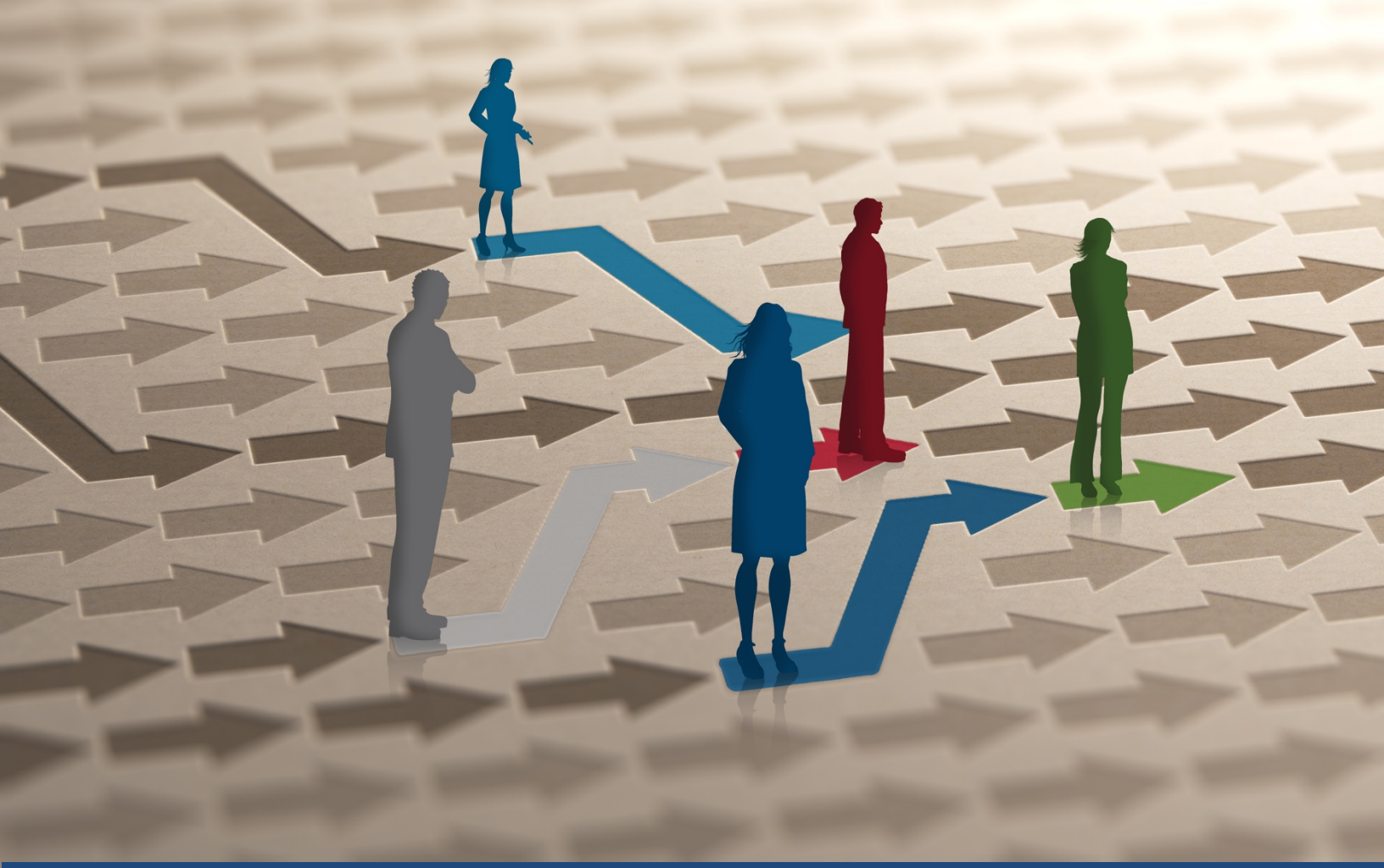

Cybersecurity Career Paths and Progression

February 2019

CISA
CYBER+INFRASTRUCTURE

Cybersecurity Career Paths and Progression

Table of Contents

I. Introduction

Pursuing a career in cybersecurity is not as straightforward as other more traditional professions. Doctors and lawyers serve as great examples. In most countries, including the United States, an advanced academic degree is required for each, along with an occupational license. Although there are exceptions to the rule, the general process includes completion of high school, earning a bachelor's degree, entrance exams and completion of a master or doctoral program, on-the-job training (residencies and internships), and state or multi-state license examinations. The cyber career pathway can include none, one, all, or any combination of similar endorsements. However, none are actually required to become a cybersecurity expert. Employers may have requirements for a candidate, which they trust are enough to demonstrate the necessary qualifications. However, one's proficiency and expertise in cybersecurity is often determined by their inquisitive nature, problem solving skills, technical aptitude, and their ability to understand the interdependencies of people, systems, and applications.

One may argue that cyber professionals do not have the same responsibilities as lawyers and doctors, and thus career pathways do not require the same structure and oversight. The opposing argument will highlight the dependence upon secure use of technology for today's financial systems, health care devices, critical infrastructure, and so much more. While there are a variety of applicable undergraduate programs, numerous industry certifications, and emerging master's level degrees, there is truly no "best way" for entering the cyber field. Instead, there are numerous paths that professionals have taken to begin and advance their careers.

According to the 2018 Cybersecurity Workforce Study, conducted by the International Information Systems Security Certification Consortium (ISC)², the shortage of cybersecurity professionals is nearing three million globally, with North America's shortfall estimated at 498,000.[1] Contributing to the lack of skilled cyber professionals are a variety of factors, including rapid technology changes, hiring constraints, inadequate understanding of cybersecurity fundamentals, along with the absence of a clear cyber career pathway. The amount of information can be overwhelming and conflicting. In addition, inconsistent language used in job titles and requirements can add to the uncertainty and discouragement.

