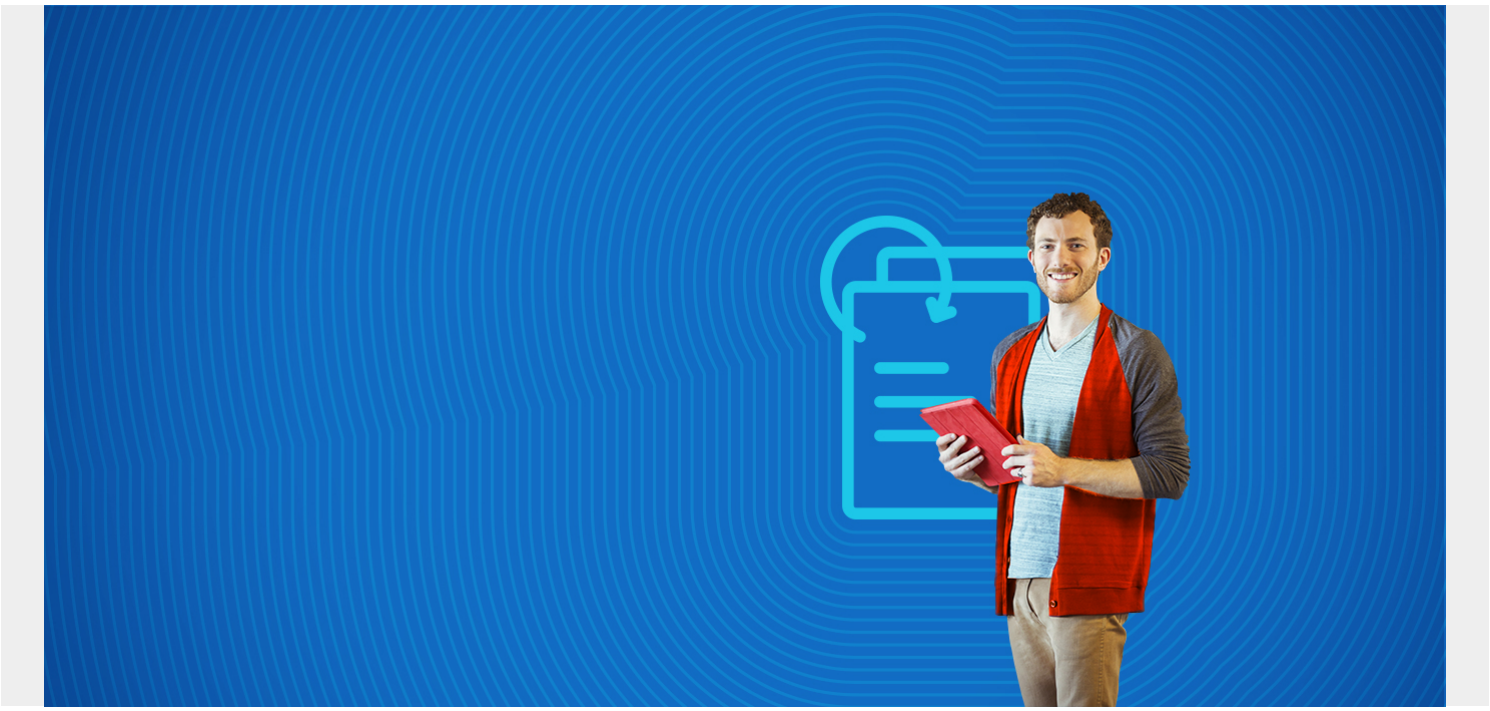
IT SECURITY CERTIFICATIONS: AN INTRODUCTION



With cyber breaches becoming increasingly prevalent, there is an increased need for cybersecurity professionals. According to the Cyber Risk Analytics 2019 Midyear Report, there were 3,800 reported breaches in the first half of the year, up by more than 50% from the previous year. Notably, of the breaches reported, more than 60% were the result of human error.

What this means is that there is an ever-increasing need for skilled and well-trained cybersecurity professionals. When looking to hire and promote employees, many companies look for professionals with highly-regarded certifications. For IT professionals, certifications are a good way to develop skills, gain a competitive edge, and to be eligible for higher salaries than peers without the certification.

While there are many benefits to having IT security certifications, with so many different certifications available, it can be hard to know which ones are worth the time, effort, and expense. To help navigate this saturated area, here is a list of some of the most sought after and highly-regard IT security certifications.

(This article is part of our Security & Compliance Guide. Use the right-hand menu to navigate.)

CompTIA Security+

The CompTIA Security+ certification is a good place to start with IT security certifications and is geared towards entry-level security professionals. This certification has the basic goal of building a strong IT security foundation. To earn this certification, professionals need two years of IT experience and then need to pass an exam that covers a range of topics including network attack strategies and defenses; components of strong security policies; best practices for security; disaster

recovery and continuity; and encryption products and standards.

This general cybersecurity certification is good for anyone that is interested in getting a good entry into IT security, and earning this certification will demonstrate expertise with some important security topics, including threat management, cryptography, identity management, security systems, security risk identification, and security infrastructure. Notably, because all IT professionals need some security experience, the CompTIA Security+ is a beneficial certification for individuals in roles outside of security, for example, developers and support analysts.

