Global Knowledge®

Expert Reference Series of White Papers

Ten Reasons You Should Consider a Career in Cybersecurity

Ten Reasons You Should Consider a Career in Cybersecurity

James Michael Stewart, CISSP, CEHv3-8, CHFIv3-8, Security+, Global Knowledge Instructor

Introduction

Cybersecurity has become a key area of job growth in the last few years. Now more than ever, individuals with computer security skills are needed to fill jobs that are currently sitting vacant. All the while, new job positions come into existence every month with few qualified applicants. There are tens of thousands of job positions sitting empty because there is a dearth of qualified applicants with the education, training, skill, or experience to take on the work. According to the July 12, 2016 Federal Cybersecurity Workforce Strategy memorandum:

> "Both Federal and private sector executives cite the lack of professionals with the requisite knowledge and skills as a significant impediment to improving their cybersecurity. However, there simply is not a sufficient supply of cybersecurity talent to meet the increasing demand of the Federal Government. Recent industry reports project this shortfall will expand rapidly over the coming years unless companies and the Federal Government act to expand the cybersecurity workforce to meet the increasing demand for talent."

Becoming a qualified applicant for a wide number of cybersecurity jobs will start you on a long, profitable, and exciting career in IT security. A career as a network security or cybersecurity expert does not limit you to only working for an IT company. Every organization across every industry is in need of security experts to support and improve their IT security infrastructure.

Are you already working in an IT position, do you have an interest in computer security, or are you still working on completing your education? If you can answer yes to any of these questions, then you are a prime candidate for switching your career path to become a cybersecurity expert. For many of you, changing your focus to IT security will simply be a minor course adjustment of your career or education. For a few of you, it may be a complete reassessment of your education or career path. Even if you must undertake a major venture to refocus your efforts on becoming a cybersecurity expert, I think the long-term rewards, benefits, and job stability are worth the effort you may need to expend. And, I think you will find that the change is not as significant as you might first expect, no matter what your current career path or education track is aimed toward. "The demand for the (cybersecurity) workforce is expected to rise to 6 million (globally) by 2019, with a projected shortfall of 1.5 million," claims Symantec CEO Michael Brown.

U.S. News & World Report cites that an information security analyst job is ranked No. 5 in the list of best technology jobs, and No. 34 in the top 100 best overall jobs. It offers nearly $90,000 in median salary (as of 2014), has an above average job satisfaction rate, and that tens of thousands of job openings are currently waiting for a qualified applicant.

Still not convinced? Then please continue reading. In this white paper, I highlight ten key reasons or issues that you should consider when thinking about a career in cybersecurity.

Copyright ©2016 Global Knowledge Training LLC. All rights reserved.

1. You Already Know the Basics

Cybersecurity is about understanding how a system works, where its weaknesses are, how someone may attempt to take advantage of those weaknesses, then working to implement protections against any compromise. If you currently work with computer technology in any way, you already understand this. Over the last twenty years as computers, networks, and even smart phones have become commonplace at work as well as everywhere else. You already know that keeping your systems current and up-to-date with your vendor's latest software version of software will provide you with the most secure and stable platform to build a security defense. You know to lock down access to your devices and data by using strong authentication processes that you keep secret from everyone else. You know to look out for social engineering attacks that may be directed at you over the phone, via email, through text message, in a social media communication, and even while surfing the web. These concepts, which you have adopted to protect your personal electronic devices and which you may have been taught at school or while on the job, are the foundational concepts of all of IT security. Keep things current, block unauthorized access, and watch out for attacks.

Experts in cybersecurity are people who have spent focused time and effort learning these basics and discovering how to adopt and apply them to any and every situation they encounter. Whether securing a home network for a grandmother or locking down a network for a global enterprise, the foundational concepts of security are always the same. So, recalibrating your education or career path will not be as hard as you might first assume.

2. Cybersecurity Is a Deep and Wide Arena with Many Options to Consider

Cybersecurity is a term often tossed around as if it means something specific. But, it is not as specific as you might think. Cybersecurity is any aspect of any position in an organization that somehow relates to computer technology and asset protection and how they intersect. Cybersecurity is really a mindset of understanding the value of assets, perceiving the vulnerabilities, comprehending the potential exploits and attacks, and implementing the proper response to minimize or eliminate compromise. This is a set of skills that many people already have and that many more can easily obtain.

