CompTIA

Cybersecurity

Training the Cybersecurity Workforce

Information security threats are on the rise around the world. A number of factors make it vital to have IT personnel and processes that can improve cybersecurity:

- Increasing sophistication of security threats and greater accessibility of data
- Human error
- Risks associated with the evolving landscape of cloud computing, mobile computing, and social media
- Browser-based threats

Especially considering the rate of security breaches due to human error, training is an area of concern and an important focus for organizations seeking to mitigate information security risks. Business enterprises and governments alike must develop a skilled workforce of technical professionals who can respond to the ever-evolving landscape of technology and the mounting security threats that come with it.

> **"It's been estimated that last year alone cyber criminals stole intellectual property from businesses worldwide worth up to $1 trillion… America's economic prosperity in the 21st century will depend on cybersecurity."**
>
> President Barack Obama, "On Securing Our Nation's Cyber Infrastructure," May 29, 2009

Common Gaps in the IT Workforce

- Lack of security expertise
- Lack of security training
- Inadequately skilled security staff
- Security policies that are inadequate to address evolving threats
- Failure of IT staff to follow security procedures

The Value of Certification

Technical certification is becoming increasingly important as new threats demand new credentials. Mandates from government agencies have also driven the need for certification, including updating many of the job roles associated with cybersecurity. Enterprises seeking to educate and train IT personnel to develop and maintain security processes can address needs and gaps by requiring some of the certifications relating to cybersecurity that are available through vendor-neutral organizations. These organizations and credentials include:

Organization	Certifications
The Computing Technology Industry Association (CompTIA)	A+, Network+, Security+, Server+, CASP*
International Information Systems Security Certification Consortium [(ISC)^2]	SSCP, CISSP
EC-Council	CEH
ISACA	CISA, CISM
Global Information Assurance Certification (GIAC)	GISF, GSEC, GSLC, GCIA

* Scheduled for release in 2011

CompTIA Supports Cybersecurity Campaign

This cybersecurity overview was developed in support of the National Cybersecurity Awareness Campaign. The "Stop. Think. Connect." campaign was initiated by the U.S. Department of Homeland Security in an effort to ensure that the public understands the risks associated with cybersecurity and the solutions that they can employ to address safety and security online.

STOP | THINK | CONNECT

Cybersecurity-Relevant Certifications

CompTIA offers a number of vendor-neutral certifications that are relevant to security roles. These certifications are an ideal starting point for professionals to begin building a foundation in cybersecurity skills.

Certification	Relevance to Cybersecurity	Competencies
CompTIA A+	CompTIA A+ is a U.S. Department of Defense (DoD) IAT Level I examination considered as a foundational technical curriculum by the DoD Cyber Crime Center. All cyber investigations, forensics, and cyber law enforcement activities rely on a fundamental understanding of computer hardware, networks, and systems.	• Hardware troubleshooting, repair, and maintenance • Operating system and software • Networking • Security • Operational procedure
CompTIA Network+	CompTIA Network+ is a DoD IAT Level I examination that is internationally recognized as validation of the technical knowledge required of foundation-level IT network practitioners.	• Network technologies • Media and topologies • Network devices • Network management • Network tools • Network security
CompTIA Security+	CompTIA Security+ is a DoD IAT Level II examination mandated by Directive 8570.1. It measures foundational security skills and is intended for professionals with a minimum of two years of network administration experience with a focus in security.	• Systems security • Network infrastructure • Access control • Assessments and audits • Cryptography • Organizational security
CompTIA Server+	CompTIA Server+ ensures that security professionals can build, maintain, and troubleshoot server hardware and software technologies. It addresses environmental issues, understanding and implementing disaster recovery, and physical and software security procedures.	• Server hardware • Server software • Storage • IT environment • Disaster recovery • Troubleshooting
CompTIA ADVANCED SECURITY PRACTITIONER C A S P *(scheduled for release in 2011)*	CompTIA Advanced Security Practitioner (CASP) is intended to be a DoD IAT Level III examination for advanced technical security certification. It is designed for information assurance professionals in technical leadership roles in an IT enterprise environment (especially military environments).	• Security systems design and engineering • Network security devices • Security network programs and network engineering • Security architecture • Security compliance and vulnerability assessments

For More Information

To read more about the importance of certification for cybersecurity and how CompTIA develops certifications that validate cybersecurity skills and knowledge, please download our free white paper, Credentialing the Cybersecurity Workforce: CompTIA Insights into the Certification Process, at **www.comptia.org/securitypaper**.