The limited understanding of prerequisite skills and knowledge required when entering the cybersecurity field, or advancing from an existing cyber role, is a significant hurdle. This paper, sponsored by the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security, and authored by the Software Engineering Institute (SEI) at Carnegie Mellon, explores the current state of cybersecurity career paths and progression.

II. Early Exposure to Technology

Technology is ubiquitous in our everyday lives; at home, work, school, and travels in between. Most schools have integrated tablets into the classroom, and homework assignments. They provide more

engaging instruction to multiple types of learners, while also evolving teaching styles with instant assignment results, many times involving several metrics.

By incorporating a tool that many children first associated with games, this creative method of learning is welcomed by students. Teachers with "21st century skills" are finding new ways to connect and inspire our youth.[2] Using technology at younger ages for problem solving and introducing new tools and applications, immerses them in the digital age and develops an aptitude for technology. It is also driving the need for good cyber hygiene and digital citizenship at an earlier age. Many districts require students to complete Internet safety training before using devices.[3] Time will tell if establishing positive cyber habits at younger ages will have an impact on future interests in a career in the field.

While K-12 classrooms are leveraging more technology for instruction, today's educators are challenged with preparing students for a career in cybersecurity. According to the findings published in an early education and development online journal, surveying 67 Head Start classrooms, teachers' self-efficacy was lower for STEM (Science, Technology, Engineering, and Mathematics)-related subjects, i.e., science and math[4], which results in these educators feeling not adequately prepared to teach these subjects. The lack of early STEM exposure, as early as sixth grade, impacts a student's likelihood to choose a STEM career.[5]

High school is when most students begin seriously considering career options; having a better understanding of what various occupations entail, would aid in this decision process. Four Raytheon reports, spanning from 2014 to 2017, describe the current state of millennials and their relationship to cybersecurity. Data was collected from over 3,000 millennials, ages 18-26, from nine countries, and summarized in these annual reports.

One-fourth of the respondents stated they did not feel qualified to pursue a career in cybersecurity. However, almost half, 47% of those millennials, indicated they would have an increased interest in the field if they learned more about what the job actually entailed. The majority, 83% believe it is important, very important, or extremely important to increase cybersecurity awareness programs in the workforce and formal education programs.[6]

Another factor weighed in the reports was where the young adults were hearing about cybersecurity. In 2017, 43% said their first cyber talk was with their parents. A similar percentage, 40%, responded that their parents held the top rank of influential figures in their lives.

The millennials who said it was a teacher who initiated awareness of the cybersecurity field, was 37%. That leaves 2/3 who had not discussed a career in cybersecurity with an educator. Awareness is paramount. Parents and teachers need at least a base level understanding of the field to adequately inform young adults and aid them in finding resources. Earlier exposure to career options in the field of cybersecurity could increase if career influencers and mentors had fundamental cyber knowledge.

Initiatives, Programs, and Resources

There are several initiatives to generate awareness in the information technology and security field. The National Initiative for Cybersecurity Careers and Studies (NICCS), managed by the Department of

Homeland Security (DHS), is probably one of the most well-known cybersecurity resources with a wealth of information on cyber education and training. NICCS maps the training within its catalog to the National Cybersecurity Workforce Framework (NICE Framework); a tool intended to establish a universally adopted terminology for cyber work roles and the knowledge, skills, and abilities (KSAs) required for each. NICCS has neatly organized links to a plethora of sources to obtain K-12 cyber-based curricula and tools for organizations to build and strengthen their own cyber workforce**.**

Aimed at K-12 audiences is GenCyber. GenCyber is a program cosponsored by the National Security Agency (NSA), and the National Science Foundation (NSF), that provides summer cybersecurity camps, at no cost, for students and teachers. GenCyber is positioning themselves to be part of the solution to the shortage of cyber talent by inspiring students' interest in the field earlier, and advancing teaching methods in related K-12 curriculums.[7]

Initiatives for middle and high school students take technical training further with hands-on skill application, and cybersecurity career information. Many of these are competitions or challenges where learners perform in scenarios that simulate common cyber operator roles. These are especially plentiful for high school, college, and post-graduate audiences. Sponsors of these events, government, industry, or academia, provide practical insight into the cybersecurity career field in an engaging way.

Career Technical Education programs, commonly referred to as CTE, are integrated into school districts across the U.S. There are currently 12.5 million students enrolled in CTE programs throughout middle school, high school, and post-secondary institutions[8]. These career programs, developed in collaboration by state education leaders, directors, and industry leaders, are designed to teach specialized career skills through applied, hands-on practice.

The CTE program has 16 occupational areas, or clusters, with more than 79 career options organized within. Each cluster has established knowledge and skill statements defining the foundational expectations of that area of work, which apply to all related career pathway options. For instance, the Health Science cluster has essential knowledge and skills common across each of its five career path options. The paths detail the coursework and training to obtain, and offers sample job titles it would be applicable to. Most paths have guidance starting at the ninth grade. This means students could potentially have four years of immersive career training before graduating high school. The CTE programs are working to prepare students to be workforce-ready through occupationally-focused training and practical hands-on experiences. CTE initiatives include standards for information technology careers, which can establish foundational proficiencies for technical cybersecurity occupations, such a networking and programming.

A program supported by DHS, US Cyber Challenge (USCC), has the aggressive goal of finding 10,000 of America's brightest to recruit into cybersecurity roles. Together with partners from government, industry, and academia, USCC conducts competitions and training camps where participants can apply and further develop their cyber skills. The Cyber Quests portion has online challenges where those who excel and show aptitude based on correct scores and time taken to complete, are invited to Cyber Camps. The camps are weeklong workshops led by college educators and cybersecurity experts

commencing with a capture-the-flag competition, and a job fair.[9] USCC also manages cybercompex.org, an online resource with references to all things cybersecurity, including a list of various cyber competitions.

