CyBe GLOBAL

A Global Initiative of

CSA Bangalore Chapter

In strategic association with

Karnataka Digital Economy Mission

GLOBAL CYBERSECURITY SKILLS GAP REPORT 2025

RESEARCH AFFILIATES

cloud security alliance®

sdmimd

VVCE

RESEARCH PARTNERSHIP FOR SKILL DEVELOPMENT

CyBe — A Global Initiative by CSA Bangalore Chapter

Karnataka Digital Economy Mission

Joint Vision

Empowering a future-ready cybersecurity workforce through research, collaboration, and innovation to secure the digital economy beyond boundaries.

Sanjeev K Gupta

CEO, Karnataka Digital Economy Mission (KDEM)

Sudheer KS

Mysuru Cybersecurity Cluster Head, KDEM

"

Karnataka Digital Economy Mission (KDEM) is advancing Karnataka's vision to be a global digital leader by fostering innovation beyond Bengaluru and nurturing inclusive, future-ready growth.

Recognizing cybersecurity as the backbone of a resilient digital economy, KDEM—through the Beyond Bengaluru initiative—is championing Mysuru's emergence as a cybersecurity and research hub.

This collaboration with CyBe underscores KDEM's commitment to building intellectual leadership, driving regional innovation, and developing skilled professionals who can secure the digital future.

Satyavathi Divadari

Founder & President, CSA Bangalore Chapter

Pooja Agrawalla

CO-Founder & Vice President, CSA Bangalore

"

Through the CyBe (Cyber & Beyond) initiative, the Cloud Security Alliance Bangalore Chapter is addressing the global cybersecurity skills gap through research, education, and collaboration.

CyBe is enabling accessible, practical, and career-focused learning pathways that connect academia, industry, and government.

Our shared goal is to cultivate a diverse, hands-on, and future-ready cybersecurity workforce capable of protecting critical digital ecosystems and powering sustainable innovation across industries.

CSA Bangalore Chapter
CyBe
Global Research

2018
CSA CCM v3.0.1 Addendum to the RBI's Gopalakrishna Committee (GKC) Report

2022
Technology & Cloud Security Maturity Global Survey in association with CSA & Micro Focus (Open Text)

2025: Report Draft Stage
Global Cybersecurity Skills Gap Report in association with KDEM, VVCE, SDM IMD

2024
AI Empowering cybersecurity in association with KDEM, VVCE, SDM IMD

2025: Ideation Stage
Quantum Cyber Dialogue in association with KDEM

SCAN ME

Table of Contents

Introduction

The cybersecurity industry faces a severe global talent shortage, threatening organizations' ability to defend against increasingly sophisticated threats [1]. Despite a slight rise in the active workforce to 5.5 million in 2024, growth remains nearly flat, while the workforce gap has surged 19% year-on-year to 4.8 million—leaving a total demand of 10.2 million professionals worldwide [1][2]. This shortage exposes 67% of organizations to heightened risk, with 58% identifying it as significant [2].

Asia-Pacific suffers the largest gap, while North America and Europe also face rising deficits [1][3]. Urgent, strategic interventions are critical to attract, develop, and retain skilled cybersecurity professionals globally.

To provide real-world insights, a global Cybersecurity Skills Gap Survey was initiated by CyBe, a global initiative of CSA Bangalore, with industry and academia partners, engaging over 1000 cybersecurity decision-makers across sectors such as IT/ITES, BFSI, telecom, healthcare, government, manufacturing, and startups.

Targeting CXOs, CISOs, CIOs, and HR leaders, the survey explored team structures, hiring needs, in-demand skills, retention challenges, upskilling effectiveness, academic readiness, and regional talent diversity. These findings form the backbone of this report, complemented by expert commentary and case studies.

The Survey

The Cloud Security Alliance Bangalore Chapter's CyBe Global Cybersecurity Skills Gap Report 2025, a research initiative capturing the perspectives of technology and security leaders on one of the most pressing issues today — the shortage of skilled cyber professionals.

Respondent Profile

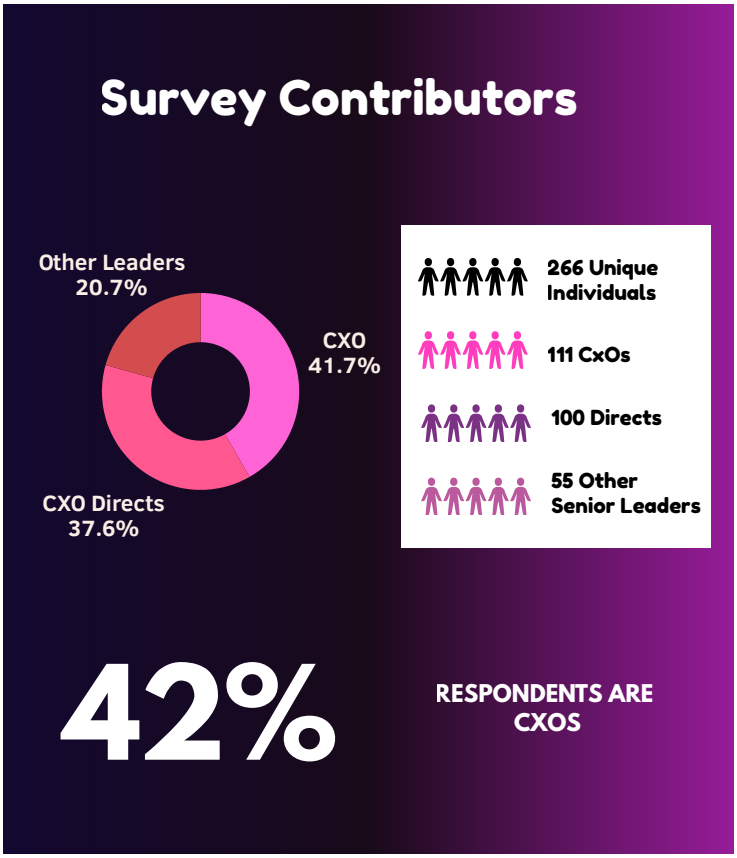
The survey collected insights from a diverse and representative set of 266 unique stakeholders

