Global Information Assurance Certification Paper

How to Become a Bona Fide IT Security Professional

Anita Dodson

October 30, 2000

Like many in the IT security profession, I arrived quite by accident. I first entered the workforce sixteen years ago, armed with a graphic communications degree. Over the years I made a somewhat logical progression from graphic designer, to web designer/developer and web server administrator. Soon after I began wearing the administrator hat for several government systems, I fell victim to a cracker. This one incident launched me into a new career. Not only was I determined not to become a victim again, I found that I really enjoyed the work.

After many hours of self-taught tutorials on IT security, I have come to a crossroads. How do I become a bona fide IT security professional? What degrees, certifications, or other credentials are employers looking for? Is it possible for me to find other employment in this field with a non-IT degree, a few certifications, and some experience? If so, which certifications should I work toward?

What Employers Are Looking For

In order to understand what qualifications employers are looking for when filling IT security positions, I took a random sampling of 52 job listings from a variety of online job banks[1]. This sample reflects job opportunities from all over the U.S. involving IT security management, administration, and implementation[2]. Out of the 52 openings, 18 of those did not specify a degree requirement. One entry level position required a 2 year degree, and 4 senior level positions preferred an MS or MBA. The remaining 29 jobs all required a BS/BA in computer science or information systems, although 13 of those allowed for equivalent experience in lieu of a degree.

Eighteen out of the 52 employers mentioned professional certifications and these were scattered among all the degree levels discussed previously. Only a few employers stated that the certification was a requirement. In these instances the requirement was specifically tailored to the networking environment of the employer. For example, two positions required a firewall expert to be certified with Check Point's CCSA/CCSE. Another employer wanted an applicant to be certified as a Microsoft Certified Systems Engineer (MCSE). In the remaining 15 listings, all employers stated that professional security certifications would be a plus. The certification that got the most mention was the ISC[2] Certified Information System Security Professional (CISSP). The SANS GIAC (no particular track) and the ISACA Certified Information Systems Auditor (CISA) tied for second most mentioned.

While many employers (16 out of the 52) are still looking for the conventional requirement of a bachelor's degree in a related field, the majority (34) either did not

[1] The complete list of job banks used can be found in Appendix A.

[2] A list of job titles reviewed can be found in Appendix B.

specify a degree requirement or stated that equivalent experience would qualify an applicant. Although only 18 mentioned certifications, all the positions required specific areas of expertise, or years of experience. For the applicant that does not possess a computer related degree, this experience and expertise becomes much more important. Undoubtedly, an excellent way to demonstrate a level of competency in a particular area is with a professional certification in IT security. But which one should you choose? Do you need multiple certifications?

Certifications for the IT Security Professional

There are currently over 25 different certifications for the IT security professional. See Appendix C for a detailed description. They range from broad-based certifications on theory and concepts, to vendor-specific for particular products. Although each of these certificates has its merits, choosing the right combination can be confusing. One logical place to start is with a certification designed to demonstrate your overall knowledge of the IT security profession.

The CISSP, from the International Information Systems Security Certifications Consortium, Inc. (ISC^2) is the most often asked for by employers. Because it covers broad security theory and concepts, it is generally sought by chief information officers and other senior level management. The ISC^2 has recently introduced a new certification for system security administrators. The System Security Certified Practitioner (SSCP) addresses the technical issues associated with implementing security policy. In addition to ISC^2, the SANS Global Incident Analysis Center (GIAC) and the Information Systems Audit and Control Association (ISACA) both offer excellent certifications, GSE and CISA respectively, covering a broad range of security management and implementation skills.

To complement the CISSP, SSCP, GSE, and the CISA, there are a number of certifications that serve to showcase your specific areas of expertise. The SANS GIAC and the High-Tech Crime Network each offer multiple certifications for different skills, such as intrusion detection and forensics. These are worth looking into, especially if you have a particular career specialty in mind. Finally, there are the many certifications that vendors offer for their products. These are sure to be an asset on your resume if you are certified for products that a potential employer uses.

College Programs in IT Security

In the 52 employment opportunities reviewed, it was evident that employers are allowing experience to augment a candidate's education. On the job experience is considered by many to be more valuable than any other source of education. But what if you wanted to pursue a college program in IT security? Are there any available?

Information Systems Management and Information Systems Technology degrees, both at the undergraduate and graduate level, appear to be readily available. However, many of these degree plans do not touch on the subject of security. Unfortunately, formal degree

plans focusing on IT security have not yet made it to the mainstream of academia. All that is changing though. Congress recently approved a scholarship program for students pursuing degrees in Information Security. In exchange, the student agrees to work for federal agencies after graduation. In the meantime, those of us already in the field will rely heavily on technical training, work experience, and the pursuit of security certifications to stay ahead.