Another example of an online cyber challenge simulating an operations environment is the NICE Challenge Project. It is managed by the National Initiative for Cybersecurity Education (NICE) and NSA, partnered with California State University, San Bernardino. The project consists of standalone challenges representing tasks detailed within the NICE Framework. Standalone meaning users can work on a single, or combination of challenges, based on their goals and solve these real-world challenges without instruction. This virtual environment can be leveraged as a training or evaluation resource.

Circling back to educational institutions, there are several collegiate programs to encourage careers in cybersecurity. CyberCorps' Scholarship for Service, commonly referred to as SFS, covers the tuition expenses of earning a degree in a cyber-related field. This program is sponsored by NSF, and in exchange for the tuition benefit, the graduate is required to work in a government organization for a term equal to the length of their scholarship. As of January 2018, there are 70 participating educational institutions, and over 2,500 SFS graduates have acquired positions in over 140 federal, state, local, or tribal agencies.[10] The program also provides guidance to hiring managers in government agencies on recruiting an SFS graduate.

National Centers of Academic Excellence (CAE) is a program sponsored by DHS and NSA. Two and four-year colleges and universities can be designated as a CAE if their degree programs meet strict requirements that include an alignment between critical cybersecurity skills and Knowledge Units (KUs). There are over 200 educational institutions that have earned the distinction as either a CAE in cyber defense (CAE-CD), or CAE in Cyber Operations (CAE-CO).[11]

The CAE-CD program focus is on higher education and research in cyber defense. There is a CAE in CD Education (CAE CDE) for all degree levels, and a CAE in CD Research (CAE-R) for schools with doctoral programs. Graduates will have an expertise in cyber defense and be prepared for a position in cybersecurity.

The second CAE distinction is Cyber Operations (CAE-CO). CAE-COs are applicable to four-year and graduate level degree granting universities, and is an intensely technical program with hands-on practical application of cyber tools and techniques. Institutions designated as a CAE-CO have established degree programs in computer science, electrical engineering, or computer engineering. Graduates will be prepared to perform specialized cyber operations in areas like collection, exploitation, and response.

There are also Intelligence Community Centers for Academic Excellence (IC CAE), supported by NSA. The Defense Intelligence Agency (DIA) manages this program, which includes working with competitively selected four-year institutions, to ensure graduates have the skills needed for employment in intelligence and national security.

Veterans who had a technology or communications-related assignment, likely have relevant experience that would complement pursuing a formal degree in cyber. The GI Bill is another government-sponsored

program that may be an attractive post-high school option for some. Active-duty service members, veterans, National Guard or reserves, or a qualified survivor or dependent, can be eligible to receive assistance with tuition expenses through the GI Bill.

Hire our Heroes (HOH) is a non-profit organization founded with the goal of helping veterans gain employment after their military service. According to an article published on the HOH website, veterans are excellent candidates for a career in cybersecurity because of their ability to "thwart cyber adversaries, make quick decisions in dynamic situations, and help defend our country".[12] One of the resources available to veterans to assist with training related to cybersecurity, is the Federal Virtual Training Environment (FedVTE). This online, on-demand training platform sponsored by DHS, contains courses covering a wide-range of cybersecurity topics for all experience levels, at no cost to HOH users. Besides experience from military service, veterans may have a security clearance making them well positioned for a career in the cyber field, especially for government-related institutions.

Cyberseek is another noteworthy project aimed at anyone interested in cybersecurity including students, educators, employers, or those desiring employment. An interactive website, cyberseek.org, contains several tools designed to help users narrow down career considerations and outline the best way to proceed. There is a career pathway tool that takes user-selected options within job categories and returns useful information, such as the average salary for a position, requested education and certifications, ideal skills to have, and potential role transition opportunities.[13] CyberSeek is supported by NICE and partners with Burning Glass Technologies, an analytics company, and the certification agency, CompTIA.

CyberSeek also has an interactive heat map tool. The map provides insight into the status of the cybersecurity career field in geographical areas. Information is available at the national level, or a more in-depth look at metro-level areas that can be filtered by population size. Selecting a state returns data for its number of job openings, total employed, and the supply to demand ratio as compared to the national average. Further, the top titles of open jobs are listed, categorized according to the NICE Framework, as well as certifications requested by openings compared to the number who currently hold it. Cyberseek provides useful data regarding the current climate of the cybersecurity career field that can help with decision-making or strategy-development.

This list of resources only scratches the surface of what's available online for information on training, education, and employment in the cybersecurity field. Some target specific audiences or a particular goal, but if an individual is interested in pursuing a job in cybersecurity, or educators need awareness or training guidance, information is a few clicks away. The cybersecurity community, from all sectors, has a vested interest in cultivating a larger pool of skilled professionals to help address the workforce shortage.

Methods of Entry into Cybersecurity

There are typically three methods of entry into the cybersecurity career field. One is directly after graduating from college or university. Companies are interested in hiring graduates because they are fresh and can be molded for specific workplace culture. The graduate will likely have had some

experience through internships or cyber competitions. Their new-hire will more readily accept the training and practices of the company without biases from previous job experiences.

Having organizations partner with educational institutions is a frequent recommendation within the community to help solve the cyber talent shortage. Making this connection keeps schools abreast of the knowledge and skills students need to prepare for a career, while the companies are connected to a pool of effectively trained recruits. There are several examples of companies who have reached into schools to help design curriculums, and provide guidance for critical skills needed in the workforce.

