EC-Council
Building A Culture Of Security

C|CISO
Certified | Chief Information Security Officer

ARE NOT JUST TECH LEADERS. THEY ARE VALUE TRANSLATORS.

MEET THE 50 LEADERS REDEFINING CYBERSECURITY LEADERSHIP

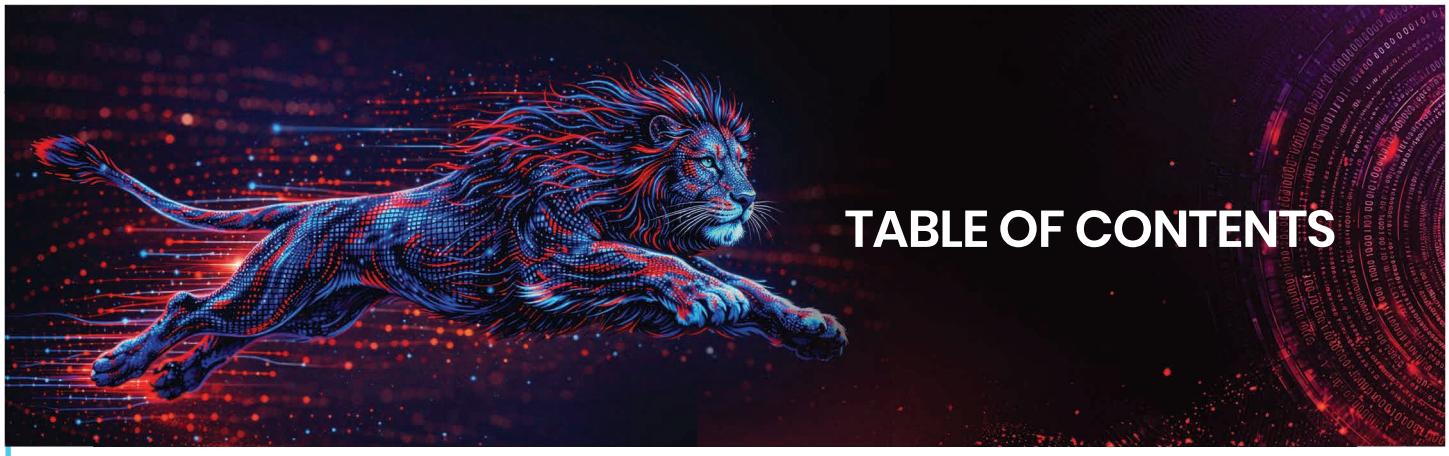


TABLE OF CONTENTS

EXECUTIVE SUMMARY

The cybersecurity threat landscape has never been more complex, more consequential, or more strategically integrated into organizational decision-making. As boards scrutinize cyber posture alongside quarterly earnings, and as regulators mandate executive accountability for data protection, the role of the Chief Information Security Officer has fundamentally transformed from a technical function into a board-level strategic mandate.

This report presents findings from the EC-Council Certified CISO (C|CISO) Hall of Fame global survey, examining how the C|CISO certification is reshaping career trajectories, organizational security posture, governance frameworks, and the long-term architecture of cybersecurity leadership.

The data tells a definitive story: how the world's most effective security leaders are building influence, driving outcomes, and shaping decisions beyond the security function.

This report recognizes CISOs not for what they manage, but for the value they translate.

DATA SOURCE AND METHODOLOGY

The findings presented in the C|CISO Hall of Fame Report 2025 have been collected via structured survey instruments deployed to C|CISO-certified professionals globally.

After deduplication and data quality validation, the final dataset comprised 346 unique respondents. The survey instrument covered four thematic pillars aligned with the C|CISO program's core domains:

- Career Acceleration and Role Attainment
- Organizational Security Transformation
- Executive Governance and Board-Level Engagement
- Thought Leadership, Community Impact, and Knowledge Sharing

Global Reach: EC-Council conducted an in-depth global survey engaging **346 C|CISO-certified professionals from more than 87 countries.**

Cross-Industry: Respondents represented a broad range of sectors, including **finance, government, healthcare, technology, manufacturing, energy, retail,** and others.

Multi-Dimensional: The survey explored executive leadership, governance, strategic decision-making, and thought leadership in cybersecurity.

From the global respondent base, a cohort of Certified **CISOs was recognized in the C|CISO Hall of Fame 2025.** They were selected through a robust evaluation process that considered executive leadership capability, governance and risk management impact, alignment of cybersecurity strategy with business objectives, and career progression following C|CISO certification.

The report blends **quantitative analysis with qualitative interpretation** to present a balanced view of leadership trends and outcomes. Where relevant, numerical figures have been rounded to the nearest whole number in line with standard reporting practices. Each insight is based on a consistent sample size of 346 respondents, reflecting the number of participants who answered each survey question. Although the findings provide strong directional insights, they may not fully represent the wider cybersecurity leadership population.

"EC-Council honors distinguished cybersecurity leaders through the C|CISO Hall of Fame."

EC-Council
Building A Culture Of Security

KEY FINDINGS AT A GLANCE

100% say the next generation of cybersecurity leaders should pursue the C|CISO certification as part of their executive career path.

9 in 10 report alignment of cybersecurity strategies with business goals as a measurable outcome of earning the C|CISO.

98% state that the C|CISO credential led to improvement in their leadership skills.

88% credit C|CISO with helping them transition from technical to executive roles.

98% say the C|CISO leads to high confidence in making business-driven cybersecurity decisions at the executive level.

88% say C|CISO was instrumental in attaining their current position.

97% say the C|CISO enhanced their ability to communicate with executive leadership or the Board of Directors.

3 in 4 say C|CISO helped them earn a promotion.

97% say the C|CISO credential prepared them better for executive leadership than previous certifications they had pursued.

3 in 4 report a salary increase after earning the C|CISO certification.

Meet the Employers of the 2025 C|CISO Hall of Fame

AWARDEES

United Nations

भारत सरकार GOVERNMENT OF INDIA

रक्षा मंत्रालय MINISTRY OF DEFENCE

Microsoft

Google

BANK OF AMERICA

ART INSTITVTE CHICAGO

AMERSON
Amerson ARD India Pvt.Ltd.

AOS Solutions

DELL

crixto

cognizant

consor

CoServ

FirstBank Since 1894

EVERGREEN

Fidelis Security

GOVTECH SINGAPORE

UNIVERSITY

PhoenixTS

itm8

KPMG

P&G

MERKEZİ KAYIT İSTANBUL

AADHAAR

LOGICALIS
Architects of Change

IGI The Cybersecurity People

LATAM AIRLINES

MoneyGram

Peraton

RTX

SAIC

accenture

EY Parthenon

AKIMA

ALPHATECHNOLOGIES


BROWARD COUNTY FLORIDA
Cargill
citibank
CISCO
CROWDSTRIKE
CYBERARK
CyberTech
Flipkart
Grant Thornton
GLS.
FORTINET
RingCentral
HITACHI
Inspire the Next
Hitachi Sunway Information Systems
AcuityBrands.
HOSPITAL SÍRIO-LIBANÊS
wipro
HBC
Interactive
Security Training
ISACA
Koniag
Government Services
LANNAN TECHNOLOGIES
Q8
MADARSONIT
Paytm
new era.
TECHNOLOGY
paloalto
NETWORKS
SEMPRA
INFRASTRUCTURE
Viasat
SOCHISI
axcend
CLOUDGRID
NETWORKS
DLTCode
WORLD BANK GROUP
pwc
CORPORATION
POTOMAC
ECONOMICS