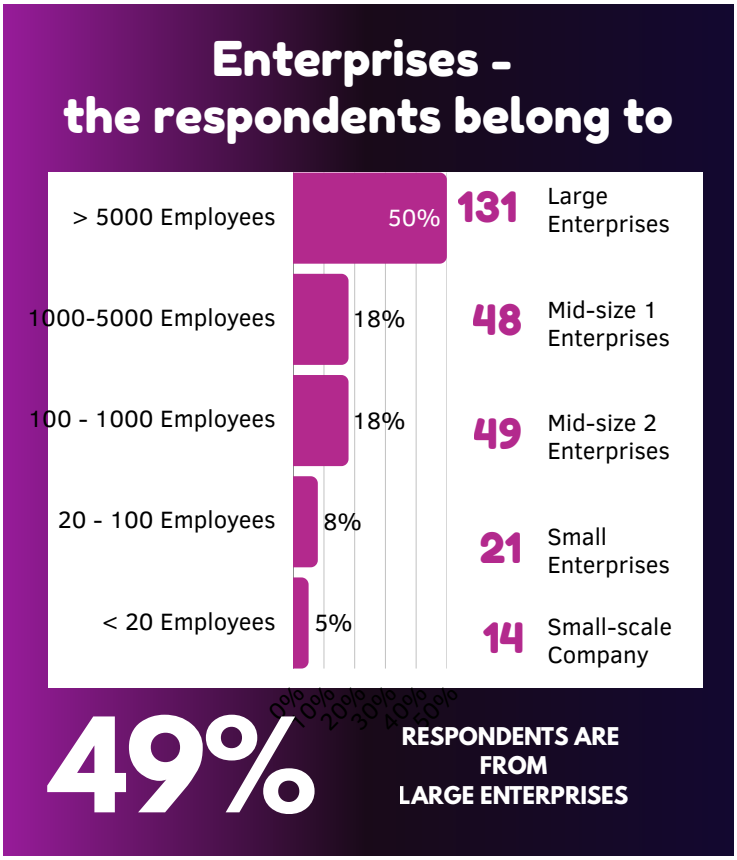
- 100 CXO Directs – senior leaders reporting directly to CXOs, with operational insights.
- 111 CXOs – CISOs, CTOs, CIOs, and CEOs, offering strategic and board-level perspectives.
- 55 Others – including security managers, architects, consultants, and industry experts.

Respondents represented organizations of all sizes, reflecting the universal nature of the skill gaps

- Large Enterprises – 131
- Mid-size Enterprises (Category 1) – 48
- Mid-size Enterprises (Category 2) – 49
- Small Enterprises – 21
- Small-scale Companies – 14

This mix provided a comprehensive, 360-degree view of industries and organizational scales.





The survey was conducted in close collaboration with government bodies such as the Karnataka Digital Economy Mission (KDEM) and the Karnataka Skill Development Authority (KSDA), as well as academic partners including VVCE (Vidyavardhaka College of Engineering) and SDM IMD (SDM Institute for Management Development).

These partnerships ensured that the report captured perspectives from policy, industry, and academia, strengthening both depth and applicability.

Key Themes Explored

The report focuses on four dimensions of the skills gap:

1. Skills Shortages – The most acute gaps identified were in cloud security, AI/ML security, SOC operations, identity management, and incident response.
2. Challenges – Respondents highlighted barriers such as lack of hands-on exposure, limited cross-domain knowledge, high attrition, and the mismatch between academic training and industry needs.
3. Impact – Skills shortages were found to affect organizational resilience, incident response times, compliance posture, and overall risk management.
4. Solutions – Leaders suggested multiple approaches including workforce reskilling, academic–industry collaborations, AI-driven learning labs, executive coaching, and global certifications.

Why This Matters

The survey highlights that the cybersecurity talent shortage is not just a pipeline issue but a strategic risk impacting innovation, resilience, and national security. It emphasizes the need for organizations to rethink workforce development by combining technical expertise, leadership skills, and AI-powered capabilities.

Way Forward

CSA Bangalore's CyBe Global Cybersecurity Skills Gap Report 2025 aims to guide governments, enterprises, and universities in:

- Scaling cyber talent pipelines in emerging markets.
- Embedding AI and cloud-first skills into training programs.
- Strengthening leadership coaching to prepare the next generation of CISOs and CXOs.

Executive Summary

Building on our prior research into AI-driven cybersecurity, this skills gap assessment highlights a critical enabler for responsible AI adoption: skilled human capital. While AI can automate detection and response, its deployment, governance, and resilience against adversarial attacks rely on experienced professionals.

The shortage of cybersecurity talent compounds integration challenges—legacy systems, siloed operations, and ethical governance gaps cannot be addressed by technology alone. By linking AI innovation with workforce readiness, this report underscores that closing the skills gap is essential for organizations to safely leverage AI's predictive power and strengthen global cyber defense strategies.

The global cybersecurity market is expanding rapidly, driven by digitization, regulation, and cybercrime costs expected to exceed USD 23 trillion by 2027 [4]. Yet, a widening skills shortage threatens security worldwide [5]. Employers need advanced technical and soft skills, creating fierce competition for talent—especially in emerging markets [5].

In India, a ₹280 billion market by 2025 faces acute shortages, with Bengaluru leading demand [6]. Despite 93% of firms increasing spending, workforce readiness lags [6]. Nearly 60% report skills gaps hindering security, with shortages most severe in AI and cloud security [5][7]. Hybrid expertise, core domains like SOC and IAM, and strong problem-solving, adaptability, and collaboration skills are urgently needed [5][7].

Skill Shortage

Overall Talent Shortage

The cybersecurity industry is facing an acute shortage of skilled professionals, with 84% of organizations citing a lack of qualified candidates as the top barrier to filling critical roles. This gap spans both technical areas—such as cloud security, AI/ML security, and SOC operations—and business-focused roles in compliance and governance.
Several factors compound the issue.

High compensation expectations limit access for small and mid-size enterprises, while lengthy hiring cycles slow recruitment across the board. Limited awareness of cybersecurity career paths reduces new entrants into the field, and soft skill gaps—in areas like communication, leadership, and cross-functional collaboration—undermine professionals' ability to connect security with business outcomes.

