INTRODUCTION

Cybersecurity Ventures estimates that there are 32,000 chief information security officers (CISOs) employed globally in 2023.

Steve Morgan, founder of Cybersecurity Ventures

The good news is that most large organizations have a CISO. The bad news is that most small businesses, and far too many mid-sized companies have been left by the wayside and they do not have a dedicated full-time leader focused exclusively on cybersecurity.

– Steve Morgan, founder of Cybersecurity Ventures and Editor-in-Chief at Cybercrime Magazine

2023 CISO HEADCOUNT REPORT

TABLE OF CONTENTS

A DIFFERENT TYPE OF CHIEF

The chief information security officer (CISO) role is vital to the enterprise but is also one of the most challenging positions in the cybersecurity industry.

A CISO's responsibilities can be difficult to define as they vary by industry and company. However, broadly, CISOs must oversee security operations, manage teams, follow board directives, drive forward new security initiatives, and handle cybersecurity incidents.

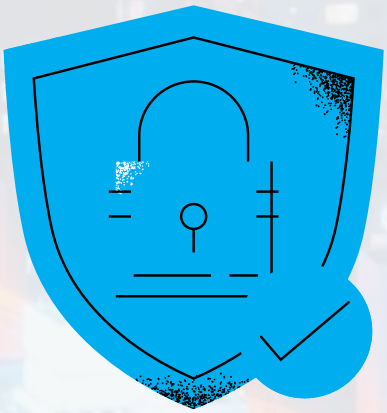
Over the years, CISOs have forged a pathway connected, but different to, other executives such as Chief Information Officers (CIOs). CISOs must be able to build bridges between technology, business operations, staff, policy, and compliance, and as such, the modern CISO is now set apart at the executive level.

100 percent of Fortune 500 companies employed a CISO in 2022, together with the majority of Global 2000 organizations.

A DIFFERENT TYPE OF CHIEF

Cybersecurity Ventures estimates there are now at least 32,000 CISOs employed worldwide.

As a measure of how critical today's CISOs are, despite many having a short tenure due to the pressure of the role, CISOs are also transitioning to the C-Suite. The modern CISO is gaining recognition and their voices are being taken more seriously in a world where global cybercrime costs are expected to reach $10.5 trillion USD annually by 2025.



THE CISO ROLE

As internet adoption, the cloud, data protection, and the introduction of legislation designed to protect consumer data and hold organizations to account for their security hygiene evolve, so do the responsibilities and expectations of the CISO.

However, the term “CISO” only dates back to 1994, at a time when information security was emerging in response to the widespread adoption of the internet in homes and businesses.

Back then, U.S.-based investment bank and financial services giant Citigroup, then Citicorp, suffered a series of cyberattacks by Russian software engineer Vladimir Levin. Levin broke into Citicorp’s systems and, together with co-conspirators, stole over $10 million USD via wire transfers.

At the time, banks were racing to modernize and cut in-house costs by implementing digital means to handle payments and transfers.

THE CISO ROLE

The attack highlighted a growing need for digital system security and oversight. Citicorp established a dedicated cybersecurity center, and the role of CISO was born, with Steve Katz at the helm.

However, Katz's fate to be anointed the first-ever CISO could be argued as a poison chalice, as his employer disclosed the hack a short time after Katz accepted the position.

Still, the security expert stayed in the role for six years and set the standard for today's emerging CISOs. He still provides mentorship and advice to current and CISOs-in-waiting to this day.

Cybersecurity threats increased from the time the world's first CISO began his tenure.

The 2001 Code Red worm that targeted Microsoft servers was one of the first security incidents which required businesses to take heed of cyberattacks as an operational risk.

THE CISO ROLE

The internet chaos caused by this stack buffer overflow exploit was followed by the 2005 TJX Companies data breach, exposing the credit card numbers of over 40 million customers.

In 2010, we were introduced to state-sponsored cyber weapons with the development of the Stuxnet worm by U.S. and Israeli intelligence. In the same year, China's Operation Aurora highlighted the hacking of U.S. private sector companies.

By the late 2000s, businesses began following Citicorp's example and started hiring dedicated security officers alongside CIOs.

Just as Katz started with a background in programming and technology, the hiring of CISOs once focused on technical backgrounds; but now, "soft" skills are equally important.

As the enterprise familiarized itself with what cybercrime meant for business continuity and risk

THE CISO ROLE

management, governments began introducing new legislation that would permanently change the responsibilities of the CISO.

Introduced in 1999, the first U.S. law of note was the Gramm-Leach-Bliley Act, which required financial institutions to safeguard sensitive data.

By 1996, the Health Insurance Portability and Accountability Act (HIPAA) was signed to protect medical data, followed by 2003's Fair and Accurate Credit Transactions Act (FACTA), intended to reduce identity theft.

Other laws followed suit, holding organizations to a higher security and data protection standard. These included the Payment Card Industry Data Security Standard (PCI DSS) (2004), the Children's Online Privacy Protection Act (COPPA) (1998), the Cybersecurity Information Sharing Act (CISA) (2015), and the E.U.'s General Data Protection Regulation (GDPR) (2018).

