Global Knowledge®

Expert Reference Series of White Papers

Planning a Career Path in Cybersecurity

Planning a Career Path in Cybersecurity

James Michael Stewart, CISSP, ISSAP, SSCP, CPTE, CDFE, Q/SA, Q/EH, CEH, CHFI, and Security+

Introduction

The field of cybersecurity is growing quickly; so quickly that there are positions sitting open waiting to be filled by qualified individuals. Are you one of those people ready to make a change in your career towards the future?

Cybersecurity is the arena of technology, methodology, and practice which focuses on protecting electronic information and the systems supporting it against compromise and attack. Cybersecurity encompasses stand-alone and networked computers, local networks and the Internet, hardware and software, private and public organizations, online and offline concerns, internal and external threats, domestic and international concerns, intentional and accidental events, all forms of attack (including electronic, physical, and social), and much, much more.

As a society, we have all become heavily dependent on computers, network, and data stores. This in turn has exposed us to the risk of loss or compromise of those data systems. The need for personnel knowledgeable and experienced in security implementation and management has never been greater, and the need is growing.

Areas of Competency

Cybersecurity has been formally defined by ISO/IEC 27001 and 27002 to include:

- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Regulatory compliance

As you can see, there is an astounding breadth of concern for the cybersecurity professional. For smaller organizations with fewer staff, cybersecurity job positions will require competence across all of these areas of concern. For larger organizations with very large staffing abilities, a team of cybersecurity professionals may be assembled, with each member being a skilled practitioner in one primary topic.

Discover What Is Hot in the Marketplace

As with anyone seeking out a new job or a change in career, the first step is to discover what opportunities exist in the marketplace. Performing an initial assessment of offerings will provide you with a better understanding of what positions are available and what the minimum requirements are for each type of job.

I usually recommend starting with a job search site, such as indeed.com (a search engine of "all" job sites), and use keywords such as "cybersecurity," "cyber security," or "security." These terms will locate the majority of jobs related to the concept of cybersecurity. Take the time to look through many of the job listings uncovered by this search. After some review, pick a position or title that seems appealing to you, such as cybersecurity manager, database security administrator, security policy chief, security trainer, or security systems quality assurance. Then, search again with your selected title or position. Find at least 20 different organizations requesting applicants for that position and then take note of several items:

1. Required certifications
2. Required specialty education
3. Required experience
4. Starting and potential salary and benefits

As an instructor, I'm often asked what certifications are required to get a specific job. Unfortunately, that is a question that does not have a universal answer. Every organization will have its own requirements when selecting a potential new hire. You need to know what the marketplace in general seems to be requesting to get an overall sense for what is common and reasonable as requirements. Many of my students seem to think the answer is a single certification on their resume to get them the job of their dreams. Unfortunately, that is almost never the case. Most individual certifications are just part of the overall picture of what a company is seeking in a new applicant. Thus, performing a real-world position survey will give your expectations a solid dose of reality.

You might be quite surprised by what you discover when performing this investigation.

What Certifications Do I Need?

Having one or two certifications under your belt is rarely sufficient to land a new job position. And those job positions that can be obtained with minimal certification are unlikely to pay at the marquee level. Salary surveys over the last year or so often indicate that some cybersecurity jobs pay in excess of $100,000 per year, plus benefits. However, if you fail to read the fine print on these eye-catching headlines, you might miss the fact that the top-paying careers could require several years of specialized secondary education, may require dozens of certifications, and often mandate 10+ years of relevant experience.

Look for Positions You Can Land Now

Be realistic. Top pay is given to those with the knowledge and ability to solve problems and improve an organization's security stance. Standing out from the crowd with excellence and a proven track record is what awards you with higher compensation. Find a position you can land now; then seek out that which is necessary to move up your career ladder toward your dream job.

Vendor-Neutral, Vendor-Specific

In your survey of available security positions, you may see several certifications commonly requested. These might include CompTIA's Security+, EC Council's Certified Ethical Hacker (CEH) or Certified Hacking Forensic Investigator (CHFI), and ISC2's Certified Information Systems Security Professional (CISSP). These are some of the widely requested certifications in the security industry today. What these certifications have in common is they are all vendor-neutral or vendor-independent certifications. In other words, they do not focus on a specific operating system or software product.

