been a CFO, understand financials. For me, that is where we have to get to with technology and cybersecurity is a key component of that. We need to get to a place where cyber resilience and digital resilience becomes something that the board has a level of understanding about similar to their understanding of financials.”

Jason Mallinder is a Client Partner, EMEA at ISTARI and formerly the Chief Information Security Officer at Credit Suisse

“In the recent high profile cases of CISOs being prosecuted, it’s less about what the CISO did and more about what the organization’s didn’t do with the information they were given. In order to give the information to the right people in the most accurate way possible, the CISO needs to be given access to the Board and the Executive Leadership. Everyone is at risk without that.”

Leading Cybersecurity Executive

Reporting Structures

Historically, the predominant reporting line of the CISO has been into the CIO, CTO, or other technology leader. This was due to the technical expertise required in the role as it was previously defined. As the role of the CISO is elevated to a broader business leader, a corresponding change to the reporting structure may be appropriate.

With a growing focus on cybersecurity risk at the board and executive leadership level, having the CISO more aligned to business functions like finance or legal, that are also focused on enterprise-wide risks appears to be logical and likely effective. The CISO and the CIO, or CTO, often have competing agendas where the CISO is focused on risk and the CIO is focused on operationalizing the business. The goal is to communicate security risks across the organization, transcending traditional technology-focused silos and ensuring security considerations are not overshadowed by competing priorities.

“Having the CISO reporting outside of technology is more effective for getting the security messages to the top. For example, if the CISO reports into the CFO or the CRO, or the CLO, then they are more aligned with others who are looking at the broader risk landscape for the business. They are speaking the same language. And they are looking across the whole organization, not just at the technology function.”

Colin Henderson is the Chief Information Security Officer at Bakkt

“At BT, our technology universe has two planets: networks and digital. Between the Chief Digital & Innovation Officer, the Chief Security & Networks Officer, and myself, our job is to balance security, operational resilience and innovation. We have board buy-in, leadership accountability and a top down, bottom up security strategy. It is those components that are more important for success than specifically who reports to who.”

Les Anderson is the Global Chief Security Officer and Vice President Cyber Security at BT Plc

Beyond the technicalities of reporting structures, a more important factor to the success of a CISO is exposure to, and explicit support from, CEOs, executive leadership, and boards. CISOs stress that regardless of hierarchical lines, having direct access to top-level executives is paramount. Naturally, a direct line into the CEO is seen as empowering for CISOs. Reporting to the CEO provides a strategic vantage point, aligning security decisions with organizational strategies such as mergers and acquisitions.

By and large, what works best in terms of structure for any business will come down to organizational culture and organizational design; is security at the heart of the business? Do the board and the leadership team take the risks seriously? Wherever the CISO reports into, the success of any cybersecurity programme hinges on strategic alignment, independence, and a nuanced understanding of risk.

Generative Artificial Intelligence

The ascent of Generative Artificial Intelligence (Gen AI) into the broader consciousness is ushering in a transformative era, disrupting conventional ways of working and forcing change across organizations. As of 2024, Gen AI has not only erupted but has become the new technology force at play, forecast to become a \$1.3 trillion market by 2032.

An important starting point for any debate around the opportunities and challenges of AI is to remember that the technology itself is not new. Research scientists, data science and machine learning engineers have been debating the utility of Large Language models (LLMs) and neural networks for over half a century. What is new, particularly this year, is the scale of access to AI tools, one popular example being ChatGPT. At the time of publication, the [ChatGPT website had 1.5 billion visits a month](#), certainly defining the last 12 months as the tipping point for use of AI, at large. Alongside the technological capabilities, it is both the accessibility and application of AI that CISOs need to consider when developing a robust strategy for implementation.

Gen AI's influence on cybersecurity is tripartite. The first facet is how hackers are implementing AI to more effectively attack organizations. AI is enabling hackers to carry out the same types of attempts on security breaches but at a larger scale and with increasing accuracy and success. AI allows for: phishing to become more convincing, automation to become more powerful, malware to become harder to detect, and passwords to

become easier to crack. AI is being used by hackers to infiltrate both the human and the technical side of security, demanding recalibration of the lines of defense in place to protect companies from the increasing threat capability.

