10 Steps to a Future-Proof Cybersecurity Workforce

Adapting to AI, Quantum, and the Skills Revolution

Jay Adusupalli

About Me:

Jay Adusupalli, CISSP

- Technical Leader at Cisco
- Security Advisory for Cisco Security Solutions
- Skill Manager for Cyber Security at WorldSkills
- Advisor for Government Upskilling Efforts in APAC
- Design and Manage Cyber Ranges
- Based in Singapore

- Serious about Coffee!

AI will automate 80% of programming jobs within a decade. The future programmer will be more of a curator than a creator

Dario Amodei – CEO, Anthropic

The future is already here. Its just not evenly distributed

William Gibson - Author

The promise of Future

10x Everything!

AI Productivity Gains:

14% Productivity Increase in Customer Support.

8-40% Productivity Increase in AI Boosted worker Productivity.

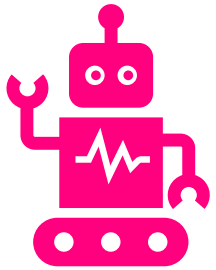
Quantum Computing:

Quantum Computers Operate 158 million times faster than the fastest supercomputer.

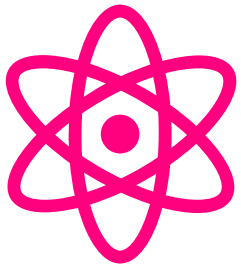
- 5000 quantum computers operational by 2030
- Superior Simulation capabilities.
- 2048-bit RSA encryption could be broken by a quantum computer running for a week.

Creates new challenges and opportunities for cybersecurity professionals.

Emerging Threats



AI-powered attacks are a major concern for 72% of orgs.



Quantum computing threatens encryption.

47% cite adversarial AI as the top risk.

The Widening Cybersecurity Skills Chasm

AI Amplifies the Gap

AI-powered attacks increase the sophistication and speed of threats, requiring specialized skills that are in short supply

New Demands

Necessitates expertise in post-quantum cryptography and quantum-resistant security measures.

Job Evolution

AI Agents can automate routine tasks, leading to evolving roles rather than outright replacement

Security for AI

New areas of focus is to Secure AI Models from attacks

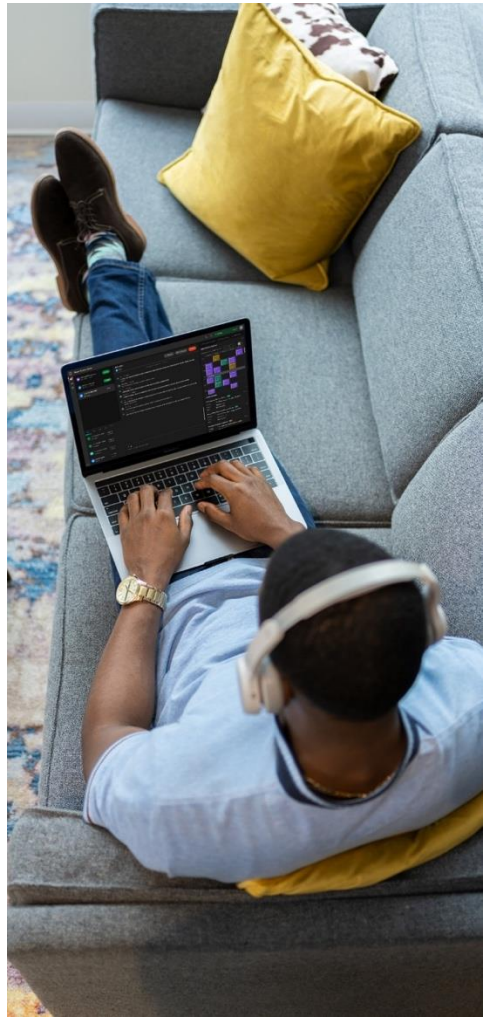
3.5 million unfilled cybersecurity jobs globally in 2025. That’s a massive shortfall of defenders

Less than 25% of organizations believe they have adequate cybersecurity skills for the new age

From Reactive to Proactive

Why structured approach is essential

- **Unprecedented pace of change**
- **Consequences of Inaction are higher**
- **Inefficiency of Fragmented efforts**



Introducing the 10-Step Framework to help build a resilient and future-proof cybersecurity workforce

Creating a Culture of Continuous Learning and Adaptation

Step 1 – Navigate the Horizon

Map the Future

- **Leverage the NIST NICE Framework:** Utilize the NIST NICE Framework to identify and categorize evolving cybersecurity roles and skills.
  E.g., AI Security Engineer, Quantum Cryptographer

- **Anticipate Skill Shifts:** Analyse how existing roles will be augmented or transformed by automation and AI.
  E.g., Security Analyst (enhanced data analysis skills), Incident Responder (AI-assisted investigation), Penetration Tester (AI-powered vulnerability exploitation)

NICE Specialty Area	Example Use Case	Associated KSATs
Threat Analysis (AN-TD)	Using AI to detect malware through behavioral analysis	- Knowledge of machine learning techniques - Skill in analyzing threat data
Cryptographic Technologies (SP-CT)	Implementing post-quantum cryptographic algorithms	- Knowledge of quantum-resistant cryptography - Skill in algorithm design

Step 2 – Charting the Course

Create Adaptive Learning Pathways

- **Move Beyond Rigid Certifications:** Supplement traditional certifications with modular, skills-based training.
- **Embrace Micro-Credentials:** Offer short, focused courses that validate specific skills and competencies.
  - Cloud Security Fundamentals, AI Threat Detection, Quantum Cryptography Basics, Secure Coding Practices.
- **Leverage AI-Powered Learning Platforms:** Utilize AI to personalize learning paths based on individual skill gaps and career goals.
- **Incorporate CTF-Based Learning:** Integrate Capture the Flag (CTF) competitions and gamified training to enhance practical skills.
  - Hack The Box, TryHackMe, OverTheWire.