THE CISO ROLE

Today's CISOs must combine technical expertise with business acumen, leadership, and an understanding of the law, auditing, risk, and incident response.

According to Cisco, security leaders report their top three areas of responsibility as CISO as leadership (35 percent), risk assessment and management (44 percent), and data privacy and governance (33 percent).

THE CISO COUNT

Zippia estimates, established through a database of 30 million profiles and verified against Census Bureau data, suggest over 7,523 chief security officers (an interchangeable term with CISOs) are "currently employed" in the U.S.

The Bureau of Economic Analysis estimates that in 2022, the U.S. Gross Domestic Product (GDP), an indicator of economic activity in a country, amounted to $25.46 trillion. Meanwhile, the International Monetary Fund (IMF) assessed 2022's global GDP as $105.5 trillion.

The 2022 FORTUNE 500 list suggests that the top businesses in the U.S. contribute approximately two-thirds of the country's GDP in terms of revenue.

According to Cybersecurity Ventures, 100 percent of Fortune 500 companies and the majority of Global 2000 organizations employed a CISO or an equivalent role in 2022, up from 70 percent in 2018.

THE CISO COUNT

Considering the economic influence of the largest, revenue-generating businesses able to impact a country's GDP – and the associated numbers of CISOs employed by them – we can estimate the global count of CISOs by analyzing the GDP of the U.S., the rate of CISO hiring in top companies, and global GDP.

Given that the U.S. alone generates over 20 percent of global GDP, we estimate there are at least 32,000 CISOs employed worldwide.

CISO SALARIES

According to Glassdoor data, the average annual salary for a CISO is $258,235, and Salary.com pegs the figure at $237,025.

Lower tier estimates, provided by Zippia, are in the $130,000 to $140,000 range.

Fortune 500 companies may be willing to pay a million dollars or more for the right candidate to head their security teams. Heidrick & Struggles estimate salaries at larger enterprises could be as much as $584,000 in the U.S.

Compensation generally rises along with company revenue and team size, according to Heidrick and Struggles. For a frame of reference, Cybersecurity Ventures publishes a list featuring CISOs at America's largest corporations.

Heidricks & Struggles notes that higher compensation did not necessarily correlate with longer tenure.

A FRACTION OF THE CISO

While all Fortune 500 companies and all 50 states now have a CISO, not every company in the U.S. has the capacity, revenue, or resources to hire a dedicated security officer full-time.

In a similar manner to industries that have evolved and implemented remote and outsourced processes, the role of the CISO has also diversified, alongside its requirements and responsibilities.

Some organizations may opt to hire “fractional” CISOs. These part-time officers work on-site, whereas “virtual” CISOs (vCISOs) provide on-call security strategy support, incident response leadership, governance, and more.

These options can be more affordable than a dedicated, full-time CISO. When we estimate how many CISOs are active, we should also remember that some security leaders may be working for multiple businesses simultaneously.

A FRACTION OF THE CISO

A number of CISOs may be more akin to contractors than full-time employees and there may be far more security leaders on duty than estimates can provide.

Furthermore, while the role of the CISO is critical, their duties may be integrated within a CIOs responsibilities, instead.

Based on Zippia estimates, there are over 69,420 CIOs employed in the U.S., compared to 7,523 CISOs. As a result, it is possible to estimate that around 90 percent of businesses with a full-time CIO have not employed a full-time CISO.

SMB RISK

The largest organizations face the highest risk of cyberattack due to their intellectual property, data, sprawling networks, and – in the event of a successful breach – their ability to pay potentially millions of dollars in ransom and extortion payments.

But we cannot forget that smaller organizations face cyber risks best tackled with dedicated cybersecurity staff. If small-to-midsized businesses (SMBs) are partners or suppliers of a large company, their lack of preparedness can also become a hazard, as they may provide a conduit for supply chain attacks.

We may have thousands of full-time and on-call CISOs operating worldwide, but millions of businesses cannot access this level of security leadership.

There are 31.7 million small businesses in the U.S., and SMBs account for 99.9 percent of them. Over 80 percent of SMBs are sole proprietors and have no employees. Despite this, 47 percent of the U.S.

SMB RISK

workforce is employed by small businesses.

It is estimated that over 600,000 new small businesses are opened every year in the U.S., and 100 million small companies open annually, worldwide.

Close to zero percent of these companies will employ a dedicated security officer, widening the chasm between adequate business protection and cyber threats every year.

CISO TURNOVER

The skillset and knowledge of today's CISOs command a high salary, but with the paycheck also comes a vast array of responsibilities and stressors.

Indeed, the average tenure for a CISO is only estimated at 18 to 26 months, a timespan far lower than the 4.9 years of the C-Suite.

Gartner estimates that by 2025, nearly half of cybersecurity leaders will change roles. 25 percent will transition to entirely different positions.

The talent churn can be attributed to workplace stressors, psychological pressure, and burnout, among other factors, such as poor organizational culture and low executive support.

A survey of 327 CISOs worldwide conducted by Heidrick & Struggles aligns with Gartner's predictions, in which stress and burnout were cited as the most significant personal risks CISOs face, coming in at 60 percent and 53 percent, respectively.

