Women Veterans: New Cybersecurity Skills

Part III in a White Paper Series

Toward Closing the Gap: Re-entry for Women Veterans into Cybersecurity Careers

Rachelle S. Heller, Costis Toregas, Taly Walsh
The George Washington University

Abstract - Closing the Gap: A DoD Conference on Re-Entry for Women Veterans into Cybersecurity Careers **addresses two crucial needs: to fill the exponentially growing cybersecurity talent gap in the U.S., and to harness the potential of female U.S. veterans, as well as military spouses, to fill that gap. In addressing these needs, the George Washington University organizers have assembled a diverse group of advisors from government, the military, academia and industry to help frame the conversation and the initiative toward meaningful action, before, during, and beyond the May 25, 2021 Conference date. "New Cybersecurity Skills" is the third in a series of white papers designed to summarize the available knowledge on challenges, best practices and potential solutions moving forward.**

Index Terms – Challenges and pathways for cybersecurity skills, cybsersecurity careers, cyber skills, women veterans.

INTRODUCTION

The importance of cybersecurity knowledge and preparedness for those serving in the military has been positioned in that "it is essential that members of the Reserve Officer Training Corps (ROTC) be well-versed in computing techniques designed to combat cyber-attacks that continually improve in sophistication and frequency levels." [7] Unfortunately, there is little agreement on exactly what those "computing techniques" are, though in general, cybersecurity jobs fall into three main categories: Security Architect, Security Engineer, and Security Analyst [3].

The National Institute of Standards and Technology (NIST) formulated the National Initiative for Cybersecurity Education (NICE) in order to provide a national focus for cybersecurity education. Within the NICE program, the problem of career progression is continuously examined. The initiative serves as a guide to both academics and employers in describing foundational *knowledge* and *skills* that learners, including students, job seekers, and employees need to obtain to succeed in the cybersecurity field. The program does not specifically cite pathways to achieving those skills, but presents five goals [10]:

- Goal #1: Promote the Discovery of Cybersecurity Careers and Multiple Pathways
- Goal #2: Transform Learning to Build and Sustain a Diverse and Skilled Workforce
- Goal #3: Modernize the Talent Management Process to Address Cybersecurity Skills Gaps
- Goal #4: Expand Use of the Workforce Framework for Cybersecurity (NICE Framework) [13]
- Goal #5: Drive Research on Effective Practices for Cybersecurity Workforce Development

In addition to the detailed description of the skills and tasks that rely on those skills, the NICE document outlines four key attributes of any guide to compiling a list of the "new cyber skills." The "new cyber skills" are noted as:

- ***Agility***—People, processes, and technology mature and must adapt to change.
- ***Flexibility***—While every organization faces similar challenges, there is no one-size-fits all solution to those common challenges.
- ***Interoperability***—While every solution to common challenges is unique, those solutions must agree upon consistent use of terms.
- ***Modularity***—While cybersecurity risk remains the basis of this document, there are other risks that organizations must manage within the enterprise.

SKILLS NEEDED FOR CYBERSECURITY CAREERS

What does a person need to know? Technically, stakeholders suggest there are "hard," "soft," and "solid" work skills necessary in cybersecurity. Actually, three things are needed: an ability to learn on your own, an ability to solve problems on your own, and an ability to communicate really difficult and technical things into language that a business person can understand. The technical skills can be learned and improved upon over time. "Soft" and "solid" work skills are often noted as:

- Problem-solving skills with strong analytical and diagnostic skills.
- Attention to detail.
- Communication skills: ability to clearly articulate complex concepts (both written and verbally).
- Ability, understanding, and usage of active listening skills (especially with customers).
- Enthusiasm and a high degree of adaptability.

