Issues in Information Systems
Volume 18, Issue 3, pp. 141-148, 2017

THE CYBERSECURITY STUDENT CAREER PATH: WHICH ONE IS RIGHT FOR ME?

Jason E. James, Robert Morris University, jejst243@mail.rmu.edu.edu

ABSTRACT

Cybersecurity jobs are plentiful, from government, financial services and utilities to manufacturing and retail. But what path should cybersecurity students choose to follow is not that simple largely in part to the education and training, certifications, and experience needed to develop the skills needed to be successful. Are you a student, current cyber worker, or career changer? Are you thinking about a job in cybersecurity? Learning about and understanding the field's unique requirements will help you determine whether a career in cybersecurity is in your future. The work environment for cyber professionals is dynamic and exciting, with competitive salaries and growing opportunities. Cybersecurity professionals often thrive in an informal atmosphere, unconventional working hours, and shifting work responsibilities aimed at keeping knowledge fresh and work exciting. There are many different jobs within the cybersecurity field that require a broad range of knowledge, skills and abilities. Cybersecurity professionals must have the ability to rapidly respond to threats as soon as they are detected. Professionals must also possess a range of technical abilities to perform a variety of activities, and be able to work in different locations and environments. (NICCS, 2015)

Keywords: Cybersecurity, education, certifications, career

INTRODUCTION

When I started my career in auditing almost 15 years ago, I originally went into the field of circulation and asset based lending auditing. It was close to what I wanted to do, which was obviously auditing. However, in 2006, I took a position with the Department of Defense Inspector General (DoD IG) and by default, I began my career in Information Technology (IT) auditing and could not imagine doing anything else.

In 2007, I oversaw the work of a contracting team hired to test information systems controls as part of the Defense Finance and Accounting Service (DFAS) annual financial statement engagement. Three years later, I took an Auditor-in-Charge position with DFAS Internal Review Systems Team and have been leading a team who is called upon time and time again to perform engagements on information systems controls.

IT today fills every aspect of our daily lives. We would be very hard pressed to find a place in the world where some type of IT is not being used.
So, over the years I have sought to expand my knowledge in the field of what we now call Cybersecurity. From online webinars and training to reading thousands of articles. Most recently, I decided to get my doctorate in Information Systems and as part of my research I have developed a mind map of the many pathways in which Cybersecurity can lead you down.

My Cybersecurity career has centered around four aspects: education, experience, certification, and training. Early in my career, I sought out and obtained a Certified Internal Auditor (CIA) and Certified Fraud Examiner (CFE) certifications because I knew they would get me promoted and you did not need years of experience. I knew I needed them to advance to the next level in my career. However, once I advanced to an Auditor-in-Charge I quickly learned that I needed certifications that would advance my knowledge in information systems. I then obtained the Certified Information Systems Auditor (CISA) (the standard in IT auditing) and the Systems Security Certified Practitioner (SSCP) certifications as these were two of most well known certifications in the systems security world. However, after deciding to get my doctorate in Information Systems and before I obtained any more degrees or certifications, I wanted to increase my understanding of the World of Cybersecurity.

In spending this time researching for my dissertation, I developed what I call the World of Cybersecurity. I wish I knew then, what I know now when pursuing my undergraduate degree. However, back in the mid to 1990s, Cybersecurity was just getting the groundwork laid. With that said, I want to make sure every college student is provided the knowledge they need to make a decision that will affect the rest of their life with the hope was someday they would have an interesting and profitable career in Cybersecurity.

Before I get started, I want to say I am by no means an expert. This article is based on what I learned from experience over the last 10+ years as an IT Auditor and education. I believe my experience and education gives me a unique perspective on the world of Cybersecurity and the career paths that can be taken. So with that said I plan to discuss what I think is a very useful tool for any Cybersecurity student starting their career and I wish I had this information to help me start my career. Let's get stated (Hayslip, 2015)

In this article, we explore the different paths a Cybersecurity student can take in their career in order to help them make a better informed decision that they wont regret years down the road, or in my case, make the wrong decision early in my career and losing years of valuable experience in the field. The article will focus on the four different aspects described earlier: education, experience, certification, and training.