CISO TURNOVER

However, while it may have once been the case that assuming the role of a CISO could result in a job loss as the result of a breach, only 28 percent of respondents agreed with this statement, suggesting that the majority of today's security leaders feel relatively secure in their positions.

When a cybersecurity incident occurs, the blame may fall on the victim organization's security leaders and operation center members – regardless of whether the business has maintained strong security hygiene for years prior. This knowledge and pressure may contribute to security leadership talent shifting careers.

"CISOs are concerned they are not being supported at the board level," says David Jemmett, CEO at CISO Global. "There are many CISOs who have changed jobs who say they could not get the support they needed to strengthen an organization's cyber posture or there wasn't the funds or resources to fix what the problem was."

CISO TALENT POOL

CISOs are urgently needed to provide calm, clear leadership to protect our organizations. However, seeking out a new role as an existing CISO doesn't mean that skilled leaders can only move laterally – especially when the U.S. government wants more businesses to bring cybersecurity expertise to the board level.

The U.S. Securities and Exchange Commission (SEC) has proposed amendments to its rules to "enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies."

SEC Chair Gary Gensler says that changes to disclosure "reflect evolving risks and investor needs," and this requires a firmer hand in the formal disclosure of directors' oversight of cybersecurity risk, alongside management expertise in cybersecurity.

These changes could become a catalyst for the

CISO TALENT POOL

appointment of board members with cyber expertise – and proven CISOs would be a natural choice.

In a survey conducted by Heidrick & Struggles, 56 percent of CISO respondents in the U.S. – and 40 percent located in Europe – said that their next ideal role would be a board member.

Cybersecurity Ventures predicts that by 2025, 35 percent of Fortune 500 companies will have board members with cybersecurity experience. This percentage is projected to increase to over 50 percent by 2031.

The transition could be a challenge for some, however, as many boards prefer to appoint new members with prior board experience.

After examining the profiles of CISOs who currently hold corporate directorships, analysts suggest that the traits required for this transition are far more than just a long cybersecurity tenure.

CISO TALENT POOL

We may see a loosening of the reigns and appointment requirements in the coming years, especially with the prospect of the board potentially becoming personally liable for cyberattacks. Gartner predicts that by 2024, 75 percent of CEOs will be held personally liable for cyber-physical attacks.

INCLUSIVITY & RECRUITMENT

The cybersecurity industry is facing a talent shortage. Cybersecurity Ventures predicts that there will be 3.5 million unfilled cybersecurity jobs globally in 2023, and without inclusivity and new recruitment initiatives, we are failing to tap into the talent pool available to tackle the problem effectively.

Women held only 25 percent of cybersecurity jobs globally in 2022. While Cybersecurity Ventures estimates that women will represent 30 percent of the global cybersecurity workforce by 2025, there is an even broader gender gap in relation to CISO roles.

Indeed, recent research conducted by Cybersecurity Ventures shows that women held only 17 percent of top security jobs at Fortune 500 organizations. According to Zippa, only 11 percent of all CISOs employed in the U.S. classify themselves as LGBT.

Recruitment should reflect the need for diversity in all security roles, and leadership can play their part by developing inclusive recruitment programs.

INCLUSIVITY & RECRUITMENT

Cyberattacks are more diverse than ever before, and so the broader range of experiences and perspectives you can acquire for your security teams, the greater the opportunities for problem-solving and defense.

This concept will need to be applied to the board, too. As technology and attack vectors continue to evolve at breakneck speed, business leaders will need to adapt and utilize the experience and talent of our CISOs to a broader degree – and this may include giving them a seat at the table.

2023 CISO HEADCOUNT REPORT

SPONSORED BY CISO GLOBAL

“CISOs are concerned they are not being supported at the board level," says David Jemmett, CEO at CISO Global.

David Jemmett, CEO
CISO Global

"There are many CISOs who have changed jobs who say they could not get the support they needed to strengthen an organization’s cyber posture or there wasn’t the funds or resources to fix what the problem was. CISOs need to have a place at the C-level. The role of a CISO is very, very important. It goes across compliance, to offboarding and onboarding, to making [the company secure. are there to help companies protect themselves."

2023 CISO HEADCOUNT REPORT

ABOUT CISO GLOBAL

At CISO Global, cybersecurity is a culture, not a product.

We are on a mission to demystify and accelerate our clients' journey to cyber resilience, empowering organizations to securely grow, operate, and innovate.

At CISO, we partner with our clients wherever they may be on their cybersecurity journey, helping them to resolve any current roadblocks and adequately anticipate future issues to achieve cyber resilience and create a culture of cybersecurity across the organization.

To learn more, visit ciso.inc

CISO GLOBAL

2023 CISO HEADCOUNT REPORT

2023 CISO WORKFORCE & HEADCOUNT REPORT is written by Charlie Osborne, Editor-at-Large for Cybercrime Magazine. Steve Morgan, founder of Cybersecurity Ventures contributed.

Cybersecurity Ventures
83 Main Street, 2nd Flr., Northport, N.Y. 11768
info@cybersecurityventures.com