Secondly, the flip side to this accelerating sophistication in adaptive attack technologies is the imperative for CISOs to defend with AI. As hackers use bots in phishing attacks, cyber leaders are responding by using bots. They are using machine learning powered email security solutions to protect against password theft and breaches. Using AI to screen huge amounts of threat data allows CISOs to code, test and release solutions previously done by humans, at a scale and complexity that people can no longer do.

Lastly, the construction and operation of AI for business purposes - and close monitoring thereof - present multifaceted challenges for any CISO. Use cases of leveraging Gen AI include employees feeding tools with company data and engineers writing code using AI. Whether companies are constructing dedicated AI spaces or putting meticulous controls in place, accessibility of the workforce to AI is an important deciding factor when it comes to security. [Samsung banning ChatGPT amongst employees](#) as the direct result of a source code leak exemplifies that access needs to be combined with education of the workforce to ensure an organization's security posture and intellectual property is not compromised.





While most organizations have a long way to go when it comes to the use of AI in a safe way, overall our interviewees believe AI will be a cybersecurity enabler. It is broadly agreed that AI is only as powerful as the data you feed it, and if that data is inaccurate you will return inaccurate results and untruths. No one has more accurate data on a company than that company has on itself. With these datasets being securely fed into an organization's LLM, the impact on threat detection will be a game changer.

One discernible trend we are seeing emerge as organizations grapple with Gen AI's integration is the gradual shift within some organization's cybersecurity entities towards becoming broader data risk management units. Through our interviews, we have heard CISOs are working more closely with their Chief Data Officer counterparts on how to effectively combine the data capturing power of the cloud with the processing power of AI to build internal cybersecurity capability. People who seamlessly traverse both domains are in short supply and invaluable assets. The convergence of data analytics and cybersecurity expertise positions these individuals as emerging champions to navigate the evolving landscape.

“Cybersecurity is the art of seeing further, understanding more, correlating better, and then responding faster. Cloud computing can now capture and process practically unlimited amounts of data and AI can perform extremely complex queries on that data using educated machine learning models. This powerful combination is giving the cybersecurity profession greater access to those very low frequency, unique anomalies at the peak of the threat pyramid, and identifying patterns that are very hard for the human eye to detect.”

Alvaro Garrido is the Group Chief Information Security Officer at Standard Chartered Bank

Turnover and Tenure

High turnover within the CISO role, often lasting less than two years, is well documented and attributable to a complex set of challenges. Our research shows 46% of Fortune 500 CISOs have been in the role for less than 24 months. The first is a simple supply and demand equation; the demand for CISOs outstrips the supply, meaning there are plenty of opportunities in a candidate-led market. The net result is ever-increasingly competitive and attractive compensation packages offered to lure top talent.

A second factor is the reality an incoming CISO steps into versus what they were promised during the hiring process. If the CISO doesn't have direct access to the board or executive leadership, or the necessary budget and resources to implement the cybersecurity strategy, then they are not being supported to effectively do their job. Sometimes this misalignment of expectations comes down to a CISO not asking the right questions during the hiring process. It can equally be that organizational realities are not accepted or fully understood on the side of the hiring company.

Ultimately, this is an often gruelling role, where there are rare moments to celebrate success and the risk of failure is devastating. Too often a CISO lacks the necessary control over critical business areas needed to decrease vulnerabilities and risks, and has to rely on influence as a primary tool. When a CISO has exhausted all possibilities - or, in some cases, becomes tired of trying - there is no shortage of other roles they can walk straight into.

Finally, the nature of the CISO role is industry-agnostic, allowing CISOs to transition successfully across diverse sectors. This adaptability, while enhancing the CISO's skill set and leaning into their natural desire to take on new learnings and complex challenges, also contributes to the constant demand for experienced leaders in the field.

“To be successful in the CISO role, you need to be able to position yourself as a leader who can be risk oriented and work with business leaders. Within the business context, a CISO is either a revenue enabler or a bottom line protector. It is a crucial part of a CISO's role to ensure the organization you're working for understands what will happen to the bottom line if there is a breach, over the short-term and the long-term.”

Arvind Raman is the Senior Vice President and Chief Information Security Officer at Blackberry

46%

of CISOs within Fortune 500 Global companies have spent less than 24 months in their current role



Diversity, Equity & Inclusion

With CISOs moving fluidly between industries, there is naturally diversity of thought present within the role. But what about other measures of diversity, particularly gender and ethnicity? Our research found that 18% of the Fortune 500 CISOs are perceived to be gender diverse and 26% are perceived to be ethnically diverse.

