Global Snapshot: The CISO in 2021

MARLIN HAWK

Executive Summary

As the world emerges into a post-pandemic reality, the importance of a robust cybersecurity function has never been more apparent. In 2020, virtually all companies were exposed to multiple security challenges in the race to accommodate a remote workforce. The first quarter of the year saw a 350% increase in phishing websites, many targeting hospitals and health care systems[01]. Banks and insurers were also primary targets: 74% of financial institutions reported a rise in cybercrime, and 42% of these attribute the reduction in security to remote working conditions.[02] In the face of these challenges and mounting fiscal pressure, the Chief Information Security Officer (CISO) emerged as one of the most resilient and dynamic members of the C-suite.

Last year, Marlin Hawk published its inaugural global CISO research report, which explored the demographics of Chief Information Security Officers around the world and the challenges faced in the rapidly evolving cybersecurity landscape. For this year's report, Marlin Hawk analysed the profiles of the top 470 CISOs across North America, Europe, and Asia Pacific with a lens on the current environment.

In addition to quantitative analysis, this report includes qualitative research gathered from semi-structured interviews with CISOs of Fortune 500 companies in North America and Europe. These conversations focused on the short- and long-term impacts of the pandemic on the CISO role, perspectives on tenure and succession, the evolution of the cyber function, and board level impact.

Key findings from Marlin Hawk's research include:

- 53% of global CISOs have been in their current role for two years or less, meaning they assumed a new position during the COVID-19 pandemic.
- Aproximately 64% of global CISOs were hired from another company, indicating that most organisations fall short when it comes to retaining a CISO successor.
- Almost half of CISOs analysed with a graduate degree received a higher degree in business administration or management.
- CISOs are more likely to serve on advisory boards or industry bodies than on the Board of Directors.
- Only 14% of the global CISOs analysed are women; approximately 21% are non-white.

Methodology

The data this research paper references is Marlin Hawk proprietary data, which surveyed 470 CISO (or equivalent) executives employed at businesses with 10,000 or more employees. This data comprises 300 North American businesses in Canada and the United States; 125 European businesses in Belgium, Denmark, Finland, France, Germany, Ireland, Italy, the Netherlands, Norway, Scotland, Spain, Sweden, Switzerland, and the United Kingdom; and 45 Asia Pacific businesses in Australia, China, Hong Kong, India, Japan, Malaysia, Singapore, and South Korea.

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, Marlin Hawk's market intelligence and data is far-reaching and diverse, encompassing multiple sectors and geographies.

The objective of this research exercise was to collect and analyse a large enough dataset to draw valid conclusions about the background and behaviours of those making cybersecurity decisions at large organisations.

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

Marlin Hawk analysed the profiles of 470 CISO executives employed at companies with 10,000 or more employees.

COVID-19 Impacts

The Chief Information Security Officer is inherently responsible for crisis management and response; they are always focused on the digital protection of the workforce, regardless of whether there is a crisis. While responding at pace to potential threats is part and parcel of the role, COVID-19 introduced a new level of complexity when CISOs were tasked with securing a remote workforce from any number of increasing threats. Additionally, a surge in e-commerce and digital activity meant that CISOs needed to act quickly to reinforce business operations.

The CISO organisation has historically been tightly linked with risk mitigation. In years past, some members of the corporate ecosystem have even colloquially referred to it as "the house of no." But the pace at which cybersecurity executives were forced to adapt during the pandemic has fundamentally changed this perception of the function as a reactive subset of technology. Over the course of the pandemic, the CISO has emerged as a key driver of business transformation.

According to Kevin Brown, who is the Managing Director at BT Security, "The CISO's role has broadened to a more rounded business leader. The historic 'hands on' role of the CISO is evolving into a strategic planning focus on how security can enable business change and digital transformation.“

Short-term, the shift to remote work has broadened the CISOs mandate to encompass the entire security ecosystem. "The CISO role has become an interesting mix of digital and physical security," notes Aman Raheja, CISO at Humana. "This combination created new risk for CISOs, who had to architect solutions to ensure access to critical services and ways of working."

