11 Best Security Certifications to Boost your Career in 2017

Security breaches are increasing in size, number and criticality, all over the world. The sheer number of recorded and unrecorded data breaches has pushed the demand for cyber security professionals across all industries. At present, the unemployment rate in the security industry is zero. IT firms across the UK, USA, Europe and Asia are worried about being vulnerable to security attacks. They are looking for expert professionals with cyber security and InfoSec skills who can fill vacant positions and make online activities safer.

Whether you are looking to begin or advance your IT career path, here are 11 certifications that will provide you with the right credentials to kick-start a successful IT security career in 2017 and beyond.

1. **CISSP - Certified Information Systems Security Professional**

The CISSP is an advanced-level certification for IT pros. CISSP credential holders have to sit an exam, which consists of 250 questions and takes an average of 6 hours to complete. The exam is specifically designed for professionals with a minimum of 3 to 5 years of experience in the industry. The exam covers a number of cyber security domains, such as access control, security management practices, security models and architecture, cryptography, telecommunications and networking. If you want to become a Chief Information Security Officer (CISO), CISSP is a must. In addition, you will also be qualified to handle other job titles, such as Systems Engineer, Analyst, Consultant and Manager. The average annual salary for CISSP holders is $121,000 but it may vary depending on the job role, experience and location.

2. **CEH - Certified Ethical Hacker**

The CEH is an intermediate-level credential which is a must for IT professionals pursuing a career in ethical hacking. Holders of the CEH certificate possess the skills, knowledge and hacking techniques required to beat their malicious counterparts in various areas, such as scanning networks, foot-printing and reconnaissance, system hacking, enumeration, worms & viruses, denial-of-service attacks, Trojans, social engineering, hacking web servers, session hijacking, web applications, cryptography, wireless networks, firewalls, penetration testing, honeypots and evading IDS. In order to be eligible for the CEH exam, you need to have at least 2 years work experience. The average annual salary of Certified Ethical Hackers is approximately $103,000.

3. CCISO - Information Security Management Training Program

The CCISO certification program is the first-of-its-kind training program aimed at producing top-level IT security executives. The focus of this program is not solely on technical knowledge but on the application of information security management principles. The program covers 5 CCISO domains:

- Governance
- IS Management Controls and Auditing Management
- Management - Projects and Operations
- Information Security Core Competencies
- Strategic Planning and Finance

Current, as well as, aspiring CISOs can hugely benefit from this certification program. To be eligible for the CCISO exam, individuals need to have 5 years of IS management experience in any 3 of the 5 CCISO domains.

4. CISM - Certified Information Security Manager

CISM is a certification program focused on information security management and is a big plus point for those looking for a lucrative Infosec management or consultant job. It is one of the top credentials for IT professionals responsible for developing the best organisational security practices. Those involved in managing, developing and overseeing information security systems in enterprise-level applications can also benefit from this program. Holders of the CISM credential possess advanced skills and knowledge in program development and management, security risk management, incident management, governance and response. To be eligible for this certification program, you need to have 5 years of verifiable experience.

5. CompTIA Security+

CompTIA Security+ is a vendor-neutral security certification and a globally-recognised benchmark for the best practices in IT security. This certification program covers all the essentials of security systems, network security and risk management, identity management, cryptography and organisational systems. If you want to have a successful career in IT security, this certification is an important stepping stone. Even though Security+ is an entry-level certification, candidates should possess a minimum of 2 years experience in network security. It will be beneficial for your IT security career to first obtain Network+ certification, followed by a Security+ certificate. Security+ credential holders can look forward to landing a job with an average annual salary of $94,000.

6. **CCSP - Certified Cloud Security Professional**

The CCSP certification program is specifically designed for information security professionals with a minimum of 5 years work experience, including a minimum of 1 year of cloud security experience and 3 years of information security experience. This certification program is suitable for mid to advanced-level professionals involved with information security, IT architecture, governance, web and cloud security engineering, risk and compliance, as well as IT auditing. CCSP credential holders are competent in the 6 CCSP domains mentioned below:

- Architectural Concepts and Design Requirements
- Cloud Data Security
- Cloud Platform and Infrastructure Security
- Cloud Application Security
- Operations
- Legal and Compliance

The average annual salary for CCSP certificate holders is $81, 374.

7. **GIAC Security Essentials Certification (GSEC)**

If you are interested in demonstrating your skills in securing IT systems, you can enrol for the GSEC exam. This certification exam is offered by GIAC or Global Information Assurance Certification. GIAC is a body which is recognised globally for its state-of-the-art cyber security certifications. GSEC is an entry-level certification offering hands-on security experience beyond terminology and knowledge. GSEC credential holders possess technical skills and knowledge in areas such as password management, identification and prevention of common and wireless attacks, DNS, authentication, IPv6, Linux, cryptography fundamentals, network mapping, ICMP and network protocols. This certification has to be renewed every 4 years. You can expect an average annual salary of $77,000.

8. **CRISC - Certified in Risk and Information Systems Control**

If you want to develop a better understanding of how IT risks are related to the overall functioning and working of an organisation, enrol for the CRISC certification program. This program will help you in developing the technical skills required to understand and manage the corporate risks and implement the right controls to prevent a security breach. This program is often a necessity for c-suite executives, as well as risk & privacy officers and chief compliance officers. To apply for this

certification program, you need a minimum experience of 3 years. The average annual salary for top-tier CRISC credential holders is $122,954.

9. PCI DSS QSA

If you are an InfoSec professional and currently handling the responsibilities of a compliance officer or are a part of the internal audit team, or if you tackle business operations and security infrastructure, PCI-QSA is an ideal job role for you. To be eligible for the PCI-DSS QSA certification, you need to have sound IT security knowledge and a strong IT and Networking background. The certification program aims to provide applicants with a general understanding of the working of the credit card industry and in-depth knowledge of security and IT applications, databases or servers and network configurations. Expertise in PCI gives individuals an edge to pursue multiple job roles within their organisation. PCI-QSA certificate holders are able to trump their competition as companies are increasingly looking for candidates with a broader range of expertise and specialised talent.

10. GIAC Security Expert (GSE) - Global Information Assurance Certificate

The GIAC GSE certification is the most esteemed and respected information security certificate and is aimed at those seeking in-depth knowledge in all areas of information security. This certificate demonstrates that the holder is fully proficient and competent in a wide variety of skills required for top-level Infosec jobs, making them the best in the field. The baseline requirements for the GSE certification are GSEC, GCIH, GCIA with two gold certifications, with the applicant also requiring previous experience in the subject areas. The GSE exam tests the ability of applicants in general security, incident handling and intrusion detection and analysis, and has 2 parts: a multiple choice exam and a hands-on lab. The certification has to be renewed every 4 years.

11. SSCP - Systems Security Certified Practitioner

SSCP is a first-rate entry-level IT security certification and is the perfect precursor to the much favoured CISSP certification. If you are hoping to land a job as a Network Security Engineer, Security Analyst, Database Administrator, Security Administrator, Systems Engineer, Security Consultant or Network/Systems Analyst, SSCP certification is ideal for you. SSCP credential holders demonstrate the ability and technical skills required for tackling the operational responsibilities and demands of security practitioners, including security testing, incident response & recovery, authentication, intrusion detection or prevention, cryptography, countermeasures for malicious code and so on.

With our first step into 2017, we can observe that cyber threats are on the rise. The need for certified and skilled cyber security personnel is going to become more prominent than ever before. If

you want to rise above the competition and carve out a lucrative IT career path for yourself, earning certifications that validate your cyber security expertise can be a very important asset.