First and foremost, change is needed at the top where representation has been proven to be a necessary prerequisite for moving the needle on diversity. [McKinsey research](#) suggests that not only does representation at the leadership level lead to better diversity across an organization, more gender and ethnically diverse companies outperform those that are less diverse. Representation is relevant across the leadership of the whole organization, as much as it is within the cybersecurity function. If you rarely, or never, see an ethnically, gender, LGBTQ or neurodiverse CISO during your career, as someone from any or all of those diversity dimensions, it's less likely you will see yourself as a potential cybersecurity leader in the future. As with all

senior positions, organizations need to make a concerted effort in reshaping their leadership team to mirror the envisioned diversity across the broader organizational spectrum.

The lack of gender diversity in the CISO seat today has been pinned on a parallel lack of diversity in STEM education, a generation ago. Many see this as needing a grassroots change at the higher educational level that encourages greater diversity in its student population and this, with time and patience, will rectify a historical issue. How can organizations take the issue of diversity into their own hands, rather than waiting for a change in the educational system, which they have no control over? Instead of focusing on academic qualifications, organizations could instead focus on the critical capabilities needed to be successful in the cybersecurity function which centre around curiosity, resilience, crisis management and critical thinking. This would help address the misconception that technical prowess is the sole determinant of success in the cybersecurity field.

Building a diverse pipeline for all levels between entry and leadership can be done through a range of initiatives. Organizations can proactively address diversity imbalances by making a commitment to diversified interview panels and candidate lists. Similar to rethinking educational requirements at entry level, companies could undergo an overall strategic reframing of cybersecurity roles, departing from a narrow technical lens and broadening out to the multifaceted skill set essential for success.

Finally, partnering with initiatives such as those focusing on gender in technology or providing opportunities for marginalized youths can become part of a comprehensive approach to addressing gender, neurodiversity, and socio-economic factors when hiring for the cybersecurity function. Importantly, it shows a commitment to holistic diversity strategies.

Ethnic Diversity

26%

of CISOs from Global Fortune 500 companies are perceived to be ethnically diverse

Gender Diversity

18%

of CISOs from Global Fortune 500 companies are perceived to be gender diverse

“One of the first things I did in my previous role was remove all requirements for college degrees at every level. Having a college degree is not a necessary requirement for any role within cybersecurity, unless it’s a legal one. Then I made the leadership team look like I expected the rest of the team to look. Lastly, for our entry level roles, we worked with an outside vendor on a boot camp program that identified diverse candidates, taught them specific requirements, assessed their skills, then we would take them on for at least six months. Our success rate was around 75%, hugely increasing our diverse pipeline while training them in a usable skill they could immediately implement. If you are passionate about making a change, it is entirely possible for any CISO to get started on building a robust program for diversity and inclusion from day one.”

Aimee Cardwell is formerly the Chief Information Security Officer at UnitedHealth Group



Succession Planning and Strategic Hiring

With cybersecurity being an enterprise-wide risk at the top of the board's agenda combined with high turnover in the CISO seat, organizations need to effectively manage succession planning when it comes to their cybersecurity leaders. Our research shows that 51% of Fortune Global 500 CISOs were appointed externally into their current role.

When looking externally, organizations may widen the talent net more broadly than previously thought relevant. As a result of the mainstream use of AI and rising threat levels, there is a convergence of cybersecurity with data, product, fraud, privacy, IT risk, infrastructure and, in the case of financial services, anti-crime and financial crime units of the business. As the CISO moves from a technical specialist to a generalist more focused on risk, the background of their career will start to look different. Additionally, as the exposure of the CISO increases, and the level of risk they are dealing with continues to elevate, it is likely that more people entering the CISO seat will come from a risk security background.

Research from Proofpoint recently published in the Wall Street Journal suggests 73% of CISOs experienced burnout in the past 12 months. Through our interviews, burnout was identified as a real issue, primarily stemming from inadequate budgeting, insufficient cybersecurity team

resources, and a lack of executive support. More CISOs are asking about organizational support and legal coverage of personal liability in the event of a breach. Additionally, regulatory pressures further compound the intense environment in which CISOs operate, adding complexity to succession planning and strategic hiring endeavors.