CERTIFIED CISO HALL OF FAME

AWARDEES

Americas (North & South)

Bob Zinga,
USNR, USA

Michael Calderin,
YAGEO Group, USA

Jai Arun,
IBM, USA

Bradley Schaufenbuel,
Paychex, Inc., USA

Mike Morrow,
Centers of Medicare & Medicaid Services, USA

José Gabriel Croci Salgado,
SABYK by Domus Global, Uruguay

Brian Phillips,
Macy's, Inc., USA

Paul Kankwende,
Bayport Financial services, USA

Lee Vorthman,
Oracle, USA

Phillip Dwayne Cuyler,
Department of the Interior, USA

Luiz Bianchi Jr,
Federal Prosecution Office (Ministério Público Federal - Brazil)

Dina Mathers,
Carvana, USA

Richard Henderson,
Govt. of Alberta, Canada

Dr Erdal Ozkaya,
Morgan State University, USA

Shaju Gangadharan,
S&P Global, USA

Dr. Victor Monga,
Virtually Testing Foundation, USA

Vinay Bhatia,
Stryker, USA

Gernette Wright,
HMG, USA

Gregory Bell,
AWS, USA

Darren Death,
Export-Import Bank of the United States, USA

Gavin Partington
CACI Ltd UK, United Kingdom

Jose Manuel Soriano Orozco
Inerco Corporacion, Spain

Mohammad Nurul Alam
Germany

Przemysław Dęba
Orange Polska, Poland

Africa, Asia, Australia

Dr. Harrison Nnaemeka Nnaji,
First Bank of Nigeria Ltd, Nigeria

SenthilKumar Iyyappan,
Ocrolus Inc, India

Mahendrakumar Soni,
Sodexo, India

Musa Salmamza,
NTT Data Inc, South Africa

Vaibhav Pandya,
Nuvoco Vistas Corp. Ltd., India

Wai Kit Cheah,
Lumen Technologies, Singapore

Sherrif Issah,
Deloitte, Ghana

Velmurugan Arumugam,
INTAS Pharmaceuticals Ltd, India

Nigel Hedges,
Chemist Warehouse, Australia

Mukul Kulshrestha,
Adani Ports & SEZ Ltd, India

Anupam Misra,
PwC, India

Vijay Suryanarayana,
Hewlett Packard Enterprise, India

Nagammai Shanmugham,
Standard Chartered Bank, India

Bhaveshkumar Bhatt,
bp, India

Xerxes Philip Kiok Kan,
DFI Retail Group, Hong Kong

Ravi Subbiah,
Tata Consultancy Services Pvt. Ltd., India

Bryan Chee,
Citibank, Singapore

Zhon Teck Tan,
NTT DATA Inc., Malaysia

Himanshu Srivastava,
Tech Mahindra, India

Dhananjay Rokde,
iManEdge Digital Services Bharat, India

Middle East

Anmar Mazin,
Iraqi General Secretart of Council of Ministers, Iraq

Majed Alshodari,
Saudi Ministry of Hajj and Umrah, Saudi Arabia

Shahid Ahmed,
UAE- IAA, UAE

Europe

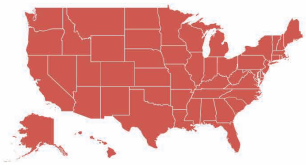
Ashwin Parankusha Narasimha Murthy,
IBM, Ireland

Claudio De Rossi,
InfoCamere, Italy

Daniel Fai,
Procter & Gamble Service GmbH, Germany

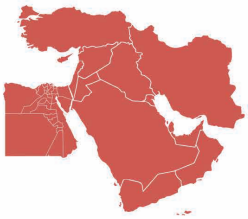
HALL OF FAME REPORT:
GLOBAL PROFILE

Geographic Distribution of Respondents



The Americas represent the largest share of C|CISO Hall of Fame leaders, reflecting highly mature cybersecurity environment where CISOs operate as strategic business partners with board-level accountability for enterprise risk.

Americas **35%**



The Middle East's share reflects deliberate investment in senior cybersecurity leadership, driven by national digital transformation programs, critical infrastructure protection, and heightened executive accountability.

Middle East **13%**

Asia's strong representation highlights the rise of executive-level cybersecurity leadership in fast-growing, complex business environments, where CISOs are increasingly responsible for aligning security strategy with rapid digital expansion.

Asia **24%**

Africa's growing contribution signals the emergence of CISO leadership as a strategic function, with increasing focus on governance, resilience, and enterprise-wide risk management.

Africa **10%**

Europe's presence indicates a governance-first cybersecurity culture, where C|CISO-level leaders play a central role in regulatory alignment, risk oversight, and long-term organizational resilience.

Europe **16%**

While smaller in proportion, Australia and Oceania show a concentrated presence of senior cybersecurity leaders operating in highly regulated, risk-aware environments.

Australia & Oceania **2%**

WHY C|CISO CERTIFICATION IS CONSIDERED THE GOLD STANDARD IN CYBERSECURITY INDUSTRY?

The C|CISO certification has earned its reputation as the **gold standard in cybersecurity leadership** by being the **only credential that validates both deep security expertise and executive-level business acumen** in a single framework. Unlike purely technical certifications, C|CISO spans five comprehensive domains covering Governance, Risk Management, Security, Compliance, Privacy and Audit Management; Organizational Executive Leadership; Information Security Controls, Security Program Management and Operations; Information Security Core Competencies; and Strategic Planning, Finance, Procurement and Vendor Management, bridging the gap between the boardroom and the SOC. This dual coverage of technology and business operations equips CISOs to speak the language of both security engineers and C-suite executives, making them uniquely effective in today's threat landscape.

The results speak for themselves:

100%

believe the next generation of cybersecurity leaders should pursue it as part of their executive career path

9 in 10

certified professionals report measurable alignment of cybersecurity strategies with business goals

98%

saw direct improvement in their leadership skills following certification

3 in 4

earned a promotion after earning the C|CISO credential

97%

say C|CISO prepared them better for executive leadership than any previous certification they had pursued

Backed by **ANAB accreditation, ISO 17024 certification, and DoD 8140/8570 approval,** and now enhanced with **AI-integrated governance and risk capabilities,** C|CISO certified professionals span industries including **technology, finance, government and military, education, and healthcare,** driving measurable improvements across business alignment, cross-functional coordination, governance engagement, compliance posture, and overall security maturity.

THE C|CISO LEADERSHIP IMPACT PILLARS

The C|CISO Leadership Impact Pillars capture how C|CISO-certified leaders translate expertise into measurable outcomes across career progression, executive impact, leadership maturity, and industry contribution.

Built on insights from cybersecurity leaders worldwide, the pillars highlight where C|CISO delivers the greatest and most consistent impact at the executive level.

01

Career Acceleration and Compensation Impact

C|CISO is accelerating executive career progression, supporting promotions, strengthening career mobility, and contributing to compensation growth in cybersecurity leadership roles.

Key focus areas

- Role Progression
- Career Mobility
- Salary Impact

02

Executive Leadership Impact

C|CISO is strengthening leadership capability at the executive level by improving decision-making confidence, financial oversight, and communication with executive stakeholders and boards.

Key focus areas

- Leadership and Decision-Making Skills
- Budget Management and Cost Optimization
- Board-Level Communication

03

Organizational Impact

C|CISO is enabling measurable improvements across core security functions, helping leaders align cybersecurity with business priorities, strengthen governance engagement, improve compliance posture, and advance cybersecurity maturity.