A job as a cybersecurity expert is not just limited to big computer companies either. Every organization has to deal with computers in one way or another, whether it's using smartphones to run the entire operation or using a massive network of systems to support mind-bogglingly huge amounts of data. Cybersecurity personnel are needed from small start-ups and businesses that are run out of a home to large corporations as well.

If you want to be a jack-of-all-trades and manage every aspect of IT security for an organization, you can either be the one IT person in a small company or be the head of the IT security division at a multi-national organization. You can work in a nonprofit, a commercial entity, a government agency, or as a military contractor. You can work in any field in any industry, including healthcare, transportation, infrastructure, construction, telecommunications, textiles, manufacturing, logistics, city management, legal, retail, entertainment, recycling, energy, and even waste management. Every organization is in need of a cybersecurity expert, whether they realize it yet or not. And if they don't know they need you now, they will as soon as their IT systems are compromised by malware, an employee mistake, or an intentional breach by an external attacker.

Copyright ©2016 Global Knowledge Training LLC. All rights reserved.

3. Security Professionals Can Focus on Design As Well As Implementation and Management

A career in cybersecurity is not only about pulling cables, configuring routers, and dealing with failures. Many choices for specialization are available for someone in IT security. One of the most overlooked or forgotten areas of cybersecurity is design. Cybersecurity design is also not a single-focused concept either. Cybersecurity design includes new concepts of security mechanisms, creating of new filtering schemes, crafting new security rules, architecting the logic of access control, configuring the back-end logic, setting up the APIs, crafting the source code, designing the user interface, and more.

Security should not focus exclusively on the ugly details of what to allow and what to deny. It should also consider how the security affects business tasks, work flows, and usability. If an end-user is frustrated by an interface, is unclear about what a function does, or is confused about the purpose of a security mechanism, then security has failed. An end-user needs to be considered when designing and implementing security. Security needs to be understood, accepted, and complied with in order for it to be successful. The success of security starts with good design and planning.

4. Professionals Are Needed at Every Level

A cybersecurity expert is more than just someone working in the company basement dealing with computers and the myriad of cables that run throughout the building. Cybersecurity experts are found at every level within an organization's hierarchy, ranging from interns to CEOs. The more an organization is dependent upon computers and networking, the more that organization needs qualified security experts managing and overseeing every aspect of their infrastructure.

A cybersecurity expert can be a general IT security worker, a security group supervisor, an IT security manager, a device specific administrator, and even a C-level executive. Additionally, getting into a cybersecurity career at a lower level of an organization does not limit your ability to move up the career ladder. In fact, as you can demonstrate skill, knowledge, and expertise, look to rise in the ranks as most organizations prefer to promote from within. You need to learn to make yourself indispensable so your employer will want to keep you around for to benefit from your extraordinary skills.

5. A Cybersecurity Career Can Include a Wide Range of Activities

Within any cybersecurity position, you can focus on many unique facets. Some roles are essential in crafting and updating security policies, while others are tasked with training and educating users on the security rules and how to accomplish their job responsibilities in a manner consistent with and in compliance with the organizational security policy. Every organization needs security personnel to evaluate new products and updates to existing products before they are allowed to be implemented into the production IT systems. Once approved, a cybersecurity expert needs to be involved in the actual production installation of software in order to ensure the proper configuration and integration with the existing infrastructure.

Other cybersecurity experts are needed to perform functional testing, compliance testing, and security testing. These employees are looking to discover where there are deficiencies in the IT infrastructure that are hampering production, placing the company at risk, and that can be exploited by criminal hackers. Cybersecurity experts are needed for backup and restoration, incident response, business continuity planning, avoiding single points of

Copyright ©2016 Global Knowledge Training LLC. All rights reserved.

failure, implementing redundancy, disaster recovery planning, system maintenance, troubleshooting, repairs, system upgrades, internal investigations, criminal investigations, and performing forensics.

6. It Is a Field That Is Always Changing and Growing

Cybersecurity is not a single concept. It is a broad and ever-changing field related to business functions, technology, and personnel. Our planet is soon to host over eight billion people in less than a decade. That means there will be more people who will need more products, services, and jobs. These are people who will not only be using computers, mobile phones, and the Internet, but who will also rely on technology to manage and support an ever-growing portion of their personal and professional lives. The concept of being a cybersecurity expert today will not be the same in five years from now, or ten years, or even fifteen years. Much of the technology we know today as computers and networks did not exist just a decade ago. Facebook, Google, Twitter, Amazon, eBay, and almost every other significant online site or service did not exist just twenty years ago. The Internet was only just barely a concept being stitched together from a few governmental, educational, and private networks just thirty years ago.