The impact is significant. Shortages delay digital transformation, increase operational risk, and strain existing teams, leading to burnout and attrition. To address this, organizations must invest in targeted training and reskilling, adopt strategic hiring practices that tap diverse talent pools, and expand academic–industry outreach to attract the next generation of cyber professionals.

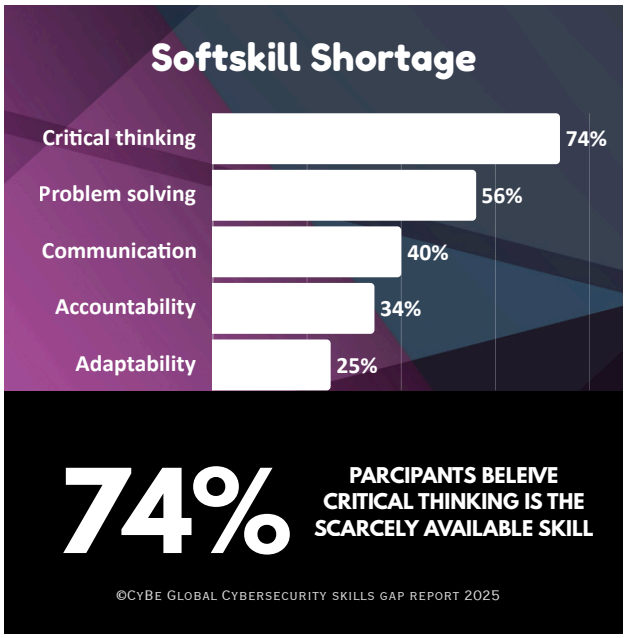
By reframing talent development as a strategic priority, enterprises can strengthen resilience and build a workforce capable of meeting today's threats while preparing for tomorrow's challenges.

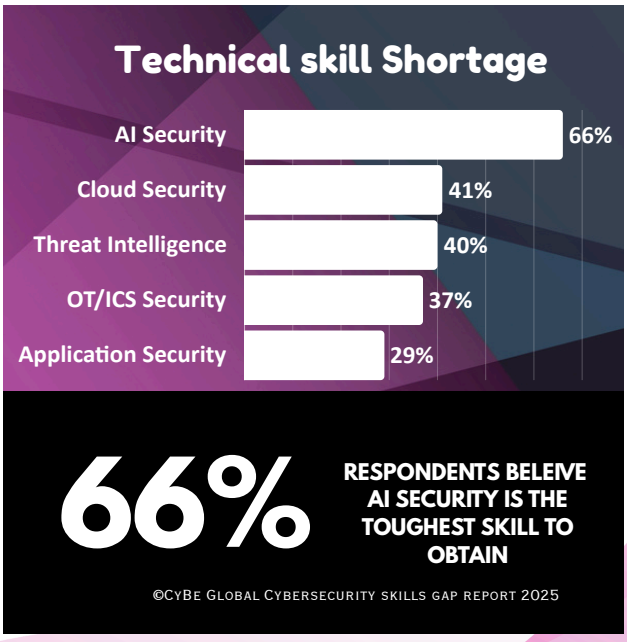
Soft skills shortage

Beyond technical expertise, organizations are finding that essential soft skills are in critically short supply. Critical thinking emerges as the most difficult capability to source, with problem-solving also highlighted as a major gap. Communication skills, accountability, and adaptability are likewise lacking, making it harder for teams to collaborate, analyze complex threats, and respond effectively under pressure. In a landscape where cybersecurity decisions increasingly involve cross-functional teams and high-stakes environments, these shortcomings can undermine resilience and slow response times. Addressing the soft skills gap is therefore as vital as technical training to build a capable and future-ready cybersecurity workforce.

Technical Skill Shortage

The cybersecurity landscape is grappling with a significant shortage of advanced technical skills. AI security stands out as the hardest capability to source, reflecting the rapid adoption of AI-driven tools and the complexity of defending them. Cloud security expertise is also in short supply, alongside critical areas such as threat intelligence, operational technology and industrial control systems security, and application security. These gaps leave organizations vulnerable as they modernize infrastructure, deploy AI, and connect OT environments. Bridging this technical skills gap is essential to safeguarding innovation, maintaining operational continuity, and strengthening defenses against increasingly sophisticated cyber threats.





Skill Gaps - Executive Layer

While nearly all boards and CEOs recognize cybersecurity as a strategic issue and most security leaders see C-suite awareness, genuine executive expertise and engagement—particularly around AI—remain insufficient.

45% cite lacking a clear GenAI strategy as a barrier [8]. Concern is higher among directors (48%) and staff (54%) than C-suite (38%) and executives (40%), revealing leadership's underestimation [8].

Only 60% of organizations involve cybersecurity teams in AI governance, falling to 50% in larger firms [9]. Limited involvement threatens weak oversight, increasing risks and unmanaged vulnerabilities in AI adoption [9].

Boards should embed cybersecurity experts in leadership, align security with business goals, and enhance executive cyber literacy to strengthen resilience and manage emerging AI-driven risks effectively.

Industry Specific Skill Gap

BFSI

Cybersecurity faces acute shortages in SOC, IR, and cloud roles, with high demand for analysts, engineers, and specialists amid gaps in forensics, threat intelligence, privacy, and compliance [10].

IT/ITES

Cybersecurity faces shortages in advanced skills like cloud architecture, AI/ML security, DevSecOps, and blockchain, alongside high demand for SOC analysts, penetration testers, and security architects [11].

Healthcare

Healthcare security remains understaffed, facing shortages of skilled professionals to protect electronic health records (EHRs), secure medical IoT devices, and provide continuous 24x7 monitoring and defense [12].

Manufacturing and Energy

Sectors with low cyber maturity need talent in basics like network and endpoint security, while emerging OT/IIoT roles—engineers, analysts, and penetration testers—are scarce and urgently required [13].

