Identifying Cybersecurity Potential Could More Quickly Grow the Cyber Workforce

By Rebecca Mulvaney

A recent Global Information Security Workforce Study projects that

1.5 million

more cyber professionals will be needed to meet growing, **world-wide demands by 2020**

47%

of organizations **cite lack of hands-on experience** as reason applicants are unqualified

the number of expected people who are **online doubles**

by 2020

What's Wrong with the Cyber Workforce?

The United States faces increasing threats, both defensive and offensive, in ensuring the cybersecurity of the nation. As adversaries become more aggressive in exploiting cyberspace to advance their agendas, posing imminent threats to national security, it is critical that the U.S. government has a cyber workforce that is sufficiently-sized and skillfully-capable. However, that is a critical challenge in today's environment. Nationwide and worldwide, there is an anemic pipeline of qualified workers to meet today's needs, much less the needs of tomorrow. A recent Global Information Security Workforce Study projects that 1.5 million more cyber professionals will be needed to meet growing, world-wide demands by 2020.[1] Given this reality, the federal government needs to effectively identify, recruit, train and retain cyber professionals to carry out its cyber operations.

Yet, even with increased efforts to attract and recruit cyber workers, reports indicate that less than half of the workers who apply for cyber jobs are qualified.[2] Individuals with the skills needed are in short supply and high-demand. Organizations are looking for individuals who have "hands-on"

[1] ISACA (2017). State of Cybersecurity 2017: Current Trends in Workforce Development. Author.; (ISC)²
2015 Global Information Security Workforce Study

[2] State of Cybersecurity: Implications for 2015: An ISACA and RSA Conference Survey

or practical experience, and can "hit the ground running". As such, 47 percent of organizations state lack of hands-on experience as the number one reason applicants are considered unqualified.[3] In addition to hands-on experience, organizations often include security certification requirements as part of their job qualifications.[4]

What are the ramifications of organizations continuing to require these types of qualifications in an industry that is just emerging and a candidate pool that is too small to meet demand? The answer is a workforce ill-equipped to manage organizational risks and costs associated with growing cybercrime and cyber espionage rates. Historic levels of cyber intrusions are currently being experienced, and that number will only continue to increase as the number of expected people who are online doubles by 2020.[5] Given these expected rises, annual global cybercrime costs are projected to reach $6 trillion in less than five years.[6]

How Should Organizations Respond?

Organizations, industry and the Federal government must change their approach to building their cybersecurity workforce. Some new approaches to recruit and train cybersecurity workers have been started through collaborations between educational institutions, industry and certification organizations, but these efforts will take a long time to bear fruit.[7] Kerry Anderson notes, "As a profession, we need to generate both near-term as well as long-term solutions to growing the cybersecurity workforce."[8]

Some of the near-term strategies that Anderson recommends are to seek individuals (internal or external to the organization) who may be interested in transitioning to cybersecurity occupations, and being less specific and restrictive in vacancy announcements. Both strategies suggest that individuals who may not have formal cybersecurity training, certifications

[3] ISACA (2017). State of Cybersecurity 2017: Current Trends in Workforce Development. Author.

[4] ISACA (2017). State of Cybersecurity 2017: Current Trends in Workforce Development. Author.

[5] Morgan, S. (December 2016). Summing up the Cybereconomy, and looking ahead to 2017. Retrieved on April 5, 2017 at http://cybersecurityventures.com/cybersecurity-and-cybercrime-statistics/.

[6] Morgan, S. (December 2016). Summing up the Cybereconomy, and looking ahead to 2017. Retrieved on April 5, 2017 at http://cybersecurityventures.com/cybersecurity-and-cybercrime-statistics/.

[7] Anderson, K (2016). Resolving the Cybersecurity workforce shortage. ISSA Journal, October 2016, 16-21.

[8] Anderson, K (2016). Resolving the Cybersecurity workforce shortage. ISSA Journal, October 2016, 16-21.

or hands-on experience, but who possess the type of aptitudes and/or have obtained necessary security clearances needed for cybersecurity work could be trained up more quickly to provide an increased number of workers near-term and build an internal pipeline. Consequently, one way to address the serious cyber workforce shortfall is to identify individuals with "cyber-potential."

Who has Cyber-Potential?

