https://doi.org/10.48009/4_iis_2020_275-284

Issues in Information Systems
Volume 21, Issue 4, pp. 275-284, 2020

CYBERSECURITY ENGINEERING: THE GROWING NEED

Jennifer Callen, PNC Bank, jennifer.callen@pnc.com
Jason E. James, Indiana State University, jason.james@indstate.edu

ABSTRACT

Cybersecurity job openings continue to grow rapidly and is why the need for cybersecurity jobs has arisen so quickly. With 3.5 million cybersecurity jobs expected to open by 2021, employers will continue to seek out prospective job candidates from technical schools and undergraduate programs to fill them. This may satisfy the immediate need well enough, but it does not address the demand for cybersecurity professionals with advanced degrees such as Cybersecurity Risk Management and Cybersecurity Engineering, which is becoming even more acute. This journal article provides and in depth look at what Cybersecurity Engineers do, why more are needed, and how universities are creating programs to tackle the need.

Keywords: cybersecurity engineering, education, penetration testing, masters

INTRODUCTION

The year 2018 saw its share of cybersecurity breaches with major breaches suffered by global entities such as Facebook (87 million records breached) and Aadhaar (more than 1.1 billion records breached). The sheer magnitude of these information security breaches equates not only with bigger losses and more media coverage but also with more jobs and opportunities for IT and programming professionals (Lindros & Tittel, 2018)

Cyber startups and legacy technology companies know exactly how to attract top undergraduates: a six-figure salary, a signing bonus, even a new car. With these luxuries in reach, choosing to forgo the job offer in pursuit of advanced higher education seems irrational for most new grads. However, this is exactly what's being asked of them by the cybersecurity industry — an industry with zero unemployment and a severe skills shortage in both private sector employment and higher education (Sherrer, 2018).

What is a security engineer? A security engineer is a specialized type of engineer. Also known as: Network Security Engineer, IT Security Engineer, Information Security Engineer, Cybersecurity Engineer, Information Systems Security Engineer (ISSE), Systems Security Engineer (What does a security engineer do, n.d.). These days, many people are asking themselves whether they should become cyber security engineers. Well, as cyber jobs increase exponentially and thousands of cyber positions remain open, it's a good time to ask this question (Silvertree. 2018).

It's no surprise that faulty software often leaves networks vulnerable to malware, spyware, adware, phishing and more. A cybersecurity engineer analyzes computer networks, ensures they're running securely, and tries to foresee possible security issues that may arise in the future. In short, cybersecurity engineering focuses on designing computer systems equipped to deal with disruptions like natural disasters and/or malicious cyber-attacks (Silvertree. 2018).

WHY A CYBERSECURITY ENGINEER

Demand in the cyber security job market is soaring while supply is running critically low. According to Cisco, there are currently 1 million unfilled cyber security jobs worldwide. In the U.S. alone, job postings are up 74% over the past five years with 209,000 current job vacancies, as reported by Forbes. Quite simply, there aren't enough qualified and skilled cyber security professionals to fill the growing need. And among the most sought after in the field are cybersecurity engineers. As the Wall Street Journal reported, "The demand is making it harder for chief information security officers to attract and retain seasoned cybersecurity engineers who can detect and neutralize threats."

As a consequence of the strong demand for cybersecurity engineers and the deficit in qualified professionals, much of academia have been creating programs and launching cybersecurity engineering degrees since salaries, job outlook

and job opportunities are great. So, if you have an engineering background and are interested in this burgeoning field, a job as a cybersecurity engineer can be an enticing and lucrative career move (Should you become a cybersecurity engineer, n.d.).

Job opportunities in the cyber security engineering field are plentiful, with unemployment in the field hovering around zero. As CSO reported, just over half (51.3%) of security executives and managers surveyed in Computerworld's 2016 IT Salary Survey said they expect IT staff headcounts to increase in the coming year. Many companies are creating Director if Information Security positions and expanding their security team focusing on technical roles such as cybersecurity architects, cybersecurity engineers and cybersecurity analysts (Should you become a cybersecurity engineer, n.d.). A 2015 Burning Glass jobs report supports this sentiment, finding that engineering job postings accounted for 26% of all the cyber security job listings in 2014, more than any other cyber security position.

