



EC-Council
Building A Culture Of Security

Certified CISO Hall of Fame Report 2023

CELEBRATING
LEADERSHIP
— **&** —
EXCELLENCE
IN INFOSEC

Meet the Top C-Suite Leaders and
Learn About Their Success Stories



Table of Contents

03	Acknowledgment and Foreword
04	Disclaimer
04	Terms and Conditions
06	About the Report
06	Key Findings
07	Introduction
08	Building a Stronger Defensive Posture
09	Invaluable Preparation for CISO Role
10	Certified CISOs Realize Greater Compensation
12	A Wealth of Experience from Industry Veterans
13	Geographically Diverse
14	A Broad Industry Reach
15	Certified CISOs Manage Substantial Security Budgets
16	Certified CISO Guide Major Investments in Cybersecurity
19	Major Challenges For Security Leaders
22	Greatest Areas of Concern in Cybersecurity
24	Certified CISO Contributions to the Cybersecurity Community
26	Certified CISO Hall of Fame 2023
27	Certified CISO Hall of Fame Winners' Organizations
29	Certified CISO Hall of Fame 2023 Awardees
29	America (North and South)
30	Asia
31	Europe and UK
31	Africa and Middle East
32	How the Certified CISO Program Enables Executive Leadership in Cybersecurity

34	Who Chooses the Certified CISO Program?
36	The Most Appreciated Program Components
38	Insights From Certified CISOs
40	Conclusion
40	About EC-Council
41	Certified Chief Information Security Officer (C CISO) Program
42	References



Acknowledgment and Forward

EC-Council is grateful for the contributions of the Certified Chief Information Security Officers (C|CISOs) who shared their experiences and wisdom. This report is based on an extensive online survey conducted among Certified CISO representing a diverse range of industries worldwide. The participants provided invaluable feedback on various topics that are highly relevant to senior security professionals, such as developing leadership skills, aligning security strategies with organizational objectives, and effectively countering evolving cyber threats.

The 2023 Certified CISO Hall of Fame Annual Report provides a captivating glimpse into the professional lives of security leaders who possess a unique blend of resilience and quick decision-making abilities necessary to thrive in a dynamic and high-stakes industry. They generously shared professional advice and openly discussed their personal experiences, offering valuable insights into their career paths. By highlighting their top concerns and sharing the security practices that have proven most effective in addressing them, they provide invaluable guidance. The viewpoints expressed by the Certified CISO of Fame winners, runners-up, and nominees included in this report will be immensely valuable to individuals aspiring to leadership roles in the cybersecurity field.

Disclaimer

This report is available to you on an as-is-where-is basis at the sole discretion of EC-Council, subject to the terms and conditions of use below (Terms of Usage). This includes the data and information in the report. This report has been produced based on the information collected as part of the Certified Chief Security Officer (C|CISO) of Fame survey and is, to the best of our knowledge to be true, reliable, and accurate. While EC-Council has made every attempt to ensure that the information contained in this report comes from reliable resources, EC-Council does not guarantee the accuracy of this report or make any other warranties or representations regarding it or the information contained therein. In addition, report updates may not be made available to you. The use of this report is at your sole discretion.

Terms and Conditions

EC-Council's intent in posting this report is to make it available for informational purposes and for the public's personal use. Without the prior written consent of EC-Council or unless indicated in the terms and conditions, neither the report nor any part thereof should be reproduced, distributed, copied, downloaded, displayed, republished, posted, or transmitted in any form, by any means. Data and information in this report may be reproduced based on certain conditions as follows:

- Disclaimers in this report shall be kept in their original form and applied to the data and information in the report.
- No modifications shall be made to the data and information.
- This report shall be identified as the original source of the data and information.
- EC-Council's website shall be identified as the reference source for the report's data and information; and the reproduction shall not be marketed or labeled as an official version of the materials in the report, nor as being endorsed by or affiliated with EC-Council.

EC-Council disclaims any representation or warranty, express or implied, as to the accuracy or completeness of the material and information contained herein, and EC-Council shall under no circumstances be liable for any damages, claims, causes of action, losses, legal fees, expenses, or any other cost whatsoever arising out of the use of this report or any part thereof, regardless of any negligence or fault, for any statements contained in or for any omissions from this report. By accessing and using this report, you agree to indemnify and hold EC-Council harmless from all claims, actions, suits, procedures, costs, expenses, damages, and liabilities, including attorneys' fees, brought as a result of misuse of the report or in violation of the authorizations as provided herein.

““

"The most impactful achievement after earning the Certified CISO was completing a transformative program fundamentally and redesigning the approach to Cyber Security at the BBC."

Justen Dyché
Head of Information Security, BBC

””

““

"Being selected as the CISO for the Social Security Administration, one of the best cybersecurity jobs within the U.S. government, was my most impactful achievement after earning the Certified CISO certification."

Joseph Stenaka
CISO, Social Security Administration, USA

””

““

"The most impactful thing after completing my Certified CISO credential was that I was appointed as Group CISO for a multinational and received Global Top 100 recognition."

Karin Hone
Groups CISO, Barloworld Limited South Africa

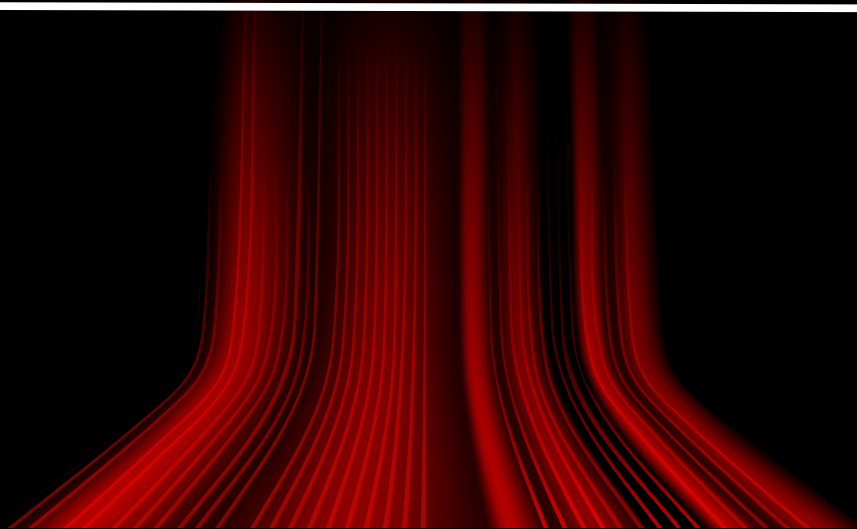
””

““

"I've been hired to the CISO position in one of the largest digital banks of Kuwait and the Middle East to protect their business against cyberthreats."

Nikolai Belstein
CISO, Bank Boubyan

””



About the Report

To gain insights into the qualities, perspectives, and practices of outstanding cybersecurity leaders, EC-Council conducted an in-depth survey in which 281 C-Suite leaders from the information security participated in its 2023 Certified CISO Hall of Fame Report. The questions covered a broad range of topics related to participants' personal and professional achievements in cybersecurity.

Key Findings

What the respondents say:

99% Reported that the Certified CISO training program vastly improved their cybersecurity leadership skills.

99% Reported that Certified CISO curricula aligns to the responsibilities of C-level cybersecurity positions.

99% Would recommend Certified CISO to colleagues and peers.

90% Gained confidence in their ability to align security strategies with organizational goals.

98% Affirm that the Certified CISO program empowered them to improve their organization's cybersecurity stance.

76% Experienced increase in compensation after obtaining Certified CISO.

60% Were able to bridge the gap between their organization's security team and the C-Suite.

100% contributed to the cybersecurity community in a meaningful way after becoming a Certified CISO.

Cloud Security was identified as the top area of concern.

These strong endorsements from C-Suite leaders highlight the impact that the Certified CISO program makes and the global acceptance of its standards as benchmarks for information security leadership roles.

Introduction

Today security leaders are particularly concerned about cyber threats, including ransomware, insider threats, financial fraud, nation-state attacks, and malware. While the core nature of these persistent problems remains consistent, the cybersecurity landscape is characterized by rapid change and volatility. Malicious actors are continuously discovering new ways to infiltrate systems and vulnerabilities that can be exploited are proliferating at an alarming rate. These conditions create an ideal environment for the development of innovative attack methods.

Many enterprises are rapidly accelerating their digitization plans and developing security policies and practices for the use of networks, devices, and processes that are not fully under their control, thanks to the recent shift to hybrid workforces.

As more organizations continue to adopt cloud technology, there is a growing need for developing effective cloud security strategies. In 2023, enterprises will likely invest more in cloud-native security solutions to protect their data and applications.

Organizations are embracing the zero-trust security model to verify resources and applications prior to allowing access. Many enterprises are investing in artificial intelligence (AI) and machine learning (ML) tools to fortify threat detection and response capabilities. Integrated security systems are gaining momentum as enterprises seek to simplify their infrastructures and encourage better collaboration between security teams and decision-makers.

Despite the shifting ground under their feet, some cybersecurity leaders have found ways to protect their organizations more effectively than ever and advance their careers in the process. One of the most reliable avenues to more solid and effective performance is education. High achievers often participate in credential programs that equip them with the knowledge, skills, and insights needed to adjust to changes with confidence.

EC-Council's Certified Chief Information Security Officer (Certified CISO) program is highly regarded among security professionals, offering numerous benefits that enable participants to effectively tackle the latest challenges in the field. Many Certified CISOs have gone above and beyond the requirements of their roles, not only delivering exceptional job performances but also making significant contributions to their communities.

The Certified CISO Hall of Fame stands as a testament to the remarkable talent and unwavering dedication of this distinguished group of CISOs. This report presents a compilation of survey responses provided by the 2023 inductees, runners-up, and nominees of the C|CISO Hall of Fame, all of whom hold the esteemed Certified CISO credential. The purpose of this report is to delve into the strategies employed by these exceptional security leaders not only to tackle but surpass the challenges they encounter in their day-to-day endeavors within the ever-evolving cybersecurity landscape.