Industry impact

Impact of Cybersecurity Skills Gaps on Financial and Operational Performance:

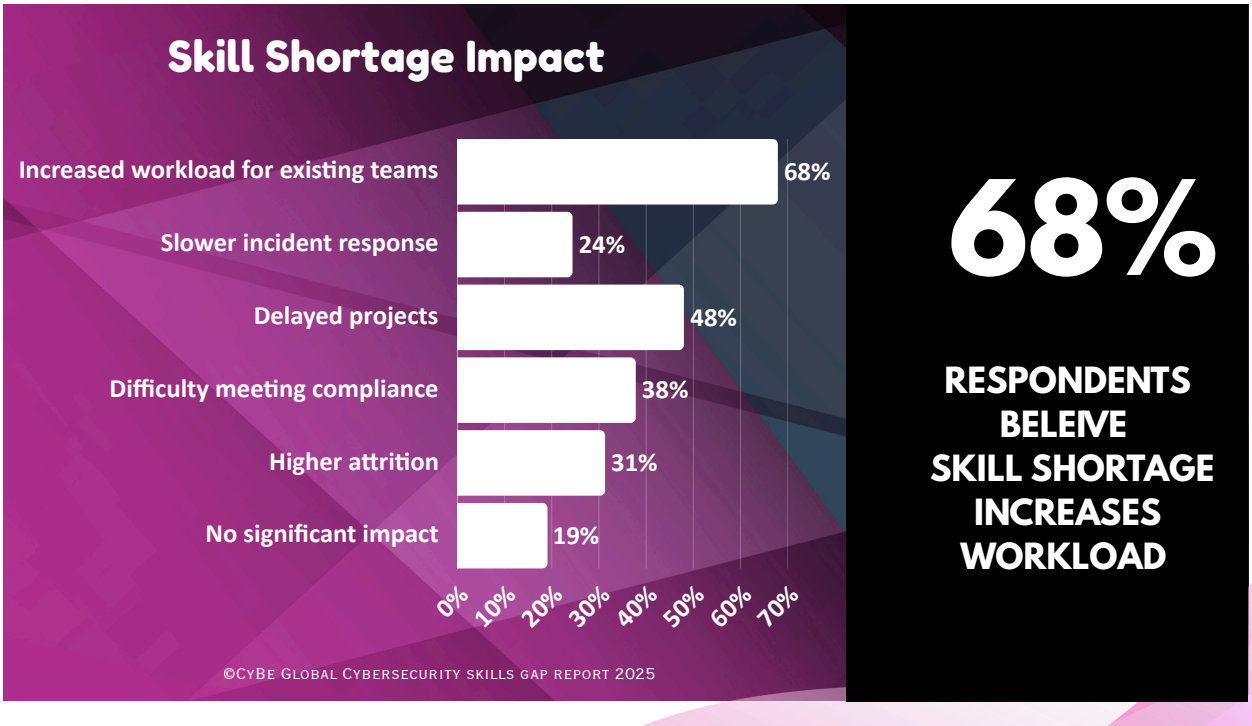
Skills gaps are driving substantial financial and operational losses. Roles most impacted by digital transformation can lose up to 25% of output. A Fortune-500 manufacturer forfeited $420M EBITDA over three years from automation rework and downtime, while AI product launches face 4–6 month delays. A fintech firm lost $1.3M revenue per quarter, and a global bank spent $98M replacing cyber talent. Roles without clear L&D paths see 2× attrition, costing 1.5–2× salaries. Post-breach costs average $4.45M, with personal liability and EU fines up to 2% of global turnover. Each 10-point skills-readiness rise links to 6% higher ROIC [14].

CXO Perspectives on Cybersecurity Skills Gaps:

CXOs identified a wide range of consequences resulting from cybersecurity skills gaps, highlighting their far-reaching impact on organizations. 58% of leaders reported delayed security or digital transformation projects, slowing innovation and weakening competitive advantage.

43% noted an increased reliance on outsourcing to external vendors, which can raise costs and introduce third-party risks. 40% cited higher stress levels and staff attrition, affecting morale and continuity. 34% pointed to regulatory compliance challenges, while 20% acknowledged lost revenue opportunities.

Finally, 18% reported increased security incidents. Together, these findings underscore the operational, financial, and human costs of unfilled or under-skilled cybersecurity roles [15].



Emerging Roles and Skills

Cybersecurity Career Path & Roadmap (2025 and Beyond)

Executive & Strategic Leadership
The CISO defines strategy, manages risk, ensures compliance, and increasingly supports resilience at national and city levels. This role demands leadership, cloud security expertise, and fluency in frameworks like NIST and ISO 27001 [16]. Alongside, the Chief Privacy & Data Protection Officer (CPDPO) is vital for handling GDPR, India's DPDP Act, and AI data governance.

- CISO: Strategy, risk, compliance, resilience
- CPDPO: Privacy law, AI governance, data protection

Architecture & Engineering
Security Architects are among the most in-demand roles for 2025, creating enterprise frameworks that embed Zero Trust and resilience by design. Cloud Security Engineers ensure the safety of AWS, Azure, and GCP while integrating DevSecOps practices. Application Security Engineers protect APIs and pipelines, and the AI/ML Security Engineer is emerging to safeguard models from adversarial ML and data poisoning [16].

- Security Architect: Enterprise frameworks, Zero Trust
- Cloud Security Engineer: Cloud platforms, DevSecOps
- AppSec Engineer: APIs, secure coding, OWASP
- AI/ML Security Engineer: Adversarial ML, model risk

Operations & Response
On the frontlines, Cybersecurity Analysts and Incident Responders monitor environments using SIEM and XDR, investigate threats, and respond to breaches. Penetration Testers (ethical hackers) simulate real-world attacks, while Threat Intelligence Analysts study adversary behaviors and AI-driven malware. Hybrid Red, Blue, and Purple Team specialists combine attacker and defender insights for advanced readiness.

- Analyst/Responder: SOC operations, SIEM, containment
- Pen Tester: Offensive security, exploit frameworks
- Threat Intel Analyst: Malware trends, CTI platforms
- Hybrid Teams: Red, Blue, Purple—attack + defense

Advisory, Compliance & Risk
Cybersecurity Consultants and Security Specialists advise across industries like BFSI, healthcare, and e-commerce, implementing frameworks and compliance controls [16]. GRC Analysts ensure regulatory alignment, while new roles like AI Risk & Compliance Officers tackle ethical AI use and emerging AI regulations.

- Consultant/Specialist: Risk assessment, audits
- GRC Analyst: NIST, ISO 27001, CSA CCM
- AI Risk Officer: Responsible AI, bias mitigation

The Specialized & Emerging Roles

Beyond core functions, OT/ICS Security Engineers protect industrial systems, while IoT/Edge Security Specialists focus on billions of devices in smart cities and healthcare. Cybersecurity Product Managers blend business and technical skills, and Cyber Resilience Managers lead ransomware readiness and crisis planning.