The growth of IT and rapid advancement of cybersecurity has resulted in the demand for workers with specialized skills and has placed a considerable demand on the traditional educational system to provide a qualified and sustainable cybersecurity workforce (Randle & Zirkle, 2005). The lack of skilled and qualified cybersecurity professionals has always been an issue in the cybersecurity industry. The rapid pace at which technology continues to evolve, creates a need for highly skilled individuals to enable, apply, support, configure, and adapt cybersecurity products and services (Randle & Zirkle, 2005). James, 2017 stated "Cybersecurity profession is a complex world with many different career paths" (see Figure 1). Cybersecurity Engineering is one of those career paths and with many higher education's institutions now offering a degree, students can pursue both a Bachelor of Science (BS) and Master of Science (MS) in Cybersecurity Engineering.

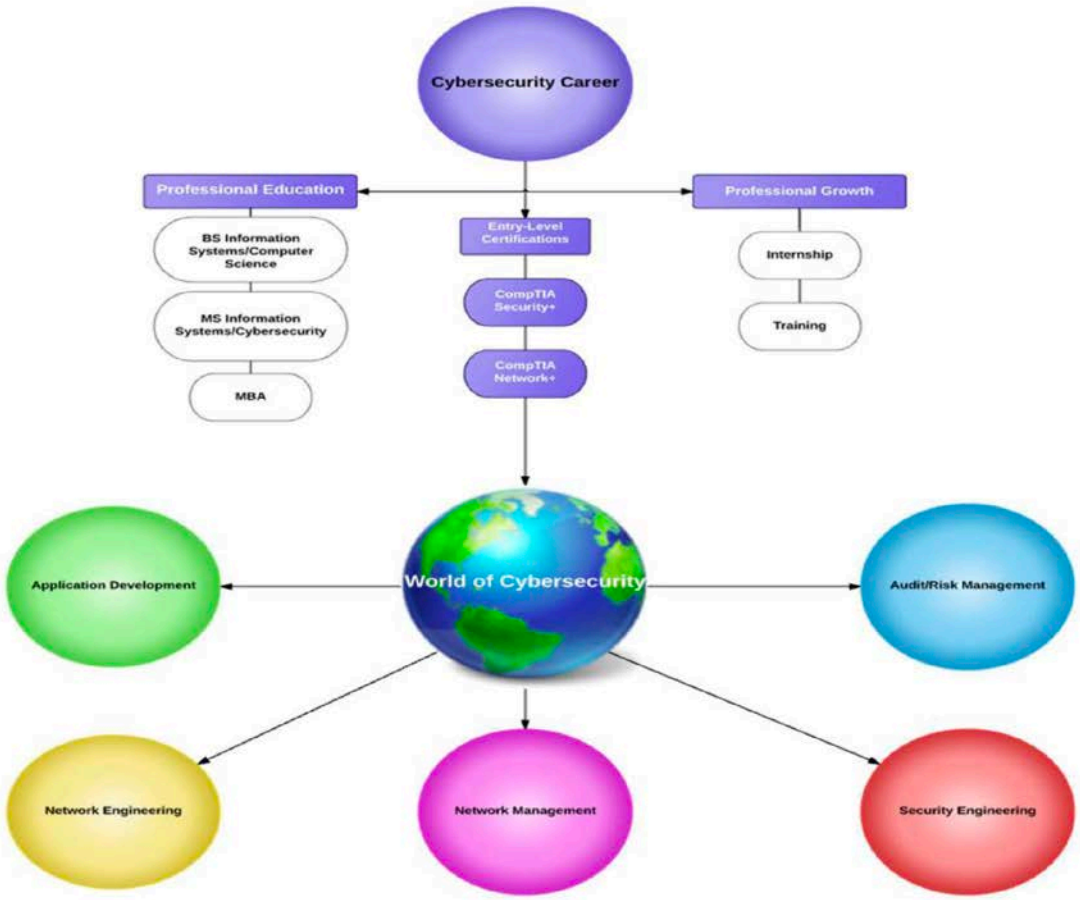

Figure 1. The World of Cybersecurity

Cybersecurity graduates compete in a global market fueled by rapid innovation and constant technological advances. In order to be able to contribute to and advance in this highly demanding and lucrative career, cybersecurity students not only require advanced scientific and technological knowledge but they also need the knowledge, skills, and abilities needed in the career. These competencies can be found and enhanced through a cybersecurity education as well as co-curricular activities, such as cybersecurity training, competitions, journal publications, webinars, seminars, and of course, certifications (Starr & Minchella, 2016).

WHAT CYBERSECURITY ENGINEERS DO

Cybersecurity engineers are responsible for testing and screening security software and for monitoring networks and systems for security breaches or intrusions. They can often resolve possible causes of security threats early on by looking at things from a security perspective and recommending enhancements to management (What does a security engineer do, n.d.).

Cyber security engineers perform assessments and penetration testing; provide development and implementation of secure network solutions by architecting and engineering trusted systems into secure systems and manage audit/intrusion and security technology systems (Should you become a cybersecurity engineer, n.d.).

As the company's first line of defense against unauthorized access from outside sources and potential security threats, security engineers have a very important job to do. Not only do they know how to pinpoint any potential threats, they also know how to plan and prepare before any security threats take place. They act as an all-in-one security team by implementing and testing strategies, reporting on any incidents for future preparation, keeping track of the status of network security, and educating other employees to raise security awareness (What does a security engineer do, n.d.).

Cyber security engineers must be able to troubleshoot, identify unauthorized access, and offer solutions regarding an organization's systems and networks related to cyber security. In this position, you'll perform very detailed work at the forefront of information protection efforts for the organization. It is your training, skills, experience, and education that stand between the organization for which you work and threats and breaches, like unauthorized access to data and information or intrusion into your organization's systems (Silvertree, 2018)