THE WORLD OF CYBERSECURITY

Chris Conacher, Manager of Security and Compliance Solutions at Tripwire, said it best in regards to the cyber security field, including how far the industry has come. "When I started out, there were no certifications or related education and only the government and its contractors had specific security roles," said Conacher. "Nowadays, there is a whole career path from entry-level all the way up to executive-level, which is great."

Professionals in the field have a variety of career options and specializations available to them. **"**You can be in operations, systems engineering, development, architecture, or testing and there is an established third-party service model, so it's easy to create your own company and get work," said Conacher.

In addition to the diversity of professions, careers in cyber security also range across numerous industry sectors. However, just remember that each path usually comes with its own education in addition to certification requirements that we will talk about in a later section (Bison, 2014).

The Cybersecurity profession is a complex world with many different career paths (see Figure 1)

The typical Cybersecurity student will obtain a Bachelor of Science (BS) in either Information Systems or Computer Science and then obtain their Master of Science (MS) in Information Systems or Cybersecurity. Some students may decide to get an MBA as well. However, these areas of study are not the only ones. Other areas of study include software engineering, information technology, and computer engineering.

Whatever, the area of study, those students also will typically have an Internship and additional training outside the classroom. Sometimes students want to get ahead and pursue entry-level certifications such as CompTIA Security+ or Network+. After they graduate, the path they choose can be overwhelming and may change over time as many Cybersecurity professionals do. Therefore, depending in the path chosen by a Cybersecurity student, whether they major in information systems, computer science, or Cybersecurity, the courses taught in security may be not be enough or and a deeper dive into information security would be needed as detailed in the next section

