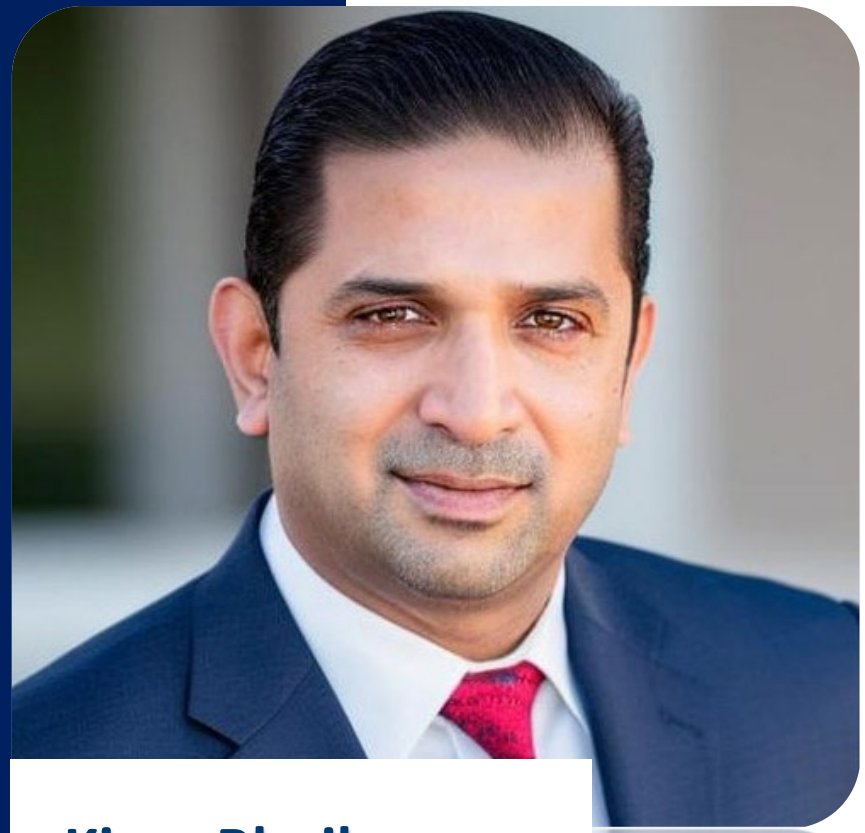
NEW YORK METRO JOINT CYBER SECURITY CONFERENCE

Trends in Cybersecurity and the Growing Talent Group



Kiran Bhujle

- **SVAM International** – Cybersecurity Practice Leader
- **Columbia University** – Faculty in the Enterprise Risk Management Masters Program
- **Forbes Technology Council** – Executive Member
- **Harvard Business Review** – Cybersecurity Advisory Board
- **Green Guerilla** – Board of Directors

Evolution of Cybersecurity Threats

1980s – 1990s

Early viruses and worms targeting **standalone computers**.

Spreading via floppy disks, although not highly sophisticated, laid the groundwork for future attacks.

Late 1990s – Early 2000s

Network-based attacks thanks to the rise of Internet.

First denial-of-service (**DoS**) and distributed denial-of-service (**DDoS**) attacks.

Malware became more sophisticated, exploiting network vulnerabilities.

2000s

More financially motivated, targeting **credit card** data.

The rise of **phishing**, targeting individuals as well as corporate systems.

2010s

State-sponsored attacks and advanced persistent threats (APTs).

Cyber warfare and espionage became significant concerns.

The rise of **ransomware**, such as encrypting data for ransom.

Late 2010s – Present

Highly sophisticated, multi-vector attacks combining multiple techniques, leveraging **AI and machine learning** for rapid evolution.

Cloud and IoT vulnerabilities are increasingly exploited.

Evolution of Cybersecurity Protection

1980s – 1990s

Early antivirus software detecting and blocking viruses and unauthorized access.

Regular backups to recover lost or corrupted data.

2000s

Web application firewalls (**WAF**): protect by filtering HTTP traffic.