The 20-year partnership between the NSA and the University of Maryland, Baltimore County (USMB) is keeping the agency's workforce pipeline flush with talented recruits. Eighty-five percent of students in the NSA/USMB programs become fulltime employees.[14] This relationship, as well as those the NSA has with CAEs, is also leveraged by existing employees to earn additional degrees and certification opportunities. Their initiative has proved successful with 1,100 USMB students employed at the NSA, and a 96 percent employee retention rate.[14] While the NSA/USMB student programs are not exclusive to cybersecurity or technology, the model of an agency partnering with an educational institution to prepare students for specific careers through training and mentoring, is one with proven results that are impactful.

Another way of entering the cybersecurity career field is through cross-training. This includes those who have worked in Information Technology (IT) or that may have a tech background. IT personnel are often responsible for both technology implementation and applying security configurations to systems and networks.[15] Having an in-depth understanding of topologies, protocols, devices, and applications provides a solid foundation to build upon when developing new cybersecurity knowledge and skills. Additional training, and obtaining industry certifications will likely be required, but having this previous experience positions them well for such a transition.

Finally, there are those with no technical background, but other expertise that can be applied in a cybersecurity-related work role. As in other professions, cybersecurity has many specialty areas. There are management roles, training, professional writing, risk assessment, legal, and so on. For those interested in more technical tracks, understanding the fundamentals of information technology and how computers operate is where to start. In a January 2019 survey of almost 40 professionals actively working in cybersecurity positions, 30% of respondents advised beginners to build a strong technical foundation by learning the basics of networking, operating systems, programming, etc.[16] Others in the survey, 28%, indicated the best place to start was learning as much as possible by reading blogs, listening to podcasts, viewing webinars, and even taking formal classes. This is consistent with many online resources providing tips and guidance for pursuing cybersecurity careers.

The website, Breakingintocybersecurity.com, published the personal stories of 55 cybersecurity professionals on their paths taken into the field, and their advice for others.[17] The advice of these professionals is very similar to the feedback from the previously mentioned survey. Both had common themes. Advice to learn new things and building a strong technical foundation were mentioned the most. Also frequently found in the Breakingintocybersecurity.com professionals' advice feedback was

the importance in first identifying an interest or passion for cybersecurity, and then letting that drive the progression.

The need for individuals to possess a strong technical foundation and a desire to learn are some of the most common tips given by current cybersecurity practitioners. In an article by Derek Carline[18] relating to getting a job in cybersecurity, published on Cybrary.it, a website dedicated to cybersecurity training, he states the first steps are to research the field, work on gaining a baseline foundation, and master the basic skills. Another article published on Forbes.com, Laurence Bradford[19] writes about starting a lucrative career in cybersecurity, and begins by declaring, the best security professionals have well-rounded experience in tech work. It continues with a similar quote from Sean Tierney, head of the cyber intelligence team at Infoblox, saying, "become a master of the fundamentals of data networks, be an expert at administering multiple operating systems or be proficient at multiple scripting languages (Python, Bash, etc.)". The consensus from these sources, representing seasoned professionals in the field, is to have the desire for success and build a strong technical foundation.

III. Cybersecurity Career Pathways

The scope of research for this paper is the current state of career paths and progression in terms of advancements within the cybersecurity field, not promotions and annual raises within the same position. It is unclear who ultimately owns the responsibility for career path progression. Traditionally, individuals guided their own interests and desire for advancement. With ever-changing technologies, and specific organizational needs, employers are taking a larger role in helping to define progression paths. Organizations investing their own resources to create clear guidance on advancing their employee's careers, shows a vested interest in personnel success while attending to their own needs for a trained, skilled workforce.

The dynamic nature of cybersecurity is challenging, compounded by work roles differing between organizations, and even departments within. With the rapidly changing nature of the domain, career pathways and required training must be reviewed and updated regularly. Referring back to the medical and legal fields examples, the necessary skills for those professions have remained relatively consistent while cybersecurity continuously demands learning new concepts. Because of this, curriculums can quickly become outdated and less reflective of the current state of cybersecurity at any given time. For instance, artificial intelligence (AI), Internet of Things (IoT), and weaponized psychology are just a few newer priorities in the cyber domain. The latter, weaponized psychology, which is commonly related to social media, is a threat thought to be especially critical. Sen. Richard Burr (R-NC) chairman of the Senate Select Committee on Intelligence, said in remarks at a January 2019 hearing on the global threat environment, "We are now living in a new age—a time characterized by hybrid warfare and weaponized disinformation, all occurring within the context of a world producing more data than mankind has ever seen." Skills required for this new attack surface, to detect and counter these influence operations, would include psychology, economics, and algorithms. Existing higher learning degrees in cybersecurity, and even position descriptions, are not likely to include these psychology and economics requirements.

Applying for positions within the cybersecurity field will require some level of higher education to demonstrate an aptitude to succeed in that position. There are rare cases where those without a degree find themselves excelling in a work role. However, earning an advanced degree, preferably in science or technology, will get candidates stronger consideration. An educational foundation in this area represents some fundamental knowledge of computer systems and how they can be applied. In a survey conducted in January 2019 including 39 professionals actively working in cybersecurity positions, 36% stated that earning a college degree was the strongest contributing factor for them entering the field.[16] Of those, 79% earned a technical degree. While this data indicates that a degree in computer science can be a strong first step for pursuing a cybersecurity career, the same survey had a higher percentage of respondents, 38%, who entered with a non-technical degree and/or unrelated field.

According to the 2018 (ISC)[2] Cybersecurity Workforce Study, 49% of hiring managers believe relevant cybersecurity work experience is one of the top qualifications they look for amongst potential candidates. Relevant experience demonstrates a candidate's interest in the field, and the likelihood they have the skills to do the job. In the 2019 SEI survey, 58% of current cybersecurity professionals had previous work experience in IT, Software Development, or Engineering.[16] This related job experience is transferable and may be a contributing factor in hiring or promotion processes.