Building a Stronger Defensive Posture

An astounding 99% of Hall of Fame survey respondents said the knowledge they gained from the Certified CISO program enabled them to better protect their organizations against cyber threats (Figure 1). Nearly 2 out of 3 realized a significant improvement in their ability to mount a strong cyber defense for their organization as a result of their Certified CISO training experience.

99%

better defended against cyber threats after completing the Certified CISO.

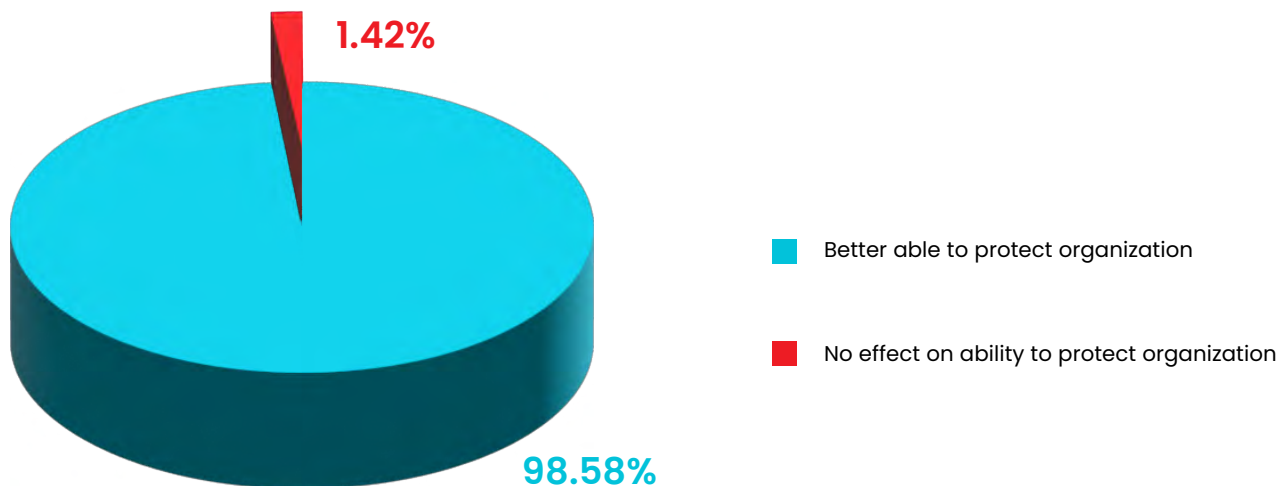


Figure 1: Program Effect on Protecting Against Cyber Threats

The knowledge, skills, and confidence Certified CISO participants gain enables them to excel in strategic planning, risk management, governance, incident management, and team leadership. These are the fundamental capabilities required to build a comprehensive defensive structure against malware, phishing, ransomware, advanced persistent threats (APTs), distributed denial of service (DDoS) attacks, and insider threats plaguing so many organizations.



"I developed an innovative security awareness program. In 12 months, it pushed the phishing failure rate down, from 30% to 9%, and the reporting rate up by 1,400%."

Federico Iaschi

Resilience Engineering Partner, Virgin Media O2



Invaluable Preparation for the CISO Role

Certified CISO participants were virtually unanimous in extolling the program's worth as preparation for taking on the CISO leadership role (Figure 2), thanks to its comprehensive curriculum, practical experience, peer learning, and industry recognition.

99%

said the Certified CISO program helps prepare professionals for a CISO role.

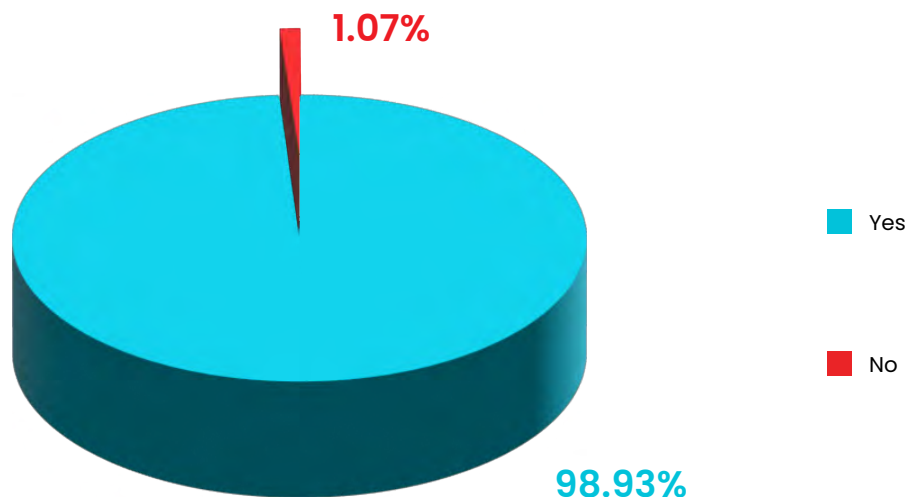


Figure 2: Preparation to Serve as CISOs



"After completing the Certified CISO program, I achieved the CISO title, and I was recently included in a list of the Top 100 CISOs in North America."

Nabeel Yousif
CISO, Flexiti



"I became Chief of Cybersecurity and Data Protection for a company with more than 90,000 employees."

Leonardo Resende Carvalho
Chief, Cybersecurity, Correios



Certified CISOs Realize Greater Compensation

76% achieved a salary hike after becoming a Certified CISO.

A whopping 76% of Certified CISO Hall of Fame nominees experienced a salary increase after successfully completing the Certified CISO Certification program. The majority enjoyed boosts of 10% or more, with 29% scoring salary hike greater than 20% (Figure 3). These rewards are understandable, as organizations often reserve the most attractive salaries for CISOs with the right skillsets. The top-performing CISOs are not focused exclusively on the technical side of their roles—they excel as business leaders. In fact, leadership and strategy are more important capabilities for today's CISOs than expertise in every aspect of cybersecurity.

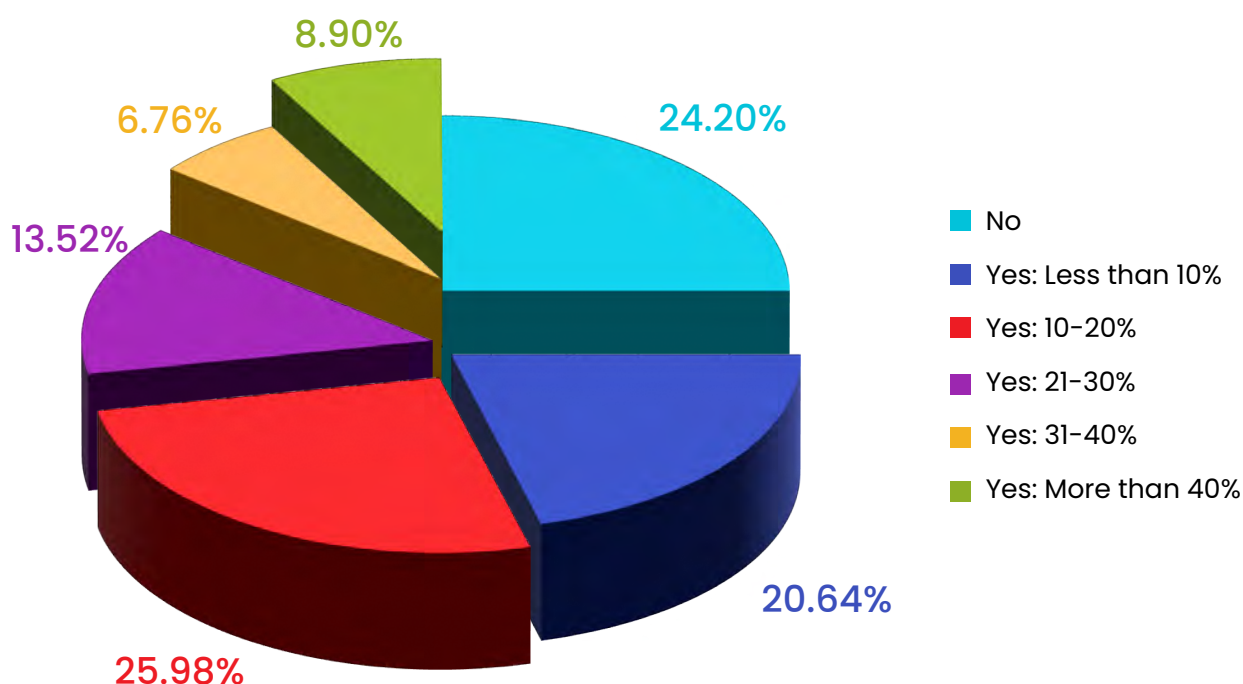


Figure 3: Salary Hike

Traditionally, leadership skills are learned on the job, but knowledge gaps often occur as practitioners move from middle management to senior and executive roles. The Certified CISO program bridges technical knowledge and critical executive management skills, enabling cybersecurity professionals to make a successful transition to the top levels of information security management.

By completing the Certified CISO program, participants gain a comprehensive understanding of the skills and knowledge required to lead and manage an organization's security program effectively. The program guides participants in developing a comprehensive security strategy, aligning it with business objectives, managing the security program, making informed decisions about security technologies, and complying with laws and regulations. Participants learn how to manage human capital, oversee audits, and maintain responsible financial stewardship. This knowledge is highly valued by employers, and it positions Certified CISOs as valuable assets to their organizations.

“

"After earning my Certified CISO, I used my management abilities to fill gaps in time-sensitive and critical projects, as well as to establish security controls to align risk and compliance policies and develop failproof strategic planning. In less than six months, I was promoted to Chief Technology Officer."