Email filtering: block phishing emails and educate users about risks.

Late 2010s – Present

Cloud Security Solutions.

Use of **AI and machine learning** to predict and identify attacks faster.

IoT security measures.

Late 1990s – Early 2000s

Firewalls to block unauthorized network access.

Intrusion detection and prevention systems (**IDS/IPS**).

Patch management.

2010s

Threat Intelligence.

Zero Trust Architecture.

SVAM INTERNATIONAL, INC.

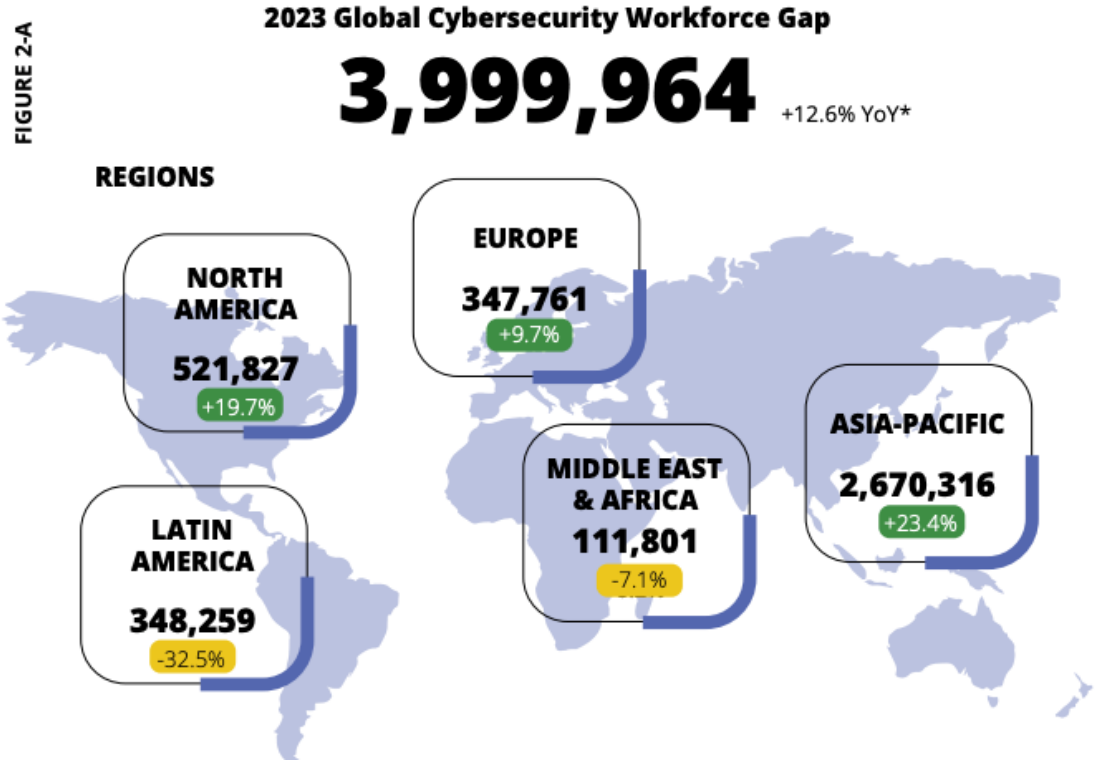
Cybersecurity Workforce Shortage

4 Million

Global cybersecurity workforce shortage reached nearly 4 million (3,999,964) while the workforce itself is estimated to be only just over 5 million (5,452,732) in 2023, according to an ISC2 report

67%

According to an ISC2 report, over two thirds (67%) of the 14,865 cybersecurity professionals surveyed in 2024 reported that their organization has a shortage of cybersecurity staff needed to prevent and troubleshoot security issues.