“Burnout is a real issue and often comes down to the individual, their workplace culture and how supported they feel to navigate complex situations. Just like anything else in life, you need to make sure you're looking after yourself - physical exercise, eating well, all the factors that contribute to mental wellbeing. Wellbeing of yourself and your cybersecurity team needs to be a key part of the culture you're creating. Cyber response teams are busy 24/7 dealing with major incidents that take up a lot of mental load. As CISOs, we need to ensure we are cultivating a workplace environment where these teams feel supported with their wellbeing so they can be their best selves at work, support their peers, and be effective in their roles, ultimately keeping Australians safe from the rising risks of cyber crime.”

Sandro Bucchianeri is the Group Chief Security Officer at National Australia Bank

What is Next for the Chief Information Security Officer?

It has been established that more and more is being expected of CISOs: more responsibilities, more risks, more regulation, more exposure. While this creates much pressure, it also creates a lot of opportunities for where a CISO can go next. There is a clear pathway for any CISO to switch to a different industry, taking with them what they know and facing new challenges. They could take a turn on the vendor side, growing and scaling a new cybersecurity product, for example.

CISOs can also expect to have more board opportunities open to them in the future. Through our interviews, we are seeing an uptick in those CISOs approached for - and in some cases accepting - external board seats at other companies. The drive for this is threefold: i) the evolving regulatory frameworks, such as the recent SEC rule may lead to a surge in CISOs joining boards; ii) the increasing sophistication of cyber threats as a result of AI and the question of personality liability (increasing the need for CISO expertise at the board level); and, iii) the organization believes it is the right thing to do to best protect its interests.

“Boards drive governance, including risk management. And cyber has become one of the most pertinent risks in terms of immediacy, likelihood and impact. With more digital attack surface area to protect than ever before, the value proposition of having a CISO on the board of directors has risen exponentially.”

Jamil Farshchi is the Executive Vice President and Chief Information Security Officer at Equifax