According to PwC's 2015 US State of Cybercrime Survey, "76% of respondents said they are more concerned about cybersecurity threats this year than in the previous 12 months, up from 59% the year before." This means that there are more organizations concerned about security than ever before, and thus new job opportunities are constantly opening and needing qualified applicants.

In the years and decades to come, there will be advances in technology and changes to its use beyond what we can conceive or imagine today. Your job as an IT security professional will always be changing. Maybe not every day and not even year to year, but the job you have in five or ten years from now will be vastly different from what it is today. Significant changes and leaps in technology are occurring at an ever-increasing pace as more people think about what they want to create, design, or do next. As more of the world comes online and begins to interact with the global cyber community, new ideas and creations will emerge. Our world is changing faster today than it ever has before.

7. You Will Be Challenged on a Regular Basis to Solve New Problems

Due to the unpredictable nature of the future, a career in cybersecurity is not and cannot be static and stale. You will be challenged on a regular basis. There will be new and unexpected failures as well as amazing and surprising discoveries. One certainty is that attackers will continue to develop new exploits on a constant basis, and your job may be to evaluate these new threats as they are uncovered in order to improve your organization's defenses.

The functions of business will change and you may be tasked with altering the existing IT infrastructure to support a new process, function, or capability which was never before considered. The company may have an unexpected popularity surge that drives up your production rate by a 1,000% or more, requiring you to ramp up capacity as fast as you can get hardware plugged in and software installed. Your company may branch out into alternate markets, spread into other countries, or adopt exotic business strategies and you will be required to make the IT adjustments, support the change, and keep things stable, available, and secure. As a cybersecurity professional, you will be solving new puzzles, fighting off new demons, and supporting new activities on a regular basis. Do you enjoy tough and constantly changing challenges?

Copyright ©2016 Global Knowledge Training LLC. All rights reserved.

8. New Attacks and Threats Need to Be Discovered and Handled

Bad guys will always exist and they are always trying to find new ways to infiltrate your systems. The job of a cybersecurity expert is never complete. The task of securing an organization is never finished. Security is always changing and adjusting based on newly discovered vulnerabilities, threats, and exploits. New attacks, new attackers, new motives to attack are generated and discovered on a daily basis. Bruce Schneier stated, "I repeat the saying I've heard came from inside the NSA: 'Attacks always get better; they never get worse.'" Schneier on Security Blog.

It is essential to understand that security is never a finished product; it is not a goal that can be reached or a finish line that can be crossed. Instead, security is a process, a method of operating an organization, a struggle, a journey toward a better tomorrow. Security is often more reactive that proactive. While every effort is made to understand and stop attacks before they become successful, all too often the world is subjected to new and unknown attacks against which we have no known defense. Thus, only after a newly discovered exploit or attack can a countermeasure be designed and implemented. The security that worked to stop yesterday's attacks may not be sufficient to stop the attacks of tomorrow. Cybersecurity experts are needed that can maintain the diligent, active focus that is required to see new threats looming and to adjust the security infrastructure to compensate for them.

There are an untold number of new and unknown exploits and attacks in the criminal hacking underground. Some of them were developed years ago and have been used sparingly while leaving little to no trace of their use. Others were developed only recently and have yet to be put to widespread use. Some exploits are just a few hours old before security professionals discover them, while others are more than a decade old. The realm of discovering unknown attacks and exploits is a bit like treasure hunting. These experts use their knowledge and experience to locate a target that they are not even certain exists. As a cybersecurity expert you can focus your career on the discovery and exposure of new attacks and exploits. This is an exciting and ever-changing occupation where there will always be something new lurking, just waiting to be discovered, analyzed, exposed, and halted. Your discoveries will help millions avoid being harmed by attackers.

You could focus on being a malware expert looking for the next virus, worm, rootkit, backdoor, remote control tool, or ransomware product to spread across the Internet. You might focus on ethical hacking and penetration testing where you use the skills, tools, techniques, and methodologies of criminal hackers to stress test the security stance of your clients. You could be a skilled programmer to craft sample or simulations of malicious code and exploits in order to develop new tools and response strategies. Perhaps you would be drawn to developing new capabilities for firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to block attacks, whether known or unknown. Or, you might become a skilled professional in tracking down perpetrators who perform attacks on computer systems or who use social engineering tactics on employees or individuals. Further yet, you could become a forensics expert who gathers evidence for use in criminal prosecution. These and many other facets of cybersecurity all focus on the ever-changing state of attack and defense that is IT security.