Through the course of the pandemic, the CISO has emerged as a key driver of business transformation.

"The CISO's role has broadened to a more rounded business leader. The historic 'hands on' role of the CISO is evolving into a strategic planning focus on how security can enable business change and digital transformation."

Kevin Brown is Managing Director at BT Security in the UK

The widening of responsibilities for cyber chiefs is in part due to the large role they've played in setting up the enterprise for remote work. To resolve (and anticipate) the various risks associated with a remote workforce, CISOs had to find ways to work quickly and effectively with key stakeholders across the enterprise. Glenn Foster, the CISO at TD Bank Group, leveraged the company's cyber operation hub to quickly collaborate with leaders across fraud management, incident response, investigations, physical security, legal, and compliance. Launched in late 2019 to enhance global threat detection and prevention efforts, TD's Fusion Centre brought a multi-disciplinary team of global threat experts together under one common umbrella. "The Fusion Centre was in its own sense an agile practice and we were able to quickly collaborate with a cross-section of the right colleagues," notes Foster. "This enabled the security teams to stand tall and deliver on the rapid shift to working from home while managing risk."

The shift to a remote or hybrid workforce also exposed serious vulnerabilities for organisations dependent on legacy technologies and made a positive example of early adopters. For Jamil Farshchi, the CISO at Equifax, it was fairly simple to replicate the requirements for a prior remote workforce across the company, thanks to the firm's recent migration to the cloud. "Pre-pandemic, Equifax was in the midst of a three-year transformation," notes Farshchi. "We rebuilt the technology stack and security controls from the ground up, so we had the right tools and processes in place to shift gears and support a far larger remote workforce."

In addition to gaining a newfound leverage over key aspects of the technology agenda, CISOs are gaining influence across the business. The change in working and purchasing habits means that security has emerged as a key differentiator for the Board, who are frequently consulting the CISO on a broad range of topics such as information security risk, business security risk, and cloud investment.

Additionally, as remote work evolves into a more permanent, hybrid model for enterprises, CISOs are being consulted on investment decisions tied to real estate. Given the various solutions that have been put in place to enable a secure remote workforce, many CISOs see the benefits to sustaining it, like access to better talent. Many organisations are indeed finding that a location-agnostic approach to hiring increases the candidate pool and raises the bar on the type of talent they can attract. As such, the CISO will need to maintain that platform and continue to strategically align with the business – a task that has proven more difficult for CISOs when there is a generational gap between key decision makers. For senior executives who are less comfortable with technology, articulating urgency over email or chat can be difficult in the absence of face-to-face meetings.

> "There are so many more industries recognising the importance of technology as a result of the pandemic, and therefore the importance of CISOs, thus creating much more demand. As this demand continues to grow, the demands on CISOs continue to evolve including the talent agenda becoming ever more challenging."
>
> **Jason Mallinder** is the Group CISO at Credit Suisse in London, UK

Indeed, internal tensions exacerbated by the pandemic have created a need for CISOs who have the soft skills to communicate across the business and manage distributed teams. As a result, cybersecurity leaders are flexing their EQ muscle. "The number one change post-COVID, is that cyber leaders will need to be more compassionate team members," notes the Global CISO at one of the largest banks in the US. "CISOs will need to prioritise making sure employees stay connected to each other and to leadership."

The resiliency that CISOs have shown throughout the pandemic has been in lieu of IT budget cuts and reduced cybersecurity spend. Given the element of fixed cost to security, the K-shaped recovery[03] from COVID is poised to widen budgetary gaps as a percentage of IT spend between larger enterprises and small-to-medium sized companies. With less discretionary budget for security, SMEs may risk losing their cybersecurity talent to larger competitors who can afford to absorb greater fixed and relative costs associated with security.