Key focus areas

- Alignment of Cybersecurity Strategies with Business Goals
- Organizational Cybersecurity Initiatives
- Measurable Security Improvements Across Five Dimensions

04

Thought Leadership and Community Impact

C|CISO is extending leadership influence beyond the organization through industry recognition, knowledge sharing, community contribution, and the development of strategies that shape the broader cybersecurity profession.

Key focus areas

- Industry Recognition
- Knowledge Sharing
- Community Contribution

1. CAREER ACCELERATION AND COMPENSATION IMPACT

Role Progression

3 in 4

Say C|CISO helped them earn a promotion

Career Mobility

88%

Say C|CISO was instrumental in attaining their current position

88%

Say C|CISO helped them transition from technical to executive roles

C|CISO Is a Catalyst for Executive Career Progression

Respondents consistently highlight the role of the C|CISO credential in supporting career advancement, particularly in roles with greater leadership responsibility and organizational influence. The certification equips professionals with the governance, strategic, and decision-making capabilities required to operate beyond technical domains and contribute at the executive level.

As cybersecurity roles expand to include accountability for risk, compliance, and business alignment, professionals are expected to engage with stakeholders across the organization and participate in strategic decision-making. The transition into such roles reflects the growing need for leadership-oriented cybersecurity capabilities.

In this context, C|CISO serves as a pathway for professionals to evolve from technical specialists into business-aligned security leaders, supporting both career mobility and progression into executive positions.

C|CISO Aligns Compensation with Leadership Responsibility

Respondents also associate the C|CISO credential with growth in compensation, reflecting the expanded scope of responsibilities undertaken following certification. As roles extend into areas such as governance, financial oversight, and strategic planning, professionals operate within a broader organizational mandate.

The certification prepares individuals to manage these responsibilities by developing competencies that align with executive expectations, including risk communication, budget management, and cross-functional leadership.

Salary Impact

3 in 4

Report a salary increase after earning the C|CISO certification

2. EXECUTIVE LEADERSHIP IMPACT

Leadership and Decision-Making Skills

98%

State that the C|CISO led to an improvement in their leadership skills, including governance, financial planning, and executive communication

98%

Report high confidence in making business-driven cybersecurity decisions at the executive level after earning the C|CISO credential

C|CISO Strengthens Executive Decision-Making and Leadership Capability

Respondents highlight the impact of the C|CISO credential on leadership development, particularly in areas that extend beyond technical expertise into governance, financial planning, and executive communication. These capabilities reflect the requirements of roles where cybersecurity decisions are closely tied to business outcomes.

The certification equips professionals to approach decision-making through a business-aligned lens, enabling them to evaluate risk, prioritize initiatives, and contribute to organizational strategy. This shift in capability supports more confident participation in executive-level discussions and decision-making processes.

C|CISO Builds Financial Oversight and Budget Accountability

The ability to manage and optimize cybersecurity budgets emerges as a key area of development following certification. As cybersecurity functions operate within defined financial constraints, professionals are required to align security investments with organizational priorities and risk exposure. C|CISO strengthens their ability to balance security needs with financial accountability.

Budget Management and Cost Optimization

96%

Say C|CISO improved their ability to manage and optimize cybersecurity budgets and costs

Board-Level Communication

97%

Say C|CISO enhanced their ability to communicate with executive leadership or the Board of Directors

C|CISO Enhances Board-Level Communication

Effective communication with executive leadership and boards is a critical component of cybersecurity leadership. Respondents associate the C|CISO credential with improved ability to communicate complex cybersecurity concepts in a manner that supports informed decision-making.

The certification develops the ability to translate technical risk into business-relevant terms, enabling professionals to engage with stakeholders at the highest levels of the organization. This capability supports clearer alignment between cybersecurity priorities and executive expectations.

3. ORGANIAZATIONAL IMPACT

Measurable Security Improvements Across Five Dimensions

9 in 10

Report alignment of cybersecurity strategies with business goals as a measurable outcome of earning the C|CISO

80%

Identify stronger alignment between IT and business as a key area they contributed to after earning the C|CISO

78%

Highlight increased board-level cybersecurity engagement as a key area they influenced post C|CISO

74%

Indicate improved compliance posture as a major area of contribution following the C|CISO

Nearly **2 in 3**

Report advancing their organization's cybersecurity maturity after earning the C|CISO.

C|CISO Drives Improvements Across Core Security Functions

Respondents highlight measurable improvements across five key areas of cybersecurity, including business alignment, cross-functional coordination, governance engagement, compliance posture, and overall maturity.

These outcomes reflect a broader role for cybersecurity within the organization, where security functions operate in closer alignment with business priorities and governance structures.

The C|CISO credential supports this by developing capabilities in governance, risk management, and strategic planning, enabling professionals to contribute across these areas in a structured and consistent manner.

Organizational Cybersecurity Initiatives

Certified CISO professionals attest to **contributing to key cybersecurity initiatives** after earning the C|CISO credential.

4 in 5

Identify stronger alignment between IT and business as a primary area of their contribution after earning the C|CISO

78%

Highlight increased board-level cybersecurity engagement as a key area they influenced post C|CISO

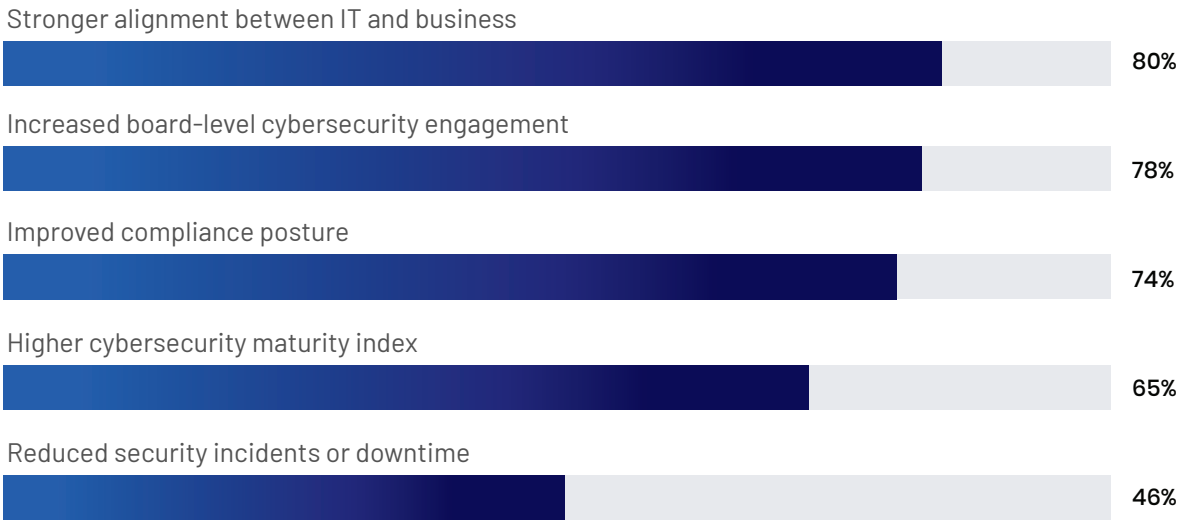
74%

Point to improved compliance posture as a major area of contribution following the C|CISO

Nearly 2 in 3

Note advancing cybersecurity maturity as an area of impact after the C|CISO

Key Transformation Areas After Certified CISO



C|CISO Enables Contribution to Key Security Initiatives

Certified CISO professionals report active contribution across key cybersecurity initiatives within their organizations, particularly in areas that require alignment, governance, and structured execution.