- OT/ICS Engineer: Critical infrastructure defense
- IoT/Edge Specialist: Smart devices & edge security
- Product Manager: AI security product strategy
- Resilience Manager: Crisis response & BCP

Roadmap Stages

Cybersecurity careers typically evolve through four stages:

1. Foundation – SOC Analyst, Security Analyst, GRC Analyst.
2. Specialization – Cloud Security Engineer, Pen Tester, AppSec Engineer.
3. Advanced – Security Architect, Threat Intel Analyst, Consultant.
4. Future – AI/ML Security Engineer, AI Risk Officer, Resilience Manager.

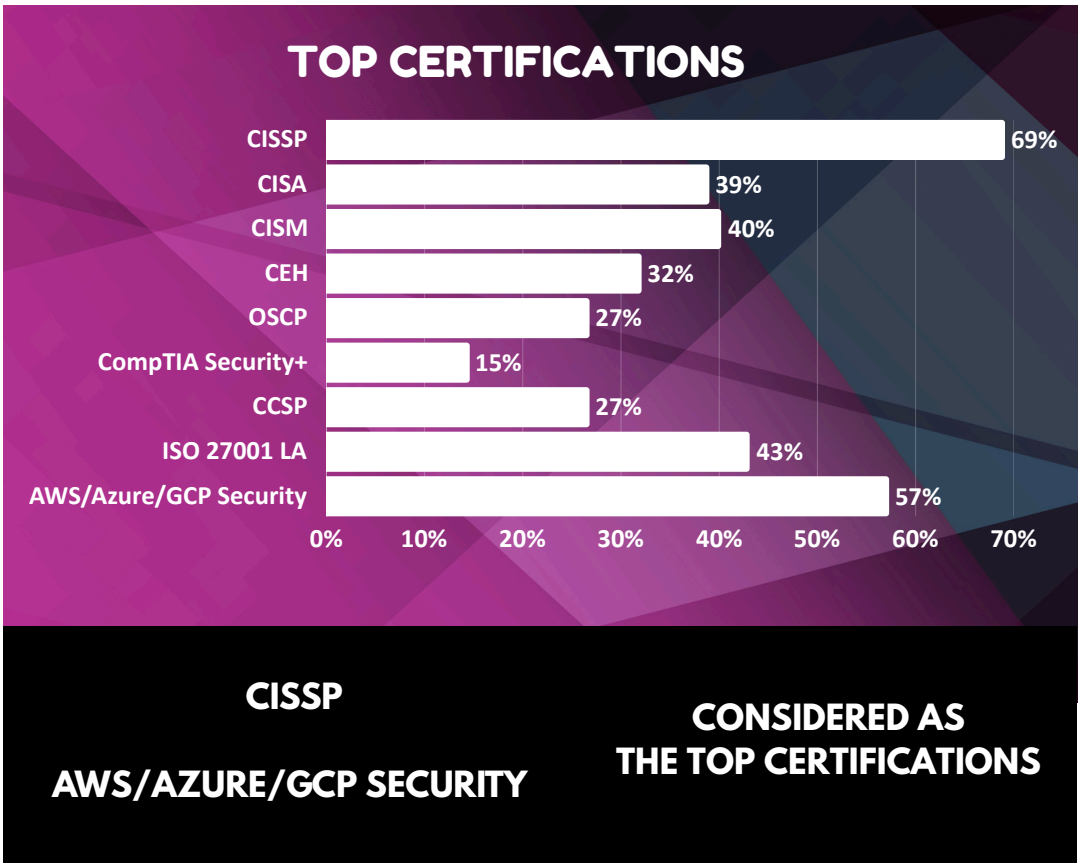
Key Trend [16]: The workforce is moving toward cloud-first, AI-driven, and compliance-focused strategies. Success now depends on not only deep technical skills but also adaptability, collaboration, and problem-solving.

Move Towards Closing the Gap

Role of Professional Certifications in Closing the Cybersecurity Skills Gap

Professional cybersecurity certifications play a pivotal role in reducing the global skills gap by validating expertise, standardizing knowledge, and signaling readiness to employers.

Key certifications such as CISSP (Certified Information Systems Security Professional), CISA (Certified Information Systems Auditor), and CISM (Certified Information Security Manager) establish advanced competencies in governance, risk, and compliance.



CEH (Certified Ethical Hacker) and OSCP (Offensive Security Certified Professional) validate hands-on penetration testing and offensive security skills, while CompTIA Security+ provides an essential foundation for entry-level professionals.
With cloud adoption accelerating, CCSP (Certified Cloud Security Professional) and AWS/Azure/GCP Security credentials ensure expertise in securing multi-cloud environments. For organizations prioritizing compliance, ISO 27001 Lead Auditor certification confirms proficiency in auditing and implementing information security management systems.

By setting global benchmarks, these certifications give hiring managers confidence in candidates' capabilities, streamline recruitment, and encourage continuous professional development—ultimately strengthening the cybersecurity workforce and improving organizational resilience against evolving threats [17].

Closing the Skills Gap: Mentorship, Academia Partnerships, and Practical Learning

Notably, 80% of respondents emphasize hands-on experience as the most critical factor for producing job-ready cybersecurity professionals. Closing the skills gap requires more than classroom learning or certifications—it demands immersive, practical exposure that mirrors real-world challenges.

Mentorship plays a pivotal role by pairing emerging professionals with experienced practitioners who can guide problem-solving approaches, share contextual insights, and foster career growth. Strong academia–industry collaboration is equally essential: universities must align curricula with evolving threat landscapes, while industry partners provide case studies, cyber ranges, and guest lectures that bring theory to life.