Reporting Lines

While reporting lines for the CISO are slowly shifting, what is clear is the CISOs continued elevation higher in the organisation. Depending on the size and culture of an organisation, the CISO can report into the Chief Operating Officer (COO), the Chief Information Officer (CIO), the Chief Risk Officer (CRO), or in some cases, the Chief Executive Officer (CEO).

CISOs still overwhelminglyly report to the head of technology. Proponents of this reporting structure argue that the elevation of the CISO goes hand in hand with the elevation of the technology head: as the CIO takes a seat on the executive committee, the CISO is properly situated as their direct report.

For others, a direct reporting line into the technology office can pose a conflict of interest. It is crucial for the CISO to report to different leaders, where they may have the most visibility, clear accountability, and separation of budgets. A CISO at a US healthcare provider we spoke to advocates for the CISO to sit under the Risk office; additionally, they do not believe CISOs should report to a CIO unless the company is culturally mature enough to treat their CISO as an independent leader around risk management.

Will the CISO reporting into the CEO ever be the norm? Ultimately, reporting level is tied to the culture and size of an organisation. For companies that have given the CISO a broader remit, such as overview of trust, it's a definite possibility. An example is Jamil Farshchi, CISO at Equifax. In some SMEs (FTE>1000) we already see this trend emerging, with 59% already reporting to the CEO.
The more visible and financially-measurable impact of ransomware, breaches and loss of public trust is playing, the closer a CEO may want their CISO by their side. In larger companies where the CISO reports to the CEO, it is often because a breach or failure in information security governance has already occurred, and the CISO was appointed to the Executive Committee as a responsive measure.

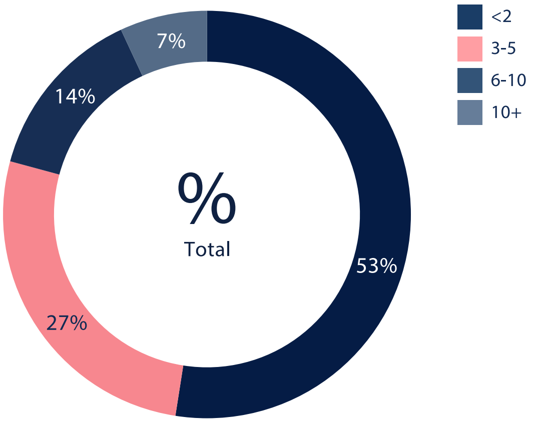
> "The CISO should sit within the Risk office until cybersecurity is no longer a risk. The CISO should only report to the CIO if the organisation is culturally mature enough to treat them as an independent leader where risk management is concerned."
>
> **Group CISO** at a leading US healthcare provider

Tenure

CISOs are in high demand and tough to retain: 53% of CISOs at large global enterprises have been in their current role for two years or less, meaning they assumed a new position during the COVID-19 pandemic. Within the concentration of CISOs who assumed a new role during the pandemic, 67% joined a different company, while just over a third took on an expanded role at their current firm.

The changing face of cybersecurity leadership across top global enterprises during the pandemic has to be attributed, in part, to the increase in data breaches and the growing cost these incur for enterprises. IBM estimates that a typical data breach now costs $4.24 million per incident for corporations - a 10% increase from the previous year.[04] Despite any movement tied to a material breach, the rate at which CISOs are turning over is still significant.

Tenure (Years)



53%

of CISOs have been in their role for two years or less, meaning they assumed a new role during the COVID-19 pandemic

High turnover for the cyber chief is often tied to compensation. The CISO salary is increasingly competitive and will regularly reach heights of over $2m in sectors like Banking and Asset Management, especially in the major financial hubs, such as New York City, San Francisco, Charlotte, Boston, London, and Switzerland, amongst others. Typically, CISOs working within multinational organisations receive even higher compensation to counter threats across multiple time zones and keep company data secure in locations around the world.

Other factors attributed to CISO turnover are poor culture and lack of resources. To retain CISOs, organisations need to work on building a culture that emphasizes cybersecurity, within IT but also more broadly. CISOs need to be given the platform and bandwidth to drive the cybersecurity agenda across the enterprise. In this vein, organisations need a cybersecurity budget that will enable CISOs to build and drive a sustainable cyber programme.