Certified Information Systems Security Professional (CISSP)

CISSP is another general security certification that is not vendor-specific. Referred to by some as the "crown jewel" of security certification, it's a high-level certification that is universally recognized and highly sought after by many employers. Offered by the International Information Systems Security Certification Consortium (ISC2), CISSP covers some key cybersecurity categories like access control, cryptography, telecommunications, and networking. Professionals with this certification have the skill sets needed to effectively design, implement, and manage cybersecurity systems.

To be eligible for this certification, individuals must have 3-5 years of relevant experience prior to taking the exam. This certification is essential for individuals wanting to move into a chief information security officer (CISO) role and is helpful for IT managers, analysts, system engineers, and consultants.

Certified Information Security Manager (CISM)

Another advanced and highly sought after certification is CISM, which requires applicants to have at least five years of relevant experience. Having this certification demonstrates skills in the areas of security risk management; program development and management; governance; and crisis management. It's geared toward higher-level IT professionals, specifically those that manage, develop, or oversee systems.

To earn this certification, professionals must commit to the Information Systems Audit and Control Association (ISACA) code of ethics, pass an exam, have five years of IT security experience with at least three years in job practice analysis areas, and submit a written application. Topics covered in this examination and corresponding prep courses include information security program development and management; incident management; risk management; and compliance. It's an ideal certification for individuals that are interested in enterprise-level information security or for individuals that have or want managerial-level roles in information security.

GIAC Security Essentials (GSEC)

Another entry-level general security certification is the Global Information Assurance Security Essentials Certification (GSEC). This tests professionals in security administration, forensics, audits, software security, management, and a variety of security best practices. With no prerequisites required, this is a good certification for IT professionals interested in security, especially since it's broadly focused on security best practices and ensures expertise in areas of preventing attacks, identifying threats, networking concepts, and secure communication.

Certified Ethical Hacker (CEH)

As many IT security professionals have learned, to effectively protect systems, they need to learn to think like hackers. In an effort to do this, there has been a rise in white hat hackers or ethical hackers working to gain the necessary hacking skills to beat hackers at their own game.

With this goal in mind, the CEH designation teaches IT professionals to think like a hacker. Individuals with this certification have developed skills in the five phases of ethical hacking, which are reconnaissance, enumeration, gaining access, maintaining access, and covering tracks. To teach these skills, it deals with topics like hacking that targets cloud computing, mobile platforms, and operating systems.

To earn this certification, professionals must pass an exam and have either attended the training or have two years of verified, IT-security experience. This is a good certification for security officers, auditors, and site administrators and is ideal preparation for individuals interested in penetration testing.

Computer Hacking Forensic Investigator (CHFI)

Forensic investigators play an important role in cybersecurity by analyzing attacks, pulling the necessary information to formally report an attack, and working to prevent future attacks. These professionals have the skills to investigate a wide range of crimes including theft of intellectual property, IT usage violations, and system fraud.

The Computer Hacking Forensic Investigator (CHFI) certification is an advanced certification that is geared towards forensic investigators and demonstrates their skill sets in key areas, including gathering evidence and helping to prosecute offenders. This EC-Council certification covers incident response, forensics, recovering information, examination, analysis, and reporting computer-based evidence. This certification is used and sought after by corporations as well as police and government investigators.

Certified Information Systems Auditor (CISA)

CISA is the best certification available for individuals that want to do audit control and assurance. Earning this certification provides evidence of skills in the CISA job practice areas of auditing, governance and management, acquisition, development and implementation, maintenance and service management, and asset protection.

This is a globally recognized certification that is necessary for professionals in high-level audit, assurance, and control roles. In addition, it's helpful for those responsible for auditors and those with roles that involve controlling, monitoring, and assessing IT systems. To earn this certification, individuals must have at least five years of experience working in information systems, pass an exam, submit an application, agree to the ISACA code of ethics, and agree to the ISACA's information systems standards.

Certified Cloud Security Professional (CCSP)

Traditional IT security practices don't work well for cloud services. As a result, those IT professionals tasked with cloud security need unique skill sets and training. The Certified Cloud Security

Professional (CCSP) certification offers that expertise and ensures that IT professionals are knowledgeable about cloud security, architecture, design, services, operations, data security, infrastructure, and compliance.

This is not an entry-level designation but instead is designed for IT professionals that already have a solid foundation in IT security and extensive IT experience. It's a good certification for systems architects, engineers, security managers, enterprise architects, and security administrators. Given the unique needs of cloud security and how quickly this area changes, the CCSP certification can be particularly beneficial to IT professionals. To earn this designation, professionals must have at least five years of IT experience, including three years in IT security and one year in one of CCSP's common body of knowledge areas.

Conclusion

Cybersecurity is a field that is constantly growing and changing. As a result, there are a lot of security opportunities for IT professionals with the necessary skills and expertise. Security certifications are an effective way to develop skills, offer evidence of skills, and gain a competitive edge.