Copyright ©2016 Global Knowledge Training LLC. All rights reserved.

9. Changing Focus or Specialization Is Possible with Only Modest Effort

Jumping into a cybersecurity job does not lock you into a singular position for decades. In fact, it is just as easy to shift your security focus or specialization as it is to select your first area of cybersecurity employment. You might not have all the knowledge, skill, and expertise for every cybersecurity job right now. But you can always learn more while on the job, take on more responsibilities in related jobs as your time allows, and study and take classes after work on your own time to expand your career opportunities.

If you already have sufficient knowledge, experience, and certifications on your resume, getting started in cybersecurity is relatively easy—basically pick an entry-level position or something more advanced and then apply for the job. Once you are hired, make yourself indispensable. Learn how to do the job you were hired to do, do it efficiently, correctly, and promptly. Ask questions and for assistance when needed. Provide a hand when asked, and be friendly and helpful to everyone from other new employees to the top executives.

Once you've begun demonstrating a solid capability for performing your job responsibilities, go beyond expectations by asking for additional responsibilities or providing others assistance in completing projects or work tasks. Even consider volunteering for additional evening tasks, weekend jobs, or emergency response events—although don't dedicate every waking moment of your life to your work. The idea is to get yourself noticed by your boss and other higher-ups as a reliable, trusted, and competent employee—someone who is willing and able to make the extra effort to support the organization. Keep a work-life balance by establishing necessary boundaries and parameters, but show some amount of additional effort and display intentional attention to detail. Often just a little more effort than everyone else makes you stand out as a superstar.

Once you understand the job responsibilities for which you were initially hired to handle and you comprehend the direction and goals of the organization, seek out interesting elements in other job positions. Nurture and develop the skills needed to excel in those positions, then offer yourself as someone willing and able to perform the harder tasks, to take on more responsibility, to help lead the organization. As you find your interest peaked by new concepts, events, elements, and job tasks lean into the challenge in order to jump to the next opportunity. Keep in mind, companies will promote from within if they perceive an employee as too valuable to lose. Be that cybersecurity employee, and you will have your choice of job positions.

10. You May Be Able to Create a Completely New Job Title, Position, or Focus

As I have already mentioned, the world of information technology is fast paced and ever changing. Many of the job positions that exist today did not exist just five or ten years ago. In fact, the job you have right now or the one you are working your way through your education to obtain may not have existed until recently. New jobs are being created at an ever-increasing rate.

Technology has produced many new jobs. As we move into the future, some jobs will disappear or be filled by automation or other forms of technology, and new types of jobs, careers, and work responsibilities will come into existence. It is already possible to name dozens of jobs that don't exist today but will soon, such as idle IT asset manager, drone manager, private air traffic controller, self-driving car technician, autonomous vehicle specialist, and human interface device integration expert. I'm sure you can imagine a few others as well.

Copyright ©2016 Global Knowledge Training LLC. All rights reserved.

Many of the jobs that will be held by a worker in ten years do not even exist today. Who would have thought that ten years ago there would be thriving career opportunities for a private space rocket engineer, smart phone app developer, digital marketing specialist, blogger, SEO specialist, and cloud services manager? IT security jobs today are only a shadow of what they will be tomorrow.

As a cybersecurity career specialist, the opportunities are endless. Because versatility is such a prominent feature in this profession, you essentially can draft your own job description. Often the job of an IT security expert is to do whatever needs to be done. A static written job position just won't account for the changing conditions of IT itself, must less security. As you gain experience and learn more about IT security, you will likely discover areas that are yet to be addressed or fulfilled by today's IT positions. You can craft your own job title, customize your position within the organization, and fine tune the focus of your day-to-day activities based on ideas, concepts, and opportunities that don't even exist today. Wow!

Conclusion

I think a career in cybersecurity is a promising and rewarding opportunity, no matter what your general area of experience, interest, or expertise. If you live in the modern world, you are already on a solid starting line of a future IT security career. Shifting gears to focus on cybersecurity is not as much of a transition as you might first think. Plus, the cybersecurity field is broad, deep, and always changing. The job you focus on initially may not be the same that you end up with. You will have to constantly refocus your attention and efforts as the realm of IT security changes. This field might not be for everyone, but I think if you are in any way interested in computers, security, the Internet, smartphones, or how businesses operate in the modern world, you are already a prime candidate for a cybersecurity career.

You might wonder where to get started. I would recommend a multi-step approach:

- First, if you already have one or more IT certifications, then scan the job postings for opportunities with the key word *security* and your certification acronyms.