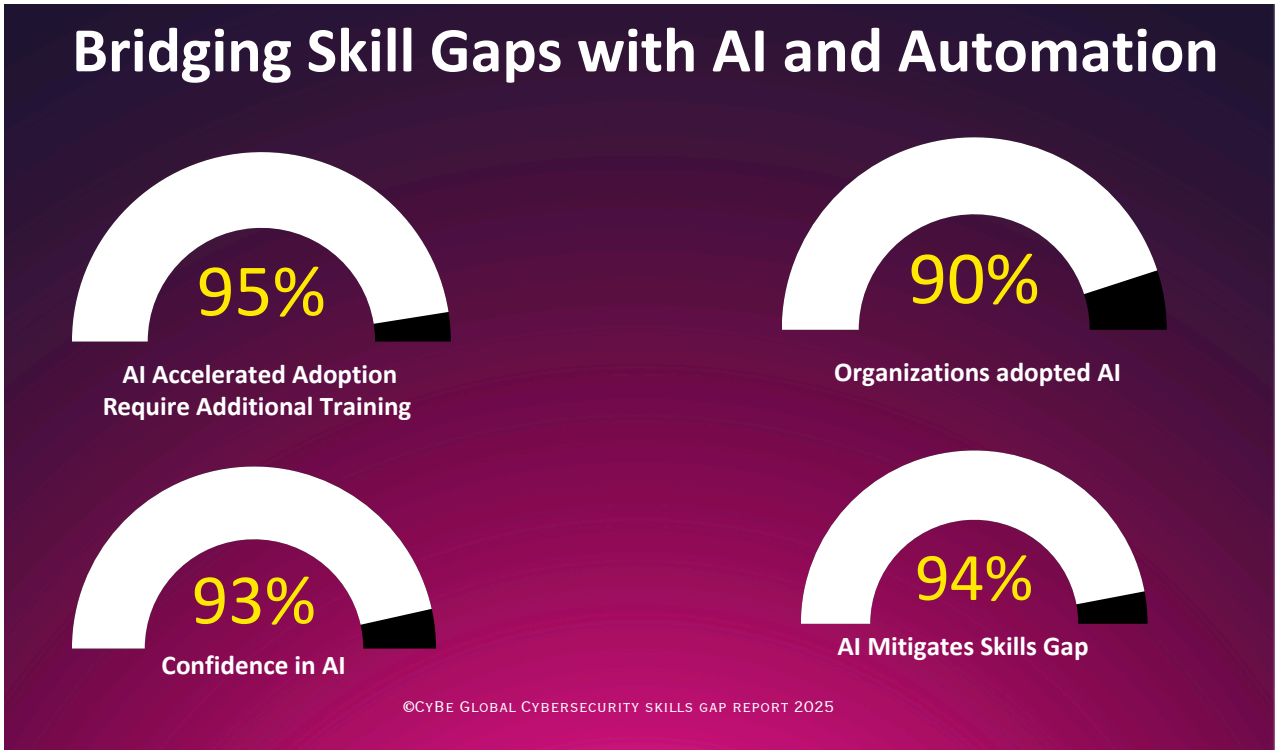
Strong academia–industry collaboration is equally essential: universities must align curricula with evolving threat landscapes, while industry partners provide case studies, cyber ranges, and guest lectures that bring theory to life. Structured internship programs bridge this gap further, giving students and entry-level hires the opportunity to work on active security projects, develop confidence, and contribute meaningfully from day one.

Organizations should also invest in in-house learning academies and upskilling programs to ensure existing teams keep pace with cloud-native security, AI-driven defense, and compliance requirements. Regular training and cross-functional workshops enhance team competency, reduce attrition, and create a culture of continuous improvement.

By combining formal education, mentorship, internships, and targeted upskilling, the cybersecurity community can develop resilient, job-ready talent. These collaborative initiatives not only strengthen organizational defenses but also build a sustainable pipeline of skilled professionals for the future.

AI's role in bridging skillsgap

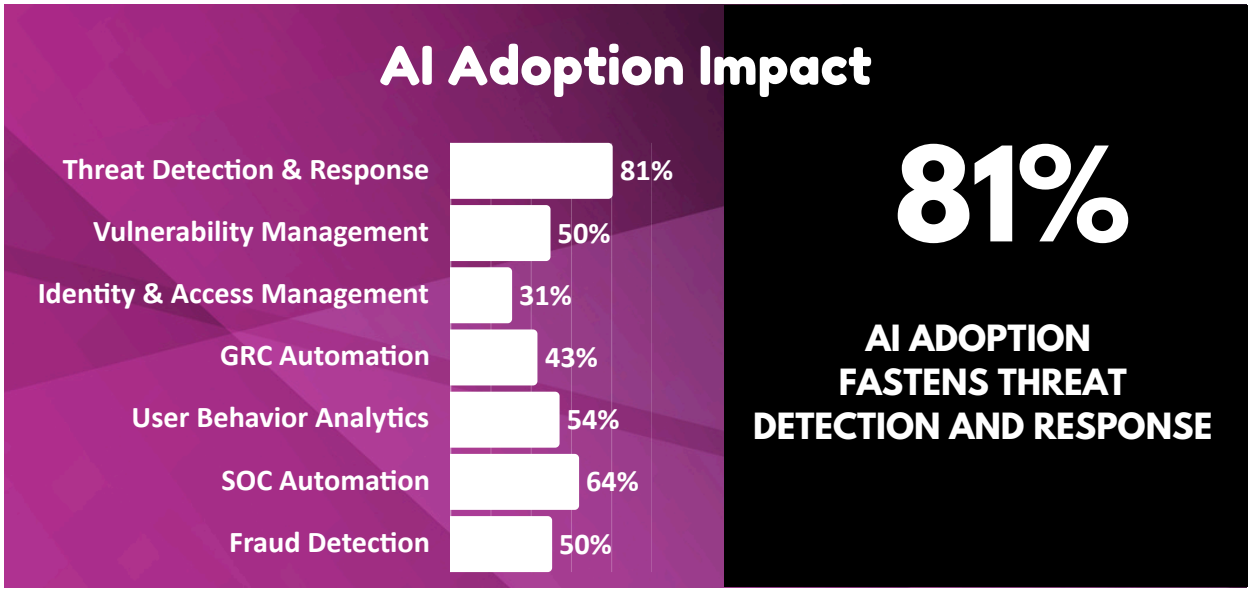
Artificial Intelligence (AI) presents a transformative opportunity to address the cybersecurity skills gap. By automating repetitive tasks such as log analysis, threat detection, vulnerability scanning, and incident triage, AI allows skilled professionals to concentrate on higher-value, complex challenges that demand human judgment and strategic thinking. Advanced AI-driven analytics, simulations, and cyber ranges can create adaptive training environments, offering hands-on, scenario-based exercises that accelerate skill development for both new and experienced professionals.