For those who seek the formality of a list of what to know, while there is no agreed-upon definition of "cybersecurity," with the NIST / NICE attributes as a guide [9], various stakeholders, such as the National Cyber League (NCL) [8], have identified the important "hard" (rather than theoretical) skills that can be demonstrated in the cybersecurity context. "Hard" skills are noted as:

- A current understanding of common web vulnerabilities.
- A desire to learn and eagerness to dig into technical questions and examine them from all sides.
- Maintaining awareness and knowledge of contemporary standards, practices, procedures and methods.
- ***Cryptography:*** identify techniques used to encrypt or obfuscate messages and leverage tools to extract the plaintext.
- ***Enumeration and Exploitation:*** identify actionable exploits and vulnerabilities and use them to bypass the security measures in code and compiled binaries.
- ***Log Analysis:*** utilize the proper tools and techniques to establish a baseline for normal operation and identify malicious activities using log files from various services.
- ***Network Traffic Analysis:*** identify malicious and benign network traffic to demonstrate an understanding of potential security breaches.
- ***Open Source Intelligence:*** utilize publicly available information such as search engines, public repositories, social media, and more to gain in-depth knowledge on a topic or target.
- ***Password Cracking:*** identify types of password hashes and apply various techniques to efficiently determine plaintext passwords.
- ***Scanning:*** identify and use the proper tools to gain intelligence about a target including its services and potential vulnerabilities.
- ***Web Application Exploitation:*** identify actionable exploits and vulnerabilities and use them to bypass the security measures in online services.
- ***Forensics:*** utilize the proper tools and techniques to establish a baseline for normal operation and identify malicious activities using log files from various services.

PATHWAYS TO PROVIDING / ACQUIRING CYBERSECURITY SKILLS

The traditional pathway to learning new material is often to return to the classroom — either for a full-time degree program, a two-year degree, or a certificate. While each provides an acknowledged degree or certificate, the formal academic route may require that a student leave his or her job or at least be ready to stretch out the timeline to the degree.

One of the new terms, "upskilling" — providing more advanced skills through additional education and training on top of existing, related ones — suggests a targeted program to learn very specific skills. These are typically handled within a company. Boot camps, on the other hand, provide a broader set of cyber-skills, often in a university setting. Both types of programs are intended to permit students to maintain their current position while "upskilling." Upskilling is not just providing skills to those with no cybersecurity experience — it might also enhance the skills of, say, trained programmers to master secure code. "The right training 'upskills' an average developer into a security-aware developer" [6].

NIST / NICE provides ideas for apprenticeship — earn while you learn — programs [5, 11]. Community Initiative Center of Excellence for Secure Software (CICESS), is the first registered cybersecurity apprenticeship program in the United States. Several platforms offer apprenticeships – colleges as well as non-profit organizations, and even corporations — and many feature a way to learn specific skills while earning some level of salary [14]. For example, Fontbonne University in St. Louis announced a partnership with CyberUp, a national non-profit organization dedicated to closing the cybersecurity talent gap by helping adults and youth pursue cybersecurity careers. The Cybersecurity Workforce Alliance (CWA), founded by SIFMA and Chief Information Security Officers (CISOs) of major financial institutions, partners with educational institutions to provide students with courses, mentors and apprenticeships in cybersecurity. JPMorgan Chase has provided funding to support the Florida Center for Cybersecurity, and is also piloting a program called Skills Passport within the bank's IT department to assess which employees could be retrained for cybersecurity roles; the Capital One Foundation has provided grants to community colleges seeking to develop cybersecurity career programs [2].

Operation Code is a non-profit organization helping veterans, military spouses, and transitioning service members to enter technology careers. Software engineers, product managers, system architects and security engineers act as mentors to members. The organization highlights accelerated code learning programs, online courses, and training providers offering paid training to veterans.

Veterans for Azure is a non-profit organization designed to help train and place veterans in careers with Microsoft Azure. Upon completing the training, veterans have the opportunity to get a paid internship and apply what they have learned to real world experience. High-tech companies such as Cisco, Amazon, Raytheon, Palo Alto Networks, Fortinet, Google, Microsoft and Splunk frequently offer no-cost or low-cost training programs or scholarships for students.

Within the government, the Department of Homeland Security (DHS) has taken up the torch of cybersecurity workforce enhancement by promoting the field to active military personnel and veterans. Its "Veterans Cybersecurity Training and Education Guide" [4] helps students familiarize themselves with the field. The CIA, FBI, ATF, Homeland Security, Cybersecurity Infrastructure Security Agency, Secret Service and NSA have a critical need for cybersecurity personnel with security clearances, which may be a natural next step for veterans interested in entering the cybersecurity workforce within the government.

Apprenticeships can be combined to receive an associate's, bachelor's, or even a master's degree [11, 12].