In addition to work experience related to cybersecurity, investing in more specialized training and certifications have been identified as factors that help professionals progress in their field. Advanced training in emerging technology and security areas such as cloud computing and artificial intelligence would significantly increase a candidate's value and competitiveness. While there has been an ongoing debate over whether or not certifications actually prove a candidate can apply what they learned through studying and passing a certification exam, certifications can be used as a way to filter out candidates[20]. In fact, according to (ISC)²'s Global Workforce Study, cybersecurity certifications are highly ranked as being most important for advancing and maintaining careers.[21]

Earning a cybersecurity-related industry certification is a solid step in pursuing a position in the field. They are valued by companies, and frequently listed as a requirement in many job descriptions; especially for entry-level. Instead of an advanced degree, combining some formal education and a certification is a common route for cybersecurity professionals. One reason is the cost and time it takes to earn a master's degree compared to the time and cost of earning a certification. For example, the average for a cyber-related master's degree is a couple years and between $20,000 and $70,000 per year,[22] depending on institution and program. The CISSP certification is considered advanced and one of the most commonly requested in job descriptions. The CISSP exam is 3-hours and costs $699.[23] There is preparation time to consider for the certification exam, and possibly the purchase of study materials, but that cost does not compare to the graduate degree, plus all the extra amenities needed to attend the courses.

However, unless the certification requires hands-on application of knowledge, it does not prove the candidate possesses the necessary skills to be successful. Instead, it only demonstrates their ability to pass the required exam. According to a 2017 Infosecurity Magazine online article, certifications may not hold the same weight as experience once a professional has reached a certain point in their career.[24]

Further, it quoted the findings of a survey conducted during the 2017 RSA conference where 93% of the attendees reported that relevant work experience outweighed qualifications.

It is common for organizations to sponsor the pursuit of advanced degrees and industry certifications for their employees. Accepting an entry-level position and gaining practical work experience while earning additional credentials is a win-win for both sides. The individual is paying little to enhance their qualifications, while the organization is investing in skill strengthening of its human capital.

Internships, apprenticeships, and rotational programs are gaining popularity as organizations strive to recruit new talent and strengthen the abilities of existing employees. Rotational programs are a progressive means for encouraging rapid transfer of knowledge, while aiding in professional growth for employees. Capital One and Boeing are examples of private sector organizations implementing rotational strategies, while the NSA serves as a model for government agencies. New NSA hires, including Center of Academic Excellence (CAE) graduates, enter a one to three year rotational development program. After initial training on core competencies by subject matter experts, employees then spend time in several departments for additional mentoring, and to gain hands-on experience. Once complete, the NSA Board of Governors decides the candidates' placement based on the individual's strengths, interests, and agency needs.

In addition to experience and education, there are qualifications and skills that may not be formally identified. So-called 'soft skills' such as communication, teamwork, attention to detail, and problem solving, are just a few of the attributes an individual also needs to be successful in a cyber role. Having skills beyond technical proficiencies is important in becoming a fully functioning member of a company.[25] Analyzing personality and behavioral traits of potential candidates is becoming a more common tool to predict whether an individual will be a good fit for an organization. IBM has produced two related tests to help evaluate workers for entry-level IT security work roles.[26] The exams assess soft skills and behavior traits as well as the cognitive aptitude required to learn technical concepts. Their Commercial Cyber Aptitude Test (CCAT) measures if an individual has the fundamental qualities that support competency development for cyber roles. The critical traits to measure include adaptability, dependability, and energy.

Another aspect, which can make a huge difference in the cybersecurity field, is a security clearance. If a candidate possesses an active clearance from a previous job, or the military, it is a tremendous benefit. This is especially true if they are applying for a government position. A security clearance proves to employers an individual has passed some level of background check, and is capable of, and willing to protect classified information.[27] Obtaining a clearance can be a costly, time-consuming process. One cannot obtain a security clearance on their own; a job that requires one and a sponsoring agency is needed first. Avoiding infractions or indiscretions that may cause delays or rejection in the background review process is paramount if a career in cybersecurity is desired.

The path to follow for a cyber career is different for every individual, and job role. The dynamic nature of the cybersecurity field and the ever-changing landscape make it difficult to design a one-size-fits-all plan that will have a long shelf life. Organizations also have different needs and priorities. Achieving

some combination of a technical foundation, an IT-related education, an industry credential, and/or applicable work experience is a solid start to the journey.

IV. Cybersecurity Career Progression

Confucius once said, “Choose a job you love, and you will never have to work a day in your life.” While most would agree, the feeling of contentment and satisfaction is oftentimes matched with a desire to improve and grow. The cybersecurity field is so diverse, opportunities for moving upward in rank, gaining more experience, or transferring positions horizontally, are achievable. The key is identifying the skills and strengths, those that bring out the most for an individual, and move from there.

For other industries, the steps for career progression are typically defined and straightforward. Recall earlier examples of careers in medical and legal fields. Because of the vastness that makes up the cyber field, and its intermingling into nearly every industry, a clear career pathway does not exist.[28] Because of this, the process of developing an individual career path may appear daunting and full of uncertainties.

Common career advice includes self-refection, goal setting, and developing a plan.[29] This same course of action can be used by a cybersecurity professional to pursue career advancement. By defining specific measurable, attainable, realistic, and timely goals, a focus is achieved that clarifies previous uncertainty.

One place to begin is by researching job boards and postings for cybersecurity roles. This can aid in identifying the essential qualifications for a new position. While this information varies from one posting to another, some commonly sought skills might include incident handling, cloud computing, or application security. Identifying these industry needs can then help guide professional development and goal setting.