To identify individuals who possess a propensity for cybersecurity work, organizations or agencies need an effective test of cybersecurity aptitude or cyber-potential. Cyber certifications and exams test for specific technical knowledge and skills, and thus have limited utility in differentiating candidates without prior cyber training and background. In addition, given the fast pace of the industry, knowledge tests also require constant updating to stay current with latest technology. Tests that measure general aptitudes are available, but they do not specifically target the capability domains that may be predictive of cybersecurity trainability and performance. Instead, organizations need a valid and reliable assessment that will measure candidates' propensity toward the key capabilities needed for success in cybersecurity. This type of assessment should measure key aptitudes within the context of cyber tasks. This approach does not require cyber knowledge, but will provide greater face validity and a realistic preview of the work to candidates. In addition, developing an agency-owned cyber aptitude test can be more efficient in two ways: (1) by avoiding per-candidate fees, which are typically associated with commercial off-the-shelf assessments; and (2) by enabling as many candidates to be tested as needed.

What Aptitudes Indicate Cyber-Potential?

The National Initiative for Cybersecurity Education (NICE) Workforce Framework outlines cybersecurity roles and competencies needed for each role; however, the competencies within the NICE framework focus on the various technical knowledges required to perform cybersecurity tasks. To evaluate cyber-potential for those who have not received formal cyber training, the focus must be on more fundamental competencies. Specifically, a test of cyber aptitude should focus on abstract thinking and problem solving capabilities that depend less on formal education and more on a person's natural inclinations. ICF has identified a preliminary list of capabilities to be measured in a cyber aptitude test. They include Complex Problem Solving, Active Learning, Critical Thinking, Proactive Thinking, and Problem Sensitivity. These critical aptitudes would underlie most, if not all, of the roles and competencies within the NICE framework.

Aptitude should focus on abstract thinking and problem solving capabilities that depend less on formal education and more on a person's natural inclinations. ICF has identified a preliminary list of capabilities to be measured in a cyber aptitude test.

Complex Problem Solving—Complex problems have multiple, interrelated factors, along with multiple goals that may compete with each other.[9] They evolve or change as one begins to address them, necessitating the person trying to solve them to continually seek out more information. Their solution requires planning and execution, and then repeating that cycle as the problem evolves.[10]

Cybersecurity problems typically meet the characteristics of a complex problem. For example, when an incident occurs in which an organization's systems are breached, cybersecurity professionals must examine multiple factors, including all of the computers, systems, and personnel actions that were taken. They have to balance the competing demands of investigating the problem to get to the root cause, while quickly implementing a solution to stop the flow of compromised data and protect the organization's systems. As they investigate the incident, they may also uncover new information that changes the nature or scope of the situation. For example, they may learn that a greater number of systems have been compromised or that PII (personally identifiable information) has been disclosed, which may change the solution or response that is needed.

Active Learning—Active learning is the discovery and application of new information. It is a critical capability for cybersecurity workers because of the rapidly changing nature of the cybersecurity environment, with new technologies being released continuously and new types of threats emerging daily. Cybersecurity workers must be willing and able to learn about "what's next" in terms of technology and how to apply that new technology to new types of threats. Thus, active learning is crucial to mission success.

Critical Thinking—Based on a comprehensive review of the critical thinking literature, we have developed and applied an integrated model of critical thinking that includes knowing what you know and how well you know it, knowing when and how to apply cognitive strategies, identifying an issue, assessing the value and relevance of information with respect to the issue, and identifying and evaluating the assumptions underlying information received.[11] Critical thinking is integral to cybersecurity work. For example, when defending networks, if malware is detected, cybersecurity professionals must analyze its capabilities, examine how its capabilities compare to the defenses that are already in place, and determine what actions need to be taken to protect the organization from the malware.

[9] Funke, J. (2012). Complex problem solving. In N.M. Seel (Ed.), Encyclopedia of the sciences of learning (pp. 682–685). New York: Springer.

[10] Zhang, B., Li, J., Drasgow, F., Zhang, H.C., & Liao, T. (2016). Complex problem solving: Development and validation of a game-based measure. Under review.

[11] Curnow, C., Mulvaney, R., Parish, C., Calderon, R., Matamala, A., & Deares, J. (2008). Deep learning and critical thinking measures: Scientific basic interim report. Center for Army Leadership.

Proactive Thinking—Proactive thinking or proactive personality is an individual's willingness or propensity to take actions to improve a situation.[12] Unlike the first three critical cyber aptitudes, proactive thinking may be an important competency for cybersecurity professionals who are involved in development (e.g., programmers, engineers) as they seek to develop solutions that will improve security. Consequently, this aptitude can be used to differentiate for which type of cybersecurity roles an individual may be most suited.