Cybersecurity engineers work with a variety of people across multiple departments in order to create and maintain the integrity of a computer network. The work of a cybersecurity engineer includes monitoring various networks to determine potential security risks, as well as designing and implementing processes that allow for the information stored on the network to be accessed by the appropriate staff members as efficiently as possible.

The basic role of a cybersecurity engineer is to ensure that an information system allows certain staff members access while preventing access by non-authorized users. By creating an efficient way for staff members to access vital information, a systems security engineer can assist companies in increasing productivity. Cybersecurity engineers also help companies operate more effectively by limiting the access to certain data to only the staff members who can best use and implement it for the benefit of the company (What does a systems ecurity engineer do, n.d.).

WHAT MUST CYBERSECURITY ENGINEERS KNOW

A systems security engineer must have a thorough understanding of the latest security principles, techniques, and protocols. Cybersecurity engineers must be diligent in their daily tasks as they will be responsible for installing, configuring, analyzing, and monitoring information networks daily. The global nature of many companies requires that a cybersecurity engineer be on-call as network security can often be a 24-hour job and issues may present themselves during inopportune times (Silvertree, 2018)].

Cybersecurity engineers' primary mission is to protect the computer systems and networks of an organization from threats and attacks (if you can picture yourself wearing a cape, that's probably a good thing). To consistently achieve this mission, there are many tasks and duties cybersecurity engineers must perform. Here are their most common functions:

- An understanding of cybersecurity methodologies
- Developing security practices and standards
- Creating new, more efficient, ways to resolve current security issues
- Making recommendations to management regarding security enhancements and improvements
- Performing penetration testing
- Proficiency in Java, Python Net, C++, bash, Powershell, Kali Linux or Ubuntu just to name a few
- Monitoring systems and networks for intrusions or security breaches
- Conducting network scans to identify weaknesses or vulnerabilities
- Installing software, including data encryption programs and firewalls
- Installing or processing of security products and procedures
- Installing appropriate software to improve notifications of intrusions
- Developing automation scripts to manage and track incidents
- Monitoring systems to identify irregular behavior
- Leading incident response efforts
- Leading investigations into breaches
- Supervising and providing feedback for changes in hardware, software, and user needs
- Reporting findings and feedback to management
- Planning and implementing information security strategies for an organization
- Training or educating network users on information security
- Recommending improvements in technical, legal, and regulatory areas as they pertain to information security
- Knowledge of current cybersecurity trends, as well as the interest in continued research of emerging trends and hacking techniques
- The ability to work well with others, including collaboration and communication with other departments
- The ability to thrive in fast-paced environments and work under pressure
- Strong attention to detail and problem-solving skills (Silvertree, 2018).