"This isn't the place to be cutting corners, reducing mandates or squeezing budgets," notes James Larkin, Partner at Marlin Hawk, "Many times we've helped CEOs bring in a new CISO following a breach, you can directly trace the genesis of the issues back to an information security department that is worryingly thin. Each industry is different, but if your information security budget is less than 5% of your total IT spend, you're making yourself a target. If you are in an industry that cyber-criminals see as appealing, then you'll want to double that ratio."

> "The CISO's number one responsibility is providing an independent voice. The role requires self-awareness and humility; good CISOs are willing to admit to themselves and others when they don't have the same set of fresh eyes as day one."

Craig Froelich is the CISO at Bank of America in North Carolina, USA

Succession

Reduced tenure and a growing mandate have led to a widening gap between the CISO and their number two, making one thing clear: maintaining a healthy pipeline of cyber talent is the primary risk facing today's cyber organisations.

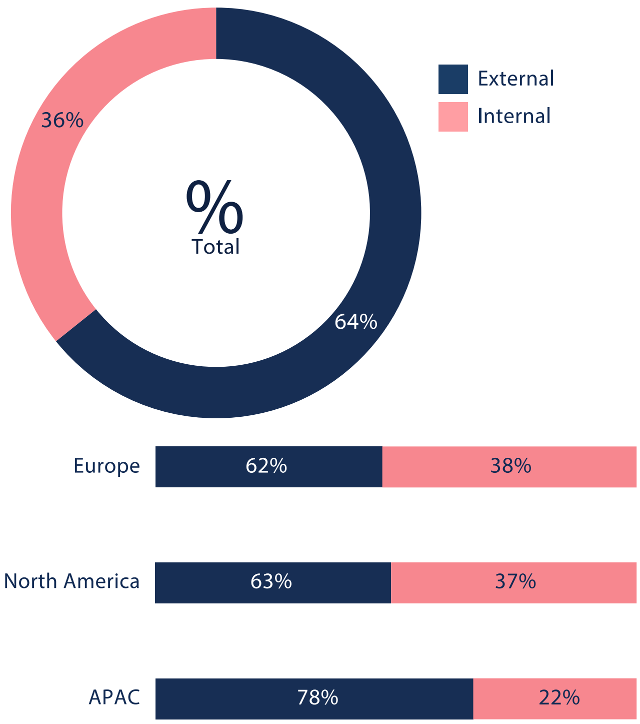
More broadly, 64% of CISOs at the large global enterprises analysed by Marlin Hawk were hired externally. The succession gap is largest in the Asia Pacific, where 78% of CISOs were hired from another firm. The margin decreases but remains high across North America and Europe, where more than 60% of CISOs were hired externally.

64%

of CISOs at the large global enterprises analysed by Marlin Hawk were hired externally

Type of Hire

External versus Internal



Organisations have generally opted to recruit externally for a CISO, partly driven by the need for external validation and 'outside in' thinking. Historically there has also been a mentality of hiring 'big hitters', or well-established CISO's, whose track record might better position them to respond in the event of a crisis.

Retaining mid-level talent is increasingly challenging for large organisations with established cyber functions, where cyber talent on the CISO's succession slate are opting to join small- or mid-cap companies as a top CISO. Because these organisations may consolidate Cyber with Risk or other areas of Security, they can offer mid-level cyber executives a more senior role with broader ownership.

In addition to gaining broader exposure across relevant functions, CISOs of small- or mid-cap companies also gain access to the company's top leaders. A recent study by IDG indicates that only 22% of CISOs at large enterprises report to the CEO, versus 59% of top security executives at SMBs with 1,000 FTE or less.[05] This elevation of the CISO is indicative of the fact that smaller companies are more concerned with the material and financial impacts of a breach than large enterprises capable of assuming any loss.