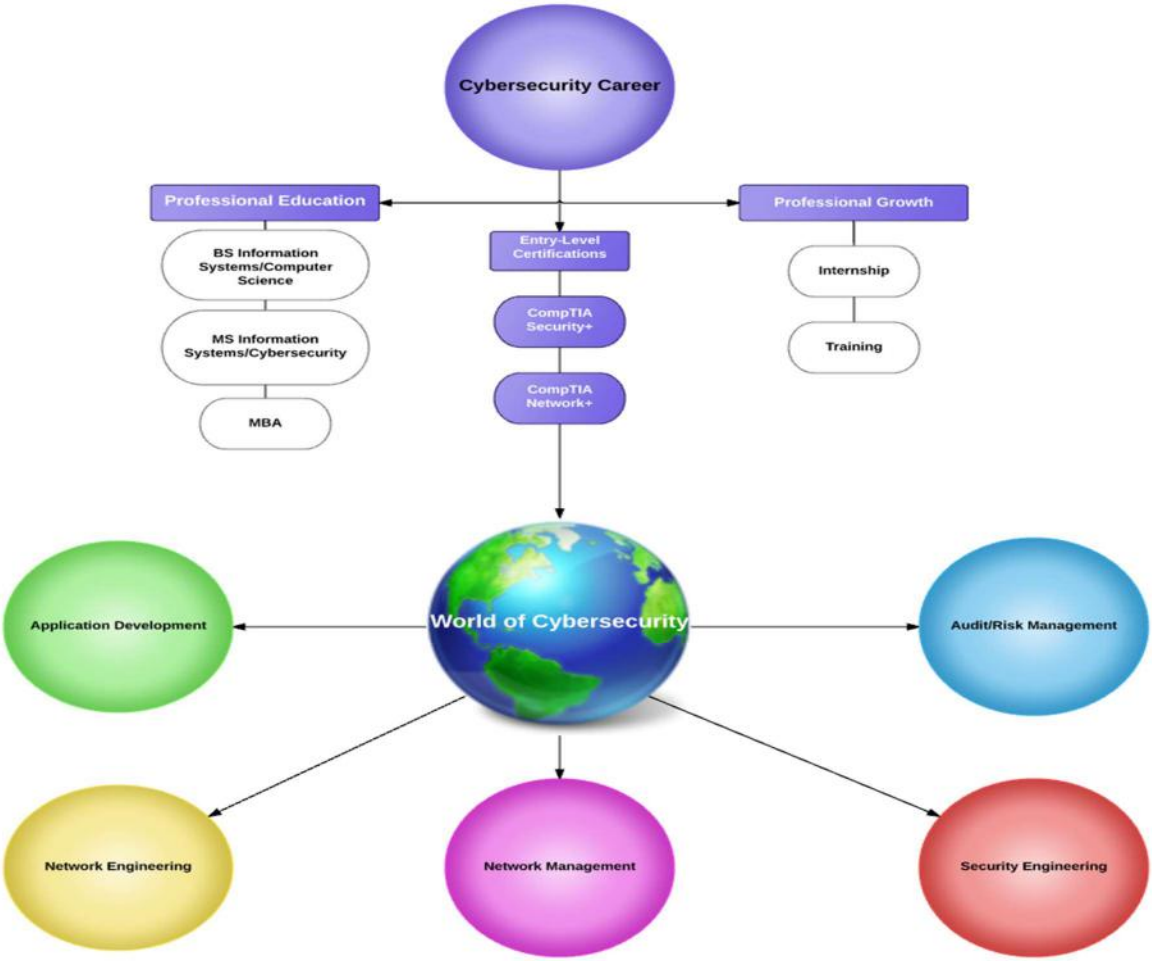

Figure 1. The World of Cybersecurity

Although there is many paths Cybersecurity professionals can follow, they typically follow a career path with one of 6 specialties as depicted in Figure 1, with each career path broken down into sub-specialties as follows:

Table 1. The World of Cybersecurity Sub-Specialties

Application Development
Mobile Application Development
Computer Programming
General Application/Programming
Network Engineering
Cloud
Linux
Juniper
Red Hat
Oracle
Microsoft
CISCO
Network Management
Project Management
ITIL
Security Engineering
Information Security
ICS/SCADA
Hack/Penetration Test
Application Hacking
Audit/Risk Management
Privacy
Physical Security
Audit/Risk General
Audit/Risk Specialties (Audit, Health IT, PCI, Risk)
Forensics

Many Cybersecurity professionals specialize in multiple sub-specialties and many experienced Cybersecurity professionals specialize across the six main paths. The sign that a Cybersecurity professional is specialized in a certain area is usually denoted by professional certifications. Overall there are approximately 2,000 different Cybersecurity certifications across over 150 different vendors (New Updated List of IT Certifications, 2016). However, as a Cybersecurity professional knows, you cannot just obtain a certification unless you have the proper years of experience and knowledge to pass the exams. Once the amount of years of experience has been met, most vendor-neutral or vendor-specific require a certain amount of training each year to maintain that certification and knowledge.

EDUCATION

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, some companies will adjust their degree requirements if you have serious real-world experience (such as 10+ years) (Stewart, 2013).

In order to decide which career path to take, an undergraduate Cybersecurity student must first decide what area of study matches what path to follow. The six main areas of study for undergraduate Cybersecurity students typically are software engineering, Cybersecurity (sometimes called information assurance and security or information security), information technology, information systems, computer engineering, and computer science. Although these are the primary areas of study for undergraduate Cybersecurity students, there are many others.

Table 2. Secondary Areas of Study for Cybersecurity Students

Computer Forensics
Computer Networks
Cybersecurity Strategy and Policy
Information Assurance
Information Systems Management
Information Systems Security
Management Information Systems
Management Information Technology
Mathematics
Network Management
Operations Research
Program Management
Software Applications & Programming
Software Development
Supply Chain Management
Systems and Network Auditor
Technology Management
Web Development

Valparaiso University website states whatever area of study an undergraduate Cybersecurity student decides to get their degree in, earning a master's degree in cyber security can only help you serve one of the many fronts in the mounting digital war. A master's degree is designed to specifically match the on-the-job skills required by government agencies and the foremost private security companies in the country. A master's degree in cyber security can further distinguish you from the competition when choosing the career path of choice– not to mention is desired by most government agencies and the foremost private security companies in the country.

The following section goes into more detail of some of the most prominent Cybersecurity career paths and job titles that are currently available in the field, including certifications.

CAREER PATH

As you recall from Figure 1, there are five career paths a Cybersecurity student can choose to follow. Although, many experienced professionals change paths once or twice in their lifetimes, by no means once a path is chosen, other paths cannot be taken.