LIFE OF A CYBERSECURITY ENGINEER

A day in the life of a cybersecurity engineer likely starts with a large pot of coffee. After that, as with other information security jobs, work as a cyber security engineer is hardly routine. While there are some aspects of the job that are handled or performed daily, you'll never really know what your day will entail until it happens. Cybersecurity engineers typically work in fast-paced, complex environments and are frequently required to work odd hours and even overtime and weekends. It's important to note that this can be stressful for people who don't thrive in these kinds of environments.

A threat or attack will always take precedence over daily activities, but when your organization is not under attack, you'll probably be:

- Ensuring that appropriate security controls are consistently in place to protect the organization's digital files and infrastructure
- Planning, implementing, managing, monitoring, and upgrading security measures for the protection of systems, networks, and data
- Undertaking various administrative tasks, reporting, and communication with other departments
- Performing penetration testing to identify system and network vulnerabilities

Day-to-day tasks and activities can vary for cyber security engineers, depending on where they work and the types of systems and networks, they're responsible for protecting. So, there you have it: a quick snapshot of the world of a cyber security engineer. It's a vast an interesting place that just might be the right spot for you (Silvertree, 2018)

CYBERSECURITY ENGINEERING EDUCATION

One reason for the worker shortage in the cyber security field is that companies are looking for highly qualified, educated and skilled professionals. Hiring managers and recruiters typically seek candidates where a bachelor's

degree, is almost always required, while a master's degree is typically preferred. In addition, many companies require specific certifications and extensive experience in the field (Should you become a cybersecurity engineer, n.d.).

Most of cybersecurity engineering positions are not entry-level and require at least 3 to 5 years of information technology experience. Those who choose to become a cybersecurity engineer typically come from a computer science or electrical engineering background. Although having a bachelor's degree in a technical field is a basic requirement for this position, many cybersecurity engineers obtain advanced degrees and certifications related to network systems security to remain competitive in the marketplace (What does a systems security engineer do, n.d.). In addition, many want at least three years of experience in identifying threats and developing effective protection countermeasures

According to the U.S. Department of Labor's Bureau of Labor Statistics, the median pay in 2018 for a cybersecurity analyst is likely to reach well over $100,000. Therefore, to encourage students to pursue the next level of education, academia must demonstrate that there is a clear path to better opportunities in terms of professional career advancement, including compensation, when entering the workforce with an advanced degree.

Despite — or because of — this challenge, universities must take a step back and listen to what industry needs before developing their cybersecurity master's and PhD programs. By focusing on the skills and experience cybersecurity departments are lacking, universities can develop curricula that prepare graduates to meet an employer's exact needs.

In order to create a new foundation for these programs, administrators and faculty must provide the educational environment to foster interest from undergraduate students earlier in their course of study, find creative ways to recruit faculty with expertise in cybersecurity, improve cybersecurity laboratory capabilities, and establish talent pipelines to corporate and government organizations that offer positions for high-quality cybersecurity talent (Sherrer, 2018).

Finding Faculty

Highly qualified cybersecurity faculty are sought after as much as — if not more than — industry professionals. To hire and foster new cybersecurity faculty, institutions need to offer meaningful cybersecurity research opportunities that enable them to test new theories and solve real-world problems, all while building the PhD pipeline. Another draw for faculty is a student body truly interested in their field of study, in this case cybersecurity engineering.