Even when plans for succession are made, they're rarely followed. Many of the CISOs that Marlin Hawk spoke to report a discrepancy between a slated successor and the candidate who is named to the role. This breakdown in the succession planning process is likely due, in part, to a lack of exposure by potential successors to the Board. Despite the current failure of existing succession plans for the CISO, many of the cybersecurity executives that Marlin Hawk interviewed believe that cybersecurity organisations should have a succession plan in place.

To ensure succession plans are followed, CISOs should take steps to give their direct reports a chance to form meaningful relationships with leadership and to broaden their exposure across the enterprise.

"There are so many more industries recognising the importance of technology as a result of the pandemic, and therefore the importance of CISOs, thus creating much more demand," says Jason Mallinder, Group CISO at Credit Suisse. "As this demand continues to grow, the demands on CISOs continue to evolve including the talent agenda becoming ever more challenging."

Diversity in the CISO Function

Settling for a homogenous CISO department is, in itself, a security risk. Beyond the fact that it is important to provide equal opportunities for all, hiring individuals purely from one demographic will significantly decrease an organisation's ability to predict, prepare and respond accurately to threats. In order to best understand their attackers, companies must furnish themselves with a diverse range of different security experts, all capable of thinking and responding in different ways.

Presenting a diverse shortlist is good practice for any recruiter, but D&I has emerged as a top priority for many clients as well. There is high demand for senior candidates who identify as either female, non-binary, or BAME (Black, Asian and minority ethnic). This demand has been driven, in part, by the social justice movements that dominated the popular consciousness throughout the COVID-19 pandemic.

It is of little value to our readership for Marlin Hawk to state that there is a distinct lack of diversity in the information security space. According to Marlin Hawk's research, women account for just 14% of information security leaders while non-white candidates account for just 21% of CISOs at large global enterprises. Without a doubt, this disparity needs to be addressed, however the issue is often compounded beyond that of equivalent roles across other functions in an organisation.

One trend currently emerging is the industry's inability to address the inclusion element of D&I. While a number of organisations have made significant improvements when it comes to diversity, many have still yet to tackle the issue of how to then integrate diverse talent into their structure. Imposter Syndrome is rife when diversity is low, and diverse candidates will often feel isolated if they cannot identify or connect with their peers. Within information security, where diversity is already an issue, this is prone to creating a vicious cycle of self-fulfilling prophecy.

It has widely been reported that working from home is here to stay. This has – naturally – increased flexibility when it comes to personal versus professional lives, and some within the executive search industry have hailed it as an opportunity for female leaders to progress further and faster in their careers. Marlin Hawk has frequently commented on the fact that women are more likely to take their family and spousal working requirements into consideration before contemplating a relocation or accepting a job that would require significant travel; however, other reports have urged caution, stating that longer-term female employees are less likely to return to the office than their male counterparts and may risk missing out on valuable face-to-face interactions.[06]