The paths are application development, network engineering, network management, security engineering, and audit/risk management. In addition to each career path there are numerous disciplines under each that one can focus on and find their passion and many areas of expertise to get certified. I will list the most popular certifications and areas of expertise, but know there are many more that I do not list. Over the course of a career some professionals have become multi-disciplined and have worked across several of the fields and disciplines. The point I want to get across is that having experience in multiple disciplines gives you a better understanding of Cybersecurity and in doing so a better understanding of why properly implemented Cybersecurity is crucial for an organization today to survive in the dynamic threat environment we currently face. (Hayslip, 2015)

Application Development

The first career path is application development and there are three disciplines to follow with each having numerous certifications that one would choose to show expertise. Although I won't get into detail in this article on the requirements of each certification, some certifications require experience while others do not.

Cybersecurity students who major in Software Engineering, or Software Applications and Programming or Software Development follow this career path. Their job titles usually include in the title, engineer, developer, or programmer such as software engineer, systems programmer, or web application developer.

The three disciplines that Cybersecurity students can elect to follow are Mobile Application Development, Computer Programming, or General Application/Programming. In the Mobile Application Development discipline, the main areas of expertise include Microsoft, Oracle, and Android. The second discipline is computer programming. In the computer programming discipline the areas of expertise include C++, Adobe, Microsoft, and Google. The last area of discipline is General Application/Programming. In General Application /Programming. The Certified Secure Software Licensed Professional (CSSLP) and CompTIA Mobility + are the 2 most popular certifications to obtain. While the Mobility + certification does not require any experience to obtain, the CSSLP does require 5 years of relative experience.

Network Management

The second career path is network management and there are two disciplines to follow, again with many certifications that one would choose to show expertise.
Although there is many majors Cybersecurity students can follow for the network management career path, some of the most common degrees are in Program Management, Information Systems Management, or Technology Management and their job titles are usually Project Managers.

The two disciplines that Cybersecurity students follow are Project Management and Information Technology Infrastructure Library (ITIL). In the Project Management discipline, the main areas of expertise include Global Information Assurance Certification (GIAC) Certified Project Manager, Certified Scrum Master, or Project Management Associate or Professional. The second discipline is ITIL. ITIL expertise progresses through five levels starting with Foundation and ending with Master.

Network Engineering

The third career path is network engineering and there are many disciplines to follow, again with many certifications that one would choose to show expertise. Except for the cloud discipline, network engineering is vendor specific and all paths focus on a specific platform.

Although there are many majors Cybersecurity students can follow for the network engineering career path, the most common degrees are in Computer Engineering and Computer Science. Their job titles are usually Network Engineers or Network Analysts.

Network Engineer career path is divided into 6 different disciplines, each focused on a specific vendor platform and 1 new emerging discipline that is not vendor specific. The vendor specific platforms include Microsoft, Cisco, Oracle, Linux, Juniper, and Red Hat. The Cloud discipline is not vendor specific but rather made up of different vendors. The cloud path is its own discipline since the expertise is unique not just for the vendor and the expertise is highly desired. CompTIA Network+ does not fall into any specific category but is a very popular entry-level certification that has become very popular in the Network Engineer career path and can be obtained no matter which discipline is chosen.

Security Engineering

The fourth career path is security engineering and there are four disciplines to follow. Security engineering is one of the most popular career paths to follow for cybersecurity students who major in Information Systems, Information Technology, or Cybersecurity. Although there are many different job functions and titles in this career path some of the most common titles include information security analyst, penetration tester, or intrusion detection specialist.

Security Engineer career path has four different disciplines each focused on information security. Information Security, or InfoSec as it is commonly known as, is probably the most popular discipline since the expertise in this discipline has some of the most popular certifications including the Certified Information Systems Security Professional (CISSP), Certified Information Systems Manager (CISM), and CompTIA Security +.

The other three disciplines, although not as popular as InfoSec, are all unique expertise that undergraduate Cybersecurity students can specialize in. They include Application Hacking, Penetration Testing, and Industrial Control Systems (ICS) Supervisory Control and Data Acquisition (SCADA). ICS are command and control networks and systems designed to support industrial processes and SCADA is the largest group.

Audit/Risk Management

The fifth and final career path is audit/risk management and there are 6 disciplines in this career path. Although there is not one degree that Audit/Risk Management Cybersecurity students choose to major in, you will find some four year schools offer a Systems and network Auditor degree but usually these students usually major in one of the degrees mentioned in the previous four career paths or even sometime a non-Cybersecurity degree. Whatever the degree may be most jobs usually include such titles as Security IT Auditor, Consultant, Computer Forensics Analyst, Disaster Recovery Analysts, or Cryptographer.

