Abstract

Across public and private sectors, there is a growing demand for qualified cybersecurity professionals. Finding those individuals with the necessary knowledge, skills, and abilities (KSAs) to fill vacant positions has proven to be difficult. This article examines the chasm between demand and supply in the cybersecurity labor market. It looks at the professional competencies established by the federal government to help align industry cyber needs with education and training initiatives and offers suggestions to enhance the partnerships between academia, industry, and professional associations that will improve the KSAs of undergraduates who will soon enter the cybersecurity workforce.

Since 2007, the demand for cybersecurity professionals has risen dramatically. The cause is likely due to multiple factors (e.g., greater connectivity, more vulnerabilities, increased intruder awareness of the value of attacking networks, and heightened public awareness of successful attacks) [14]. According to Burning Glass Technologies, cybersecurity job postings grew 74 percent from 2007-2013, more than twice the rate of all other information technology (IT) jobs [3]. They also took 36 percent longer to fill than all job postings [3]. Last year, Cisco estimated an industry shortage of more than one million security professionals worldwide [4]. A recent Ponemon Institute survey of 504 human resources and IT security specialists in the United States found that the IT security function in most organizations was understaffed, with 70 percent of the respondents reporting that they had neither the depth nor breadth of qualified security professionals [21]. In January 2015, ISACA conducted a global survey of 3,439 business and IT professionals in 129 countries [12]. Ninety percent of the respondents said there was a national shortage of skilled cybersecurity professionals [21]. Another survey conducted earlier this year [13] seemed to corroborate this. More than half of the 926 respondents reported that it took their organizations anywhere from three to six months to fill an open position, and that fewer than 25 percent of the applicants were qualified to fill the positions for which they applied.

The demand for cybersecurity professionals is projected to intensify over the next several years, largely due to the increasing sophistication and persistence of cyber threats, and...
While billions of dollars are being spent on new technologies to secure the US Government in cyberspace, it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success. However, there are not enough cybersecurity experts within the Federal Government or private sector to implement the CNCI, nor is there an adequately established Federal cybersecurity career field. Existing cybersecurity training and personnel development programs, while good, are limited in focus and lack unity of effort. In order to effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees. It will take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950s, to meet this challenge [6].

In 2010, in response to CNCI Initiative #8, the National Initiative for Cybersecurity Education (NICE) was established. Led by the National Institute of Standards and Technology (NIST), NICE consists of more than twenty federal departments and agencies. To achieve its mission of enhancing the overall cybersecurity posture of the United States, NICE has three goals: To increase national cybersecurity awareness, to expand the pool of individuals prepared to enter the cybersecurity workforce, and to develop a globally competitive cybersecurity workforce [17].

NICE National Cybersecurity Workforce Framework

The foundation of the NICE effort to standardize the cybersecurity field is the National Cybersecurity Workforce Framework [8]. Version 1.0, released in August 2012, organized cybersecurity into seven high-level categories, each comprised of several specialty areas. Related job titles, tasks, and KSAs needed to successfully complete those tasks were further de-
Improving Cybersecurity Workforce Capacity and Capability | Marie A. Wright

<table>
<thead>
<tr>
<th>Categories</th>
<th>Specialty Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Securely Provision</strong></td>
<td>Secure Acquisition&lt;br&gt;Secure Software Engineering&lt;br&gt;Systems Security Architecture&lt;br&gt;Technology Research and Development&lt;br&gt;Systems Requirements Planning&lt;br&gt;Test and Evaluation&lt;br&gt;Systems Development</td>
</tr>
<tr>
<td><strong>Operate and Maintain</strong></td>
<td>Data Administration&lt;br&gt;Customer Service and Technical Support&lt;br&gt;Network Services&lt;br&gt;System Administration&lt;br&gt;Systems Security Analysis</td>
</tr>
<tr>
<td><strong>Protect and Defend</strong></td>
<td>Enterprise Network Defense Analysis&lt;br&gt;Incident Response&lt;br&gt;Enterprise Network Defense Infrastructure Support&lt;br&gt;Vulnerability Assessment and Management</td>
</tr>
<tr>
<td><strong>Investigate</strong></td>
<td>Digital Forensics&lt;br&gt;Cyber Investigation</td>
</tr>
<tr>
<td><strong>Oversee and Govern</strong></td>
<td>Legal Advice and Advocacy&lt;br&gt;Strategic Planning and Policy Development&lt;br&gt;Training, Education, and Awareness&lt;br&gt;Information Systems Security Operations&lt;br&gt;Security Program Management&lt;br&gt;Risk Management&lt;br&gt;Knowledge Management</td>
</tr>
<tr>
<td><strong>Collect and Operate</strong></td>
<td>Collection Operations&lt;br&gt;Cyber Operations&lt;br&gt;Cyber Operations Planning</td>
</tr>
<tr>
<td><strong>Analyze</strong></td>
<td>All Source Intelligence&lt;br&gt;Exploitation Analysis&lt;br&gt;Targets&lt;br&gt;Threat Analysis</td>
</tr>
</tbody>
</table>