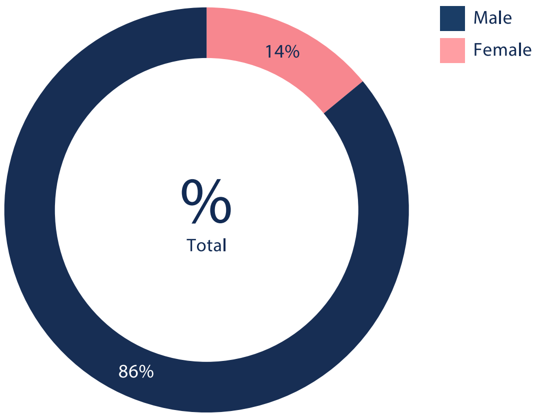
14%

of CISOs at the large global enterprises analysed by Marlin Hawk are women

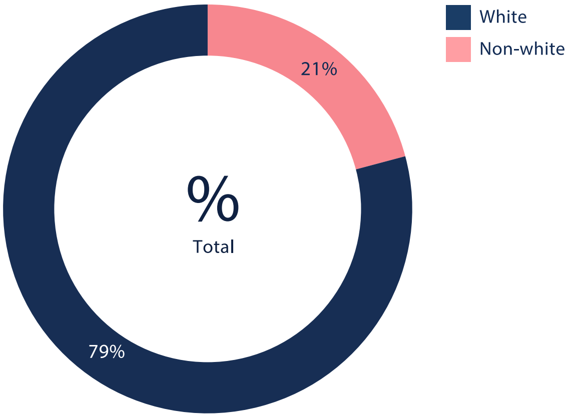
21%

of CISOs at the large global enterprises analysed by Marlin Hawk are non-white

Gender Diversity



Ethnic Diversity



From a strictly information security perspective, concerns have also been raised regarding the ability for a CISO to tackle threats remotely. According to one CISO at a US healthcare provider, "Remote work has undoubtedly made it more challenging for CISOs to articulate urgency, versus being able to have those conversations face-to-face." Despite the undeniable challenges to remote work for cybersecurity experts, there are some upsides to a more flexible work-from-home policy. According to Raheja, "When measuring up against the risk, there is a real business value introduced by a longer-term shift to remote work and maintaining a distributed workforce." While many CISOs still believe that the best way to address and solve security issues is to travel and respond in person, companies should also consider the potential benefits gained from the broader access to diverse talent that is enabled by remote working.

The Changing Role of the CISO

While once a role dependent mostly on technical subject matter expertise alone, CISOs are now embracing a hybrid remit including soft skills like influence, negotiation, people leadership, and having broader interactions with the business about strategy and customers. This move allows for greater variety when it comes to the acceptance of different educational backgrounds. While once upon a time a CISO would have been expected to have studied a STEM subject, other degrees and qualifications may now be considered. In the US, women earned 22% of all bachelor's degrees in engineering and 19% of all bachelor's degrees in computer science; Black students earned 7% of STEM bachelor's degrees; and Hispanic students earned 12% of STEM bachelor's degrees.[07] In the UK, women account for only 35% of STEM students[08], while black students account for only 6.2%.[09] Twenty years ago, these figures were significantly lower, and therefore those now reaching the age whereby they might consider a CISO position are likely to be even less diverse.

By expanding the role and diversifying the skillset, organisations allow diverse candidates who may previously never have considered the role to contemplate the possibility of a career as a CISO.

James Larkin, Partner at Marlin Hawk adds, "We cannot go back in time and add to the graduating classes of the '80s, '90s, or '00s. If organisations want to bolster their cyber talent ranks, while maintaining the technical watermarks already set, then internal training, management rotations, accreditation and broader career experience have to be taken into account. Otherwise, we will see a continued supply shortage for another decade waiting for the next generation of leaders to arrive."

"When measuring up against the risk, there is a real business value introduced by a longer-term shift to remote work and maintaining a distributed workforce."

Aman Raheja is the CISO at Humana in Washington D.C., USA

The Future CISO

Digitalisation has spurred the rapid growth of the CISO role in a relatively short period of time. Five years ago, information security was the core of the role; today, the CISO’s mandate extends out into areas like business risk, operational resiliency, product design and technology architecture.

“There is a technology strategist role that is continuing to emerge,” says Glenn Foster, CISO at TD Bank Group, “It goes beyond the security stack more broadly into questioning trust in our legacy technologies and where we need to make investments to mitigate against those risks. Where the CIO would traditionally be leading conversations about operational efficiency, you now see the CISO championing them too.”

Within industries that have greater financial and reputational risk, data security, and data monetization have naturally pooled within the CISO’s mandate. In the technology industry, questions about the use of customer data have fueled organisations to establish a clearer link between digital trust and data privacy by expanding the CISO role into that of a Chief Trust Officer.[10]

To be successful in the role today, cyber chiefs need to be more than just good technologists. Business leadership and talent management are now on par with subject matter expertise. CISOs need to able to lead large, distributed teams and be capable of influencing across multiple facets of the enterprise, including the CEO and Board.

