Cyber Security Survey

The cybersecurity profession continues to evolve rapidly, shaped by emerging technologies, evolving threats, and increasing global demand for skilled professionals. Each year, leading industry organizations such as ISACA, (ISC)², and CompTIA release workforce studies that highlight the realities of the cybersecurity job market. The 2025–2026 findings reveal a growing imbalance between employer expectations and workforce readiness particularly in hands-on experience, certification alignment, and strategic thinking.

Industry Findings – ISACA 2025 State of Cybersecurity Survey

The ISACA Annual State of Cybersecurity Survey provides key insights into hiring trends, workforce challenges, and organizational needs. The 2025 edition highlights a persistent talent shortage and underscores the importance of practical experience, governance knowledge, and business-context understanding.

Key Findings:

1. **Talent Acquisition Challenges:**
   - 25% of enterprises take six months or more to fill cybersecurity positions due to the **lack of qualified applicants**.
   - Although 59% of organizations receive at least five applications for each position, most applicants lack the required qualifications.
2. **Top Candidate Qualifications:**
   - **Practical Hands-On Experience**: 55% of enterprises rank this as the most important qualification.
   - **Certifications**: Nearly 70% of employers require certifications such as **CompTIA Security+**, **CISM**, or **CGRC**.
   - **Understanding Business Impact**: 45% of respondents emphasize the importance of candidates understanding how cybersecurity aligns with business objectives.
3. **Business Integration:**
   - 45% of respondents emphasize the importance of professionals who understand how cybersecurity supports organizational goals, compliance, and risk posture.
4. **Key Gaps in Applicant Readiness:**
   - Lack of practical skills and technical expertise is the leading reason applicants are deemed unqualified.
   - Many candidates fail to demonstrate the ability to address cybersecurity challenges in a business context.

Implications for Workforce Development

These findings reaffirm the industry's call for performance-based training that bridges the gap between theory and applied competence. Employers now seek professionals who can demonstrate real-world proficiency in system documentation, risk assessments, and compliance reviews. As automation and artificial intelligence redefine how security operations are performed, analytical thinking, adaptability, and governance awareness are emerging as essential traits for future cybersecurity leaders.

February 7, 2026

Cyber Security Survey

Landmark CyberTech Response:

Landmark CyberTech Solutions has strategically aligned its Cybersecurity Career Training Program with these global workforce trends. Through its **AI-enhanced Governance, Risk, and Compliance (GRC) specialization**, the program prepares students to meet employer expectations and excel in today's AI-driven security environment.

Rather than operating as a conventional training institute, Landmark CyberTech functions as a professional workshop; an experiential learning hub where participants learn how to do the job before they get the job. We're dedicated to bridging these gaps by:

- **Emphasizing performance-based training** that equips learners with the practical, job-ready skills employers demand.
- **Integration of AI-assisted compliance tools** and automation awareness to prepare graduates for the evolving cybersecurity landscape.
- **Aligning coursework with industry certifications** to enhance employability and credibility.
- **Developing strategic thinkers** who understand cybersecurity within the broader context of organizational governance and risk.
- **Providing mentorship and post-training support** through the Phase 2 Career Acceleration Pathway.

This approach ensures graduates possess not only technical skills but also the governance mindset necessary to evaluate, communicate, and manage cybersecurity risks in both federal and commercial environments.

Call to Action for Students:

As a participant in Landmark CyberTech's Cybersecurity Career Training Program, you are part of a new generation of professionals ready to bridge the gap between security operations and strategic governance. By combining technical foundations with real-world documentation and AI-supported risk management, you will gain the expertise to thrive in the evolving cybersecurity landscape.

The cybersecurity industry urgently needs practitioners who can connect technology, compliance, and business outcomes. Your journey at Landmark CyberTech equips you to become one of those leaders - driving resilience, accountability, and innovation in the digital age.

Disclaimer: *This is an educational resource and may not contain all the information required to ensure a successful outcome. Readers should use their own professional judgment in their individual situations.*

February 7, 2026