In order to drive this interest, cybersecurity must be "baked in" at the undergraduate engineering level, particularly in programs that deal directly with coursework like computer science. Offering immediate exposure to introductory cybersecurity courses at the undergraduate level – as opposed to one or two courses as part of computer science major requirements – will help engage students earlier. This exposure will incite interest in pursuing the opportunities of advanced graduate degrees and careers in cybersecurity engineering. Key throughout the educational experience is that students develop and hone "real-world" cybersecurity engineering skills (Sherrer, 2018).

Focusing the coursework

Whether students are mathematicians, computer scientists, computer engineers, or electrical engineers, masters and PhD programs in cybersecurity must provide both theoretical and hands-on engineering expertise to solve the complex cybersecurity problems affecting all public and private enterprises.

With regard to program content, many cybersecurity master's programs blend the managerial with the technical. Given the demand — and the need — for highly skilled cybersecurity experts, it's time to transition away from this approach and elevate cybersecurity to a standalone engineering discipline.

Master's and PhD candidates in cybersecurity engineering must cultivate the acumen to design, engineer, and assess the software, hardware, applications, and technology that comprise our information and communications infrastructures (Sherrer, 2018).

Equipping laboratories

These infrastructures have impacted every industry through advances in computing. Cybersecurity can no longer be an afterthought in technology design and development. For example, the "WannaCry" ransomware that hit global organizations, affecting hundreds of thousands of businesses, universities, and even hospitals, exploited a known vulnerability in computer systems. Programmers were aware of the potential trouble months prior to the attack, but playing catch-up to remedy the problem is more challenging that understanding how to cyber-harden technology from the beginning and provide ongoing security protections throughout its lifespan.

This is why universities must develop cybersecurity laboratories and ranges that mimic real-world environments. In laboratories, students can evaluate cyberattack vectors, assess cyber defense methods, and design and develop new methods, protocols, and techniques. These environments also enable faculty and students to secure funding from private and public organizations to advance research. Compared to other fields, cybersecurity research in academia is nearly non-existent. Without the laboratory capabilities and program infrastructure to ensure we progress the field forward, we will continue to react to cyberattacks and pay the price (Sherrer, 2018).

Partnering with industry

Leading cybersecurity executives claim it takes multiple years to effectively train a new hire to become proficient in the range of skills required of a cybersecurity engineer. In order to reduce the large amount of time and resources that takes, industry should help shoulder the burden with universities to develop and improve cybersecurity engineering degree programs.

Similarly, universities must listen to their clients and create courses that align with the needs of corporate and government clients. By building cybersecurity masters and PhD programs with the client in mind, while also considering the growing academic body of knowledge, academia can expand the pipeline of skilled cybersecurity engineers. While master's candidates will enter professional roles ready to perform on day one, those students who become PhD candidates will advance the state of the art in cybersecurity research while also building a cadre of much-needed academicians in the field (Sherrer, 2018).

Accreditation

Accreditation is a major factor in students applying and choosing the right school to further their education. In order to respond to increasing demand for skilled professionals, there is rapid, but unfocused, expansion in cybersecurity educational programs – without broad, universal expectations for graduates. Broad skills based on the entire cyber domain are needed, and those skills need to be taught in the context of a well-understood disciplinary foundation. Over the past decade, several universities have stepped up to deliver undergraduate programs in cybersecurity, but the growth in such programs has been slow due to little consensus on program name, objectives and scope.

Building on prior work by the NSA/DHS Centers of Academic Excellence, the NICE Cybersecurity Workforce Framework and the Cyber Education Project initiative, ABET has released proposed accreditation criteria for cybersecurity engineering programs. The program criteria for cybersecurity engineering will complement existing ABET Engineering Accreditation Commission (EAC) criteria for engineering programs and focus on fundamental knowledge and principles of cybersecurity cast into engineering discipline.

The approved cybersecurity engineering program criteria applies to engineering programs that include "security", "cybersecurity", "computer security", "cyber operations", "information assurance", "information security", or similar modifiers in their titles (ABET, 2017).

With ABET, or any accreditation, the structure of the curriculum must provide both breadth and depth across the range of cybersecurity engineering topics implied by the title of the program. The curriculum must include:

1. probability, statistics, and cryptographic topics including applications appropriate to the program.
2. discrete math and specialized math appropriate to the program, such as, abstract algebra, information theory, number theory, complexity theory, finite fields.