AI's predictive capabilities enable organizations to anticipate emerging threats and evolving attack vectors, ensuring teams remain proactive rather than reactive. Furthermore, AI-powered assessment tools can identify skill deficiencies within security teams, enabling leaders to implement targeted upskilling and resource allocation strategies. This not only optimizes training investments but also strengthens overall security posture.

When strategically integrated with human expertise and ethical governance, AI becomes more than a productivity tool—it becomes a catalyst for workforce readiness, operational resilience, and sustainable cybersecurity defense in a rapidly shifting threat landscape.

CXO Perspectives: AI's Greatest Impact Areas in Cybersecurity



A significant 81% of CXOs believe that Threat Detection & Response would benefit the most from AI adoption, underscoring its critical role in strengthening organizational security posture. As cyber threats grow in complexity and volume, AI-driven systems can rapidly analyze vast datasets, detect anomalies, and respond to incidents faster than traditional methods—reducing dwell time and minimizing damage.

Beyond detection and response, CXOs see broad potential for AI across multiple domains. Vulnerability Management can leverage AI to prioritize risks dynamically, while Identity & Access Management (IAM) benefits from intelligent authentication and anomaly detection. GRC Automation (Governance, Risk, and Compliance) can be streamlined through AI-powered policy enforcement and reporting. User Behavior Analytics enables early identification of insider threats, while SOC Automation reduces manual workload, improving efficiency. Finally, Fraud Detection gains from AI's ability to uncover subtle, previously undetectable patterns. Collectively, these insights reflect AI's transformative potential across the cybersecurity ecosystem.

Conclusions

The cybersecurity skills gap is a pressing and growing threat to global resilience. Despite record investments and modest workforce growth, the gap has surged to 4.8 million professionals worldwide, undermining organizations' ability to counter escalating cybercrime projected to exceed USD 23 trillion by 2027. Asia-Pacific faces the largest deficits, while North America, Europe, and emerging markets also struggle to keep pace with demand.

Our survey of 500+ cybersecurity decision-makers reveals that shortages are both numerical and qualitative: expertise in AI security, cloud security, and hybrid domains like DevSecOps, OT, and privacy engineering remains scarce. The consequences are significant—delayed projects, increased outsourcing, compliance risks, attrition, financial losses, and greater exposure to security incidents.

Bridging this gap demands a multi-pronged strategy. Certifications, ongoing training, mentorship, and academia collaboration are vital to develop job-ready professionals. With 80% of leaders emphasizing hands-on experience, organizations must invest in real-world training, cyber ranges, and adaptive learning.

AI offers a promising lever—automating routine tasks, enhancing detection, and providing analytics to guide upskilling—yet its success depends on skilled professionals, ethical governance, and cross-functional collaboration. Urgent, coordinated action

Satyavathi Divadari — Founder & President, CSA Bangalore Chapter — Editor

Madhu Bhat — Head - Research and Innovation, CSA Bangalore Chapter — Sub-Editor

CONTRIBUTORS

Authors	Name	Designation	Organization
	Nidhi Varshney Singhai	Principal Engineer	Red Piranha
	Pradeep Kumar	Senior Program Director	Ericsson
	Anju Gupta	Information Security Engimeer	Wells Fargo
	Dr. Anand Ellur	Associate Professor	SDM Institute for Management Development
	Seema Khandelwal	Senior manager	LTIMindtree
	Madhukeshwar Bhat	Head of Research	CSA Bangalore chapter
	Satyavathi Divadari	Founder, President	CSA Bangalore chapter
	Pooja Agrawalla	Co-Founder, vice President	CSA Bangalore chapter
	Dr. Keerthan Raj	Associate Professor	SDM Institute for Management Development

CONTRIBUTORS

Reviewers	Name	Designation	Organization
Reviewer	Nagammai shanmugham	Vice president	Standard Chartered Bank
Reviewer	Dr Ramkumari H Iyer	CIO and CISO	Reliscale
Reviewer	Shashank Gidbidi	Cybersecurity Lead	I2E Consulting
Reviewer	Mahesh T	Head of Product Security	Atlan
Reviewer	Anand Kumar Jha	Vice President- Lead systems Architect	Wells Fargo
Reviewer	Prem Kumar	Founder	Power of Knowing Forum

ORGANIZATIONS OF THE CONTRIBUTIORS

3M India Ltd	Alliance University	AuthenticOne	Biocon
Accenture	Allstate India Pvt Ltd	AuthenticOne CyberSecurity Pvt Ltd.	Blue Mantle Ventures
Accorian	Ankura Consulting India Pvt Ltd	Axisbank	BNI Global
Acko	ANZ	Ayana Renewable Power Pvt. Ltd.	Bosch
Airtel Africa	A-One Steel India Limited	Baker Hughes	Brillio Technologies
Alcatel Lucent Enterprise	Apraava Energy	Baxter	Buhlergroup
AliceBlue	Aravind Eye Care Sytem	BDO RISE	CanopusGBS
AliceBlue Financial Services Pvt Ltd	Aster DM healthcare	Bennett, Coleman & Co. Ltd.	Capgemini
Allcargo Logistics Limited	AT&T	Bergworx	CBA India
ALLEN Career Institutes Pvt. Ltd	AtyaSecure	BIAL	C-DAC
Chargebee	Diageo	Envision Energy	Flipkart
Cognizant	Digiplug Technologies Pvt. Ltd.	Ephicacy Lifescience Analytics	Flora Food Group
Computer society of india / trcimpex	DMI Finance Pvt Ltd	Ericsson	Frontline FinTech
Coralogix	DNV business Assurance	ETC Management	GBS
Harbinger Group	ISACA SRILANKA	JPMorgan Chase	LogiCoy
HDFC Bank	ISC2 Bangalore Chapter	Justdial Ltd	LTIMINDTREE