These contributions span improved coordination between IT and business functions, increased engagement with leadership, and strengthened compliance and maturity efforts. Together, they reflect a broader involvement in initiatives that shape how cybersecurity is implemented and managed at an organizational level.

The C|CISO credential supports this by equipping professionals with the skills required to contribute across these areas, enabling them to play a more integrated role in driving cybersecurity initiatives.

4. THOUGHT LEADERSHIP AND COMMUNITY IMPACT

1 in 2

Have received formal industry recognition or awards, reflecting their impact on the cybersecurity profession

89%

Volunteer their time and expertise to nonprofit organizations or community initiatives related to cybersecurity

78%

Regularly share knowledge and insights through blog posts, articles, or social media channels

77%

Have implemented or influenced cybersecurity strategies that are now used as models in their industry or region

46%

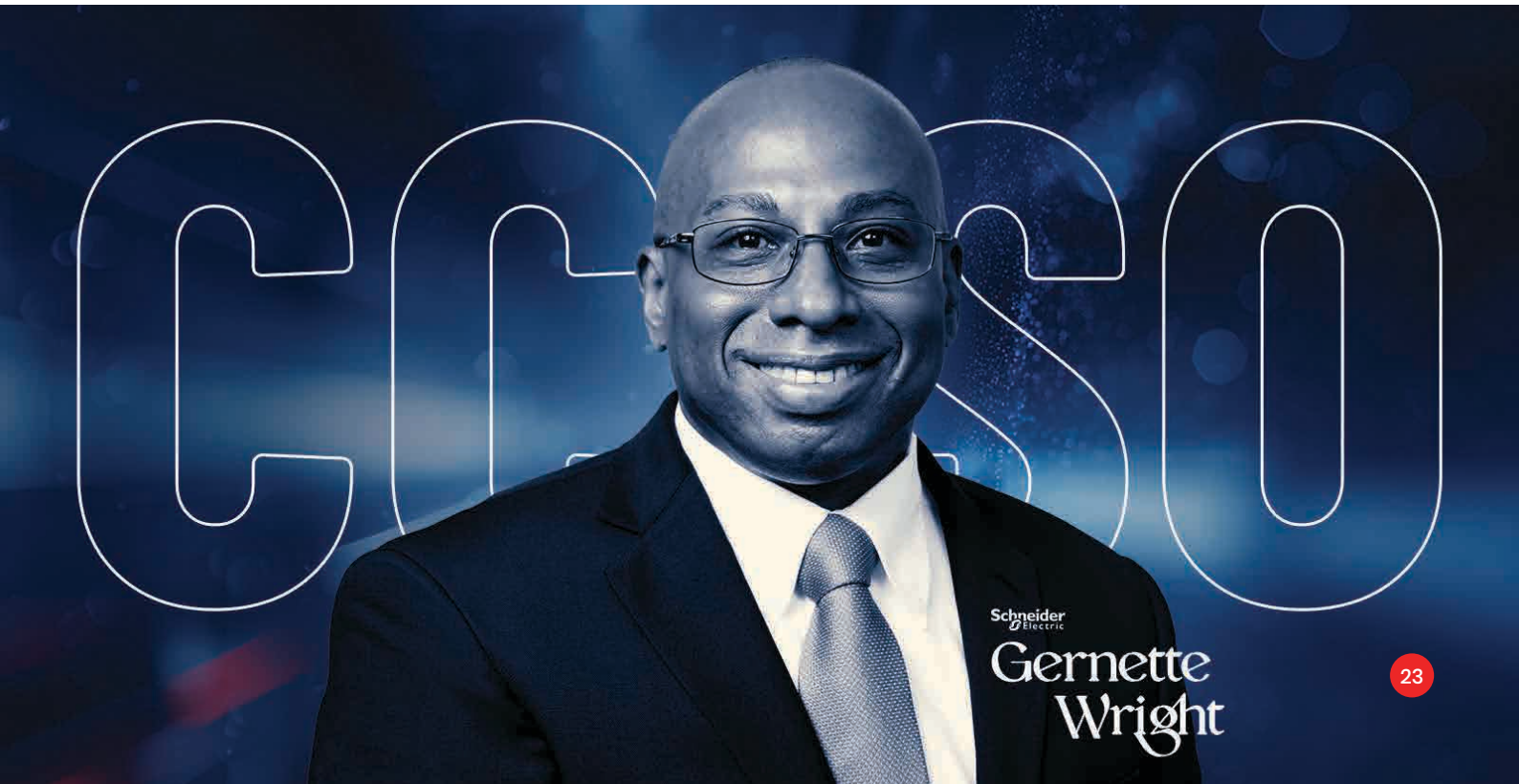
Report advancing their organization's cybersecurity maturity after earning the C|CISO.

C|CISO Extends Impact Beyond the Organization

Certified CISO professionals report active engagement beyond their organizational roles, contributing to the broader cybersecurity community through knowledge sharing, mentorship, and industry participation.

These contributions include involvement in community initiatives, regular dissemination of insights through professional platforms, and participation in activities that support the development of cybersecurity practices. In several cases, professionals also contribute to strategies and frameworks that are adopted within their organizations or wider ecosystems.

The C|CISO credential supports this level of engagement by strengthening leadership, communication, and strategic capabilities, enabling professionals to contribute not only within their organizations but also across the cybersecurity community.



THE C|CISO CREDENTIAL: A DIFFERENTIATED STANDARD FOR EXECUTIVE SECURITY LEADERSHIP

EC-Council
Building A Culture Of Security

100%

Say the next generation of cybersecurity leaders should pursue the C|CISO certification as part of their executive career path

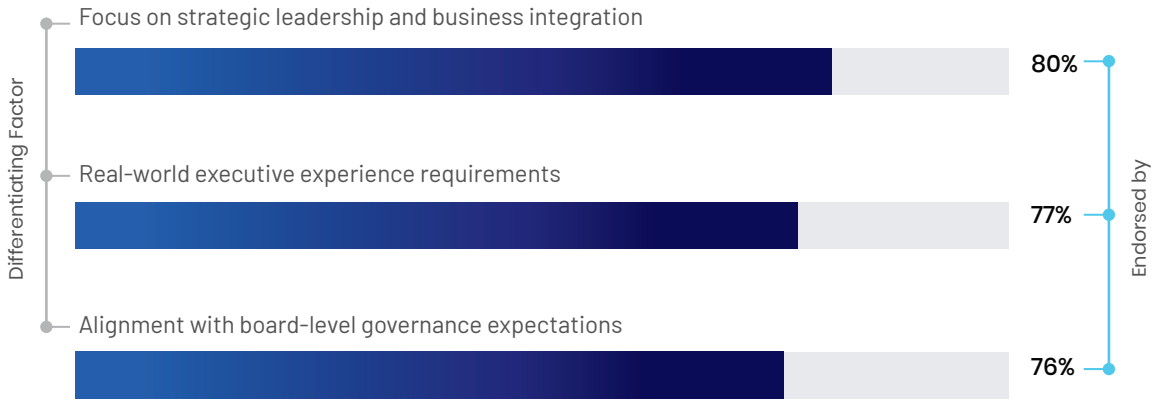
97%

Say C|CISO credential prepared them better for executive leadership than previous certifications they pursued

These findings indicate a strong and consistent pattern. 97% of respondents report that the C|CISO credential prepared them more effectively for executive leadership than certifications they had previously pursued. In parallel, 100% believe that the next generation of cybersecurity leaders should consider C|CISO as part of their executive career path.

Taken together, this reflects a shared industry perspective: the transition from technical expertise to executive responsibility requires a distinct set of capabilities, ones that respondents associate more closely with C|CISO than with traditional certification pathways.

