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.

Top Areas of Security Deficiencies

Cloud Security - 56%

Mobile Security - 48%

Data Loss Prevention - 46%

Overall Risk Analysis - 35%

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:

Oganization	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

CompTIA SUPPORTS CYBERSECURITY 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. For more information: www.dhs.gov/stopthinkconnect

Top Cybersecurity Threats	Moderate Concern	Serious Concern
Malware (e.g. viruses, worms, trojans, botnets, etc.)	38%	53%
Hacking (e.g. DoS attack, APT, etc.)	42%	44%
Social engineering/Phishing	45%	37%

Source: *11th Annual Information Security Trends study, November 2013*

CompTIA CYBERSECURITY CERTIFICATION PORTFOLIO

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. 1 million individuals in 267 countries have achieved CompTIA A+ certification.	• 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. Held by nearly 400,000, CompTIA Network+ prepares candidates for more advanced CompTIA certifications including CompTIA Security+™.	• Network technologies • Media and topologies • Network devices • Network management • Network tools • Network security
CompTIA Security+	CompTIA Security+ is approved for IAT Level II and IAM Level I in U.S. DoD Information Assurance directive 8570.01-M. 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. Held by over 300,000 IT professionals, Security+ is embraced industry-wide as the starting point in cybersecurity certifications.	• Systems security • Network infrastructure • Access control • Assessments and audits • Cryptography • Organizational security
CompTIA Cloud+	The CompTIA Cloud+ certification validates the knowledge and best practices required of IT practitioners working in cloud computing environments, who must understand and deliver cloud infrastructure.	• Cloud concepts and models • Virtualization • Infrastructure • Resource management • Security • Systems management • Business continuity in the cloud
CompTIA Mobility+	The CompTIA Mobility+ certification covers the knowledge and skills required to understand and research capabilities of various mobile devices and aspects of over-the-air technologies.	• Over-the-air technologies • Network infrastructure • Mobile device management • Security • Troubleshooting
CompTIA Mobile App Security+	The CompTIA Mobile App Security+ certification ensures that developers have the knowledge and skills necessary to design and build secure applications.	**For Android** • Mobile application security, SDLC, and threat models • Android SDK, APIs, and security features • Web service and network security • Data security and implementing encryption • Application hardening and reverse engineering • Secure Java coding **For iOS** • Application security and SDLC fundamentals • Objective-C coding • iOS SDK, APIs, and security features • Web service and network security • Data Security and implementing encryption • Application hardening
CompTIA Advanced Security Practitioner CASP	CompTIA Advanced Security Practitioner (CASP) is CompTIA's first mastery level certification exam and was voted on to the DoD 8570 exam list in early 2013. CASP is approved for IAT Level III, IAM Level II, IASAE Level I, and IASAE Level II in U.S. DoD Information Assurance directive 8570.01-M. 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

Need training? Visit Certification.CompTIA.org/training for the learning option right for you. CompTIA vouchers can be purchased through the CompTIA Marketplace at CompTIAstore.com, through Pearson VUE at pearsonvue.com/vouchers/pricelist/comptia.asp and via GSA Schedule at gsamart.com/comptia.

CompTIA Headquarters
3500 Lacey Road, Suite 100
Downers Grove, Illinois 60515
630-678-8300