3. Cybersecurity engineering topics necessary to analyze and design complex devices, software, and systems containing hardware, software and human components.

The cybersecurity engineering provide must provide both breadth and depth across the range of engineering and computer science topics necessary for the:

- application of security principles and practices to the design, implementation, and operations of the physical, software, and human components of the system as appropriate to the program
- application of protective technologies and forensic techniques
- analyzing and evaluation of components and systems with respect to security and to maintaining operations in the presence of risks and threats
- consideration of legal, regulatory, privacy, ethics, and human behavior topics as appropriate to the program (ABET, 2017).

Cybersecurity engineering programs must demonstrate that faculty members teaching core engineering topics understand methods of engineering design, engineering problem solving, and engineering practice with specific relevance to security. These program criteria provide a foundation for lifelong learning in a dynamic field. They provide a uniform set of sound principles to help students, employers and programs (ABET, 2017).

Regardless of whether graduate students ultimately choose industry or academia, one thing is clear: Cybersecurity engineers who pursue higher levels of education will make a direct and positive impact on our collective digital security anywhere they may land (Sherrer, 2018).

Schools Offering MS in Cybersecurity Engineering

Some of the schools in the U.S. that offer a Master of Science in Cybersecurity Engineering include the following:

- University of Maryland Institute for Advanced Computer Studies in College Park, MD
- Embry-Riddle Aeronautical University in Daytona Beach, FL
- University of Southern California Viterbi in Los Angeles, CA
- University of Washington Bothell in Bothell, WA
- University of Maryland Eastern Shore in Princess Anne, MD [Online Only]
- University of San Diego in San Diego, CA [Online Only]
- Colorado Technical University in Colorado Springs, Colorado
- Washington University in St. Louis, MO
- Illinois Institute of Technology in Chicago, IL

Since the global shortage of cybersecurity professionals is expected to reach 3.5 million unfilled positions by 2021, up from 1 million in 2014, many universities are responding to the labor crunch with diverse programs focused on cybercrime, cybersecurity, and related coursework and even a select few have started masters in cybersecurity engineering degrees and this number will only continue to grow in the coming years. What first started as universities creating information assurance and security programs and then cybersecurity programs, now are specializing in more unique degrees such as cybersecurity engineering, cybersecurity risk management and even cybersecurity management and policy.

CERTIFICATIONS

Professional certifications are another way cybersecurity engineer can enhance their knowledge and expertise. Industry vendors or professional organizations typically offer certifications. Most require professionals to pass a test, though candidates should be mindful of pre-exam requirements such as a minimum number of years of professional experience. When evaluating prospective cybersecurity engineering candidates, employers frequently look to certification as an important measure of excellence and commitment to quality. The most popular professional certifications and the organizations that sponsor them include, but are not limited to, the following:

Certified Ethical Hacker (CEH) – International Council of E-commerce Consultants (EC-Council)

Hackers are innovators and constantly find new ways to attack information systems and exploit system vulnerabilities. Savvy businesses proactively protect their information systems by engaging the services and expertise of IT professionals skilled in beating hackers at their own game (often called "white hat hackers" or simply "white hats"). Such professionals use the very skills and techniques hackers themselves use to identify system vulnerabilities and access points for penetration to prevent hackers' unwanted access to network and information systems (Lindros and Tittel, 2018).

The Certified Ethical Hacker (CEH) is an intermediate-level credential offered by the International Council of E-Commerce Consultants (EC-Council). It's a must-have for IT professionals pursuing careers in cybersecurity engineering and ethical hacking. CEH credential holders possess skills and knowledge on hacking practices in areas such as foot printing and reconnaissance, scanning networks, enumeration, system hacking, Trojans, worms and viruses, sniffers, denial-of-service attacks, social engineering, session hijacking, hacking web servers, wireless networks and web applications, SQL injection, cryptography, penetration testing, evading IDS, firewalls, and honeypots (Lindros and Tittel, 2018).