Table 1 – National Cybersecurity Workforce Framework

scribed within each specialty area [11]. By establishing a common taxonomy and lexicon for cybersecurity workers, and developing a baseline of tasks and KSAs associated with cybersecurity professionals [17], the framework defines cybersecurity work irrespective of organizational structure or job title, and is flexible enough to allow organizations to adapt its content to their own workforce planning needs [16]. In 2013, work began on updating the framework to reflect the latest changes in IT and the cybersecurity field. The most recent version of the framework is shown in Table 1. Source: “DRAFT National Cybersecurity Workforce Framework Version 2.0,” National Initiative for Cybersecurity Careers and Studies.¹

ETA Cybersecurity Competency Model

In 2013, the Employment and Training Administration (ETA) of the US Department of Labor began working with the more than twenty federal departments and agencies that contributed to the

Improving Cybersecurity Workforce Capacity and Capability | Marie A. Wright

1 – Industry security professionals and board members from regional chapters of professional security associations should volunteer to be guest speakers in the IT and security classes offered at local colleges and universities. In spite of the fact that millennials (young adults, ages 18 to 26) have grown up in a digital environment, only one in four indicates an interest in a career as a cybersecurity professional [23]. Most students are uncertain about cybersecurity job responsibilities, and they need information, advice, and encouragement from others outside of the academic sphere. There is no more effective way to share career experiences, to influence individual career choices, or to emphasize the need for a stronger cybersecurity workforce, than to speak directly to those still in school.

2 – Security professionals from industry and board members from regional chapters of professional security associations should volunteer to serve as advisory board members for college or university departments that offer cybersecurity or information security courses. Active board participation is essential, and contributing to the advancement of cybersecurity education is equally important. Academic administrators listen to the feedback provided by external professionals, and they typically listen more carefully than they do to the information provided by their own faculty.

3 – Businesses should establish more paid internships and co-ops in cybersecurity. These offer the best of both worlds to businesses and to students. Businesses have the opportunity to hire, without obligation, knowledgeable and energetic individuals from local colleges and universities who are eager to contribute, and to do so at a (typically) lower pay scale on a short-term basis. Students have the opportunity to gain the practical, entry-level experience necessary for them to begin their cybersecurity careers, while earning much-needed money for their tuition expenses.

4 – Businesses should make a more concerted effort to donate their unused equipment to local colleges and universities that are trying to develop their cybersecurity programs. Academic institutions operate in the real world. They continually face budget cuts, and oftentimes funding that should go to improve the classroom learning environment instead becomes redirected toward administrative and operating expenses. Today, many publicly-funded universities receive less than 50 percent of their revenue from the state. Businesses can help by donating equipment they no longer need to colleges or universities for educational purposes. By doing so, businesses not only help students who may be aspiring cybersecurity professionals, they may be able to claim a tax deduction for their equipment donations as well.

5 – Business professionals and academics need to strongly encourage students to join professional associations, attend local chapter meetings, and network. Particularly for those on the cusp of starting their careers, “what you know” has to be supplemented with “who you know.” The benefits of professional association membership are well known to those already in the field, but students have not yet learned the advantages of developing professional relationships, being mentored, or having access to an array of resources and services that are offered only to members. Students need help in determining which of the many good security-related professional associations they should join. For example, by joining the ISSA, students could take advantage of the Cybersecurity Career Lifecycle (CSCL) program. As pre-professionals, they could do a self-assessment of their KSAs, which would help them to better understand what an aspiring professional needs to know to enter the field, as well as the types of industry roles they might be best suited to fill [20].

6 – All security-related professional associations should have low-cost student membership rates, and they should offer scholarships for student members who are studying cybersecurity. Some professional associations offer student memberships at reduced costs, but not all do. Even fewer offer student scholarships. Student membership in security-related professional associations might be better spurred if student financial needs were better understood. Since 2008, public colleges and universities nationwide have increased tuition by more than 27 percent to compensate for state funding cuts [19]. Most of the nation’s undergraduates hold jobs while going to college, but their financial needs were better understood. Since 2008, public colleges and universities nationwide have increased tuition by more than 27 percent to compensate for state funding cuts [19].