- Second, if you don't have any IT certifications or you discover you have too few, then seek to obtain the certifications that lead you down the path to being qualified for your desired job position. If you are starting from scratch, I recommend Security+ and Network+. If you are already moderately knowledgeable in IT and security, consider Certified Ethical Hacking (CEH) and Computer Hacking Forensic Investigation (CHFI). If you are an advanced IT worker, a manager of an organization, a designer and architect of security, then consider becoming a Certified Information Systems Security Professional (CISSP).

  According to Burning Glass' "Job Market Intelligence: Cybersecurity Jobs, 2015" report,

  > ". . . there were nearly 50,000 postings for workers with a CISSP certification in 2014, the primary credential in cybersecurity work. That amounts to three-quarters of all the people who hold that certification in the United States—and presumably most of them already have jobs.

  Thus, if you obtain the certifications that businesses want you to have (which is disclosed in their public job postings), then there are a wide range of opportunities for you to land a job.

- Third, keep in mind that no single certification or even a large set of certifications will get you a dream job. However, certifications are what will keep your résumé on the desk of the person responsible for hiring. You want to meet and exceed their minimal requirements to be qualified for the job, without having any negatives that would disqualify you.

Copyright ©2016 Global Knowledge Training LLC. All rights reserved.

- Fourth, in order to keep your resume in consideration, highlight any recent college degrees, volunteer work in an appropriate field or capacity as the job you are seeking, and any related on-the-job experience. The more of these extras that you have, the higher up the job ladder you can jump to initially. Otherwise, you may have to start off on a lower rung, but there is always more ladder to climb in an IT security career path.

- Fifth, the job you seek may not be available to you. It might get filled before you even apply. It might be filled before you even see the initial online posting. You might need to take three to twelve months to obtain certifications, finish education, or gain some experience. The job may be gone by the time you complete these steps. It is your responsibility to keep an eye on the job market as you are seeking to gain all of the qualifications of your targeted job position. So, find three to ten similar job positions from different organizations, then use them as a survey of the marketplace upon which to set your sights for personal development. Every three months, re-evaluate the job market to see how things have adjusted or changed. Also consider new positions that were not previously available. Use this new information to readjust your development goals. Maybe you will need more education or experience to land the job, or possibly you will have achieved enough progress to be considered as a viable candidate.

According to Burning Glass', "Job Market Intelligence: Cybersecurity Jobs, 2015" report, "Cybersecurity postings have grown 91% from 2010–2014. This growth rate is more than faster than IT jobs generally." Thus, the job market is changing quickly. So, keep an eye on your goal and readjust your plan as the marketplace changes focus.

Landing any job in any field can be challenging. But having the right initial qualifications will go a long way to getting you hired. Be qualified. Be available. Be an asset that cannot be passed up.

Bibliography

Burning Glass Technologies. 2015. "Job Market Intelligence: Cybersecurity Jobs, 2015. http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf

Executive Office of the President. July 12, 2016. "Federal Cybersecurity Workforce Strategy." The White House. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-15.pdf

Morgan, Steve. July 28, 2015. "Cybersecurity Job Market to Suffer Severe Workforce Shortage." CXO Media, Inc. http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html

PwC. July 2015. "US Cybersecurity: Progress Stalled." http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf

U.S. News & World Report. Accessed August 8, 2016. http://money.usnews.com/careers/best-jobs/information-security-analyst

Copyright ©2016 Global Knowledge Training LLC. All rights reserved.

Learn More

Learn more about what it means to be a cybersecurity professional and how you can better assist your organization in ramping up for cyber preparedness.

Cybersecurity Training

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 over thirty years. His work focuses on security, certification, and various operating systems. Recently, Michael has been teaching job skill and certification courses, such as CISSP, ethical hacking/penetration testing, computer forensics, and Security+. He is the primary author of *CISSP Study Guide, 6th Edition; CompTIA Security+ Review Guide: SY0-401; Security+ Review Guide, 2nd Edition (SY0-301)*; *CompTIA Security+ Training Kit (Exam SY0-301)*; and *Network Security, Firewalls, and VPNs*.

Michael has also contributed to many other security-focused materials including exam preparation guides, practice exams, DVD video instruction, and courseware. In addition, Michael 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.

Michael holds a variety of certifications, including: CISSP, CEH, CHFI, and Security+. Michael 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 Michael by email at michael@impactonline.com.

Copyright ©2016 Global Knowledge Training LLC. All rights reserved.