Atif Munir

Chief Technology Officer, Quadrangle Development Corporation

”

“

"I was hired to rebuild the entire security program for a \$1 billion-plus retail company and healthcare provider that was being purchased. The challenge was enormous but highly rewarding. As a result of my success, I was promoted by our new parent company to oversee the retail and healthcare operation, along with several other national and international lines of business."

Sean Walls

CISO, VSP Vision

”

“

"Certified CISO can differentiate me from other professionals in my field. It shows I have a demonstrated commitment to understanding and excelling in my profession. It gives me an advantage, which is particularly important in today's competitive market."

Gerry Ligon

Head of Network Architect, Dept of Defence Australia

”

The Certified CISO program transfers critical knowledge to participants, enabling them to pursue organizational strategies in the safest, most secure manner possible. The Certified CISO program was designed by CISOs and is guided by advisory and international boards to deliver excellence based on operational experience and program management expertise.

A Wealth of Experience from Industry Veterans

All nominees were senior cybersecurity leaders with five years or more experience in the security field, and a commanding majority had more than 10 years of experience. Roughly 20% had worked as security professionals for more than 20 years.

80%

had more than 10 years
of experience.

20%

had more than 20 years
of experience.

More than half of the participating Certified CISO were either CISOs, directors, department heads or held comparable leadership positions.

Over 53%

held leadership roles at their organization.

These experienced professionals can more easily identify potential threats and more effectively develop solutions tailored to the specific needs of their organizations. Their ability to understand the nuances and details of complex cybersecurity challenges can make all the difference in a field where even the smallest mistake can have significant consequences.



"The ability to establish positive internal and external C-level and boardroom relationships to effect significant change and drive a cybersecurity risk management strategy forward while enabling organizational growth are my most significant achievements."

Bob Fabien Zinga

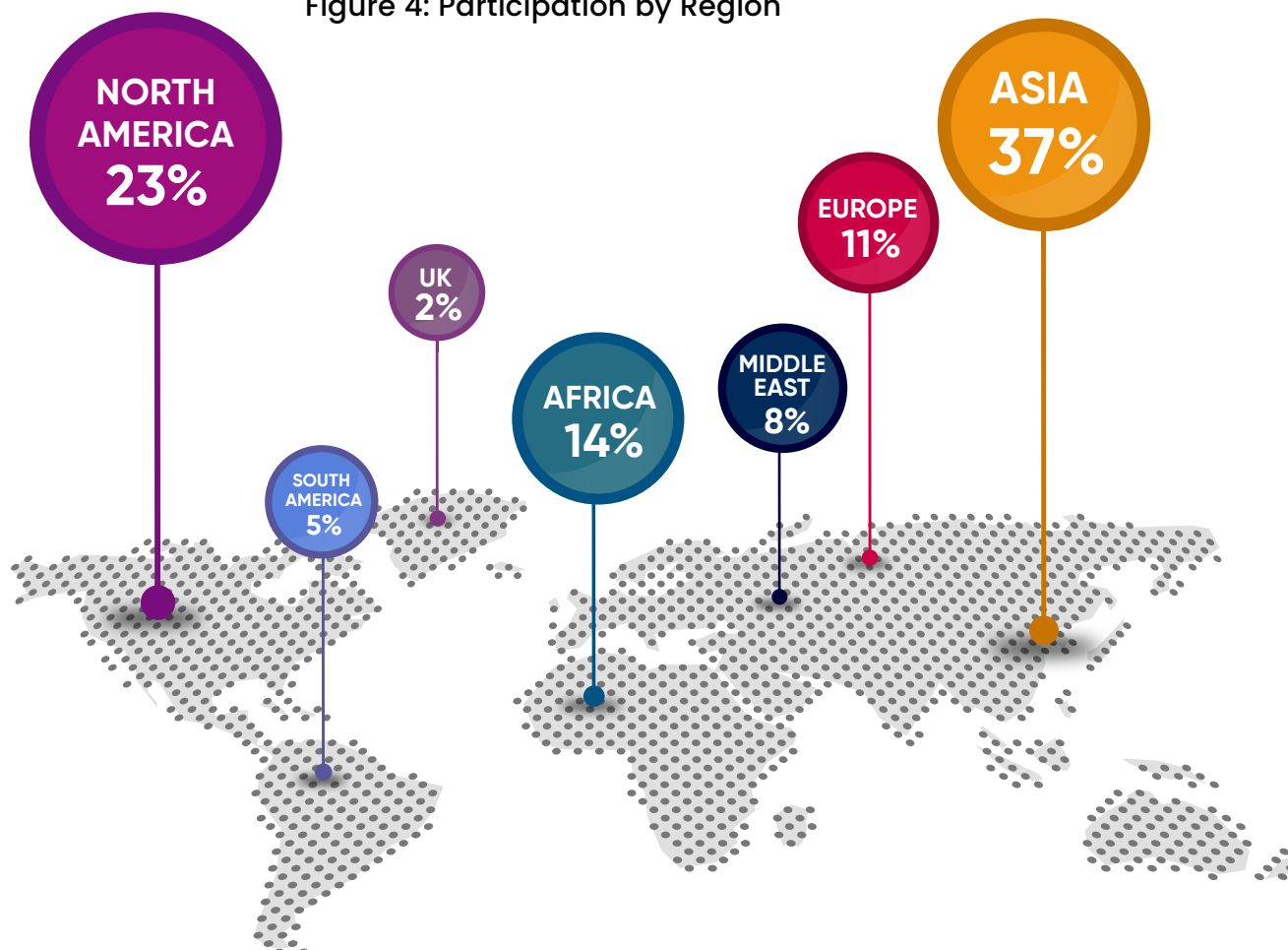
Head of Security Architect, U.S. Navy Reserve



Geographically Diverse

The Certified CISO Hall of Fame survey respondents were dispersed across every region of the globe, with the highest concentrations in Asia and North America (Figure 4). With rapid development of technology and digitalization, Asia is increasingly vulnerable to cyber threats. North America faces significant cybersecurity challenges due to the advanced technological infrastructures, large-scale businesses, and high-value targets in the United States and Canada. In Africa and the Middle East, critical infrastructure, government agencies, and businesses are subject to a growing onslaught of cyberattacks. Europe is also facing significant cybersecurity challenges, particularly with the rise of cybercrime, state-sponsored hacking, and the growth of IoT devices.

Figure 4: Participation by Region



As Figure 4 shows, professionals from all over the world are developing the leadership and technological skills necessary to bolster security in their regions by participating in the Certified CISO program. Its global reach means that talent is being widely dispersed, helping to alleviate the pressure created by the ongoing cybersecurity skills gap.

A Broad Industry Reach

The Certified CISO Hall of Fame nominees were employed primarily in technology, financial services, government, retail, healthcare, education, transportation and automotive, and entertainment and hospitality, as shown in Figure 5.



Figure 5: Representation by Industry

Almost 50% were from technology fields, including cybersecurity, cloud services, software solutions, managed IT services, systems integration, and security software/hardware development. At one-fifth of the total, 20%, financial services were also well represented, including professionals in banking, insurance, auditing, and payment processing roles. 12% of the Certified CISOs surveyed held leadership positions in government organizations, in both military and nonmilitary settings.

Because every industry is plagued by cyberattacks, it is essential for organizations of all sizes and in all sectors to have well-developed cybersecurity defenses. Leaders who complete the Certified CISO training are especially capable of ensuring that their organizations will implement the highest levels of data protection and regulatory compliance, and that they will have strategies in place for business continuity in the event of a disruption. CISOs have the knowledge to develop effective strategies and make intelligent investments in tools that will reinforce customer trust and help them stay abreast of the changing currents in the cybersecurity world.

Certified CISOs Manage Substantial Security Budgets

Cybersecurity is a critical investment for organizations of all sizes and industries, as cyber threats increase in number and sophistication. CISOs and other security leaders are expected to manage sizable budgets, optimizing investments to get the best return possible for organization expenditures. More than two-thirds of the Certified CISO Hall of Fame survey respondents were responsible for budgets in excess of USD 5,00,000, while more than half year managed budgets of USD 1 million or more—some approaching the USD 20 million mark.

As Figure 6 shows, 32% of CISOs surveyed managed annual budgets of less than 500,000 USD. 23% percent were responsible for 500,000–1,000,000 USD; 15% for 1–2 million USD; 12% for 2–5 million USD; almost 8% for 5–10 million USD; 5% for 10–20 million USD; and 5% for 20 million USD or more. More than two-thirds of the CISOs who controlled budgets of 10–20 million USD were in the technology, government, and financial services industries.