CompTIA Security +

CompTIA's Security+ is a well-respected, vendor-neutral security certification. Security+ credential holders are recognized as possessing superior technical skills, broad knowledge and expertise in multiple security-related disciplines.

While Security+ is an entry-level certification, successful candidates should possess at least two years of experience working in network security and should consider first obtaining the Network+ certification. IT pros who obtain this certification possess expertise in areas such as threat management, cryptography, identity management, security systems, security risk identification and mitigation, network access control, and security infrastructure (Lindros and Tittel, 2018).

Certified Information Systems Security Professional (CISSP) - International Information System Security Certification Consortium, or (ISC)²

The Certified Information Systems Security Professional (CISSP) The Certified Information Systems Security Professional (CISSP) is an advanced-level certification for IT pros serious about careers in information security. Offered by the International Information Systems Security Certification Consortium, known as (ISC)2 (pronounced "ISC squared"), this vendor-neutral credential is recognized worldwide for its standards of excellence.

CISSP credential holders are decision-makers who possess expert knowledge and technical skills necessary to develop, guide and then manage security standards, policies and procedures within their organizations. The CISSP continues to be highly sought after by IT professionals and is well recognized by IT organizations. It is a regular fixture on most-wanted and must-have security certification surveys (Lindros and Tittel, 2018).

Cisco Certified Network Professional Security (CCNP Security)

According to Cisco’s website, Cisco Certified Network Professional Security (CCNP Security) certification program is aligned specifically to the job role of the Cisco Network Security Engineer responsible for Security in Routers, Switches, Networking devices and appliances, as well as choosing, deploying, supporting and troubleshooting Firewalls, VPNS, and IDS/IPS solutions for their networking environments.

CCNP Security certification focuses on the daily job tasks of experienced cybersecurity engineers. Achieving CCNP Security certification confirms that you have the knowledge and skills needed to test, deploy, configure, maintain, and troubleshoot the Cisco network security appliances and the Cisco IOS Software devices that comprise a network's security.

CCNP Security professionals provide and maintain security for Cisco router and switch-based networks, develop perimeter solutions, deploy security solutions, provide operation support for Cisco network systems, and plan for and mitigate network security risk.

PENETRATION TESTING

One of the main job duties and requirements of a cybersecurity engineer is performing penetration testing. This is a unique skill where many penetration testers don't hold a specialized degree. Since ethical hacking is more about skills than course credits, a bachelor or master's degree in is unnecessary if you have appropriate job experience, until now. Hence, comes a cybersecurity engineering degree. Employers are looking for 2-4 years of security-related experience with practice in penetration testing and vulnerability assessments. Cybersecurity engineering students are getting experience now with the tool's penetration testing utilize (What does a penetration tester do, n.d.).

Cybersecurity engineers use penetration testing to improve the security of organizations by using penetration tools to locate and exploit security vulnerabilities. Most commonly associated with "hacking", cybersecurity engineers use penetration testing to ethically break into a company with the goal of exposing key issues in computer systems or software and therefore improve the security of an organization (Become a penetration tester, n.d.).

Penetration testers conduct security audits, develop code, automate processes, reverse engineer binaries – the list goes on. Cybersecurity engineers who do penetration testing have specific technical skills such as:

- Windows, UNIX and Linux operating systems
- C, C++, C#, Java, ASM, PHP, PERL
- Network servers and networking tools including Kali Linux (e.g. Nessus, nmap, Burp, etc.)
- Computer hardware and software systems
- Web-based applications
- Security frameworks (e.g. ISO 27001/27002, NIST, HIPPA, SOX, etc.)
- Security tools and products (Fortify, AppScan, etc.)
- Vulnerability analysis and reverse engineering
- Metasploit framework
- Forensics tools
- Cryptography principles (What does a penetration tester do, n.d.).

When a cybersecurity engineer performs penetration testing, they usually travel between different sites and work evenings or weekends to not disrupt the work flow of the company, or they may be able to perform some duties remotely or by telecommuting. But, the heart of the cybersecurity engineer when performing penetration testing is identifying security system vulnerabilities by attempting to exploit them and then coming up with solutions to resolve the weaknesses to keep their organization's information safe.