2 ISSA offers student memberships. The ISSA Education Foundation (issaef.org) awards annual scholarships and administers ISSA chapter scholarships, such as Denver and San Francisco chapters. In addition, several other ISSA chapters conduct their own scholarship programs.
Improving Cybersecurity Workforce Capacity and Capability

Strong understanding of the security field, having technical knowledge is important, recent studies [9][13] have suggested that other attributes, such as law. [15] Although technical knowledge is important, recent studies [14] have suggested that other attributes, such as having a broad understanding of the security field, having strong communications skills, and being able to understand the business, may be more important for success as a cybersecurity professional.

7 – Academics should encourage students to pursue certification. There are hundreds of cybersecurity-related certifications, and navigating through the confusing array can be a daunting challenge. To make the process easier, the National Initiative for Cybersecurity Careers and Studies (NICCS) developed a list of organizations that provide the professional certifications needed for entry or promotion in the cybersecurity career field [22]. The list supports NICE’s goal of facilitating the development of a globally competitive cybersecurity workforce. Certification standards can help academia to better align their cybersecurity curricula with current industry needs [24]; however, these standards have a training focus that should supplement, but not replace, education.

8 – Academics should employ a multidisciplinary approach to cybersecurity education. Traditionally, security courses and programs have been housed in Computer Science or Engineering departments, which necessarily emphasize highly-specialized, technical knowledge; however, cybersecurity is more than just a technical discipline. It is “a complex subject, whose understanding requires knowledge and expertise from multiple disciplines, including but not limited to computer science and information technology, psychology, economics, organizational behavior, political science, engineering, sociology, decision sciences, international relations, and law.” [15] Although technical knowledge is important, recent studies [9][13] have suggested that other attributes, such as having a broad understanding of the security field, having strong communications skills, and being able to understand the business, may be more important for success as a cybersecurity professional.

9 – Academics should incorporate realistic case studies and practical simulations into the cybersecurity curriculum. Classroom theory and hands-on practice have a reciprocal relationship, where one informs and reinforces the other. The case method, originally championed by the Harvard Business School, uses case studies to emulate realistic business challenges. The information provided is typically complex and insufficiently detailed, so students are challenged while their judgment and leadership skills are strengthened. In the case of simulations, learning occurs through hands-on actions, and preferred outcomes tend to be based on experience. The simulation environment provides constant and immediate feedback, so students can adjust their actions based on the information they receive. Both case studies and simulations are operational scenarios in which specific skills are learned and performance is evaluated within a realistic context. Mistakes will be made, and they often provide the best learning experiences.

10 – Industry professionals should work more closely with academia to sponsor mock cybersecurity competitions. Unlike large-scale competitions, such as the annual National Collegiate Cyber Defense Competition sponsored by the Department of Homeland Security Science and Technology Directorate’s Cyber Security Division, these mock competitions should be much smaller and should occur more frequently (e.g., monthly). They should have a practical, hands-on focus, but they should not require the high level of technical proficiency demanded by national cyber competitions in order to encourage as much student participation as possible, including those who are not majoring in Computer Science or IT. After all, students majoring in non-technical disciplines may have the right set of skills to become cybersecurity professionals [14].

Conclusion

Since 2007, the sharp increase in demand for cybersecurity professionals has been met with a relatively small increase in the number of individuals qualified to fill those jobs. In spite of the federal government’s initiatives to increase the supply of cybersecurity professionals, the labor market is tight and is projected to remain so for the next decade. It will take years to educate and train a sufficiently qualified workforce. In the meantime, there are actions that can be undertaken in partnership by industry, academia, and professional associations that can help to improve the capacity and capability of the cybersecurity workforce.

References

Today’s Warfighter requires the best tools to conduct combat in Cyberspace. Our field-proven and award-winning network security products ensure your critical data is safe from the inside out.

With solutions configured to Military-grade specs, you can deploy the fastest and most advanced network security platform on the market.

Call to Schedule Your Free Application and Risk Analysis of Your Network (571) 449-8375
fortinet.com/solutions/federal.html
Improving Cybersecurity Workforce Capacity and Capability | Marie A. Wright


[18] “Number of Agencies in the Federal Government” – [link]


About the Author
Marie A. Wright, PhD, is a Distinguished Professor of Management Information Systems at Western Connecticut State University. She has been actively involved in the field of information security for more than twenty-five years. She may be reached at wrightm@wcsu.edu.