> “There is a technology strategist role that is continuing to emerge… Where the CIO would traditionally be leading conversations about operational efficiency, you now see the CISO championing them too.”
>
> **Glenn Foster** is the CISO at TD Bank Group

This growing need for cyber chiefs with high calibre leadership skills is evidenced by the fact that 46% of CISOs with a higher degree opted to study Business Administration or Management.

46%

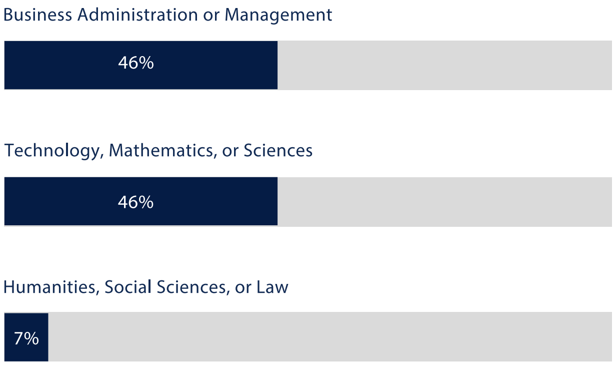
of CISOs with a Masters or PhD pursued a degree in Business Admininstration or Management

68%

of CISOs have experience across two to three industries. Only 15% of CISOs have experience across one industry.

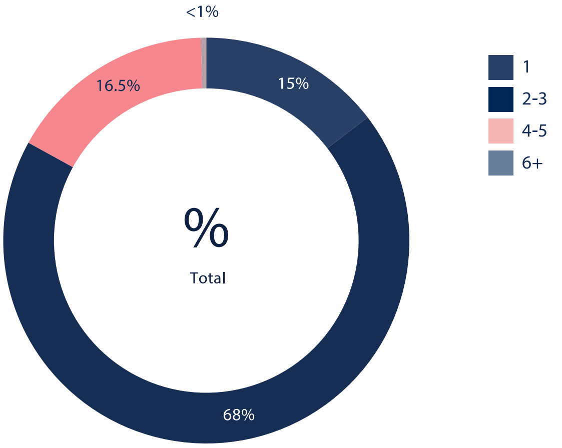
Higher Education

Areas of Study for CISOs with a Masters or PhD



Industry Exposure

Number of Industries where a CISO has worked



While we are seeing more CISOs turn to education to round-out their soft skills, hands-on experience and a fundamental security mindset will continue to be an important criteria.

CISOs across the large global enterprises analysed by Marlin Hawk possess an average of 25 years of experience. Only 3% of CISOs have 10 to 15 years of experience, and just under 20% have a career that spans more than 30 years - pre-dating the origin of the CISO role itself.

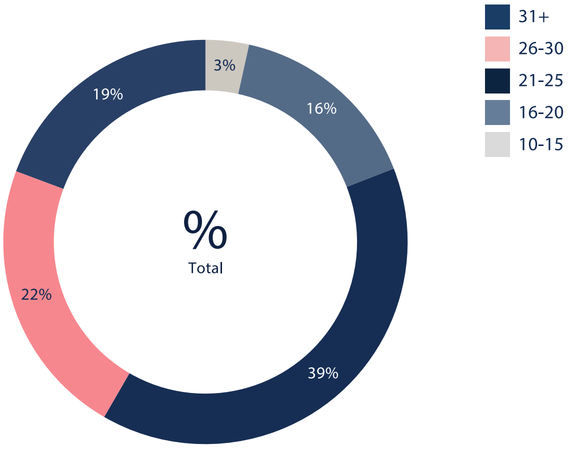
Given the complex nature of the threat environment for large enterprises, CISOs are increasingly expected to have experience working across multiple industries. The vast majority of CISOs that Marlin Hawk analysed have experience across two to three industries, whereas only 15% of CISOs have stayed within one industry.