In order to perform penetration testing, a cybersecurity engineer usually follows a specific process including:

- Planning a specific penetration test
- Creating or selecting the appropriate testing tools
- Performing the penetration test on networks, applications, or systems
- Documenting methodologies
- Identifying vulnerabilities using the data gathered
- Reviewing and evaluating findings
- Establishing possible solutions for the weaknesses
- Provide feedback and recommendations to management or clients (Become a penetration tester, n.d.).

CONCLUSION

In conclusion, cybersecurity engineers are the professionals where their primary skill set is utilized to protect computer and networking systems from potential hackers and cybercrimes. With the increased use of technology within the businesses it has become vital for the businesses to protect their data from the potential threats. So, a growing demand

has been seen in last few years for cybersecurity engineers. As they do with other programs, higher education institutions and companies need to work together to attract students to this lucrative career and all the perks that comes with it, such as guaranteed internships and scholarships for those that choose the degree.

As you have read, the career path to become a successful cybersecurity engineer is not that easy. It takes a lot of effort and also a commitment from the individual to get proper education, the right certifications, and understand the theoretical concepts of hacking and what is ethical hacking. After all, saving millions and millions worth of money and trust of an organization is going to be in your hands. So be wise and make sure you put your hearts into it (How to become a cybersecurity engineer, n.d.)

REFERENCES

ABET. (2017). ABET Seeks Feedback On Proposed Accreditation Criteria For Cybersecurity Engineering Academic Programs. [Online]. Available: https://www.abet.org/abet-seeks-feedback-on-proposed-accreditation-criteria-for-cybersecurity-engineering-academic-programs/

Author unknown. (n.d.). Become a penetration tester. [Online]. Available: https://www.cybrary.it/become-penetration-tester/

Author unknown. (2017). How to Become a Cyber Security Engineer. [Online]. Available: https://mindmajix.com/how-to-become-a-cyber-security-engineer

Author unknown. (n.d.). Should You Become a Cyber Security Engineer? [Online] Available: https://onlinedegrees.sandiego.edu/case-career-cyber-security-engineer/

Author unknown. (n.d.). What does a penetration tester do. [Online]. Available: https://www.cyberdegrees.org/jobs/penetration-tester/

Author unknown. (n.d.). What does a security engineer do? [Online]. Available: https://www.sokanu.com/careers/security-engineer/#what-does-a-security-engineer-do

Authour unknown. (n.d.). What Does a Systems Security Engineer Do? [Online]. Available: http://www.wisegeek.net/what-does-a-systems-security-engineer-do.htm

James, J. (2017). The Cybersecurity student career path: Which one is right for me? Issues in Information Systems, Vol. 18, Issue 3, pp. 141-148 [Online]. Available: *http://www.iacis.org/iis/2017/3_iis_2017_141-148.pdf*

Lindros, K., and Tittel, E. (2018). Best Information Security Certifications 2019. [Online]. Available: https://www.businessnewsdaily.com/10708-information-security-certifications.html#CEH

Randall, M. H., & Zirkle, C. J. (2005). Information technology student-based certification in formal education settings: Who benefits and what are needed. *Journal of Information Technology Education*, 4, 287-306 [Online]. Available: https://reddog.rmu.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=ehh&AN=19763457&site=eds-live&scope=site

Sherrer, J.. (2018). Cybersecurity engineering: A new academic discipline. [Online]. Available: https://venturebeat.com/2018/04/15/cybersecurity-engineering-a-new-academic-discipline/

Silvertree. G. (2018). Should You Become a Cyber Security Engineer? [Online]. Available: https://www.cybrary.it/2018/08/become-cyber-security-engineer/

Starr, L., & Minchella, D. (2016). Learning beyond the science classroom: A roadmap to success. *Journal of STEM Education: Innovations and Research*, 17(1), 52-57 [Online]. Available: https://reddog.rmu.edu/login?url=http://reddog.rmu.edu:2077/docview/1785759031?accountid=28365