Shortfalls were especially acute in:

- **Japan**: up 97.6% to 110,000 (nearly doubled)
- **Canada**: up 53% to 39,000
- **India**: up 40.2% to 790,000
- **U.K.**: up 29.3% to 73,000

SVAM INTERNATIONAL, INC.

https://www.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf

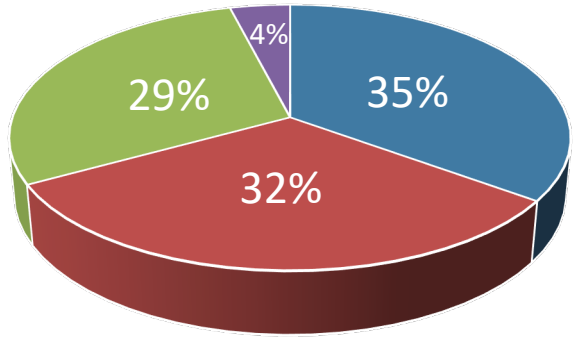
But What Is Even Worse Is…

Cybersecurity **skill gaps** are more challenging compared to workforce shortages.

92%

92% of cybersecurity professionals report skills gaps within their organizations, according to an ISC2 report.

Cybersecurity Skill Gaps Reported by Professionals within Their Organizations



https://www.isc2.org/Insights/2023/10/ISC2-Reveals-Workforce-Growth-But-Record-Breaking-Gap-4-Million-Cybersecurity-Professionals

Cybersecurity Workforce Shortage

Lengthy Time to Hire and to Train

It takes a company **6 months to a year** to hire qualified cybersecurity personnel or to train employees in the latest cybersecurity and privacy approaches.

Becoming a skilled cybersecurity expert, capable of understanding the latest trends, can take **3 to 5 years**, or even longer for deep expertise.

High level Specialization and Instability in Workforce

Cybersecurity has evolved into a field with **numerous specialties**, making it unrealistic for individuals to master all areas, similar to specializations within medicine.

The cybersecurity field is known for **high turnover rates**, with professionals frequently moving between companies, making it more challenging for companies to maintain a stable and skilled workforce.

Industry-Academia Gap

Academic curricula often struggle to keep pace with the rapidly evolving new threats and constantly emerging technologies, resulting in graduates' **lack of the most up-to-date knowledge and skills**.

Lack of hands-on practical experience can leave graduates unprepared for the demands of the cybersecurity workforce.

Economic Costs Due to Cybersecurity Talent Shortage and Skill Gaps

$10 Trillion

Cybercrime projected by Forbes Tech Council to cost the U.S. economy over 10 trillion dollars annually in 2025, a substantial rise from the $3 trillion in 2015

78%

Cyber breaches reported in the U.S. increased by 78% in 2023 compared to 2022, according to secureframe stats.

Financial companies, in particular, are hit by an average of 50 cyberattacks every month, leading to significant financial losses

$9.48 Million

According to the Forbes Tech Council, the average cost of a corporate cybersecurity breach in the U.S. is $9.48 million, more than double of the global average of $4.45 million

https://www.forbes.com/councils/forbestechcouncil/2023/02/22/105-trillion-reasons-why-we-need-a-united-response-to-cyber-risk/

https://www.forbes.com/councils/forbestechcouncil/2024/03/06/the-state-of-cybersecurity-part-one-why-are-there-still-so-many-data-breaches/

https://secureframe.com/blog/data-breach-statistics

Cyber Talent Gaps Pose Threats Not Only to Our Economy, But Also to…

Disruption of Essential Services

According to a Forescout research, over **420 million attacks** targeting network infrastructure and IoT devices, including IP cameras and building automation systems happened in 2023 — translating to **13 attacks per second** — a 30% increase from the previous year.

About **53%** of those cyberattacks were directed at government or private-sector organizations that play crucial roles in maintaining critical infrastructure.

Compromise of National Defense

Cyberattacks have targeted over 120 countries in 2023, with nearly **half aimed at NATO member states,** according to a Microsoft report.

DoD 2024 documents highlighted cyber threats to our national defense by **nation-state adversaries**. Threats include intrusions into critical defense infrastructure, potentially disrupting national security systems and military operations

Threat to Public Health and Safety

Disruption of Healthcare Services: Cyber attacks on healthcare systems can lead to the shutdown of critical medical devices and hospital operations, and may also disrupt emergency services and communications.