The Top Three Factors That Set C|CISO Certification Apart from Other Cybersecurity Leadership Credentials



Certified professionals were asked what they believe sets the C|CISO apart from other cybersecurity leadership credentials. The data on credential differentiation reveals a consistent theme: the C|CISO is distinguished not by what it teaches about technology, but by what it develops in executives. The top three differentiating factors: strategic leadership and business integration, real-world executive experience requirements, and alignment with board-level governance expectations, all point to the same conclusion: the C|CISO is uniquely positioned as the credential that bridges the gap between security expertise and executive leadership credibility.

EC-Council
Building A Culture Of Security

THE FUTURE OF CYBERSECURITY LEADERSHIP

Leadership Traits for the Next Three Years

When asked to identify the cybersecurity leadership traits that will be most essential through 2028, C|CISO-certified executives painted a clear picture of the competency landscape, one defined by artificial intelligence readiness, strategic communication, regulatory agility, and the governance skills required to navigate an increasingly complex risk environment.

The cybersecurity leadership traits that will be most essential in the next three years:

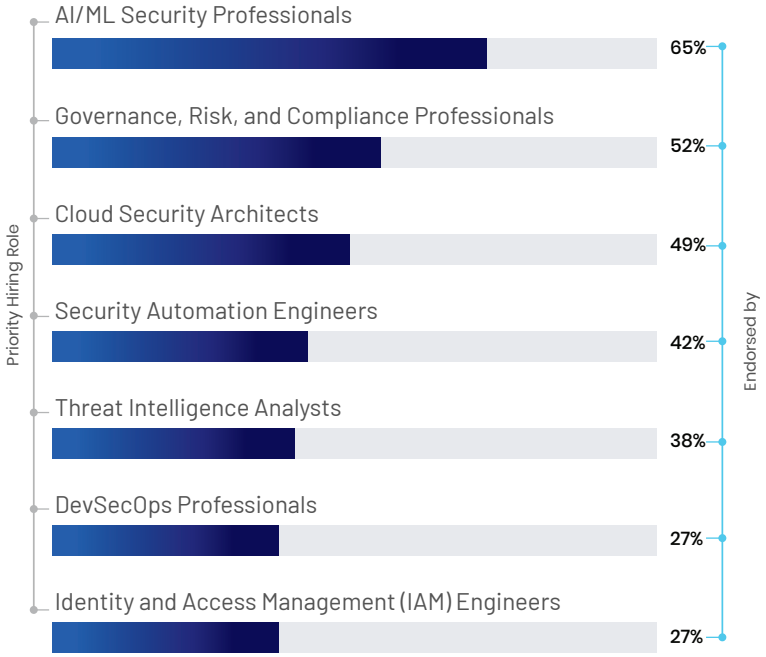
The dominance of AI threat response at 73.9% reflects an industry-wide consensus that has been forming over the past 24 months: artificial intelligence is simultaneously the most powerful tool available to security teams and the most consequential new attack vector they must defend against. C|CISO-certified executives recognize both dimensions and are prioritizing AI literacy as an executive competency.

The prominence of strategic communication at 57.5% reinforces a recurring theme across this report: technical proficiency alone is no longer sufficient for cybersecurity leadership. The executives who will define the next generation of organizational security posture are those who can translate technical risk into strategic language, and who can build the institutional relationships required to secure genuine executive and board commitment to security investment.

Hiring Priorities: Building the Next-Generation Security Team

The talent decisions of today's C|CISO-certified executives will shape the capabilities of tomorrow's security organizations. Their hiring priorities reveal a clear strategic direction: automation, artificial intelligence, cloud security, and governance, the competency clusters required to operate effective security at enterprise scale in an AI-accelerated threat environment.

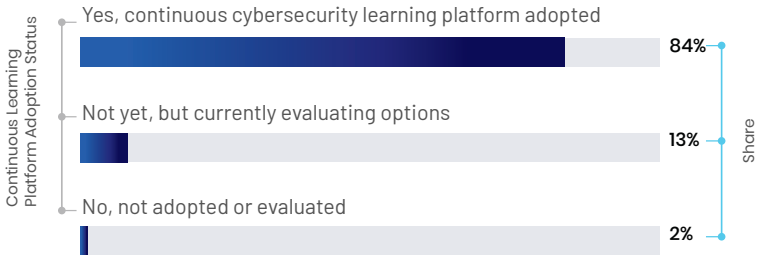
Job roles prioritized in hiring for cybersecurity teams in 2025–26



Continuous Learning as Organizational Infrastructure

Given the rapid evolution of cyber threats and skill requirements, adoption of continuous cybersecurity learning platforms to keep their teams up to date is widespread among organizations represented in the survey

Adoption of continuous learning platforms

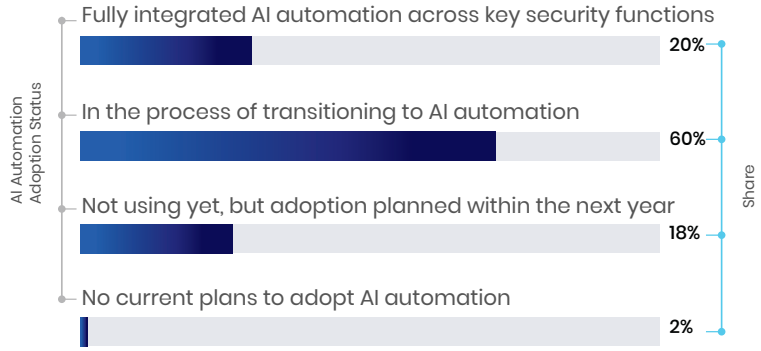


84% of organizations have adopted a continuous cybersecurity learning platform, with a further 13% evaluating options. This near-universal adoption rate reflects a fundamental shift in how security leadership thinks about workforce capability: not as a static credential portfolio, but as a dynamic, continuously refreshed competency infrastructure.

AI Automation Adoption: Where Organizations Stand Today

The survey explored the current state of AI automation integration within cybersecurity operations. Respondents were asked to characterize where their organizations stand in implementing AI automation solutions to enhance their cybersecurity posture. The findings reveal an industry in rapid transition, with the majority of organizations actively engaged in adoption, but only a minority having fully completed it.

Current organizational status in implementing AI automation solutions to enhance cybersecurity posture

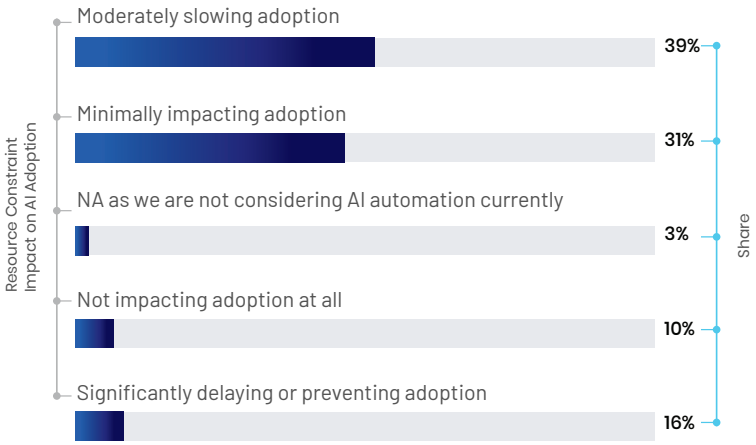


The combined 80% who are either fully integrated or actively transitioning represents a decisive commitment to AI-powered cybersecurity. A further 18% plan adoption within the next year, meaning that within twelve months, approximately 98% of organizations will be operating with some level of AI automation in their security function. The 2% with no current plans represent a statistical outlier, and a strategic vulnerability. In a threat landscape where adversaries are already deploying AI offensively, organizations without defensive AI automation are operating at a structural disadvantage that will compound over time.