In the blog article, *Why It’s Important to Establish Yourself as a Subject Matter Expert*, the author states that establishing yourself as a subject matter expert (SME) is the key to projecting your professionalism and setting yourself apart from your competition.[30] Leveraging pre-existing skills or experience, such as those in mathematics or programming to specialize in more emerging technologies like blockchain development, would set one apart from the rest of the field. According to Linkedin’s 2018 *U.S. Emerging Jobs* report, “Blockchain Developer” came in at number one.[31] Looking at opportunities in emerging technologies to develop unique skills shows commitment to a specialization and professional growth. Regularly published reports and surveys from within the industry identify emerging concepts and technologies. Pursuing a level of competency in those areas can help one remain competitive in the field. Determining areas to become a SME should not only be driven by industry needs or emerging technologies, but also relate to overall career goals, strengths, abilities, and interests.

Many certification agencies, such as ISACA and (ISC)^2, provide career paths to follow, with each credential representing a different level of expertise. Data from CyberSeek.org, shows (ISC)^2’s advanced Certified Information Systems Security Professional, or CISSP, is one of the most requested certifications in the current cybersecurity job market. The runner-up is ISACA’s Certified Information Systems Auditor, or CISA. As of January 2019, there are over 77,000 CISSP and over 44,000 CISA job openings for these two certifications.[32]

ISACA, a globally known nonprofit organization, helps in the building, adoption, and utilization of global and prominent industry knowledge and practices for information systems. ISACA holds a handful of conferences around the world and exhibits at conferences to promote the association. $(ISC)^2$ is an international organization providing industry-related education and professional certifications, that holds summit events internationally and a series of monthly webinars. Black Hat is also an international organization providing the latest security information in research, development, and security trends, as well as cybersecurity training during conferences. Joining an industry-related association and attending conferences helps keep professionals informed of the latest advancements while building a professional network.

The Information Systems Security Association (ISSA) is yet another cybersecurity related organization. ISSA has created the Cybersecurity Career Lifecycle (CSCL) website, which provides members, a tool to help plan out their career roadmap. The CSCL's model is based on the Cumulative Knowledge model, which focuses on gaining the foundational knowledge demonstrated by experience gained through higher education and/or certifications, continuous and responsive learning, followed by cumulative knowledge gained over time.[33] The CSCL model provides a career level description, and the suggested skills and knowledge required at each career stage (i.e., Pre-Professional, Mid-Level, Senior-Level, and Security-Leader). Additional information, such as education, meet-ups, and mentorships, is available.

Cybersecurity associations, working groups, and conferences provide an excellent opportunity for professionals to enhance both their personal and professional development. The National Initiative for Cybersecurity and Education (NICE) working group, which is made up of six-sub groups, is another excellent example of how professionals from the private and public sectors have come together to share industry-related knowledge, develop new ideas, design strategies, and work on advancing cybersecurity through education, training, and workforce development.[34]

According to a 2017 study involving 15,905 LinkedIn members, almost 80% of professionals consider professional networking to be important to career success.[35] The flip side of that is, 38% say it is difficult keeping in touch with members of their network; half of those respondents attributing it to time constraints. Building a reliable network of professionals is an excellent resource for referrals, advice, friendships, mentors/mentees, and jobs. Being well connected, and knowing how to network effectively, will cultivate valuable relationships that will help with career advancement.

Building this network of peers is also a good strategy for identifying mentors. There are programs such as the Multi-State Information Sharing and Analysis Center (MS-ISAC) that match those new to leadership positions with seasoned professionals working in a similar role. Participants share industry experiences, useful insights, and lessons learned relating to security concerns and best practices. According to a 2015 survey conducted by the Harvard Business Review, 84% of the 45 CEOs credited mentors with helping them avoid costly mistakes and become proficient in their roles faster.[36] Professionals can give back to the cybersecurity community by becoming a mentor to someone else.

There are numerous other ways a seasoned professional can contribute to the cybersecurity community. According to Michi Ancheta,[37] a writer for CareerAddict.com, blogging has professional

benefits, such as providing a creative outlet, growing both a personal and professional network, and a way to establish authority or individual brand. Blogging is an excellent way to share expert knowledge with fellow cybersecurity professionals and gain credibility in the community. In addition, having work published in industry-related sources and speaking at networking events also contributes to the growth of one's professional career, as well as oral and written communication skills.

IT Security Guru is an industry source for the latest IT Security news and blogs, as well as a medium for submitting security-related blog content. There is a fairly extensive community with over 13,000 followers on Twitter[38] and just under 2,000 on Facebook.[39] *Krebs on Security* is a well-known industry blog featuring the latest security news and investigative articles for recent security breaches. The author, Brian Krebs, is an excellent example of a professional without the technical education or experience, who successfully used his writing abilities and experience, combined with an interest in security, to launch a successful career as cybersecurity blogger.[40] His blog surpasses *IT Security Guru* popularity with 243,000 Twitter followers[41] and 33,000 followers[42] on Facebook.

V. Conclusion

The cybersecurity workforce shortage is continuing to grow. For those who have interest in entering, and/or talents that could make them successful in a cyber position, information on what a career entails is overwhelming, confusing, and conflicting. For organizations, there are difficulties with identifying requirements needed for open positions, recruiting and retaining talent, while trying to maintain a strong cybersecurity posture. Contributors to these issues are agreed upon within the community, as well as the acknowledgement of solutions that can improve the current state.

Beginning at the grassroots level, part of the solution is providing teachers, especially at the elementary level, professional development and training needed to teach technology in the classroom. The goal is to get students thinking about careers in cybersecurity earlier, just like if they wanted to become a doctor, teacher, or musician.