Compromise of Patient Data: Cyber incidents can expose or corrupt patient records, leading to privacy breaches and potential misdiagnoses or incorrect treatments, with serious implications for patient health.

https://www.forescout.com/press-releases/2023-threat-roundup/
https://news.microsoft.com/en-cee/2023/10/12/microsoft-issued-annual-digital-defense-report-espionage-fuels-global-cyberattacks/
https://media.defense.gov/2024/Mar/28/2003424523/-1/-1/1/DOD_DOB_CS_STRATEGY_DSD_SIGNED_20240325.PDF

How Can Different Sectors Help Address the Growing Cyber Talent Gaps?

Government: Establish Frameworks, Create Policies, and Fund Initiatives to Address the Talent Gap

Refine National Cybersecurity Strategies

- Continuous update on national cybersecurity strategies
- Extend focus beyond defense to talent development.

Public-Private Partnerships for Training

- Resource sharing with tech companies
- Talent sharing during crises
- Joint initiatives for training and research

National Campaigns for Cybersecurity Careers

- National awareness campaigns
- Attract the new generation

Private Sector: Build, Retain, and Grow a Skilled Cyber Workforce

Expand the Cyber Talent Pool through Flexible Hiring and Training

- Hire individuals with transferable skills from IT or adjacent fields
- Provide on-the-job training

Invest in Internal Training and Upskilling

- Professional development programs in emerging fields like AI-driven threats, cloud security, and incident response.
- Offer certifications and specialized training tracks to employees interested in transitioning into cybersecurity roles.

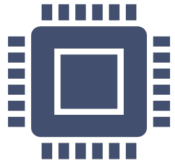
Enhance Compensation, Benefits, and Career Development

- Competitive compensation packages and flexible working conditions to improve job satisfaction
- Well-defined career paths
- Long-term and customized professional development plans.

Educational Institutions: Inspire Future Cyber Leaders with Industry-Academia Partnership and Innovative Trainings Plans

Industry-Academia Collaborations

- Encourage industry experts and executives to teach at high educational institutions
- Flexible teaching schedules and streamlined hiring process for industry professionals.
- Internships and co-operative education programs with industry partners



Education Program Expansion and Innovation

- Incorporate emerging technologies and trends (e.g. AI-driven security, cryptography, and Zero Trust architectures) into coursework
- Integrate preparation for industry-recognized certifications (e.g. CISSP, CEH, and CompTIA Security+) into curricula
- Ensure graduates are immediately employable in the cybersecurity workforce.

Civil Society: Promote Awareness, Inclusivity, and Early Community Engagement in Cybersecurity.

Promote Inclusivity and Diversity in Cybersecurity

- Boost the cyber workforce with underrepresented groups
- Attract talents with non-technical backgrounds
- Bring innovative problem-solving and cyber threat defense strategies

Raise Awareness and Advocacy

- Public cybersecurity career awareness campaigns organized by NGOs
- Target both K-12 students and mid-career professionals

International Organizations: Foster Global Collaboration and Establish Consistent Standards

Facilitate Cross-Border Collaboration and Knowledge Sharing

- Promote cross-border partnerships to encourage countries to share best practices
- Facilitate cross-border sharing of training resources and talents

Set Global Standards for Cybersecurity Education

- Organizations like ISO, NIST, and ISACA can lead in developing global cybersecurity education standards
- Promote consistent training and qualifications across countries.

Support Global Capacity Building in Emerging Markets

- Provide technical assistance and capacity-building programs to emerging markets
- Help developing regions gain access to cybersecurity training and resources.

NEW YORK METRO JOINT CYBER SECURITY CONFERENCE

Presented by:

Kiran Bhujle

New York Metro Joint Cyber Security Conference
September 26th, 2024

kbhujle@svam.com

908-590-1445

SVAM INTERNATIONAL, INC.