Resource Constraints Impacting the Organization's Adoption of AI Automation in Security

The willingness to adopt AI automation is one dimension of organizational readiness; the financial and resource capacity to do so is another. Respondents were asked two inter-related questions: the degree to which resource constraints are impacting AI adoption, and whether their organization has adequate budget allocated for AI-driven cybersecurity initiatives.

Resource constraints in AI Adoption



Resource constraints are a material factor in AI cybersecurity adoption, with 57% of respondents reporting that they are either significantly delaying or moderately slowing down their adoption journey. This finding has direct implications for security investment planning. However, it is equally notable that 40% report minimal or no resource constraint impact.

Budget allocation for AI-driven cybersecurity initiatives

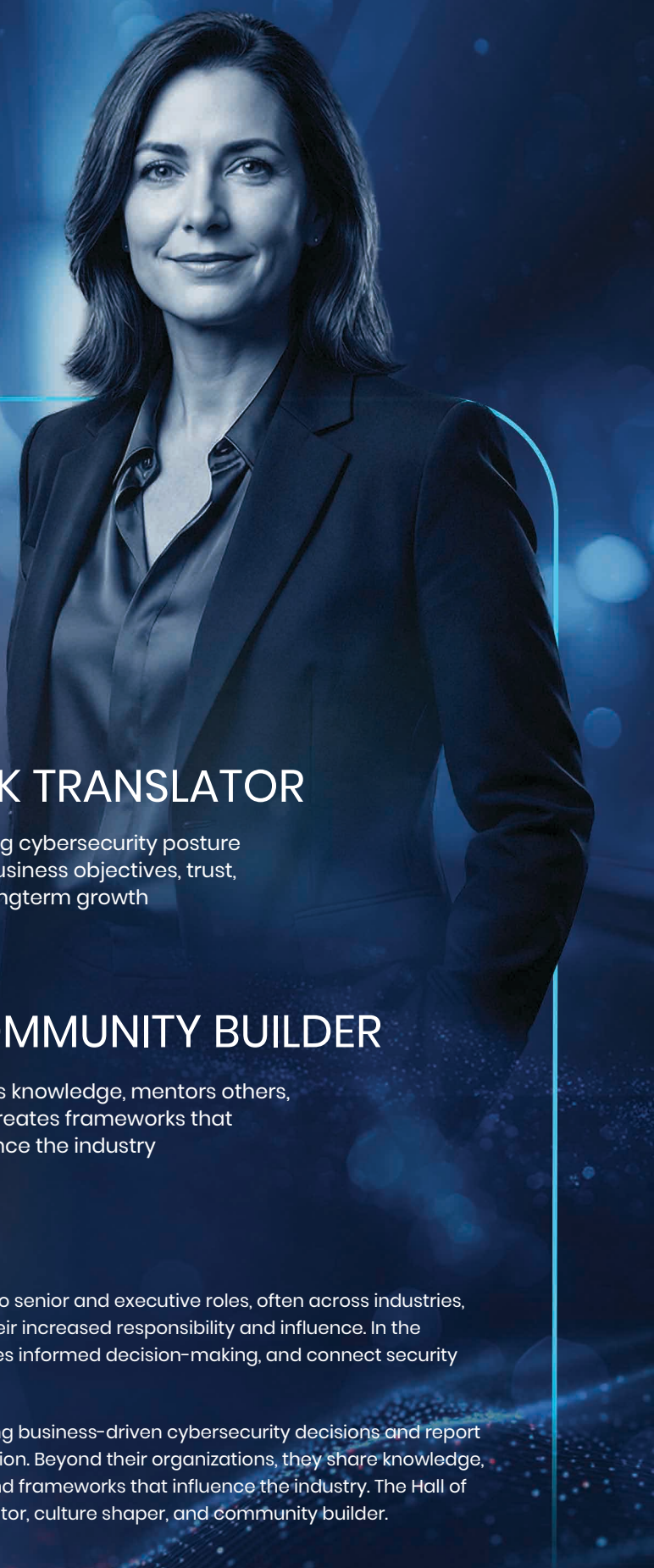
68%
Say adequate budget allocated for AI-driven cybersecurity

22%
Say AI initiatives postponed due to budget constraints

9%
Are not aware of the budget allocation

68% of respondents confirm their organizations have adequate budget allocated for AI-driven cybersecurity. The 22% reporting postponed AI initiatives due to budget constraints represents a strategic risk: in a threat environment where adversaries are actively deploying AI offensively, organizations that defer defensive AI investment are not simply falling behind technically, they are accepting an asymmetric risk position.

The C|CISO HALL OF FAME ARCHETYPE



Synthesizing the four dimensions of the C|CISO Leadership Impact Index yields a clear archetype of the Hall of Fame CISO: A leader who is both a strategic anchor and a force multiplier for the enterprise.

EXECUTIVE STRATEGIST

Advances into senior and executive roles, supporting promotions and compensation growth

RISK TRANSLATOR

Aligning cybersecurity posture with business objectives, trust, and longterm growth

CULTURE SHAPER

Demonstrates confidence in business-driven cybersecurity decisions, grounded in governance capability

COMMUNITY BUILDER

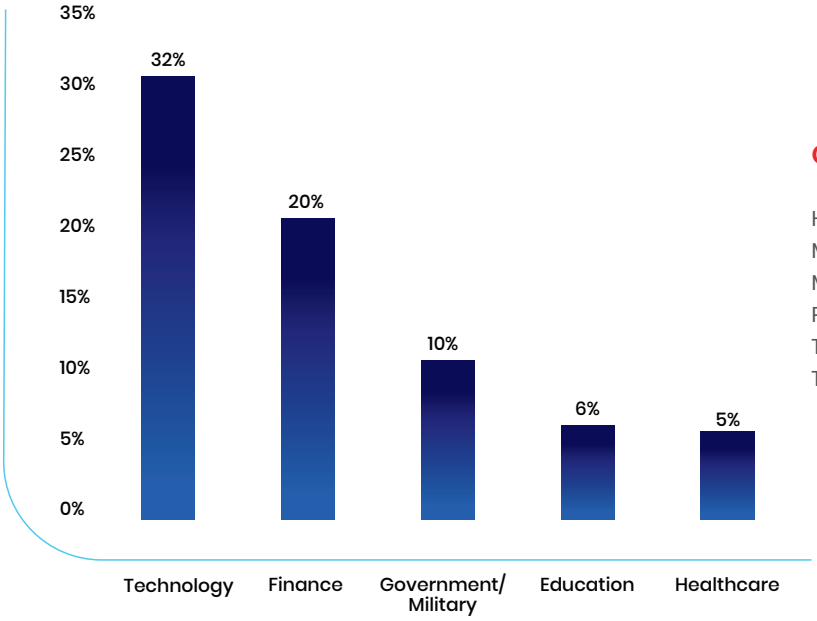
Shares knowledge, mentors others, and creates frameworks that influence the industry

Certified CISOs have leveraged their skills and capabilities to move into senior and executive roles, often across industries, while achieving promotions and compensation growth that reflect their increased responsibility and influence. In the boardroom, they communicate complex risks in language that enables informed decision-making, and connect security investments directly to business outcomes and cost optimization.