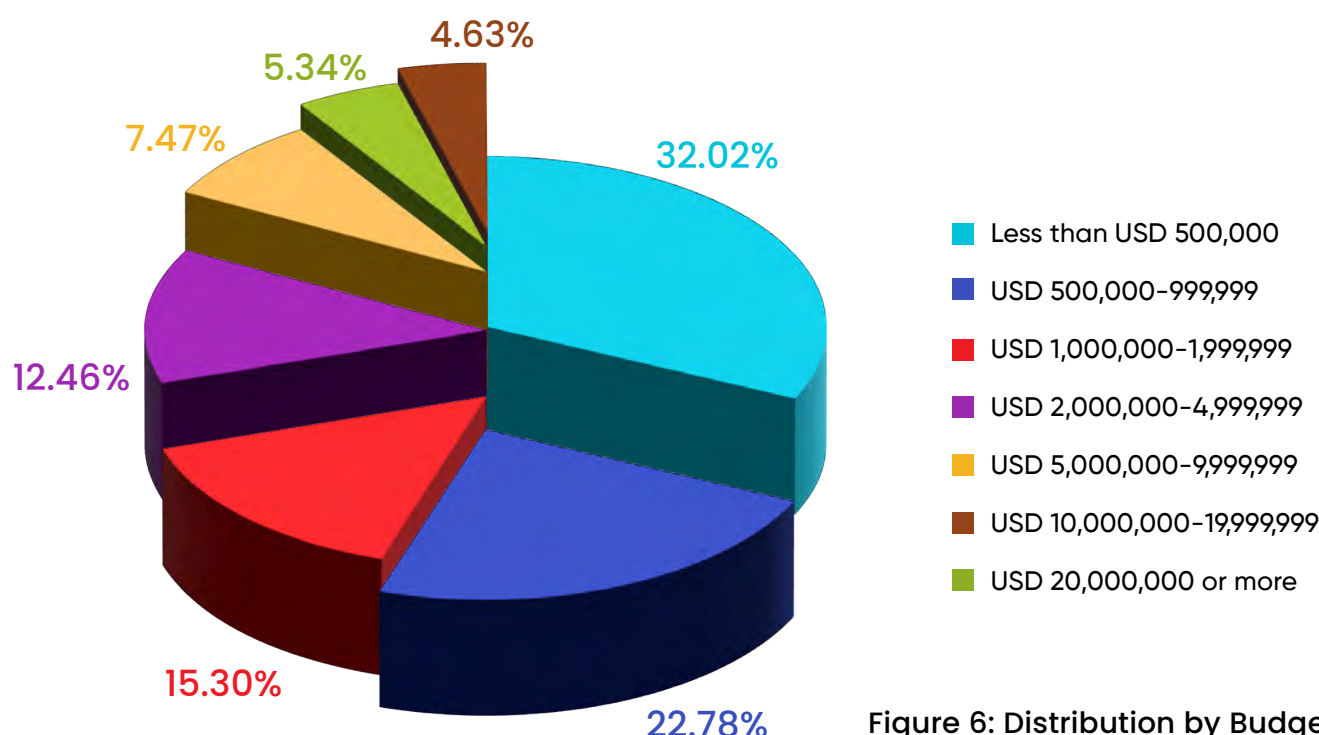


Figure 6: Distribution by Budget Size

Security spending is expected to top USD 188 billion in 2023, according to Gartner (Gartner, 2022). The research firm highlighted the increase in remote work, the increased adoption of Zero Trust Network Access (ZTNA), and migration to cloud-hosted models as the three most significant drivers of growth.

Certified CISO Guide **Major Investments** in Cybersecurity

Effective cybersecurity leaders recognize that not aligning security strategy with business goals carries the risk of heavy consequences, whereas a good cybersecurity strategy helps organizations improve profitability and avoid litigation. How well an organization manages its cybersecurity depends largely on the CISO's ability to design a convincing strategy and win buy-in from the board of directors.

63%

allocated more than 5% of their overall budget for security.

37%

allocated more than 11% of their overall budget for security.

3 out of 5 of the 2023 Certified CISO Hall of Fame nominees said their organizations spent more than 5% of their annual budgets on security. At least 37% spent more than 11% to shore up their cyber defenses. 17% of the respondents said their organizations devoted more than one-fifth of their annual budgets to cybersecurity spending (Figure 7). The actual percentages could be somewhat higher, though, as 12% of respondents did not know how much of their organizations' budgets were devoted to cybersecurity investments.

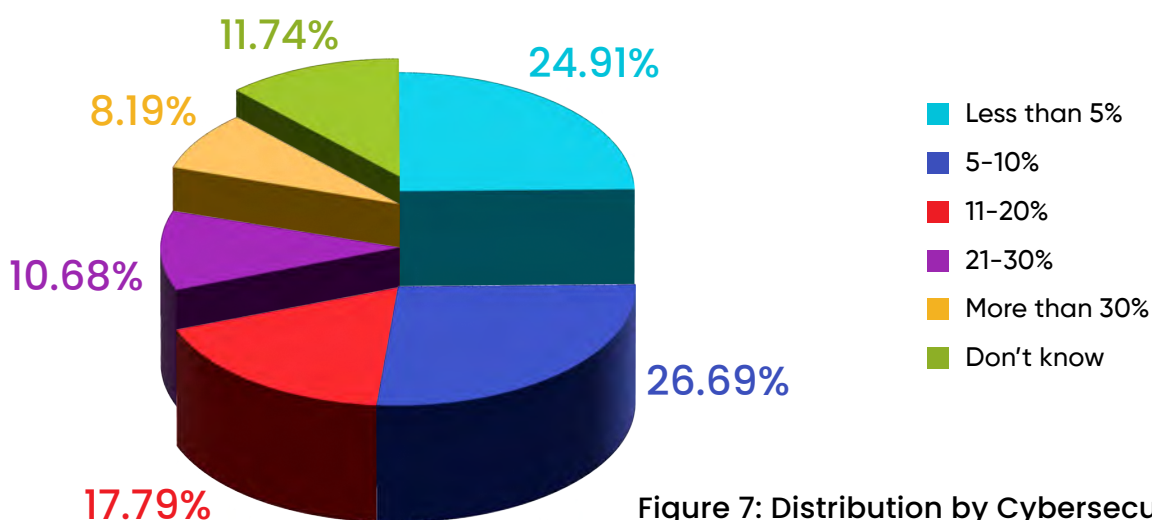


Figure 7: Distribution by Cybersecurity Spending

It's easy to see why businesses are committing so much of their budgets to cybersecurity. The stakes are incredibly high. Recent high-profile security incidents have dramatized the potential for severe consequences due to breaches or lapses in compliance with laws and regulations.

EC-Council's **Certified CISO program provides a structured road map for developing a cybersecurity strategy that is in tune with the organization's priorities:**

Develop security support for business operations subject to regulatory and standards-based compliance.

Certified CISO participants gain a comprehensive understanding of compliance requirements and learn effective ways to assess compliance risks. The program offers guidance on how to build strategies and maintain effective communications with key stakeholders to develop support for initiatives.

Understand risk management frameworks, including the NIST Risk Management Framework, ISO/IEC 27005, COBIT, TARA, OCTAVE, FAIR, and ITIL.

The Certified CISO program delivers a comprehensive overview of risk management frameworks, their key components, and how they can be implemented within an organization. Practical examples of how to apply these frameworks to real-world scenarios, as well as case studies and hands-on exercises, allow participants to understand how each framework can be tailored to their organization's specific needs.

Use effective tools and techniques for robust contract and vendor management.

The Certified CISO program covers key topics relevant to contract and vendor management, such as the procurement life cycle, vendor selection and evaluation, contract negotiation and drafting, and performance monitoring to ensure that vendors meet their contractual obligations. The program includes practical examples that illustrate how to apply these tools and techniques.

Build and mature a security program from the ground up.

Certified CISO participants learn how to design, implement, and manage security policies, procedures, and standards. The program covers key topics such as security governance, risk management, compliance, and incident response, and provides practical guidance on how to implement best practices within each area. Participants also learn about the security frameworks and standards that can guide the development of a security program, such as ISO/IEC 27001, NIST Cybersecurity Framework, and COBIT.

Gain a CISO-level view of transformative technologies, including artificial intelligence, augmented reality, autonomous security operations centers, and dynamic deception.

Certified CISO participants learn how these technologies can be used to enhance the security posture of their organization and how to effectively manage the associated risks. The program covers a variety of use cases in the context of cybersecurity and addresses the potential impact of these technologies on business operations and continuity.

Engage in strategic planning and business alignment for security program efficiency and effectiveness.

The Certified CISO program addresses how to identify and prioritize the risks that could affect the organization's ability to achieve its objectives. Participants learn to communicate the value of the security program to stakeholders to ensure integration with the overall business strategy. The program covers how to develop policies and procedures that are aligned with the organization's goals. Participants also learn how to evaluate the security program's effectiveness regularly to ensure it remains aligned with the organization's overall strategy.



Major Challenges For Security Leaders

The role of chief information security officer (CISO) made its first appearance in the security world in 1994, when Citi Corp (later Citi Group) hired Steve Katz to establish an architecture specifically designed to make technology more secure (Morgan, 2020). In the decades that followed, the importance of adequate cybersecurity grew, as it became clear in the boardroom that the likelihood of experiencing an incident had become a matter of "when, not if."

The primary concerns keeping cybersecurity leaders awake at night are cloud security, data security, and cybersecurity governance. After becoming a Certified CISO, most of the Hall of Fame survey participants said they provided executive leadership by executing one or more of the following functions:



Bridging the gap between their organization's security team and the C-Suite or board of directors



Building critical security practices for internal and external parties



Training peers or other staff to perform better

However, respondents observed that critical security skill gaps exist within cloud implementations, executive management, and incident management.

The best-in-class cybersecurity leaders focus squarely on ensuring the strongest-possible protection while enabling enterprise priorities. They require a broad range of capabilities and competencies to be effective in what is now a multifaceted role, including the following:

- Extreme agility to keep pace in a rapidly evolving business and technology climate.
- Unfailing vigilance across a diverse attack surface that includes on-premises, cloud, and managed environments, along with vendor and third-party engagements.
- Rigorous attention to compliance with rapid changes in data and privacy laws and regulations across the globe.
- A flexible approach to implementing security across new technologies while retaining holistic security frameworks, policies, and standards.
- The ability to sustain an alert posture to detect and defend against future unknown threats and emerging technological vulnerabilities.
- Interpersonal skills needed to retain, train, and develop the staff required to implement effective security programs and portfolios.



Becoming an outstanding CISO requires an executive to be a strong influencer, stress navigator, workforce architect, and manager of unknown risk. Gone are the days of being primarily a technologist: the CISO must function as the organization's guardian, strategist, and business advisor. Top CISOs constantly prove their value by demonstrating their ability to apply the right knowledge, skills, and temperament to meet daily challenges with speed and confidence.

“

"The world today needs the right people to protect organizations from cyber threats," says Jay Bavisi, President and CEO of EC-Council. "The need in corporations is for CISOs to have a strong balance of business acumen and technical knowledge that comes from professional training."

”



JAY BAVISI,
President and CEO
of EC-Council

EC-Council's Certified CISO certification program provides executives with the tools and techniques they need to answer today's pressing need for excellent cybersecurity leadership.