Problem Sensitivity—Before a problem can be solved, it must first be identified. Problem sensitivity is the ability to detect when something is wrong or when something is likely to go wrong.[13] Cybersecurity professionals engaged in defense of networks must monitor the security of networks and the security applications installed in those networks to detect problems. As such, problem sensitivity is a critical capability for defense and exploitation roles.

How Can Organizations Test for Cyber-Potential?

Assessment Types/Technology

Through cyber aptitude assessments, agencies can evaluate whether workers in their current workforce would be well-suited for cyber jobs. Since current employees are well-vetted, both in security and performance aspects, these workers are a potentially valuable source of cyber workers. To evaluate these workers, we recommend leveraging advances in new assessment technologies, namely high-fidelity simulation gaming techniques that are more engaging for test-takers, to develop a cyber aptitude test that efficiently and effectively measures the types of capabilities that indicate cyber potential. High-fidelity assessments provide an immersive experience that allows test-takers to get a realistic preview of the job to assess job fit. In our research, we have found that these types of assessments also brand the organization as cutting-edge and indicate its commitment to employing a high quality workforce.[14]

A high-fidelity simulation allows for a more in-depth assessment of the test-taker's underlying thought process in real-time when faced with complex situations. Simulations are highly applicable to the cyber environment, as cyber professionals are often inundated with large amounts of information at high speed. Simulations also enable the assessment of the test-taker's proclivity to learn cyber tasks.

[12] Bateman, T. S., & Grant, J. M. (1993). The proactive component of organizational behavior. Journal of Organizational Behavior, 14, 103-118.

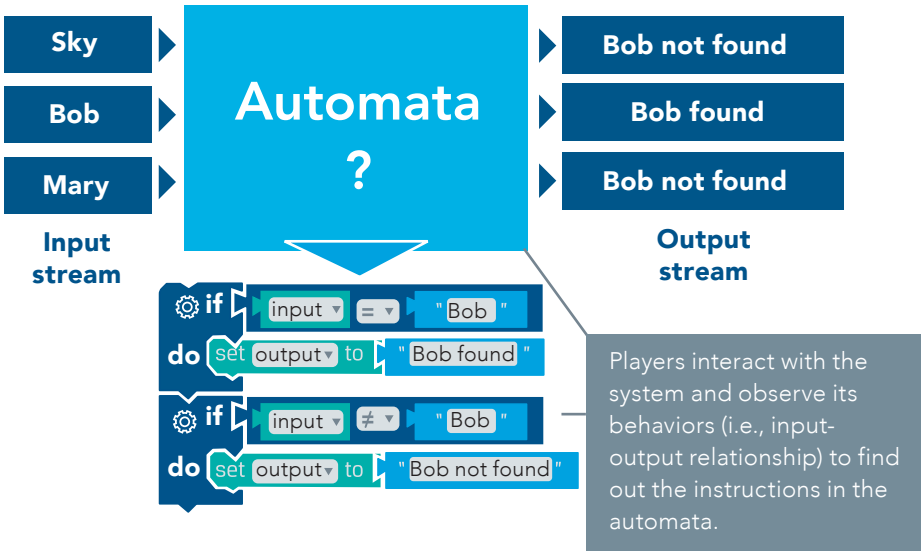
[13] Department of Labor (2017). Occupational Network: Abilities. Retrieved on July 26, 2017 from https://www.onetonline.org/find/descriptor/browse/Abilities/1.A.1/.

[14] Hatfield, J., Gurira, C., & Harvey, J. (2013). High Definition Animations: Enhancing Realistic Job Preview and Organization Perceptions. Symposium presentation given at the annual Society for Industrial/Organizational Psychology conference (April 12, 2013), Houston, TX.

The tasks in the simulation game would be simple or basic "cyber-like" tasks that would require minimal instruction to complete successfully and would not require prior cyber knowledge. The instructional information in the assessment could be used to "teach" test-takers what to look for when completing the task, thereby assessing their ability to quickly learn and apply new information and use their critical thinking skills in a cyber context.

One example scenario in the game might include some hidden objects (e.g., a server with a fictitious operating system), and the player may be directed to interact with the environment to find out about the objects. The test-taker would need to interact with the server to discern and assess its rules and algorithms. Once he or she acquires the new information, the test-taker would then need to apply the information to accomplish the task. Figure 1 shows a sample task from a high-fidelity simulation game where players get a "black box" problem and need to learn about how a specific system functions by observing the input-outputbstream (i.e., they can input anything into the operating system and based on theboutput they will need to figure out the underlying instructions in the automata[15] of the system).