Appendix A: Online Job Banks

Name	URL
Information Security Magazine/ ICSA	http://www.infosecuritymag.com/securecareers
InfoSysSec Security Portal	http://www.infosyssec.net/infosyssec/jobsec1.htm
International Information Systems Security Certifications Consortium, Inc. (ISC^2)	http://www.isc2.org/careers.html
Carnegie Mellon Software Engineering Institute, CERT Coordination Center	http://www.cert.org/jobs
Net Temps Job Search	http://www.net-temps.com
Alta Associates	http://www.altaassociates.com
Career Builder	http://www.careerbuilder.com
Career Mosaic	http://jobs.careermosaic.com
CareerNet	http://www.careernet.com
Deja News	http://deja.news
Career.com	http://www.career.com
CareerMag.com	http://www.careermag.com
Career Path	http://www.careerpath.org
CareerSite	http://www.careersite.com
Brainhunter	http://www.brainhunter.com
Headhunter.net	http://www.headhunter.net/JobSeeker/index.htm
The Employment Guide's CareerWeb	http://www.cweb.com
Job Options	http://ww1.joboptions.com
Job Bank USA	http://www.jobbankusa.com
BrassRing.com	http://www.jobcenter.com
Monster.com	http://www.monster.com
Job Source Online	http://www.jobsourceonline.com
Dice – High Tech Jobs Online	http://dice.com
Jobs.Internet.com	http://jobs.internet.com
Hot Jobs	http://www.hotjobs.com
Security Jobs Network	http://www.securityjobs.net
CipherSearch	http://www.ciphersearch.com

Appendix B: List of job titles reviewed.

Network Security Engineer/Specialist/Manager
Web Security Engineer/Administrator
System Security Specialist/Analyst/Administrator/Auditor
IT Security Officer/Manager/Consultant

Appendix C: Certifications for IT Security Professionals

Certification	Description	Organization/URL	Comments
General/Broad Category			
CISSP	Certified Information System Security Professional	International Information Systems Security Certification Consortium (ISC^2) www.isc2.org	Considered the top level certification for system security professionals. Intended for those responsible for developing IT security policies and standards, and managing their implementation across an organization.
SSCP	System Security Certified Practitioner	International Information Systems Security Certification Consortium (ISC^2) www.isc2.org	Tailored for system security and network administrators who implement policies and procedures on hardware and software.
GSEC	GIAC Security Essentials Certified	SANS Global Incident Analysis Center (GIAC) www.sans.org	Broad-based overall, but does focus on technical elements of both theory and practice of IT security.
GSE	GIAC Security Engineer	SANS Global Incident Analysis Center (GIAC) www.sans.org	GIAC Honors Certification. Certifies in-depth knowledge in all areas of IT security.
CISA	Certified Information Systems Auditor	Information Systems Audit and Control Association and Foundation www.isaca.org	For professionals who apply information systems audit, control and security practices within IT environments.
CCP	Certified Computer Professional	Institute for Certification of Computing Professionals www.iccp.org	Encompasses broad range of computer related fields including programming, communications, software engineering and well as systems security.

SNSCP	System and Network Security Certified Professional	Learning Tree International www.learningtree.com	Certifies skills and knowledge critical to maintaining security of mission-critical data and systems.
Specific Skill Area			
CPP	Certified Protection Professional	American Society for Industrial Security www.asisonline.org	Emphasis on managing the protection of people, property, and information.
CBCP	Certified Business Continuity Planner	Disaster Recovery Institute (DRI) www.dr.org	Aimed at business continuity/disaster recovery planners.
GCIA	GIAC Certified Intrusion Analyst	SANS Global Incident Analysis Center (GIAC) www.sans.org	Certifies in-depth knowledge of intrusion detection.
GCIH	GIAC Certified Incident Handling Analysts	SANS Global Incident Analysis Center (GIAC) www.sans.org	Certifies in-depth knowledge of incident handling.
GCFW	GIAC Certified Firewall Analyst	SANS Global Incident Analysis Center (GIAC) www.sans.org	Certifies in-depth knowledge of firewalls.
GCUX	GIAC Certified UNIX Security Analyst	SANS Global Incident Analysis Center (GIAC) www.sans.org	Certifies in-depth knowledge of UNIX security administration.
GCNT	GIAC Certified Windows NT Security Analyst	SANS Global Incident Analysis Center (GIAC) www.sans.org	Certifies in-depth knowledge of NT security administration.
CCCI ***Basic & Advanced***	Certified Computer Crime Investigator	High-Tech Crime Network www.htcn.org	Certifies technical knowledge and experience in investigations and computer crime.
CCCT ***Basic & Advanced***	Certified Computer Forensic Technician	High-Tech Crime Network www.htcn.org	Certifies technical knowledge and experience in investigations and computer forensics.
CCCP	Certified Computer Crime Prosecutor	High-Tech Crime Network www.htcn.org	Certifies knowledge and experience in prosecuting computer crime.
CCCA	Certified Computer Crime Attorney	High-Tech Crime Network www.htcn.org	Certifies knowledge and experience in legal issues regarding computer crime.