Greatest Areas of Concern in Cybersecurity

Respondents to the Certified CISO Hall of Fame survey identified more than a dozen areas of cybersecurity concerns within their organizations, including cloud security, data security, and cybersecurity governance (Figure 8).

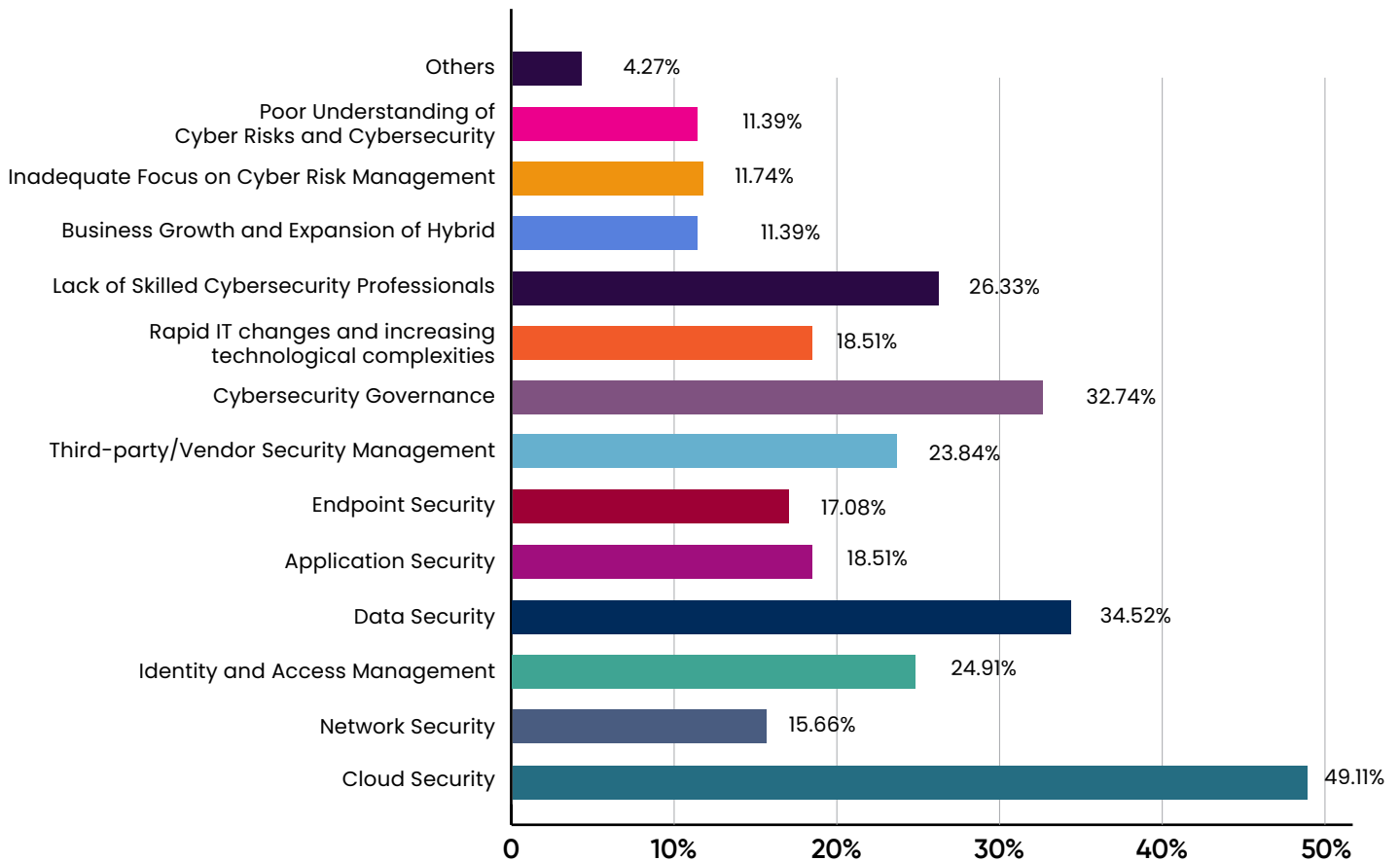


Figure 8: Greatest Areas of Concern in Cybersecurity

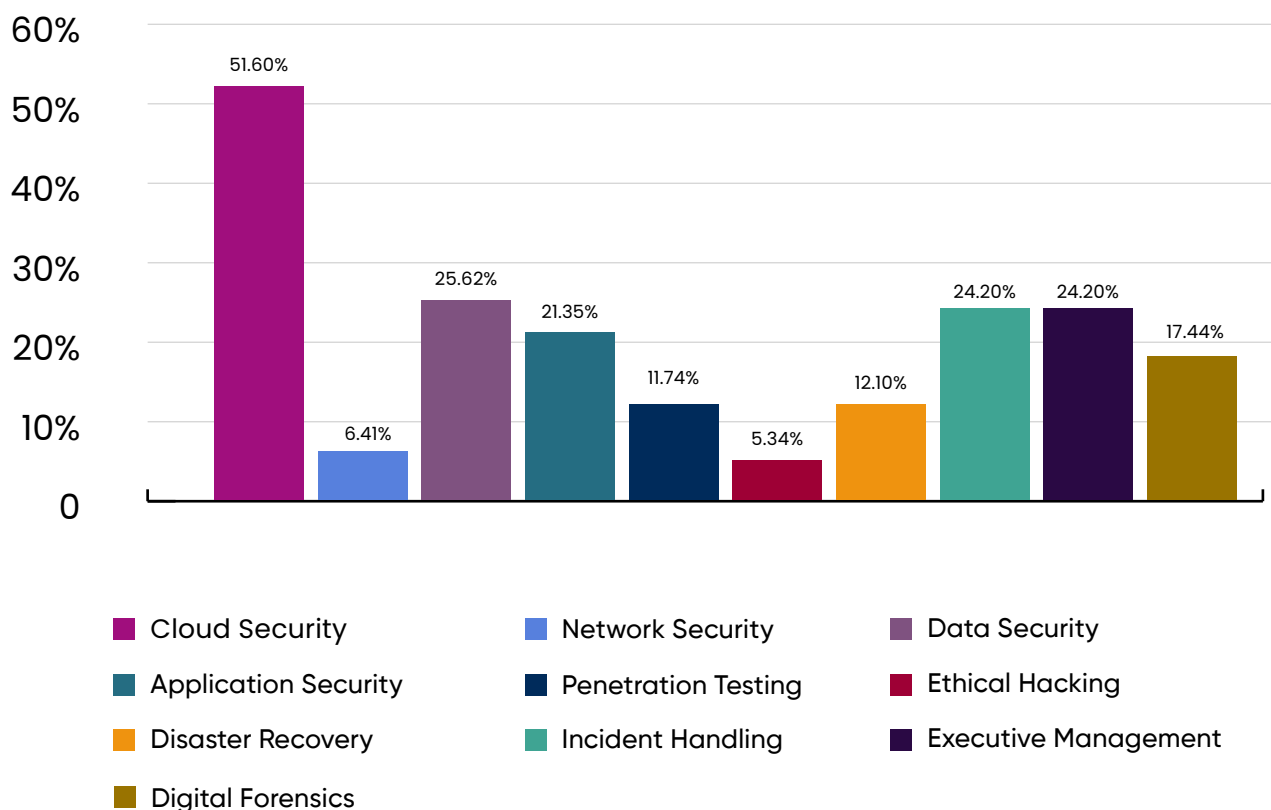


Figure 9: Gaps Between Needs and Talent

The team size, however, does not necessarily correspond with the ability to ensure a solid cybersecurity posture. The limitations in team size often mean that each member needs to be multi-skilled to protect the organization from cyber threats. The Certified CISO program provides the breadth of training needed to manage multiple known threats while monitoring the landscape for the emergence of new threats, reducing an organization's vulnerability to cyberattacks.

EC-Council's Certified CISO program helps leaders remove some of the burden resulting from tight resources by equipping them with the necessary skills, knowledge, tools and techniques to lead an organization's cybersecurity efforts. Areas of coverage include the following:

- **Strategy Development:** How to align the organization's cybersecurity strategy with the overall strategy of the organization, including its goals, objectives, and priorities.
- **Workforce Planning:** How to identify the roles and responsibilities needed, the required qualifications, and the training and development required for the existing workforce.
- **Performance Management:** How to set performance goals, provide feedback, and conduct performance evaluations.
- **Succession Planning:** How to identify potential successors, develop their skills and competencies, and ensure a smooth transition when the CISO role changes hands.

Certified CISO Contributions to the **Cybersecurity Community**

All of the 2023 Certified CISO Hall of Fame nominees contributed to the security profession beyond the work they do in their daily roles. 3 out of 5 were able to bridge the gap between their organization's security team and its C-Suite and board of directors. Forty-five percent built critical security practices for internal and external parties. Close to a quarter of Certified CISO survey respondents pointed to their work in training peers and other staff to improve performance. Certified CISO Hall of Fame nominees also delivered free virtual lectures, trainings, or webinars, and used their expertise to help NGOs, charities, foundations, or similar organizations (Figure 10).

60%

Bridged the gap between security teams and C-Suites.