In their day-to-day leadership, they demonstrate confidence in making business-driven cybersecurity decisions and report growth in governance, financial planning, and executive communication. Beyond their organizations, they share knowledge, mentor others, volunteer in the community, and develop strategies and frameworks that influence the industry. The Hall of Fame archetype is a composite of the executive strategist, risk translator, culture shaper, and community builder.

Industry/Sector Representation

Top Industries



Other Sectors Represented:

Hospitality, Insurance, Manufacturing/Engineering, Mining/Construction/Petroleum/Agriculture, Pharmaceutical, Retail, Telecommunications/Communications, Transport/Automotive

"SUCCESS STORIES" OF CERTIFIED CISO PROFESSIONALS

Gavin Partington
Principal Technical Consultant
CACI Ltd, UK

Since achieving Certified CISO I have been able to implement ISO 27001 and SOC 2 in the organization, knowing the wider requirements from business and technical perspectives. This has allowed me to get buy-in from stakeholders.

Luiz Bianchi Jr
Federal Prosecution Office
Ministério Público Federal, Brazil

By consolidating Brazilwide, underleveraged talent into a single Cybersecurity Center of Excellence, we replaced fragmented efforts with a structured program spanning Governance, Identity, Business Continuity, Defensive Operations, Incident Response, and Endpoint Security. Centralization helped sharpen alignment with corporate strategy, unlock executive sponsorship, and enable endtoend process mapping. The resulting maturity was validated in external audits that highlighted best practices and continuous improvement loops. Two Certified CISO credentialed leaders on the team were instrumental—providing strategic vision, standardized frameworks, and mentoring—accelerating our ascent from reactive support to a proactive, riskdriven security posture.

Paul Kankwende
Group Head of Information Security
Bayport Management Limited, US

Earning the Certified CISO accreditation greatly impacted my cybersecurity strategy at Bayport by improving my executive-level understanding of how to align security initiatives with business objectives. It enabled me to transition from a strictly technical perspective to one that is centered on risk and guided by governance. I spearheaded the implementation of a comprehensive cybersecurity framework across the enterprise, aligned with ISO 27001, which enhanced regulatory compliance and decreased audit findings by 40%. The Certified CISO principles shaped the creation of board-level reporting dashboards, facilitating informed decision-making and promoting a security-first culture throughout departments. This strategic alignment enhanced stakeholder confidence and optimized cybersecurity investments towards areas with the greatest business impact.

Zhon Teck Tan
Head of Cybersecurity Consulting - Malaysia
NTT DATA Inc., Malaysia

I have implemented influential cybersecurity strategies in the financial services and government sectors. Notably, I enhanced the cybersecurity maturity of a Singaporean government agency post-SingHealth breach, aligning it with the Singapore Cybersecurity Act 2018. At a major Malaysian banking group, I led the adoption of Zero Trust architecture and cloud security transformation, establishing best practices for the industry. Now, as Head of Cybersecurity Consulting at NTT DATA, I advise clients on developing cyber resilience strategies, including AI-driven defense and offensive security, which have been recognized as benchmarks for regional transformation.

WHAT IT TAKES TO BE A HALL OF FAME CISO

From the data and narratives in this report, a practical checklist emerges for what it takes to be considered a Hall of Fame CISO.

Hall of Fame candidates demonstrate clear evidence of career elevation tied to C|CISO, including progression into executive roles and increased scope of responsibility.

They can show measurable organizational impact, including stronger alignment between security and business, enhanced governance, and tangible improvements such as incident reduction, stronger compliance posture, or better budget optimization.

They embody leadership maturity, exhibiting confidence and judgment in business-driven decision-making, especially in complex, high-stakes situations.

They also operate as thought leaders and ecosystem contributors, sharing knowledge widely, mentoring the next generation, and designing model practices that influence the profession well beyond their own organizations.

The C|CISO Hall of Fame is not simply an honorific; it is a standard. By articulating the traits and outcomes that define Hall of Fame–level performance, this report provides a roadmap for aspiring leaders and a benchmark for organizations seeking to recognize and empower their most impactful CISOs.

Why C|CISO Is a Top Choice for Developing Visionary CISOs

The **Certified Chief Information Security Officer (C|CISO)** program is the world's premier executive cybersecurity certification designed to help experienced security professionals transform into strategic, business-aligned security leaders. It bridges the critical gap between technical expertise and enterprise-level leadership, preparing professionals for real-world CISO responsibilities.

A. Core Benefits

Executive-level Curriculum Grounded in Reality: C|CISO reflects the responsibilities, challenges, and decision-making expectations of CISOs worldwide.

Holistic Leadership Framework: Unlike technical certifications, Certified CISO equips leaders with **governance, financial planning, compliance, business alignment, and executive communication skills** which are the key drivers of effective CISO leadership.

Role-based Skill Development: Each domain is mapped directly to a real CISO function, from threat prevention to risk management to M&A risk analysis, making it **the most job-relevant CISO program globally.**

A 360° Organizational View: C|CISO graduates are equipped to lead people, processes, and technology with clarity, maturity, and measurable business outcomes.

B. Core Domains with a User-Value Focus

C|CISO's five domains represent the core competencies needed by every high-performing CISO:

Domain 1: Governance and Program Management

Master policy design, security governance, staffing, vendor strategy, audits, and enterprise-wide oversight—skills that are crucial for building a scalable, compliant, and mature security program.

Domain 2: Risk Management

Quantify, communicate, and prioritize risk using clear metrics and business-aligned reasoning; strengthen resilience by mastering assessments, third-party risk, and enterprise risk reporting.

Domain 3: Security Architecture and Engineering

Drive secure design across cloud, applications, networks, and infrastructure. Learn to minimize failure surfaces, guide engineering teams, and align technology with long-term business strategy