However, there are also many vendor and product-specific certifications. These include Cisco, Avaya, EMC, HP, Juniper, Microsoft, Red Hat, VMware, RSA, and SAP. The more specialized the organization on a specific product or the more focused a job position, the more likely vendor- or product-specific certifications may be requested.

Vendor-neutral certifications have broad appeal and will be applicable to most job offerings. However, be cautious about investing in vendor-specific certifications until you are positive you wish to stay in job positions that focus on that vendor.

Long Shelf Life

Most security certifications offer solid and directly usable knowledge that can be applied to every cybersecurity job position. While other certifications are more ethereal and are popular for a few years, they can then be surpassed by another trending certification concept. Be sure to re-assess the marketplace every six months to see any shifts in hiring practices. Take this opportunity to adjust your bearings and re-focus your efforts on the now-closer target. If you have already achieved certifications that are no longer on the required hit list, then just buck-up and move forward. Don't continue to pursue any certification once it is no longer requested by at least 75 percent of the job positions you are interested in. Or at least, not until you are honing in on a specific position key to your path and need to achieve the last few outstanding requirements.

Many certifications are based on your experience and knowledge, but only test you with standardized exam questions, such as multiple choice and fill-in-the-blank. A growing number of certifications now include more practical or hands-on forms of testing, such as solving complex problems, applying knowledge to a scenario, or performing functions or commands in a system simulator. There are also certifications that require work experience in order to qualify to take an examination. For example, the CISSP certification requires five years of relevant security experience (however, that experience can be obtained prior to or after taking the exam).

College Degree

A significant number of cybersecurity positions require a college degree; some even require an advanced degree, such as a Masters or Ph.D. This could be an automatic disqualification if you don't have the degrees. However, if you have serious real-world experience (such as 10+ years), some companies will adjust their degree requirements.

Experience Required?

There are companies that are interested in hiring new recruits directly out of college or just after achieving certification benchmarks. These companies often want to train and mold employees for their corporate culture before they have learned other competing strategies. These companies might think that re-training someone is more difficult or costly than teaching someone for the first time. However, such new-hire types of situations are also more difficult to advance out of. As such an employee, you may be narrowly trained for specific job tasks and have little opportunity to develop skills needed to advance into other positions. Additionally, being brought in with minimal experience might also limit your initial earning potential. If you need a job based on certifications or education alone, these types of jobs may be just the right fit for you.

If you have a reasonable level of experience, such as at least five years, then you may need to seek out job offerings that require experience. This will move you into job areas that will have fewer applicants, but which will have more strict compliance requirements. In such cases, certifications will ensure that you meet the minimal qualifications, but, ultimately, your experience and abilities will determine whether or not you are a good fit for the company to hire you.

Some say that experience is everything. While that is not always true, most of the job positions you seek will have some level of experience requirements. While you are working your way through gaining education and obtaining certifications, don't overlook opportunities to gain experience. It may be worthwhile to take a more entry-level position to get experience time on your resume, even if it is not exactly in line with your ultimate career goal, does not have great earning potential, is not with an organization you want to be with for your entire career, or from which there is no opportunity for internal advancement. If you can afford to live lean while you take a lower-paying position or internship to gain experience, then you might be making the right sacrifice in the short term that will allow you to achieve your long term career goal.

Military and Government

One of the cybersecurity industries or sectors that is growing the fastest is that of government and military. Many such job positions may require education, certification, and experience to achieve, while others may offer on-the-job training as part of the position. You might find that working for your government or being a part of the military is in line with your career goals. It is also likely that there is ample room for advancement within the public sector far beyond what you might experience in the private sector. Government and military cybersecurity positions often include specialized training and experience that cannot be obtained in the private sector. A government or military job position could be your chosen career path, or a means to develop relevant experience for a future private sector career.