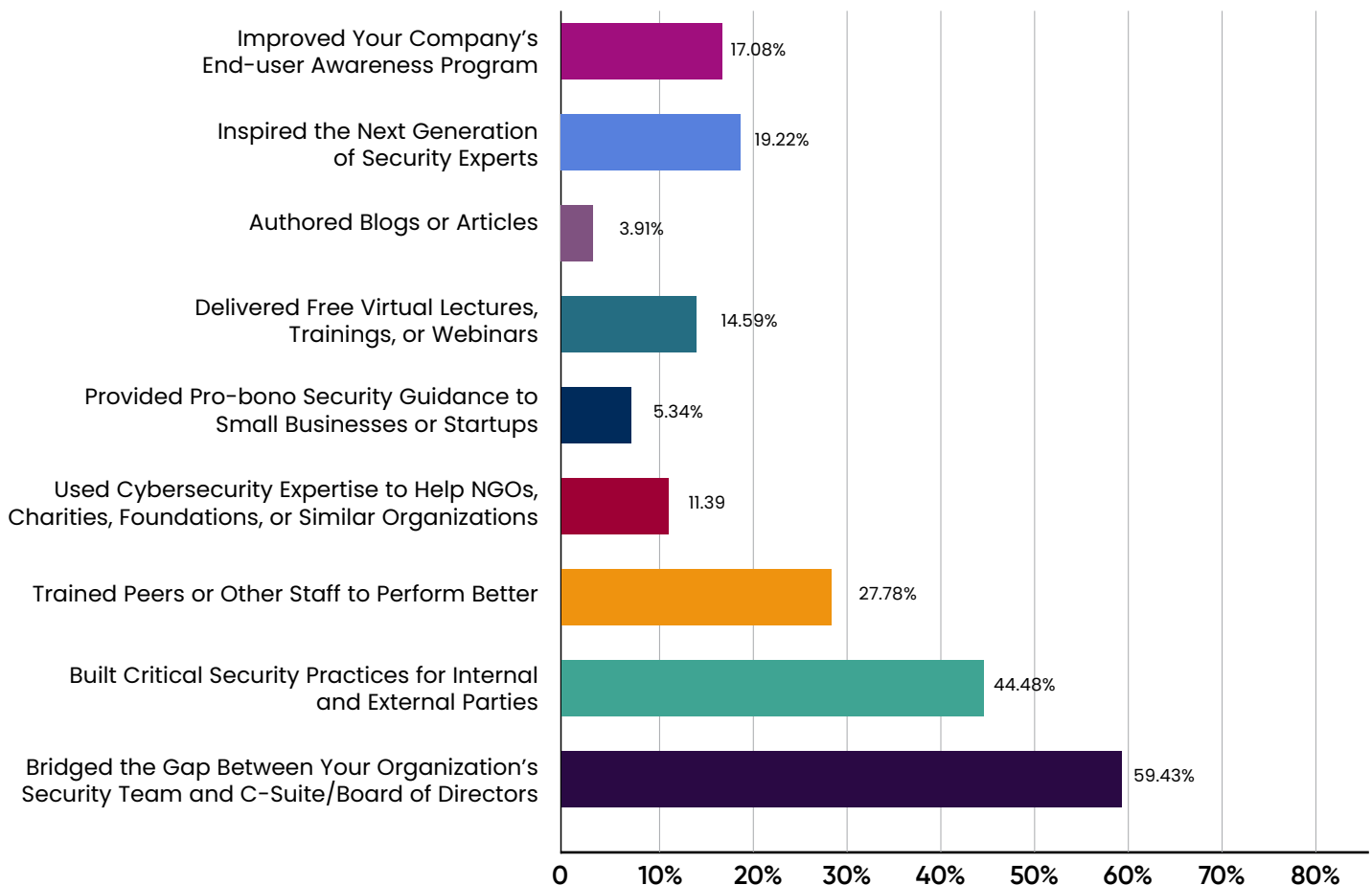


Figure 10: Contributions to the Cybersecurity Community

The Certified CISO program enables participants to develop a stronger understanding of business operations, drivers, and strategies to help them articulate the value and relevance of cybersecurity initiatives to senior executives. It provides them with the tools to design a security strategy that aligns with their organizations' business objectives, risk appetites, and compliance requirements. It equips them with the knowledge to identify, assess, and mitigate risks, protecting the most critical assets from the most dangerous threats.

Those abilities, plus the communication skills the program emphasizes, help participants learn how to build relationships more effectively, establish trust, and convey security information to upper-level executives in a clear and concise manner.



"Since earning my Certified CISO certification, I managed to get approval from my board to initiate several critical cybersecurity transformation programs to improve our overall security posture. One program involved identifying our crown jewels and putting in place security control measures to protect them. In another program, focused on Red Teams and wargaming, we involved our senior management and board members to ensure we were prepared for cyber incidents."

Mark Lim Choon Lye
CIO, Pacific International Lines



Certified CISOs shared their wealth of information and expertise with others, both within and outside of their organizations, through training, lectures, and webinars. Their efforts extended beyond the business realm to non-governmental organizations (NGOs), charities, foundations, and other nonprofit groups.



"I implemented a cybersecurity awareness program during a time when teachers and operational staff continued to be bombarded with multiple priorities and lacked the attention span to focus on cyber issues."

Mark Grysiuk
Privacy Records Manager, Halton Catholic District School Board



"The certification helped me bridge the gap between function and management, improve risk management processes, strengthen information security strategies, and develop plans, policies, and procedures to reduce regulatory risks."

Pawan Chawla
CISO, Future Generali



Certified CISO **Hall of Fame** 2023

Through a rigorous selection process, EC-Council narrowed the group of nominees to 50 Hall of Fame winners. These honorees demonstrated exceptional performance in their leadership roles and exceeded the range of their responsibilities by contributing to the community in a significant way.

“

“The Certified CISO certification enabled me to solve complex U.S. State Department issues related to sensitive data, financial data, workflow functions, or network-related security. Most importantly, I was able to effectively resolve a critical cyber incident and data breach within the organization.”

Frank Ofori

Lead Technologist, Booz Allen Hamilton

”

“

“I realigned the whole IT administration, orienting it towards a more secure mindset, which had been missing in the organization. I successfully developed IT security policy and cyber crisis management documents with the knowledge gained through the CERTIFIED CISO certification.”

Vamsi Krishna

CISO, SVP National Police Academy

”

“

“I was able to set up the West Africa Affiliate of Women in Cybersecurity, and I am currently the president.”

Olayinka Naa Dzama Wilson-Kofi

Information Security and Privacy Specialist, Ericsson

”

Certified CISO Hall of Fame Winners' Organizations

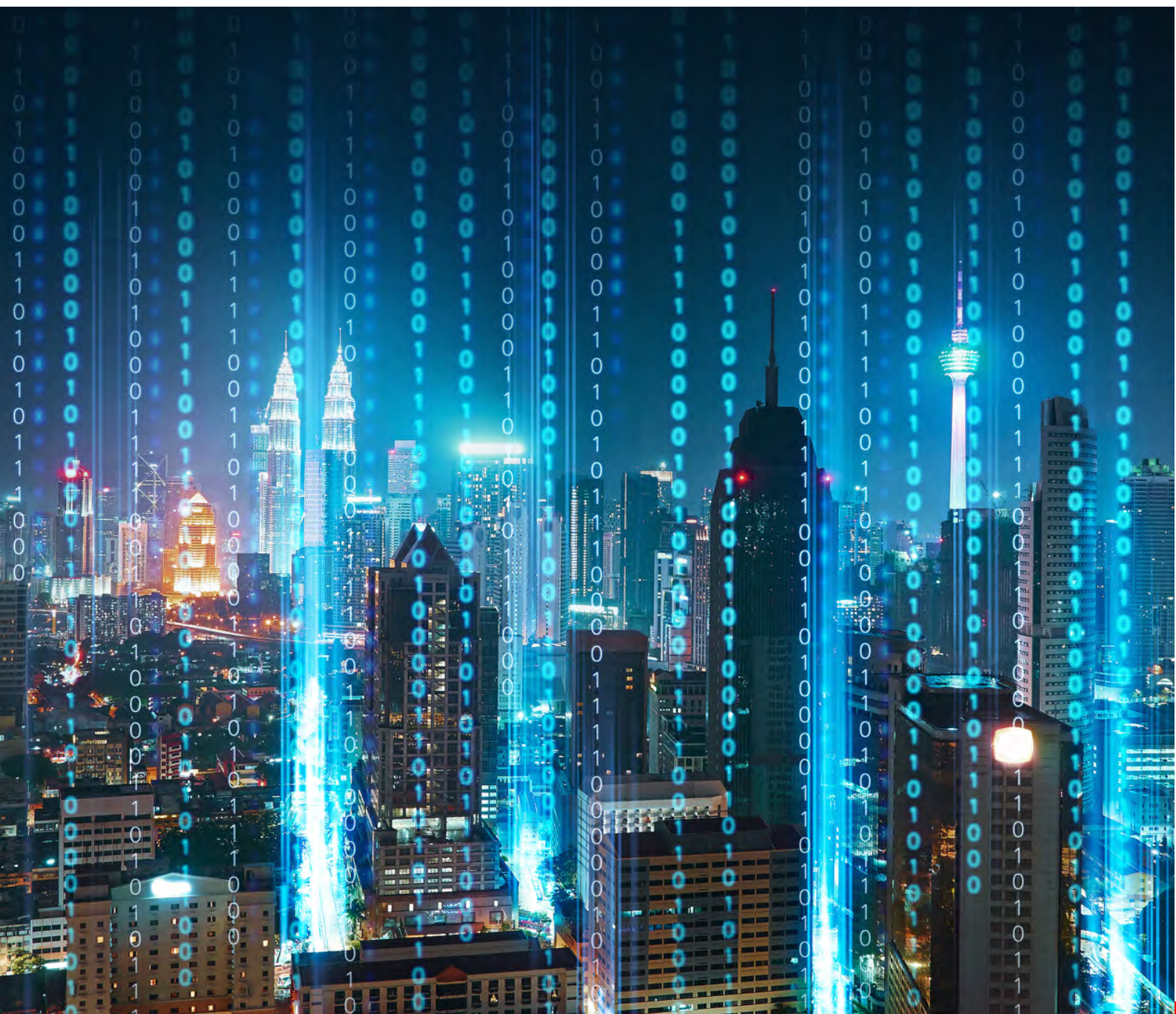


TEMASEK



Willfortify

Strategicmate
LLC



CERTIFIED CISO HALL OF FAME 2023 AWARDEES

AMERICA (NORTH AND SOUTH)