Honeywell International	Itc infotech	Klickstart Business	Manufacturing MNC
IAF	iValue Infosolutions	Kotak Mahindra Bank Limited	Mara Labs Inc. (Locus.sh)
Ideassion Technology Solutions	JBM Group	KPMG	Marvell Technology, Inc
iManEdge Services	Jio Platforms ltd	Kyndryl	Marven Data Systems
Indus Marks IP Consulting	Jio Platforms Ltd	Leadsquared	Mashreq
Infosys Limited	JPMC	Lenovo	Matrimony.com
Intuitiveshield Pvt Ltd	JPMorgan Chase	Liminal Custody	MetaMagic Global
MetricStream	NeevNaav	Nokia Solutions & Networks India Pvt Ltd	PayPal
MGC Global Risk Advisory LLP	NeST Group, SFO Technologies	Norwin Technologies	Paytm
Microland Ltd	Nestle Global Services Limited	NPSTX	Philips
MIDLAND CREDIT MANAGEMENT	NetApp	NTT DATA	Play Games24x7
Milestone Technologies Inc	NetNXT Network Pvt Ltd	o9 solutions	Power of Knowing Forum
Morgan Stanley	Netskope	Ocrolus Inc	Pricol Limited
mPokket Financial Services Pvt Ltd	Neurealm	Onit	Muthoot Fincorp Ltd
	NewsCorp	Opentext	PrivacyPillar

NAVI	NextWealth Entrepreneurs	OWASP	PropertyGuru Group
NCB Management Services Inc	NIC-National Informatics Centre	Ozonegroup	Rakuten India
Rakuten Mobile	ShunyEka Systems	Techants Solutions Pvt Ltd	Trinet Inc
RBL	Siemens Healthineers	Teleperformance Global Services	Tripura University
Reliscale Consulting	SISA Information Security Services	Tessolve Semiconductor	Tsaaro Consulting
Rockwell Automation	State Street	Teva Pharmaceuticals	TTK PRESTIGE LIMITED
Rossell Techsys Ltd	STL DIGITAL LIMITED	The Federal Bank	TVS Automobile Solutions
S&P Global	Subex Ltd	The Hindu Group of Publications	TVS Group
Scienaptic Systems Inc	Swinkpay Fintech Private Limited	The Ramco Cements Limited	TVS Motor Company
Secure369	Swiss Re	Thomson Reuters	TVSM
ServiceNow	Takeda	Thoucentric	UBX Cloud
Shinhan Bank	Tamilnad Mercantile Bank	Toradex Systems India Pvt. Ltd	udaan
Unisys	Valsoft Corporation Inc	ValueX Technologies	VAPT Consultants Pvt Ltd
Vee Healthtek	VFS Global Services	Virsec Systems Inc	Virtusa Corp
Vodafone	Vodafone India Services	Volvo Group	Vonage Business Communication
Wells Fargo	Wipro	Xerox	Zee Entertainment
Zeotap	Zeta	Zetwerk	Zoomcar
ZSCALER INC			

REFERENCES

[1] ISC² Cybersecurity Workforce Study 2024 – Global workforce and gap data.
[2] ISC² Insights 2024 – Organizational risk percentages and YoY gap increase.
[3] ISC² Regional Workforce Breakdown 2024 – Asia-Pacific, North America, and Europe gap trends.
[4] Cybersecurity Ventures / Embroker – Global cybercrime costs projection to exceed USD 23 T by 2027.
[5] ISC² Cybersecurity Workforce Study 2024 – Global skills shortage and competition for talent.
[6] NASSCOM / DSCI Cybersecurity India Market Report 2025 – Indian market size, regional demand, and spending trends.
[7] ISC² Insights 2024 – Skills gaps (AI and cloud security) and soft skills importance.
[8] Gartner Research. 2024 Generative AI in Cybersecurity Survey – Strategy Gaps and Leadership Perception Findings.
[9] Forrester Research. AI Governance and Security Oversight Report 2024 – Cybersecurity Team Involvement and Risk Implications.
[10] ISC² Cybersecurity Workforce Study 2024 – Industry-Specific Shortages and Demand in BFSI Sector.
[11] ISC² Cybersecurity Workforce Study 2024 – Advanced Skills Shortages and Role Demand in IT/ITES Sector.
[12] Healthcare Cybersecurity Workforce Shortage, HIMSS, 2023.
[13] "Addressing the Ongoing OT Security Skills Gap," Manufacturing.net, December 21, 2023.
[14] "Cybersecurity Skills Shortage Directly Tied to Financial Losses," IBM Think, October 17, 2024. https://www.ibm.com/think/insights/cybersecurity-skills-gap-contributed-increase-average-breach-costs
[15] "2024 Cybersecurity Workforce Report: Bridging the Workforce Shortage and Skills Gap," Boston Consulting Group (BCG), October 2, 2024. https://www.bcg.com/publications/2024/cybersecurity-talent-shortage-close-the-gap
[16] "2025 Cybersecurity Workforce Research Report," SANS | GIAC, 2025. https://www.sans.org/mlp/2025-attract-hire-retain-cybersecurity-roles
[17] "2024 Cybersecurity Skills Gap Report," Fortinet, June 20, 2024. https://www.fortinet.com/content/dam/fortinet/assets/reports/2024-cybersecurity-skills-gap-report.pdf

CALL TO ACTION

The cybersecurity skills gap is more than a workforce challenge — it affects innovation, operational resilience, and national security. But addressing it presents a tremendous opportunity.

We invite professionals, educators, policymakers, and organizations to collaborate in advancing research, sharing insights, and developing actionable solutions. Whether as a contributor, mentor, institutional partner, or advocate for workforce development, your involvement is crucial. Let's work together to build a skilled, resilient cybersecurity ecosystem that can meet today's threats and tomorrow's challenges.

Ready to make an impact
Reach out to us at
support@cybe.global

Join our community — it's free and open to all:
www.cybe.global

CyBe GLOBAL

A Global Initiative by

CSA | Bangalore Chapter

About CSA Bangalore & CyBe Global

The CyBe Global, an initiative by CSA Bangalore is a national movement to build 1 million cyber defenders by 2030 through accessible, career-focused cybersecurity and AI education. As one of CSA Global's most recognized chapters, CSA Bangalore drives this mission by blending industry collaboration, academic partnerships, and community innovation.

Through CyBe, we aim to equip students, professionals, and institutions with the skills, tools, and knowledge needed to navigate and secure the digital future.