FIGURE 1. SAMPLE SIMULATION TASK ON ACTIVE LEARNING



[15] Automata is defined as something that acts automatically without an external force. Retrieved on November 1, 2017 from Dictionary.com.

Figure 2 shows another sample high-fidelity simulation game task where players are provided information on the properties and restrictions of different computing devices. Then, players are given information on several automata and are asked to evaluate and determine which device would be most appropriate for the automata. Players indicate their response by dragging and dropping the automata into their appropriate device. This type of scenario would assess critical thinking skills.

FIGURE 2. SAMPLE SIMULATION TASK ON CRITICAL THINKING

Mobile Device

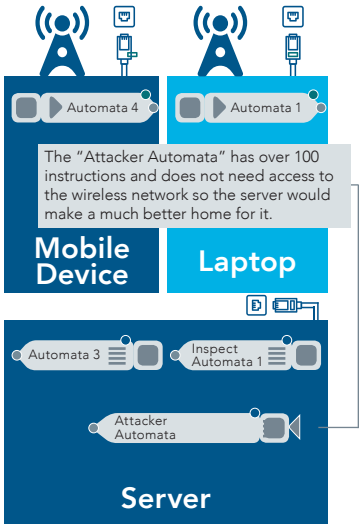
- Can only run a small amount of automata, has access to WiFi
- Automata limited in number of instructions it can use
- Automata limited in the number of variables it can use (low memory)

Laptop

- Can run a medium amount of automata.
- Automata can use significantly more instructions
- Automata use significantly more vatiables
- Has access to WiFi and possibly wired networks

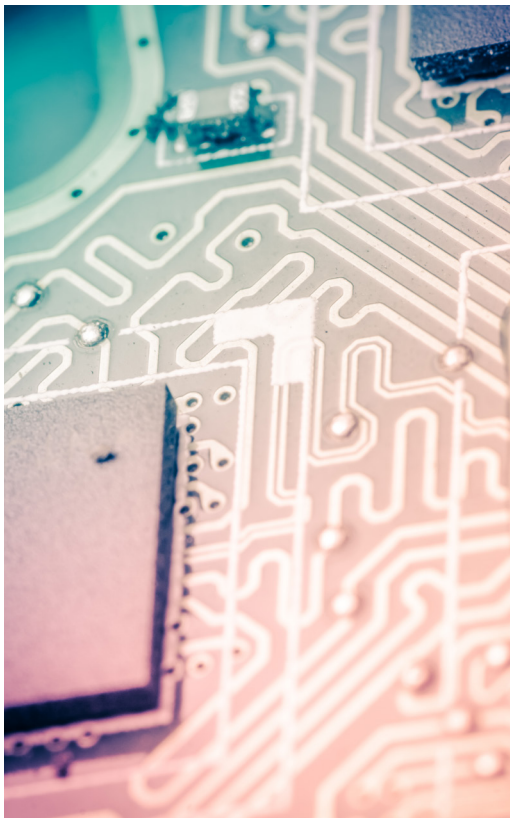
Server

- Can run a large amount of automata
- Automata can use almost infinite amount of instructions
- Automata can use almost infinite amount of variables
- Only has access to wired networks, but has multiple network ports increasing the amount of data it can handle on the network