At the secondary and post-secondary education levels, cyber-related programs and scholarships help prepare students with the skills and experience needed to enter the workforce. Organizations that partner with schools to create these programs, have access to recruits they helped to mold, while keeping the school's curriculums current with needs of the evolving cyber field. Employers can also get a return on investment by sponsoring professional development and continuing education for employees.

While there are several initiatives aimed at combating the cyber workforce shortage, the path to follow in preparation for a cyber career and progression once in the field, is less straightforward. A November 2018 paper published by Aspen Cybersecurity Group, *Principles for Growing and Sustaining the Nations Cybersecurity Workforce*, their forum of cybersecurity professionals representing every sector, documented how pressing concerns such as skills gap can be addressed with real actions. They called out the four root causes for the skills gap: demand for skills outpacing supply growth, large pools of skilled candidates untapped, employer requirements make many applicants unqualified, and lack of

awareness of opportunities and careers paths. Their eight recommendations to help close the gap, and strategies to improve hiring, training, and employee development, reiterate the findings of this paper.[43]

- Widen candidate pipelines by stop making degrees mandatory; they termed this New Collar principles
- Focus job postings on core requirements
- Simplify career models by leveraging the NICE Framework for consistency
- Adopt new ways to hire and train making technical and professional skills a priority, allowing cybersecurity to be taught
- Use apprenticeship programs for training
- Commit to employee development
- Adopt productive, focused partnerships and programs
- Advocate and make cybersecurity education widely available

Security consultant, Mark Carney, has a slightly different view of the issue; he asserted there is not so much a skills gap as there is a skill mismatch. It is hard to miss his frustration through satire as he details with real examples of how industry is at fault because of improperly defined job descriptions that lead to unqualified applicants and/or discourages good candidates. His hypothesis in the article, *We Need to Kill the 'Security Analyst'*, published February 2019, perfectly summarizes the conundrum: "If students knew better what to learn, educators knew better what they needed to teach, and hiring and tech managers knew better what to look for when hiring, then businesses will be better protected against threats".[44] His proposed solution is a skills matrix that is reminiscent of the NICE Framework, with the addition of a rating system to signal the criticality of a skill within a role. Created with collaboration from individuals representing a spectrum of vested interest in cybersecurity careers, the Infosec Skills Matrix is intended to be a regularly updated living document.

One of the consistently highlighted problems with finding talent to fill vacant positions is that job descriptions do not accurately represent the qualifications needed for a position. This causes inadequately qualified candidates to apply, and discourages others that may actually be a better fit. The Infosec and NICE frameworks are examples of tools that if widely adopted, would create a standard for how cyber roles are described. Using common definitions for work roles, including the skills and abilities required to perform the duties, would help employers write more appropriate job descriptions. This would also provide educational institutions better guidance when designing cybersecurity curricula. Incorporating relevant soft skills would further help candidates target roles that best align to their strengths. A cross-matrix of work role attributes mapping the commonalities between positions might then yield additional insight into training and education needs for career growth and/or transition to different roles. Adoption of one standard by the government, industry, and academia, will help achieve this, and ideally combat the shortage of skilled cybersecurity professionals.

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

DM19-0158

[1] (ISC)[2]. *Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens.* 2018. https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0.

[2] Tynan-Wood, Christina. iPads in the classroom: the promise and the problems. *Great! Schools.* March 7, 2016. https://www.greatschools.org/gk/articles/ipad-technology-in-the-classroom/

[3] Cortez, Meghan Bogardus *3 Cyberhygine Tips for K-12 End Users* https://edtechmagazine.com/k12/article/2017/10/3-cyberhygiene-tips-k-12-end-users. Oct 2017

[4] Gerde, Hope K.; Pierce , Steven J.; Lee, Kyungsook, & Van Egeren, Laurie A. 2018. *Early Childhood Educators' Self-Efficacy in Science, Math, and Literacy Instruction and Science Practice in the Classroom*. *Early Education and Development*. 2017 https://www.tandfonline.com/doi/full/10.1080/10409289.2017.1360127

[5] Gerlach, Johathan W. All Teachers Are STEM Teachers. *Education Week Teacher.* July 10, 2015. https://www.edweek.org/tm/articles/2015/07/10/all-teachers-are-stem-teachers.html

[6] Raytheon. *Securing Our Future: Cybersecurity and the Millennial Workforce*. 2017. https://www.raytheon.com/sites/default/files/2017-12/2017_cyber_report_rev1.pdf

[7] GenCyber. January 14, 2019 [accessed]. https://www.gen-cyber.com/about/

[8] Career Technical Education. January 2019 [accessed]. https://careertech.org/cctc

[9] USCC*. Our Mission.* January 21, 2019 [accessed]. https://www.uscyberchallenge.org/our-mission/

[10] SFS*.* January 17, 2019 [accessed]. https://www.sfs.opm.gov/Overview-History.aspx

[11] NSA. *Criteria for Measurement for CAE in Cyber Operations Fundamental.* January 15, 2019 [accessed]. https://www.nsa.gov/resources/students-educators/centers-academic-excellence/cae-co-fundamental/

[12] Kuss, Lauren. The cybersecurity Veterans Toolkit. *Hire Our Heroes*. April 18 2018. https://hireourheroes.org/cybersecurity-veterans-toolkit/

[13] Cyber Seek. *Hack the Gap: Close the Cybersecurity Talent Gap with Interactive Tools and Data.* January 7, 2019 [accessed] https://www.cyberseek.org/index.html

[14] Miller, Jason. Federal News Network. October 19, 2018. https://federalnewsnetwork.com/ask-the-cio/2018/10/how-nsa-is-winning-the-war-for-cyber-talent/

[15] Young, Carl S *The Enemies of Data Security: Convenience and Collaboration* https://hbr.org/2015/02/the-enemies-of-data-security-convenience-and-collaboration October 2015

