



## Cybersecurity Labor Shortage – Winter 2026 Class

The global cybersecurity industry stands at a defining moment. As cyber threats grow in scale and sophistication, organizations around the world are struggling to fill millions of open cybersecurity positions. The rapid adoption of artificial intelligence (AI), cloud computing, and digital transformation has expanded both opportunity and risk widening the global skills gap and creating an urgent demand for qualified professionals.

### The Global Labor Shortage in Context

According to the 2024 ISC<sup>2</sup> Cybersecurity Workforce Study, the global cybersecurity workforce gap has reached an unprecedented 4 million professionals, representing a 12% increase over the previous year. While over 5.5 million cybersecurity professionals are currently employed worldwide, demand continues to outpace supply. In the United States alone, more than 440,000 new cybersecurity positions were created last year.

Cybersecurity Ventures further projects that by 2025, global unfilled positions will remain around 3.5 million, marking the fifth consecutive year this figure has persisted. This ongoing shortage has positioned cybersecurity as one of the most resilient and opportunity-rich career paths in the digital economy.

### Key Drivers Behind the Shortage

Several factors have contributed to the persistent cybersecurity workforce gap:

- Increasing complexity of technology ecosystems, including hybrid and multi-cloud environments.
- A surge in AI-driven cyberattacks, requiring new defense strategies and specialized expertise.
- Expanding compliance and data privacy regulations, creating high demand for Governance, Risk, and Compliance (GRC) professionals.
- A lack of integration between traditional IT education and real-world, performance-based cybersecurity training.

The emergence of AI governance as a new discipline has deepened the demand for professionals who can assess risk, ensure transparency, and maintain accountability in AI-enabled systems.





## Cybersecurity Labor Shortage – Winter 2026 Class

### Industry and Government Response

Recognizing the scale of the shortage, global technology leaders and government agencies are investing heavily in workforce development:

- **Microsoft** has partnered with U.S. community colleges to train 250,000 cybersecurity professionals by 2025.
- **Google** is expanding its Career Certificate program to prepare 100,000 Americans for careers in privacy, security, and AI governance.
- The **U.S. Cybersecurity and Infrastructure Security Agency (CISA)** continues to drive the National Cyber Workforce and Education Strategy (NCWES), promoting early talent development and career mobility.

Despite these initiatives, the cybersecurity talent gap continues to grow faster than training pipelines can supply skilled professionals particularly in non-technical areas such as compliance, risk management, and policy oversight.

### Landmark CyberTech’s Role in Closing the Gap

- At Landmark CyberTech Solutions, we are addressing the workforce shortage head-on by empowering individuals from all backgrounds to transition into cybersecurity through our hands-on, AI-enhanced GRC training model. Our approach combines practical skill development, real-world projects, and mentorship to produce job-ready professionals who can immediately contribute to organizational security and compliance operations.

#### **Key features of our training program include:**

- Live, federal-style GRC project labs simulating NIST RMF and ISO 27001 environments.
- Integration of AI-assisted compliance tools and automation awareness.
- Capstone projects aligned with real-world Authorization to Operate (ATO) and Risk Assessment processes.
- Post-training mentorship, resume consultation, and job placement guidance through our Phase 2 Career Acceleration Pathway.





## Cybersecurity Labor Shortage – Winter 2026 Class

### The Future Workforce - AI, GRC, and Beyond

As artificial intelligence reshapes every facet of cybersecurity, future professionals will be expected to bridge the gap between technology and governance. The next generation of cybersecurity experts must combine technical knowledge with an understanding of risk, compliance, ethics, and responsible AI implementation.

**Landmark CyberTech** is preparing that workforce today, building the next generation of Cyber and AI-Ready GRC Professionals capable of securing the future digital ecosystem with innovation, accountability, and integrity.

*Landmark CyberTech Solutions - Innovative Training, Real-World Skills, Empowering the Future of Cybersecurity*

February 2026