Assessment Development Process

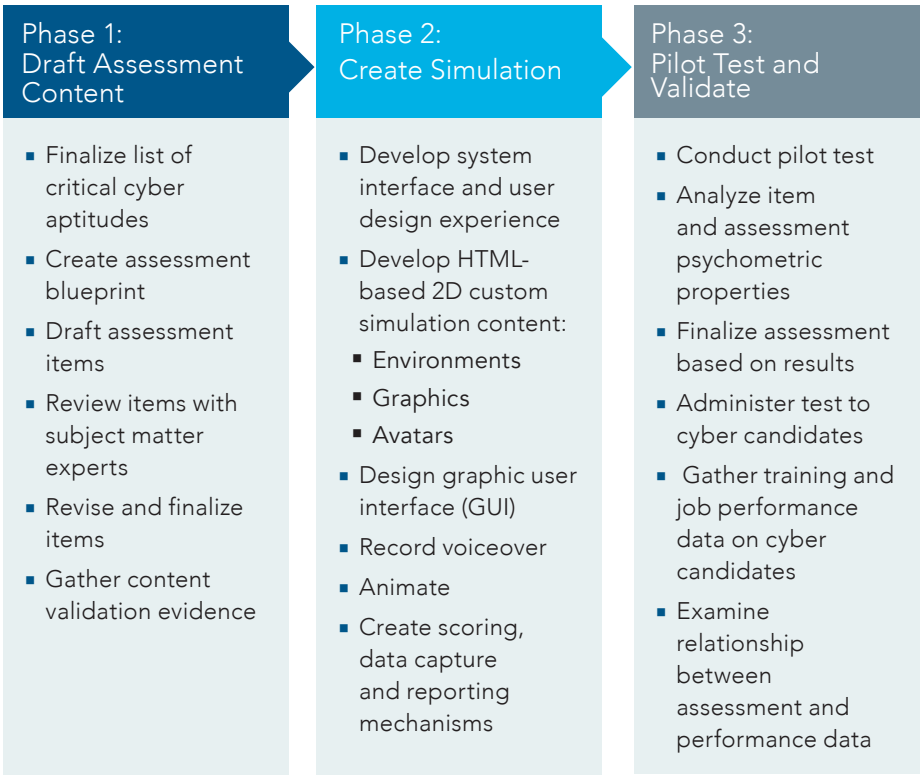
Figure 3 summarizes ICF's overall test development and validation process for developing a cyber aptitude test using the high-fidelity simulation gaming techniques approach. This process begins by working in close collaboration with the client organization to identify any additional aptitudes or competencies required for the cyber roles in the organization. Once the full list of aptitudes is determined, our process relies on both ICF assessment experts and subject matter experts to draft and refine content that will enable the assessment of those aptitudes. Next, ICF's



simulation and modeling team develops the simulation system interface, art assets, game mechanics, and scoring and data capture mechanisms. The last phase of the process focuses on evaluating the functioning and effectiveness of the assessment by conducting a pilot test and analyzing the psychometric properties of the assessment. Then, we administer the test to employees, and track those who are selected through their training and performance on the job to examine the relationship between scores on the assessment and how well they perform as cyber workers. If you are interested in this process and developing a cyber aptitude test for your organization, ICF offers:

- Robust test development and validation expertise to develop innovative, client-proprietary assessment tools, including high-fidelity simulation. We have developed assessments for over 100 job classes, ranging from technical to managerial jobs, and we specialize in high-quality assessments that include computer animation and/or video components. Our assessment experts work hand-in-hand with ICF's award-winning multimedia studio and graphic artists to create test items that simulate an endless range of situations.
- In-house cyber expertise and deep domain reach-back capability. The ICF team includes world-class cyber experts who have in-depth understanding of cyberspace requirements. ICF's cyber team represented the U.S. in the Global CyberLympics World Finals where they took second place. This technical reach-back capability will augment our cyber aptitude understanding, allow us to create face-valid assessments, and facilitate a more efficient process that enables the rapid development of the cyber aptitude test.

FIGURE 3. ICF'S APPROACH FOR DEVELOPING A CYBER APTITUDE SIMULATION ASSESSMENT



What Does this Approach Get You?

By partnering with ICF to create a custom cyber aptitude assessment, your organization can tap into another rich source for cyber workers, and build your own, internal, cyber workforce pipeline. Assessing interested employees from within your own organization enables you to quickly find cyber workers who already have cleared security requirements and who are strong performers. In addition, by looking for specific aptitudes, you can target those cybersecurity roles you may be missing. This approach also enables you to more quickly train and certify cyber workers without having to go through the lengthy hiring process. Lastly, by identifying current employees with cyber-potential and using on-the-job training, you increase your current capacity, while simultaneously developing the in-house cyber expertise you need. To talk about this approach in more detail or to learn how to partner with ICF to develop a custom cyber aptitude simulation assessment, please contact us.

Identifying Cybersecurity Potential Could More Quickly Grow the Cyber Workforce

Visit us at icf.com/cyber

For more information, contact:

Rebecca Mulvaney
rebecca.mulvaney@icf.com +1.703.934.3582

twitter.com/ICF
linkedin.com/company/icf-international
facebook.com/ThisIsICF

About ICF

ICF (NASDAQ:ICFI) is a global consulting services company with over 7,000 full- and part-time employees, but we are not your typical consultants. At ICF, business analysts and policy specialists work together with digital strategists, data scientists and creatives. We combine unmatched industry expertise with cutting-edge engagement capabilities to help organizations solve their most complex challenges. Since 1969, public and private sector clients have worked with ICF to navigate change and shape the future. Learn more at **icf.com**.