[16] Carnegie Mellon Software Engineering Institute Survey 2019 Qualtrics Survey on Cybersecurity Career Path [accessed] https://sei.az1.qualtrics.com/jfe/form/SV_3WMKzBERjsguerP Posted January 16, 2019

[17] Breaking Into Cybersecurity. January 25, 2019 [accessed]. https://breakingintocybersecurity.com/

[18] Carlin, Derek. *Breaking into the Cybersecurity Field. Cybrary.* April 2017. https://www.cybrary.it/0p3n/breaking-cybersecurity-field/

[19] Bradford, Laurence. Career in Cybersecurity*. Forbes.* February 27 2017. https://www.forbes.com/sites/laurencebradford/2017/02/27/how-to-start-a-lucrative-career-in-cybersecurity/#7bd253cf1066

[20] Sundaram, Aurobindo. Security Certifications are Useless, Right? *Infosecurity Magazine*. March 2017. https://www.infosecurity-magazine.com/news-features/security-certifications-useless/

[21] (ISC) [2]. Cybersecurity Hiring – An Issue for All [blog post]. *(ISC)[2] Blog.* Februrary 2018. https://blog.isc2.org/isc2_blog/2018/02/cybersecurity-hiring.html

[22] USD. 8 Reasons Why a Cyber Security Degree is Worth It. *Master of Science in Cyber Security.* January 29, 2019 [accessed]. https://onlinedegrees.sandiego.edu/8-reasons-to-get-your-masters-degree-in-cyber-security/

[23] (ISC) [2]. Cybersecurity Hiring – An Issue for All [blog post]. *(ISC)[2] Blog.* Februrary 2018. https://blog.isc2.org/isc2_blog/2018/02/cybersecurity-hiring.html

[24] Sundaram, Aurobindo. Security Certifications are Useless, Right? *Infosecurity Magazine*. March 2017. https://www.infosecurity-magazine.com/news-features/security-certifications-useless/

[25] Bonderud, Douglas. Soft Skills, Solid Benefits: Cybersecurity Staffing Shifts Gears to Bring in New Skill Sets. *Security Intelligence.* November 19, 2018. https://securityintelligence.com/soft-skills-solid-benefits-cybersecurity-staffing-shifts-gears-to-bring-in-new-skill-sets/

[26] IBM. Commerical Cyber Aptitude Test. *IBM Offerint Information.* March 2018. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=67014167USEN

[27] Stone, Kyle. The Benefit of Having Security Clearance. *Gov Central*. January 29,2019 [accessed]. http://govcentral.monster.com/benefits/articles/2329-the-benefit-of-having-security-clearance

[28] New Horizons. *4 Cybersecurity Career Paths (And the Training to Get You There).* July 19 2018. https://www.newhorizons.com/resources/article/articleid/41/title/4-cybersecurity-career-paths-and-the-training-to-get-you-there

[29] Stahl, Ashely. 3 Steps To Develop Your Career Plan. *Forbes.* August 29, 2018. https://www.forbes.com/sites/ashleystahl/2018/08/29/3-steps-to-develop-your-career-plan/#3f0ae7c4910f

[30] Ondemand CMO. Why It's Important to Establish Yourself as a Subject Matter Expert [blog post]. *On Demand CMO, Insightful & Impactful Marketing Blog.* September 7, 2017. https://www.ondemandcmo.com/blog/important-establish-subject-matter-expertise/

[31] Economic Graph Linkedin. *LinkedIin's 2018 Emerging Jobs Report.* December 13, 2018. https://economicgraph.linkedin.com/en-us/research/linkedin-2018-emerging-jobs-report

[32] Cyber Seek. *Cybersecurity Supply/Demand Heat Map.* January 11, 2019 [accessed] https://www.cyberseek.org/heatmap.html

[33] ISSA. *CSCL Introduction.* January 26, 2019 [accessed]. https://www.issa.org/page/CSCL

[34] NIST. *National Initiative for Cybersecurity Education (NICE) Working Group.* January 17, 2019 [accessed]. https://www.nist.gov/itl/applied-cybersecurity/nice/about/working-group

[35] Linkedin Corporate Communications Team. Eighty-percent of professionals consider networking important to career success. *News Linkedin.* June 22, 2017. https://news.linkedin.com/2017/6/eighty-percent-of-professionals-consider-networking-important-to-career-success

[36] De Janasz, Suzanne, & Peiperl, Maury. CEOs Need Mentors Too. *Harvard Business Review.* April 2015. https://hbr.org/2015/04/ceos-need-mentors-too

[37] Ancheta, Michi. The 10 Biggest Benefits of Blogging. *Career Addict.* August 3, 2018. https://www.careeraddict.com/blogging-benefits

[38] Twitter-IT. *IT Security Guru*. January 26, 2019 [accessed]. https://twitter.com/IT_SecGuru

[39] Facebook-IT. IT Seucurity Guru. January 26, 2019 [accessed]. https://www.facebook.com/IT-Security-Guru-370776192982726/

[40] Krebs on Security. About the Author. January 26, 2019 [accessed]. https://krebsonsecurity.com/about/

[41] Twitter-Krebs. *Brian Krebs*. January 26, 2019 [accessed]. https://twitter.com/briankrebs

[42] Facebook-Krebs. *Brian Krebs*. January 26, 2019 [accessed]. https://www.facebook.com/Brian-Krebs-119740914725557/

[43] Aspen Cybersecurity Group. Principles for Growing and Sustaining the Nation's Cybersecurity Workforce. November 2018

[44] Carney, Mark. We Need to Kill the 'Security Analyst'. Medium February 2019. https://medium.com/@LargeCardinal/we-need-to-kill-the-security-analyst-79ec205651f5