Many companies will offer higher compensation packages to those who are ex-military or former federal employees, based on the unique and proprietary training and experience they may have received.

Testing the Waters

If you are unsure whether or not your current experience, education, and certifications are sufficient for a particular position, you can always contact the organization with the job opening and ask for a phone or in-person consultation. Not every HR manager will be willing to talk with someone that might not be qualified for a position, but others are happy to discuss their requirements and your qualifications. You may need to inquire of several organizations before you find someone willing to talk with you. You might also be surprised to discover that while you might not completely meet their listed requirements, after an intelligent discussion with you, that you are offered a job anyway.

Fresh Out of the Gate

If you are a student at a college or university, there are often career counselors available. Don't forget about the professors or instructors of your security and technology courses; they can often provide career insight into their respective fields. There are even free and fee-based career counselors available. You might find that spending some time in a focused consultation can be a solid starting point for your career.

Requested Knowledge Areas

Many of the cybersecurity positions available today are requesting knowledge and experience in one or more of several specific areas, such as:

- Information and data security
- Firewall management
- IDS/IPS administration
- Network and networking security
- O/S security
- Cryptography
- Protocol security
- Secure and defensive programming
- System configuration
- Audit log analysis

However, realize that these areas of interest and concern are for job applications filled today. If you spend six months or six years building up your knowledge and skills, those areas of interest may shift.

What to Do Now?

I'm sure you have heard the adages of "look before you leap" or "if you fail to plan, then you plan to fail." Both of these statements offer solid guidance for anyone seeking a cybersecurity job position. It is important to think

ahead before you make your first steps. One of the most important questions to answer is where do you want to be in 5, 10, or 20 years in terms of a career? Once you have that goal in mind, find the path that helps you to achieve that goal. That will include seeking out education, obtaining certifications, and gaining experience in relevant job positions.

Conclusion

Before taking a job, consider how that job will assist or hinder you towards obtaining your long-term goal. If you are looking to be hired by a smaller organization, is there sufficient room for career advancement, or will you need to leapfrog to another company when you are ready to move ahead? If you are interested in being hired at a large organization, will there be lots of competition for job openings and will you be able to be recognized apart from the crowd?

Take every opportunity availed to you to obtain education and certification, as long as it is in line with your career path. Global Knowledge offers a wide range of training courses that focus on both job skill as well as certification achievement, especially in the growing field of cybersecurity.

Before booking your first class, take a few moments to step back and look at the big picture. Many of the new workers of the next 10 to 20 years will be in positions that don't even exist yet . work Be cautious about picking a career path based on only historical concepts of work opportunities. Look around for new technologies and growing industries; you might find exciting new jobs in new fields. Some very exciting areas include bio-technology, genetics, social networking, wearable computing, virtual experiences, mobile, cloud, and big data management. Think big. Look to the future. Then, take the first step towards your new career in the expanding world of cybersecurity.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

- Cybersecurity Foundations
- Security+ Prep Course
- CISSP Prep Course
- Certified Ethical Hacker v8

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

James Michael Stewart has been working with computers and technology for nearly thirty years. His work focuses on security, certification, and various operating systems. Recently, he has been teaching job skill and certification courses, such as CISSP, ethical hacking/penetration testing, computer forensics, and Security+.

He is the primary author on the *CISSP Study Guide 6th Edition*, the *Security+ Review Guide 2nd Edition (SY0-301)*, and *Network Security, Firewalls, and VPNs*. He has also contributed to many other security-focused materials, including exam preparation guides, practice exams, DVD video instruction, and courseware. In addition, he has co-authored numerous books on other security, certification, and administration topics. He has developed certification courseware and training materials as well as presented these materials in the classroom.

James Michael holds a variety of certifications, including CISSP, ISSAP, SSCP, CPTE, CDFE, Q/SA, Q/EH, CEH, CHFI, and Security+. He graduated in 1992 from the University of Texas at Austin with a bachelor's degree in Philosophy. Despite his degree, his computer knowledge is self-acquired, based on seat-of-the-pants, hands-on "street smarts" experience. You can reach him by e-mail at michael@impactonline.com.