Abu Sadeq,
Zartech, USA



Alex SC
Department of Revenue,
USA



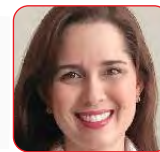
Andrew Wilder,
Hillenbrand, USA



Anthony Leatherwood,
Centre Technologies, USA



Ashish Patil
Karma Automotive, USA



Beatriz Silveira,
Citi, South America



Ben Howard,
Inari, USA



Bernard Peter Robichau II
Category 3 Partners, LLC,
USA



Bob Fabien Zinga,
US Navy Reserve/Directly,
USA



Carlos Lyons,
CGS, USA



Darren Death,
ASRC Federal, USA



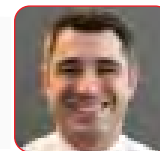
Dick Wilkinson,
Proof Labs, USA



Donna Gallaher,
New Oceans Enterprises,
LLC, USA



Dr. Frank Ofori
US Department of State,
USA



Gregory Will,
Fortify, USA



Jason Wright,
Department of Defense,
USA



Jay Nambi
Ernst & Young, USA



Joseph Stenaka,
US Social Security
Administration, USA



Kristen Sanders,
Aquila, USA



**Leonardo Resende
Carvalho**
Correios, South America



Manish Gupta,
Starbucks, USA



Marcos Parra,
Avanade Brasil,
South America



Mark Grysiuk,
Halton Catholic District
School Board, Canada



Matt Long,
MasterCraft, USA



Michael Goetzman,
Solano Security, USA



Nabeel Yousif,
Flexiti Financial, Canada



**Robert Chandler
Johnson**
Harbor Compliance, USA



Rodney Gullatte,
Firma IT Solutions, USA



Samer Mansour,
Panasonic, USA



Saurabh Kumar,
ACEGeTS, Canada



Tim Manley,
Google, USA

ASIA



Anupam Misra,
PwC India, Asia



Vamsi Krishna,
SVP National Police
Academy, Asia



Jitendra Tripathi,
Reliance Jio, Asia



Mark Lim Choon Lye,
Temasek International,
Asia



Leslie Yee,
Pacific International Lines,
Asia



**Salvador Chio
Guarino Jr**
PwC, Asia



Shin Che Lin,
Taipei Fubon Bank, Asia

EUROPE & UK

Andrew Green,
UK Department for Business,
Energy & Industrial Strategy,
UK



Arijana Trkulja,
Ingram Micro, Europe



Attila Mate Kovacs,
Strategicmate LLC,
Europe



Francesco Di Maio,
ENAV – Italian Air
Navigation Services, Europe



Justen Dyche,
BBC, UK



Natascha Westen,
CiC, Europe



Pedurand Direction,
Generale Armement, Europe

AFRICA & THE MIDDLE EAST

Abdul Rahman,
Middle East



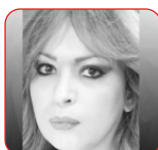
Karin Höne,
Barloworld, Africa



Nkiruka Aimienoho,
PwC, Africa



**Olayinka Naa Dzama
Wilson-Kofi**
Ericsson, Africa



Oraib Qaraeen,
Asiacell, Middle East



How the Certified CISO Program Enables Executive **Leadership in Cybersecurity**

To protect networks, systems, and data, organizations are investing in technologies and tools like firewalls, intrusion detection systems, encryption software, and antivirus software. Substantial budget allocations are going toward training internal teams and hiring personnel, such as security analysts, engineers, administrators, and consultants.

Through a combination of lectures, case studies, and hands-on exercises, EC-Council's Certified CISO program enables C-Suite Leaders to prioritize the use of available funds to align security expenditures with the organization's business goals.

Analyze, Forecast, and Develop Operational Budgets

Participants learn how to develop budgets that consider potential risks, identify areas where additional investments might be needed, and develop business cases for budget requests. Participants also learn how to ensure compliance with various regulatory requirements.

Allocate Financial Resources to Projects and Critical Functions

Certified CISO Participants learn to identify the costs associated with various projects and functions, prioritize spending, and monitor expenses to stay within budget.

Monitor and Oversee Cost Management of Information Security Projects

Participants learn to assess financial benefits to optimize ROI and align projects to organizational needs.

Create and Report Financial Metrics to Stakeholders

Participants learn to report financial metrics through case studies, lectures, online videos, interactive quizzes, and hands-on workshops.

Understand the Acquisition Life Cycle and Determine the Importance of Procurement

Certified CISO Participants learn how to select procurement methods and develop procurement schedules. They also learn about the elements of procurement management, including market research, preparation of documentation, evaluation of proposals, contract negotiation, and contractor performance management.

Effectively Guide the Processes Involved in Procuring an Information System

Participants learn how to use cost-benefit analysis to evaluate risk and negotiate contracts and proposals. They also learn how to reduce costs and negotiate for the most favorable conditions.

Understand Basic Procurement Concepts

Participants learn about the structure of master service agreements (MSAs), statements of work (SOWs), the total cost of ownership (TCO), as well as best practices for developing and negotiating these documents for their own organizations.



"My most impactful achievement since earning the Certified CISO certification was being able to streamline and guide my approach to obtaining higher management buy-in for implementing complex cybersecurity solutions."

Oraib Qaraeen

Director of Security Operations, Asiacell



Who Chooses the Certified CISO Program?

There are only a few programs that are designed for leadership training in the cybersecurity domain. Most cybersecurity programs revolve around the technical concepts of training, while Certified CISO equips professionals with business and technical knowledge. That may explain why the vast majority of Certified CISOs participants come from cybersecurity executive leadership backgrounds (Figure 11).

More than one-fourth of the Certified CISO Hall of Fame survey respondents were CISOs, or equivalent, at their organizations. 23% were directors of security or security managers. Another 15% were IT directors or managers.



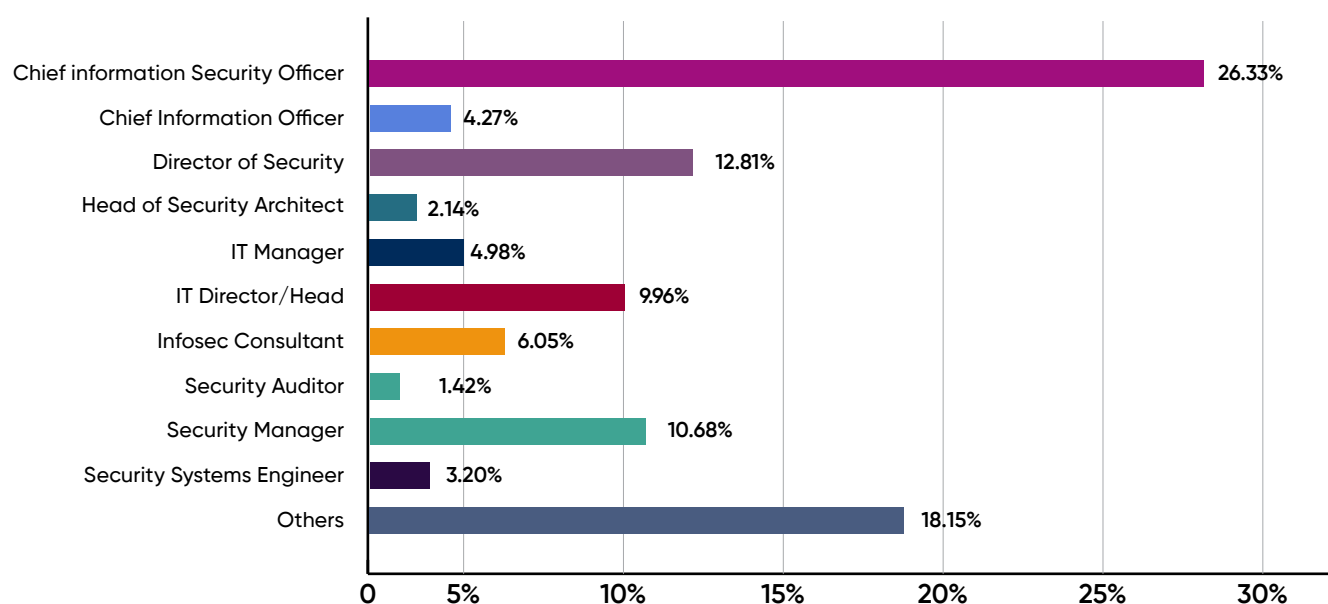


Figure 11: Participant Roles

Cybersecurity leaders choose the Certified CISO program because it focuses not only on how to apply technical knowledge to an information security executive's day-to-day workflow but also on how to strategically align operations with business objectives. While technical knowledge is important, it is not sufficient for senior-level information security professionals who need to communicate effectively with executives, manage budgets, and develop strategies that align with the organization's business objectives.

Another aspect of the Certified CISO program that is important to cybersecurity leaders is its comprehensive curriculum, which combines business alignment, security strategy development, security program management, technical skills, and compliance in one highly effective experience.

Participants appreciate the practical approach the Certified CISO program takes to learning, incorporating case studies, group discussions, and simulated scenarios that help illustrate applications in real-world settings.

The Certified CISO program is highly recognized in the industry for its focus on the training senior-level executives need to manage and lead their organizations' security programs effectively.

Another boon to participants is the Certified CISO program's networking potential. The ability to make connections with other senior-level industry professionals helps participants to improve their security programs and advance their careers.

The success of an organization's security program depends on the success of its CISO. Effective executive information security leaders must understand audit management, information security controls, human capital management, governance, strategic program development, and financial stewardship.

The Most Appreciated Program Components

Certified CISO Hall of Fame survey respondents identified seven attributes of the program they found especially valuable: accreditation, alignment of the curriculum with the CISO role, practical applicability of knowledge gained, training options and study materials, the five Certified CISO domains, duration, and course structure.