CHALLENGES IN PROVIDING CYBERSECURITY SKILLS

Sifting through the diversity and sheer number of training and apprenticeship opportunities available to veterans may in itself be the most daunting challenge, and there is no one-size-fits-all solution. The task at hand is to simplify the pathways to decision-making while ensuring that women are given clear knowledge and assistance in choosing their specific steps to a cybersecurity career beyond the service.

The academic pathway to new or enhanced skills requires veterans to find the right academic, financial, and social fit among academic possibilities. Understanding the options among a 4-year institution or a community college or private for-profit is in itself challenging. Once an academic pathway is decided upon, how can the veteran leverage military experience with required coursework and degree requirements? Who can provide assistance in translating between course requirements and military job codes? Unique responses from the private sector have sprung in the marketplace that specialize as "in-between" organizations that take veterans and provide them with practical steps to cybersecurity jobs. Two such organizations are ISG and Rightvarsity.

Upskilling is typically accomplished within a corporation. That means companies have to absorb the cost of the program until they accrue the benefits and loyalty of the trained individuals. Such corporate questions have to be resolved for the success of such a program. Apprenticeships, while an age-old model, are relatively new within the cyber field.

SUMMARY

While there is no definitive definition of the skills and competencies for work in cyber, outlines and guidelines exist. In addition to the skills and competencies defined in the NIST / NICE Cybersecurity Workforce Framework and their many standards for specific job classifications, the National Initiative for Cybersecurity Careers and Studies (NICCS), in partnership with the Interagency Federal Cyber Career Pathways Working Group, has created a helpful online interactive Cyber Careers Pathways Tool that depicts the Cyber Workforce according to the NICE Framework [13]. The Comparitech network lists more than 35 skill building and training options for women seeking positions in cybersecurity [1]. Finally, the role of certifications (such as CompTIA and many others) must be understood whether as a complement to, or substitute for, academic credentials for veterans aspiring to a cybersecurity career.

Additionally, the national attention to the need for cyber-workers has encouraged many government and private sector initiatives to provide the necessary training or "upskilling." These range from formal education to boot-camps to on-the-job advancement.

REFERENCES

[1] A. Zaharia, "35+ initiatives to get more women into cybersecurity," *Comparitech*, March 31, 2021.

[2] Carnegie Endowment for International Peace, "Priority #4: Cybersecurity Workforce Challenges," *International Strategy to Better Protect the Financial System Against Cyber Threats,* November 18, 2020.

[3] C. Franklin Jr., "How to Decipher InfoSec Job Titles' Mysteries," *DarkReading*, July 29, 2020.

[4] Cybersecurity Guide, "Veteran's guide to a cybersecurity career," *Cybersecurity Guide,* May 5, 2020.

[5] Department of Labor (DOL), U.S., "Apprenticeships," *Employment and Training Administration.*

[6] M. Henriquez, "Addressing the Cybersecurity Skills Shortage Through Upskilling and Retention," *Security Magazine,* December 3, 2019.

[7] N. A. Mack, K. Womack, E. Huff, R. Cummings, N. Dowling, and K. Gosha, "From Midshipmen to Cyber Pros: Training Minority Naval Reserve Officer Training Corp Students for Cybersecurity," *SIGCSE '19: Proceedings of the 50th ACM Technical Symposium on Computer Science Education,* February 27, 2019, pp. 726–730.

[8] National Research Council, "Professionalizing the Nation's Cybersecurity Workforce?" *Criteria for Decision-Making,* The National Academies Press, 2013.

[9] National Cyber League (NCL), "NCL Individual Game Scouting Report," 2020.

[10] National Initiative For Cybersecurity Education (NICE), "NICE Strategic Goals," *Information Technology Laboratory / Applied Cybersecurity Division,* April 19, 2021.

[11] National Institute of Standards and Technology (NIST), "Cybersecurity Apprenticeships," 2018.

[12] Purdue University, "Purdue Cyber Apprenticeship Program," *Purdue University,* 2021.

[13] R. Petersen, D. Santos, M. Smith, K. Wetzel, and G. Witte, "Workforce Framework for Cybersecurity (NICE Framework)," *NIST Special Publication 800-181 Revision 1*, November 2020.

[14] Task Force on Apprenticeships, "Final Report to: The President of the United States," *Task Force on Apprenticeship Expansions,* March 10, 2018.