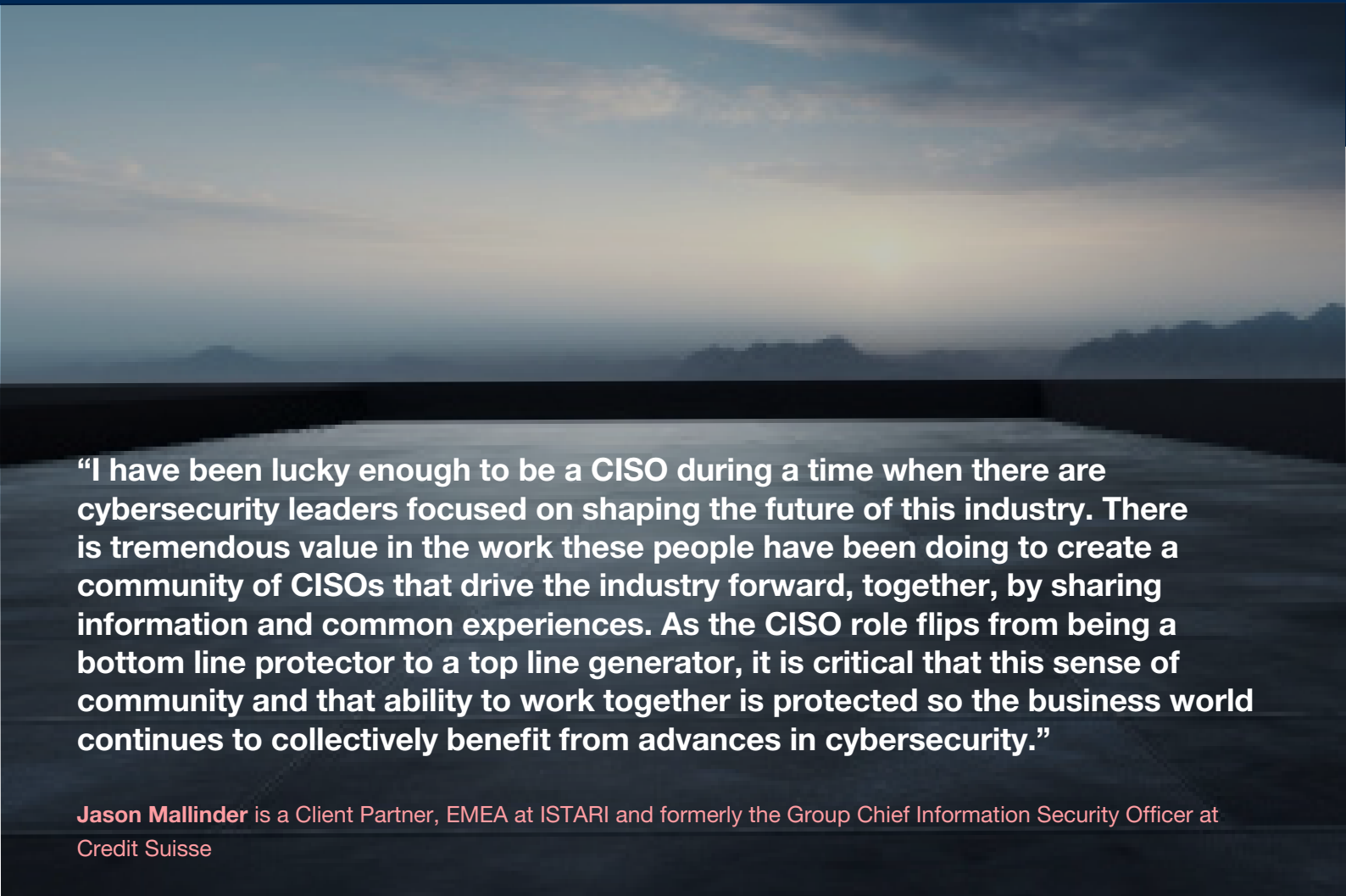


In addition to the increasingly relevant experience CISOs can bring to external board appointments, their influence within their own company will continue to expand. There is likely to be more standardization in what the CISO role is as it reaches its maturation in the same way other C-Suite roles have in the past. This maturity of the function will be reflected in formal training paths at universities and continued professional development programmes. As CISOs and their teams infuse security at every level of the business - rather than the cybersecurity function being layered on top - we are likely to see a continual shift from cybersecurity leadership towards everyone becoming a cyber leader. This will only further elevate the CISO's role to a more advisory level.

While the future looks bright for the next generation of CISOs, in many ways this is due to the painfully chartered course navigated by the current generation. Stressful conditions, long working hours, high levels of burnout, and sometimes catastrophic outcomes just being "part of the job," it is a challenging time to be a CISO; this should not be overlooked.

"It's always been my personal goal to get to a point where there is no need for my role as a CISO. We have to get to a point where cybersecurity has been operationalised across the business and it has become a fundamental part of everyone's role and everything works. If CISOs could migrate from their current operational role into an advisory board level role, and help other companies get to where they need to be, that would be the ideal."

Sandro Bucchianeri is the Group Chief Security Officer at National Australia Bank



"I have been lucky enough to be a CISO during a time when there are cybersecurity leaders focused on shaping the future of this industry. There is tremendous value in the work these people have been doing to create a community of CISOs that drive the industry forward, together, by sharing information and common experiences. As the CISO role flips from being a bottom line protector to a top line generator, it is critical that this sense of community and that ability to work together is protected so the business world continues to collectively benefit from advances in cybersecurity."

Jason Mallinder is a Client Partner, EMEA at ISTAR1 and formerly the Group Chief Information Security Officer at Credit Suisse

Acknowledgements

We would like to thank all of those who contributed to the content of this article, some of whom have graciously consented to be listed below:

Aimee Cardwell, Non-Executive Board Member, WEX

- *Previously: Chief Information Security Officer, UnitedHealth Group*

Alvaro Garrido, Group Chief Information Security Officer, Standard Chartered Bank

Andrew Dell, Group Chief Security Officer, QBE Insurance

Arvind Raman, Senior Vice President and Chief Information Security Officer, Blackberry

Brenton McKinney, Partner, Fortium Partners

- *Previously: Senior Vice President and Chief Information Security Officer, Bright Health*

Colin Henderson, Chief Information Security Officer, Bakkt

Jamil Farshchi, Executive Vice President and Chief Information Security Officer, Equifax

Jason Mallinder, Client Partner, EMEA, ISTAR

- *Previously: Group Chief Information Security Officer, Managing Director, Credit Suisse*

Jenny Menna, Chief Security Officer, Sallie Mae

Les Anderson, Global Chief Security Officer and Vice President Cyber Security, BT Plc

Sandro Bucchianeri, Group Chief Security Officer, National Australia Bank



MARLIN HAWK