Step 3 – Decode the Future

Infuse AI and Quantum Literacy

- **Foundational Training:** Provide basic AI and quantum computing training for all employees, regardless of their role.
  - Online courses on AI basics, introductory quantum computing webinars.
- **Specialized Training:** Offer in-depth training for cybersecurity professionals on AI security, prompt engineering, and post-quantum cryptography.
  - Courses on adversarial AI, AI-powered threat detection, quantum key distribution, lattice-based cryptography.
- **Awareness Programs:** Conduct regular awareness campaigns to educate employees about the risks and opportunities associated with AI and quantum technologies.
  - Lunch-and-learn sessions, newsletters, and infographics on AI and quantum security.

Step 4 – Beyond the Code

Cultivate Multi-Disciplinary Thinking

- **Cross-Functional Teams:** Create teams that include professionals from different backgrounds, such as psychology, law, data science, and business.
  - E.g., Incident response teams that include legal counsel, PR representatives, and technical experts.
- **Training Programs:** Offer training programs that expose cybersecurity professionals to other disciplines.
  - Courses on behavioral psychology for security awareness training, legal aspects of data privacy, and data science for threat intelligence.
- **Mentorship Programs:** Pair cybersecurity professionals with mentors from other fields.
  - E.g., Pairing a security analyst with a data scientist to learn about machine learning techniques.

Step 5 – Fueling Innovation

Develop a Growth Mindset Culture

Promote Continuous Learning: Encourage employees to pursue ongoing training and development opportunities.

Reward Experimentation: Create a safe space for experimentation with new technologies and approaches, even if they fail.

Creating a “Fail-Fast” Culture.

Recognize Achievements: Publicly acknowledge and reward who demonstrate a growth mindset.

Step 6 – Real World Readiness

Invest in Simulations and Labs

- **Breach and Attack Simulations:** Regular breach and attack simulations to test your defenses and identify vulnerabilities.
- **Cyber Ranges:** Create or utilize cyber ranges to provide realistic training environments for incident response and threat hunting.
- **Red/Blue/Purple Team Exercises:** Conduct regular red team/blue team exercises to improve your organization's security posture.
- **AI Attack Simulations:** Data Poisoning, Model Inversion Attacks, Bias Exploitation etc.,

Step 7 – Power of Partnership:

Build Public-Private-Academic Alliances

- **Curriculum Alignment:** Collaborate with academic institutions to align cybersecurity curricula with industry needs.
  - Participating in advisory boards for university cybersecurity programs, providing guest lectures, and offering feedback on course content.
- **Co-Creation of Programs:** Partner with government agencies and vendors to co-create training programs and research initiatives.
  - Partnering with government agencies, collaborating with security vendors on research projects.
- **Internship and Apprenticeship Programs:** Offer internship and apprenticeship programs to provide students with real-world experience.

Step 8 – Investing in the Future

Empower Cybersecurity Educators

- **Sabbaticals and Industry Immersion:** Offer sabbaticals and industry immersion opportunities for educators to stay up-to-date on the latest trends.
  - Partnering with local companies to offer internships for cybersecurity educators, providing funding for educators to attend industry conferences
- **Funding for Training and Certifications:** Provide funding for educators to attend conferences, take courses, and earn certifications.
- **Curriculum Development Support:** Offer support for educators to develop and update their curricula.

Step 9 – Strength in Diversity

Drive Inclusion and Diversity

Tap into non-traditional Talent Pools

Embrace Neuro-diversity and Cross Diversity Backgrounds

Step 10 – Continuous Improvement

Measure and Iterate

Track KPIs on upskilling, role mobility IR readiness

Build dashboards to assess effectiveness

Call to Action Educators

- Agile Curriculum Updates
- Industry Partnerships
- Experiential Learning
- Promote Diversity and Inclusion

Call to Action Employers

- **Allocate Budgets for Reskilling:** Dedicate resources to upskilling and reskilling your existing workforce.
- **Make Learning Part of Performance Plans:** Integrate learning and development goals into employee performance plans.
- **Support Employee Certifications:** Encourage and support employees in pursuing industry-recognized certifications.

Call to Action Students

- **Embrace Continuous Learning:** Commit to lifelong learning and stay up-to-date on the latest cybersecurity trends.
- **Seek Mentorship:** Find a mentor who can provide guidance and support.
- **Gain Hands-On Experience:** Participate in internships, CTF competitions, and other practical learning opportunities.
- **Network with Professionals:** Attend industry events and connect with cybersecurity professionals.

Thank you!

scan this qr-code to connect with me!