70%
especially valued
the five Certified
CISO domains.

More than 70% appreciated the program's trademark organization by five Certified CISO domains:

1. Governance and risk management
2. Information security controls, compliance, and audit management
3. Security program management and operations
4. Information security core concepts
5. Strategic planning, finance, procurement, and vendor management

“

“Knowledge I acquired during the Certified CISO course enhanced my security skill set and most importantly gave me a different mentality towards security to develop comprehensive and holistic risk management and security policies and controls that meet business goals.”

David Siah

Vice President of CyberTech Support, Trend Micro Inc

”

71% of respondents also praised the alignment of the curriculum with the CISO role, achieved through its emphasis on leadership and executive management, availability of real-world experiences, and comprehensive knowledge offerings.

71%
**especially valued
alignment with the CISO role.**

Three out of four Certified CISO Hall of Fame survey 2023 respondents valued the practical applicability of knowledge gained from exercises in developing and implementing effective cybersecurity policies and procedures, identifying and mitigating cybersecurity risks, leading and managing cybersecurity teams, conducting cybersecurity audits and assessments, and developing and implementing incident response and disaster recovery plans.

The Certified CISO program is globally recognized and highly regarded in cybersecurity. The roster of instructors is filled with professionals who are experts in their field.

The course structure was very appealing to many participants, with its comprehensive curriculum packed with real-world experiences. It provides flexible learning options, including in-person, online, and self-paced.

“

" I have been able to deliver InfoSec programs and presentations to the Board of Directors, regulators, etc. since earning the Certified CISO certification."

Jay Nambi

Managing Director of Cybersecurity, EY

”

“

" I believe I've improved my ability to build security programs and communicate clearly with C-Level executives ."

Marcos Parra

Direction of Security, Avanade

”

Insights From Certified CISOs

The Certified CISO Hall of Fame survey 2023 respondents were openly enthusiastic about the program after earning their credentials. Among many other expressions of satisfaction, they expressed high confidence in their ability to more effectively align security program strategies with their organizations' goals.

91%

could better align their security programs with organizational goals.

“

"I built cybersecurity programs that mitigate risk, establish governance, and verify compliance."

Gregory Bell

Chief Information Officer,
Amazon Web Services

”

“

"I expanded cybersecurity capabilities into board level communications."

Michael Goetzman

CISO, Solano Security

”

“

"I implemented a comprehensive program to address IT transformation aimed at the reduction of cyber risk."

Bernard Peter Robichau II

Director of Security,
Category 3 Partners

”

“

"I developed and implemented an enterprise security strategy and framework that consists of strategically integrated elements of NIST risk management and cybersecurity frameworks, CIS CSC. I improved the security posture by 80%"

LonDarius

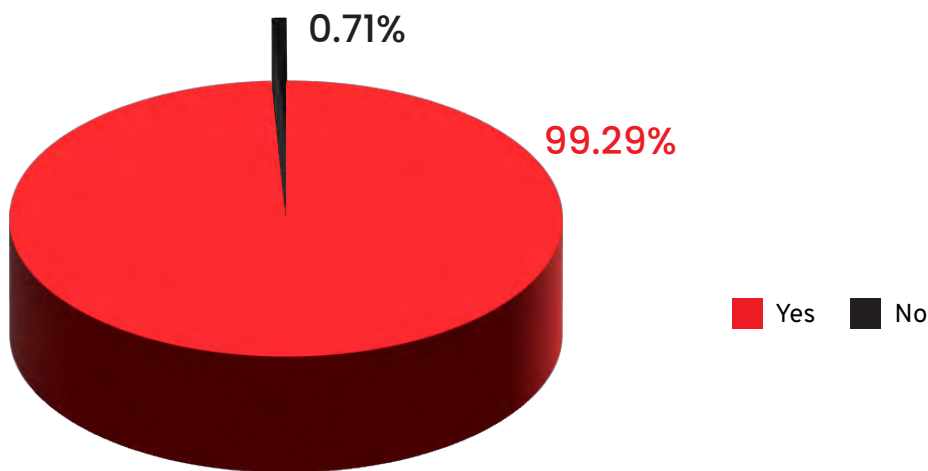
Cunningham, McKinsey & Company

”

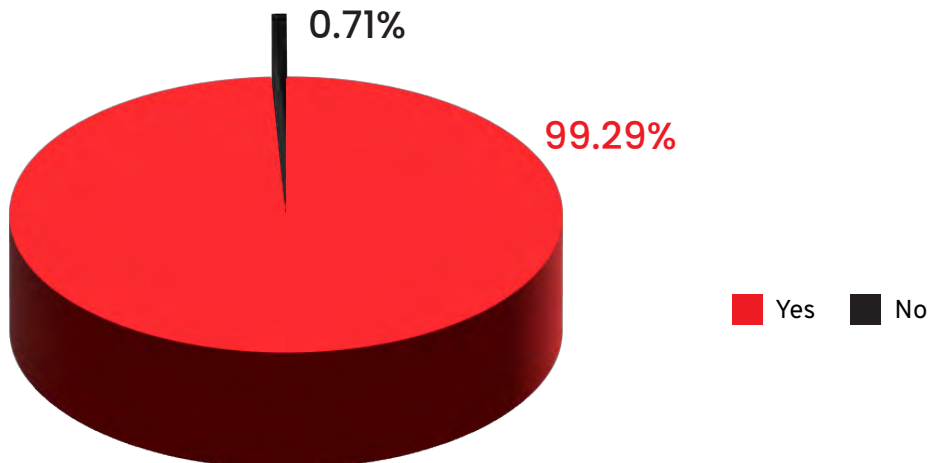
The 2023 Certified CISO Hall of Fame survey respondents voiced nearly unanimous agreement that the Certified CISO program made them more effective cybersecurity leaders and that they would not hesitate to recommend it to their peers.

They voiced nearly unanimously that the Certified CISO program made them more effective cybersecurity leaders and that they would not hesitate to recommend it to their peers.

More than **99%**
could better align their security
programs with organizational goals.



More than **99%** would recommend the
Certified CISO
program to their peers.



Conclusion

The feedback and insights shared by the 2023 Hall of Fame winners and runners-up affirm the tremendous value of the Certified CISO experience. This program fosters critical thinking by reflecting on past successes and failures, enabling participants to leverage their collective expertise. The collaborative nature of the program encourages knowledge sharing among peers, resulting in deeper insights and the development of advanced leadership and operational management approaches for critical teams.

The Certified CISO program establishes enduring connections among peers throughout the cybersecurity industry. Those who earn the Certified CISO credential can count on having access to a broad range of experienced, energetic, and knowledgeable security professionals.

In essence, the Certified CISO program empowers individuals to continuously advance their knowledge and experience, ensuring that their learning journey never comes to a halt. It is a testament to the commitment of CISO leaders to stay at the forefront of the ever-evolving field of cybersecurity.

About EC-Council

EC-Council invented the Certified Ethical Hacker. Founded in 2001 in response to 9/11, EC-Council's mission is to provide training and certifications to apprentice and experienced cybersecurity professionals need to keep corporations, government agencies and others who employ them safe from attack.

Best known for its Certified Ethical Hacker program, EC-Council today offers 200 different trainings, certificates, and degrees in everything from Computer Forensic Investigation and Security Analysis to Threat Intelligence and Information Security. An ISO/IEC 17024 Accredited Organization recognized under the US Defense Department Directive 8140/8570 and many other authoritative cybersecurity bodies worldwide, the company has certified 300,000 professionals across the globe. Trusted by seven of the Fortune 10, half of the Fortune 100, and the intelligence communities of 150 nations, EC-Council is the gold standard in cybersecurity education and certification.

A truly global organization with a driving belief in bringing diversity, equity and inclusion to the modern cybersecurity workforce, EC-Council maintains 11 offices in the US, the UK, India, Malaysia, Singapore, and Indonesia.

Certified Chief Information Security Officer (C|CISO) Program

EC-Council's Certified CISO program has certified leading information security professionals around the world. A core group of high-level information security executives, the Certified CISO Advisory Board, contributed by forming the foundation of the program and outlining the content that would be covered by the exam, body of knowledge, and training. Some members of the Board contributed as authors, others as exam writers, others as quality assurance checks, and still others as trainers. Each segment of the program was developed with the aspiring CISO in mind and looks to transfer the knowledge of seasoned professionals to the next generation in the areas that are most critical in the development and maintenance of a successful information security program.

The Certified CISO program is the first of its kind training and certification program aimed at producing top-level information security executives. The Certified CISO does not focus solely on technical knowledge but on the application of information security management principles from an executive management point of view. The program was developed by sitting CISOs for current and aspiring CISOs.

In order to sit for the Certified CISO exam and earn the certification, candidates must meet the basic Certified CISO requirements. Candidates who do not yet meet the C|CISO requirements but are interested in information security management can pursue the EC-Council Associate C|CISO certification.



**Become an
Industry-Leading
C-Suite
Information
Security Leader
with EC-Council's
Certified CISO
Certification.**

References

Gartner (2022, October 13). "Gartner Identifies Three Factors Influencing Growth in Security Spending" [Press Release].

IBM (2022). "Cost of a Data Breach 2022."

Lohrman, D. (2018, January 13). "The Case for Cybersecurity Certifications." Government Technology.

Lomas, N. (2022, September 5). "Instagram fined €405M in EU over children's privacy." TechCrunch.

Morgan, S. (2020, October 13). "Backstory Of The World's First Chief Information Security Officer." Cybercrime Magazine.

Petrosyan, A. (2022, September 12). "U.S. Government: Proposed Cyber Security Spending in FY 2017-2023." Statista.

Shead, S. (2021, July 30). "Amazon Hit With \$887 Million Fine by European Privacy Watchdog." CNBC

World Economic Forum (2023, January). "Global Cybersecurity Outlook 2023."



EC-Council

Building A Culture Of Security

www.eccouncil.org