Audit/Risk Management career path has 6 different disciplines. Audit/Risk General is the discipline most choose first when going down this career path since the expertise in this discipline has some of the most popular certifications including the Certified Information Systems Auditor (CISA) and Certified in Risk and Information Systems Control (CRISC). However, most will then use this expertise and acquire more specific expertise in one of the other five disciplines.

Forensics discipline is for those who want to acquire expertise in fraud and investigations while the privacy discipline is focused more protecting data and the risks associated with it. As for the Business/Disaster Recovery discipline, these individuals are experts in how to plan for continuing operations in a disaster and how continue business in the wake of a disaster. The least popular discipline in Audit/Risk Management, however, the expertise is still highly desirable, is Physical Security. Physical security experts focus on the protection of assets - people, property, and/or information. The final career path is one that although is defined as Audit/Risk Specialties, actually is four distinct areas of expertise. They include Health IT, Audit, Risk, and Payment Card Industry (PCI).

CONCLUSIONS

My advice to young folks wanting to choose a career path in Cybersecurity is to choose a career path that you will enjoy and love. When you do, gaining the experience is ever so valuable along with the necessary certifications that show your expertise. However, that does not mean you are stuck in that career path the rest of your life. As I mentioned earlier, many Cybersecurity professionals are multi-disciplined and have had jobs in multiple career paths just discussed. A career in cybersecurity means you're capable of everything a traditional IT person is capable of, and more. So as you start in Cybersecurity, you will get some experience and certifications, oh yeah and some good money, and you can grow from that into a well-established career in Cybersecurity.

Then, as you develop specialized interests and expertise, you can become and expert in the field and move up the career chain and make more money. One thing you can do that I have do everyday and is completely free, read. There are a ton of good online sites that you can read to follow what's happening. Keeping up on the business will give you strong insights into where to go. Read avidly on the topic (news as well as tech stuff). Make yourself knowledgeable, read daily if you can. The more you know, the better you will be in your career. That's good advice for pretty much anything, but it works here, too. Don't just read technical information, but dive deeply into each individual case and learn about the business ramifications and how the actual breaches and attacks unfolded.

Keep in mind that many organizations want you. There is a huge shortfall in trained cybersecurity professionals. Always be networking and socializing because you never know whom you will meet for your next opportunity.

One thing I would suggest, which I just started doing recently is getting your hands on old, discarded machines and get familiar with the hardware and how to break it down and build it back up again. I have learned much more doing hands-on work and have actually made me better in my career. A word of advice, never hack or crack. Stay away from the criminal and unethical stuff. Even though there is expertise in this area, it should only be done professionally

There's a tremendous amount of opportunity out there, but you're going to have to work hard to get into this career (Gerwitz, 2015).

REFERENCES

Bison, D. (2014). *Cyber security careers: What you need to know to advance in the security field.* Tripwire.com. Retrieved June 29, 2016 from http://www.tripwire.com/state-of-security/security-awareness/cyber-security-careers-what-you-need-to-know-to-advance-in-the-security-field/

Gerwitz, D. (2015). *Getting started with a career in cybersecurity.* ZDNet.com. Retrieved June 29, 2016 from http://www.zdnet.com/article/getting-started-with-a-career-in-cybersecurity/

Hayslip, G. (2015). *Path to a career in cyber*. Securitycurrent.com. Retrieved June 29, 2016 from http://www.securitycurrent.com/en/writers/gary-hayslip/path-to-a-career-in-cyber

National Initiative for Cybersecurity Careers and Studies (NICCS). (2015). *Cybersecurity careers: Explore a career in cybersecurity.* Retrieved June 28, 2016 from https://niccs.us-cert.gov/careers/cybersecurity-careers

New Updated List of IT Certifications accessed March 21, 2016 from http://itcertificationmaster.com/updated-list-certifications-2304-160-companies/

Stewart, J. (2013). Planning a Career Path in Cybersecurity. Retrieved, June 28, 2016 from https://dockoc.com/kadahsh-k-kadahsh/wp-cs-cybersecurity-jobs-24fotq.html