CNSP Advanced	Certified Network Security Professional	High-Tech Crime Network www.htcn.org	Certifies in-depth knowledge and experience of networking and network security.
Vendor Specific *			
MSCE	Microsoft Certified Systems Engineer	Microsoft www.microsoft.com/trainingandservices/	Designing and implementing infrastructure based on Microsoft's products.
CCIE	Cisco Certified Internetwork Expert	Cisco Systems, Inc. www.cisco.com	Professional benchmark for internetworking expertise for Cisco products.
CCSA	Check Point Certified Security Administrator	Check Point www.checkpoint.com	Validates knowledge of Check Point's Firewall-1 product.
CCSE	Check Point Certified Security Engineer	Check Point www.checkpoint.com	Validates knowledge of Check Point's Firewall VPN-1 and Firewall-1 products.

** The vendor specific certifications listed here include only those that appeared in the original query of 52 IT security job openings. As a result, this list should not be considered complete.*

References

Frank, Diane. "Congress Funds Future Digital Defenders." Federal Computer Week. 24 Oct. 2000. URL: http://www.fcw.com/fcw/articles/2000/1023/web-cyber-10-24-00.asp (30 Oct. 2000).

Haraf, Jo M. "A Case for Professional Certification." The Institute for Certification of Computing Professionals (ICCP). URL: http://www.iccp.org/haraf.html (26 Oct. 2000).

"Information Assurance Curriculum and Certification: State of the Practice." Carnegie Mellon Software Engineering Institute. 1999. URL: http://www.sei.cmu.edu/publications/documents/99.reports/99tr021/99tr021chap02.html. (25 Oct. 2000).

Lambert, Mike. "Certifications held by Information (Computer) Security Professionals." URL: http://www.frontiernet.net/~mlambert/certifications.htm (26 Oct. 2000).

Matthews, Donna L. "Certifications for IT Security Professionals." About: The Human Internet. 21 June 1999. URL: http://certification.about.com/compute/certification/library/weekly/aa062199.htm (26 Oct. 2000).

Merritt, James W. "Need Security? Get a Real Expert." Information Week Online. 3 April 2000. URL: http://www.informationweek.com/780/80uwjm.htm (26 Oct. 2000).

Northcutt, Steven. "Can Security Certification Make a Difference?" SANS GIAC. May 2000. URL: http://www.sans.org/giactc/cert_dif.htm. (25 Oct. 2000).

Radcliff, Deborah. "Secure With Your Security Pros." ComputerWorld. 21 August 2000. URL: http://www.computerworld.com/cwi/story/frame/0,1213,NAV47_STO48432,00.html (7 Sept. 2000).

Rothke, Ben. "A Look at CISSP Certification." SC Security Magazine. April 1998.
URL: http://www.scmagazine.com/scmagazine/1998_04/lastword/lastword.html (26 Oct. 2000).

Suarez, Pat. "Certification Leads to Role as Author, Trainer." 1 April 2000. URL:
http://gocertify.earthweb.com. (27 Oct. 2000).

Suarez, Pat. "Professional Profile: Cheryl Jackson, CISSP, CBCP." 25 Sept. 2000. URL:
http://gocertify.earthweb.com. (27 Oct. 2000).

"The New Microsoft Windows 2000 Designing Network Security Exam." URL:
http://gocertify.earthweb.com. (27 Oct. 2000).

Thibodeau, Patrick. "Government Faces Security Skills Shortage." ComputerWorld. 12 August 1999.
URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO28662,00.html (26 Oct. 2000).

Wade, Jim. "President's Message." International Information Systems Security Certifications Consortium,
Inc. URL: http://www.isc2.org/pressmess.html. (25 Oct. 2000).