Domain 4: Security Operations and Threat Management

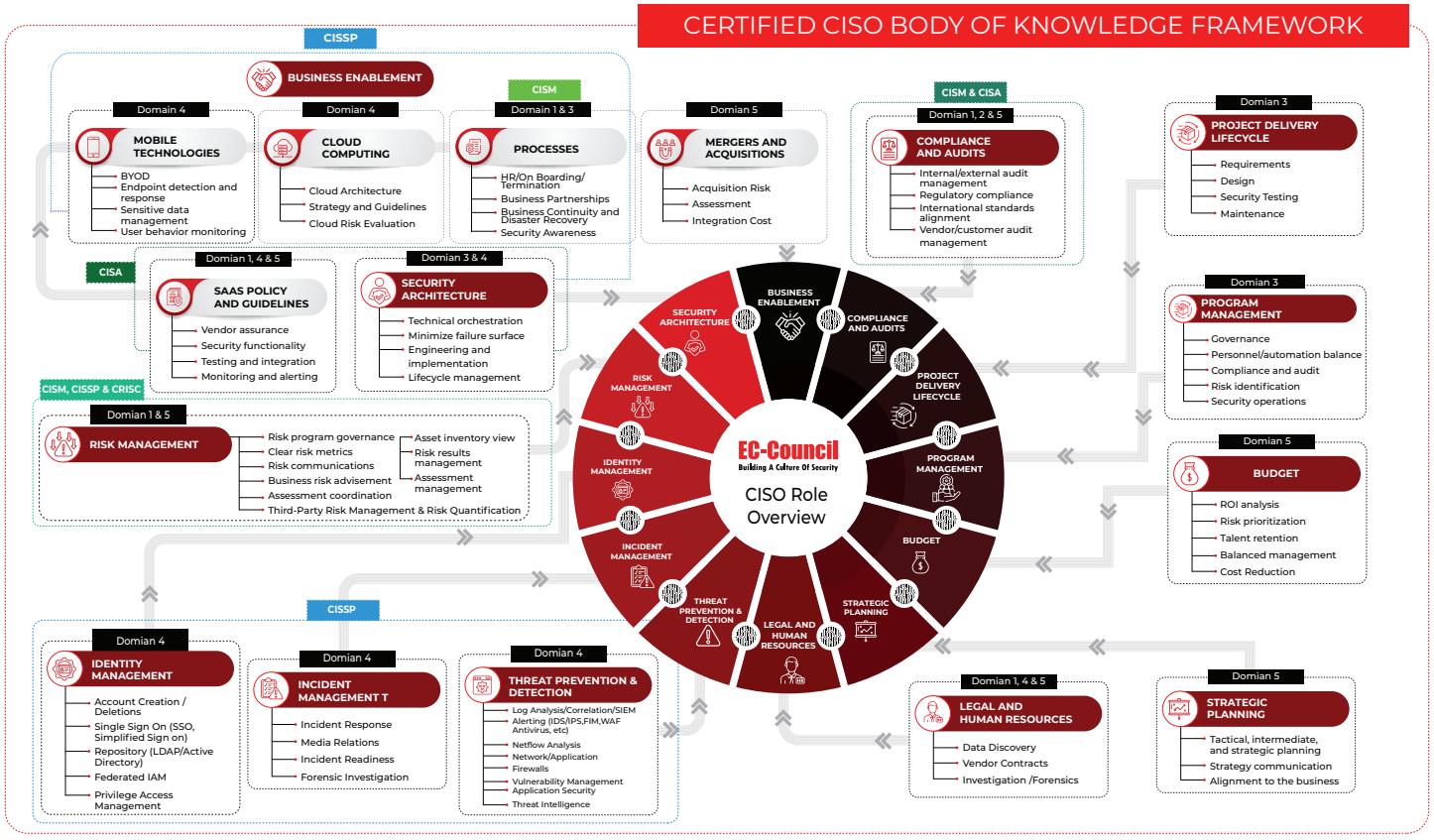
Lead SOC operations, threat intelligence, IAM, forensics, mobile and cloud security, vulnerability management, and incident response—enabling CISOs to protect at scale and maintain operational readiness.

Strategic Planning, Finance, and Executive Leadership

Strengthen budgeting, ROI analysis, talent retention, M&A risk assessments, and board communication, capabilities that differentiate CISOs in modern organizations.

C. How the Framework Reflects the CISO Role and How Certified CISO Covers It

The C|CISO Body of Knowledge Framework represents the core responsibilities a modern CISO owns. The C|CISO certification develops leaders across these responsibilities through a practical, role-based approach. Each section of the framework (shown in the image) maps directly to a CISO function, and C|CISO ensures mastery across all of them.



C|CISO Coverage of Core CISO Responsibilities

I. Business Enablement • Secure cloud, mobile, and SaaS adoption • Business continuity and secure partnerships	C|CISO teaches CISOs to enable growth while managing risk
II. Security Architecture • Enterprise architecture governance • Cloud, app, and network security baselines	C|CISO prepares leaders to design resilient, scalable architectures
III. Compliance & Audits • Regulatory alignment and audit readiness • Vendor/customer assurance	C|CISO builds in-depth competency in governance and compliance leadership
IV. Project Delivery Life Cycle • Secure design, testing, and implementation	C|CISO trains CISOs to embed security in every technology initiative
V. Program Management • Governance, KPIs, and resource balance	C|CISO shapes leaders who can run mature, measurable security programs
VI. Budget and Financial Leadership • ROI, risk-based prioritization, and talent retention	C|CISO develops strong financial and strategic decision-making skills
VII. Legal & HR • Forensics, investigations, vendor contracts, and insider risk	C|CISO covers critical non-technical aspects of security leadership
VIII. Risk Management • Risk quantification, communication, and third-party risk	C|CISO ensures CISOs think, communicate, and act in business-risk terms
IX. Identity and Access Management • IAM, SSO, PAM, and lifecycle governance	C|CISO trains leaders to secure modern identity ecosystems
X. Incident and Threat Management • Incident response, SOC oversight, and threat intelligence	C|CISO provides end-to-end operational and crisis response leadership
XI. Strategic Planning • Long-term roadmaps, maturity planning, and board communication	C|CISO builds CISOs who can influence executives and shape enterprise strategy

Every block in the diagram represents a real CISO responsibility, and C|CISO is the only certification designed to develop the leadership skills needed to integrate them into one unified CISO function. It is comprehensive, practical, and mapped to how CISOs operate today and in the future.

JOB ROLES MAPPED TO C|CISO

- Chief Executive Officer
- Managing Director
- Chief Information Security Officer
- Chief Information Officer
- Chief Technical Officer
- Chief of information Security
- Vice President of Information Security
- Associate Vice President
- Information Security Officer
- Chief Compliance Officer
- Regional Chief Information Officer
- Director Of Security
- IT Director/Head or equivalent
- IT Manager Data Security
- Director Cloud security
- Head Project Manager
- Delivery Manager
- Security Systems Engineer
- Security Auditor
- Head of Security Architect
- Head Of Network Architect
- Infosec Consultant And Advisory
- Senior cyber Security CIO SME

EC-Council
Building A Culture Of Security

REDEFINING WHAT IT MEANS TO BE A CISO

The C|CISO Hall of Fame 2025 Report confirms that C|CISO-certified leaders are redefining what it means to be a CISO. They are not just technologists; they are value translators who sit at the intersection of risk, finance, and strategy, and who shape decisions at the highest levels of the enterprise. Through the four dimensions of the C|CISO Leadership Impact Index, the survey demonstrates that C|CISO serves as a powerful catalyst for career advancement, executive readiness, leadership transformation, and ecosystem-level impact.

For enterprises, the call to action is clear: Recognize and integrate C|CISO-certified leaders as strategic partners, not just security specialists. Involve them in board-level risk discussions, strategic planning, M&A due diligence, and digital transformation initiatives, and leverage their capabilities in financial stewardship and governance.

For security professionals, C|CISO offers a pathway to Hall of Fame–level leadership. It demands not only technical excellence but also business acumen, strong communication, and a commitment to raising the bar for the entire cybersecurity community.

As cyber threats continue to evolve and the stakes of digital trust rise higher, the need for value-translating CISOs has never been greater.

The C|CISO Hall of Fame exists to honor those who have already stepped into this role and to inspire the next generation of leaders who will define the future of cybersecurity at the executive level.

ABOUT EC-Council

EC-Council is the creator of the Certified Ethical Hacker (C|EH) program and a leader in cybersecurity education. Founded in 2001, EC-Council's mission is to provide high-quality training and certifications for cybersecurity professionals to keep organizations safe from cyber threats. EC-Council offers over 200 certifications and degrees in various cybersecurity domains, including forensics, security analysis, threat intelligence, and information security.

An ISO/IEC 17024 accredited organization, EC-Council has certified over 350,000 professionals worldwide, with clients ranging from government agencies to Fortune 100 companies. EC-Council is the gold standard in cybersecurity certification, trusted by the U.S. Department of Defense, the Army, Navy, Air Force, and leading global corporations.

TERMS AND CONDITIONS OF USE

EC-Council's intent in posting this report is to make the report available for informational purposes and personal use of the public. You are welcome to post, repost, and distribute the report provided it remains unmodified and in its original form, and you reference and link to the following source. 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.


EC-Council
Building A Culture Of Security