25 years

of experience is the average for CISOs at large global enterprises

Career Experience

Total number of years experience



Board and Non-Executive Representation

Despite the fact that cybersecurity has emerged as a key priority for many corporate boards, representation of CISOs at the board-level is low. Recent Marlin Hawk research reveals that only 1% of Boards include an executive that has spent the majority of their career as a CISO. Rather, information security leaders typically transition to the Boards of IT security providers, security platform companies, technology companies, or move to government posts. This distinct lack of cyber security oversight on the Boards of Fortune 100, FTSE 100 and other major listed organisations, is concerning.

“Lack of CISO representation on corporate boards is a big oversight and a missed opportunity for companies,” notes the Global CISO at a Fortune 500 insurance provider. “Helping your CISO gain a Board seat can have positive impacts on talent development and serve as a tool for retention.”

Many CISOs emphasize the importance of at least including CISOs on advisory boards, which is where security executives tend to sit. CISOs may also chair the risk and controls committee for IT subsidiaries or technology companies where their employer holds a majority stake. Regardless of whether cyber talent is represented on the board, CISOs attested to the value of educating the board on how to ask insightful questions related to cyber security.

“The size of the boardroom table continues to grow, as governing a modern corporation continues to become more complex, and less rooted in the purely financial lenses of the past,” says James Larkin, Partner at Marlin Hawk. “If companies aren’t ready to add another seat (for the CISO) to their Board, then councils and committees must bridge this gap until they are – be it internal, or advisory adjuncts to the Board. Starting with a cyber security & customer trust committee is a good first step. Technology governance, data privacy, customer trust and cyber risk are all starting to feel like different flavors of the same governance issue, and the issue is growing, not shrinking.”

Endnotes

01 Lederer, Edith. “UN reports sharp increase in cybercrime during pandemic.” Associated Press. 7 August 2020. https://apnews.com/article/virus-outbreak-counterterrorism-health-crime-phishing-824b3e8cd5002fe238fb9cbd99115bca

02 “COVID Cyber Crime: 74% of Financial Institutions Experience Significant Spike in Threats Linked To COVID-19 .“ Business Wire. 28 APril 2021. https://www.businesswire.com/news/home/20210428005365/en/COVID-Cyber-Crime-74-of-Financial-Institutions-Experience-Significant-Spike-in-Threats-Linked-To-COVID-19

03 Saraiva, Catarina. “How a k-shaped recovery is widening US inequality quicktake.” Bloomberg. 10 December 2020. https://www.bloomberg.com/news/articles/2020-12-10/how-a-k-shaped-recovery-is-widening-u-s-in equality-quicktake

04 “Cost of Data Breach Report 2021.” IBM. 28 July 2021. https://www.ibm.com/security/data-breach

05 Fruhlinger, Josh. “Does it matter who the CISO reports to?” CSO. 23 March 2021. https://www.csoonline.com/article/3278020/does-it-matter-who-the-ciso-reports-to.html

06 Partridge, Joanna. “Switch to more home working after Covid ‘will make gender inequality worse’.” The Guardian. June 2021. https://www.theguardian.com/business/2021/jun/19/switch-to-more-home-working-after-covid-will-make-gender-inequality-worse

07 Kennedy, Brian. “6 facts about America’s STEM workforce and those training for it.” Pew Research Center. 14 April 2021. https://www.pewresearch.org/fact-tank/2021/04/14/6-facts-about-americas-stem-workforce-and-those-training-for-it/

08 “Women in STEM. Percentages of Women in STEM Statistics.” Stem Women. 22 January 2021. https://www.stemwomen.co.uk/blog/2021/01/women-in-stem-percentages-of-women-in-stem-statistics

09 “BAME Women in STEM.” Stem Women. 02 March 2021. https://www.stemwomen.co.uk/blog/2021/03/bame-women-in-stem

10 Salvatore, Stolfo. “Make Room for the Chief Trust Officer.” Forbes. 2 March 2021. https://www.forbes.com/sites/forbestechcouncil/2021/03/02/make-room-for-the-chief-trust-officer-in-the-C-suite/?sh=78eabcc41d6a

MARLIN HAWK