ACCENTURE FEDERAL SERVICES

U.S. Department of Commerce

Cybersecurity Workforce RFI

August 02, 2017

Submitted to:
cybersecurityworkforce@nist.gov

Submitted by:
Accenture Federal Services, LLC
800 N. Glebe Road, Suite 300
Arlington, VA 22203-2151

Stefano Maci
Contracts Manager
Accenture Federal Services
Phone: 571-317-6450
Email: Stefano.Maci@accenturefederal.com

Table of Contents

1.0 Background

The National Institute of Standards and Technology (NIST), a non-regulatory agency within the U.S Department of Commerce, has led public and private sector collaboration to develop and iterate the NIST Cybersecurity Framework (CSF) since Executive Order 13636 (*Improving Critical Infrastructure Cybersecurity*) signed on February 12th, 2013. With Executive Order 13800's signature (*Strengthening the Cybersecurity of Federal Networks & Critical Infrastructure* on May 11th, 2017), recommended best practice has now become policy, and NIST is remobilizing public and private sector thought leaders to respond to the workforce development component of the mandate.

Accenture has supported the Department since 1994 in diverse capacities and shares NIST's commitment to U.S. innovation and industrial competitiveness through measurement science, standards, and technology advancements. The firm has gained cross-industry experience assessing public and private sector clients' enterprise cybersecurity posture and successfully implementing CSF-aligned transformations.

NIST is surveying the cybersecurity community to create a composite of recommendations from the most salient and actionable insights about developing, growing, and sustaining a future-ready public and private sector cybersecurity workforce. Each question in the recently-published Request for Information (RFI) addresses a facet of NIST's complex information needs and highlights stakeholders' responsibilities to support mandate execution. Government (at the local, state, and federal levels), providers (of education, training, and technology), as well as private industry have critical roles to play in realizing this common goal.

By evaluating the adequacy and enforcement of their organizational cybersecurity development, education, and training policies, government and private industry can identify and remediate deficiencies. Technology providers in particular, can share expertise regarding the anticipated effects of technological advances on the cybersecurity workforce. Analyzing cybersecurity education, training, and workforce development efficacy metrics may identify re-creatable and scalable successes as well as avoidable shortcomings. Identifying program material collection, organization, and sharing improvement opportunities may lower access barriers, consequently increasing audience reach. Assessing cybersecurity workforce category, specialty area, role, and knowledge-skill-ability (KSA) definitions for consistency as well as necessary variations by industry and sector will identify where necessary variations exist by industry and sector as well as determine standards for building a talent pipeline.

2.0 Executive Summary

82% of employees say they expect digital to transform their work in the next three years[1]. 92% of executives say it is important or critical to take actions now to transition their workforce to succeed in the digital economy[1].

In the next five years security professionals will increasingly use more artificial intelligence, automation, and other digital capabilities to predict, detect, respond to and remediate digital attacks. Enterprises will rely on new, more flexible staffing models to make sure they have the top security expertise they need, when they need it.

These changes will enhance and scale the security workforce's capabilities to address the growing threat and diversity of digital attacks that enterprises can expect in the coming years. Their combined impact will fundamentally affect the careers and workday lives of security professionals.

However, technology alone can never resolve all of an enterprise's security threats. To carry out effective cyber hunting, which requires organizations both to understand the full scope of a breach and to seek out indications of

breaches as yet undetected, enterprises need to take a "people first" approach. That means focusing not only on attracting highly skilled resources, which remain in short supply, but also further developing the skills within their current workforce. Security-focused executives need to understand and prepare for the change that's coming in order to position their organizations to survive in the rapidly evolving digital age[3].

3.0 Considerations for Cyber Workforce Development

3.1 Design and deploy an effective cybersecurity talent ecosystem

An analysis from the U.S. Bureau of Labor Statistics showed that there were 209,000 cybersecurity-related jobs that were unfilled in the United States during the calendar year 2015[5]. Additional reports indicate the global cybersecurity workforce shortage is expected to reach 1.5 million by 2019[8]. The Center for Strategic and International Studies alongside with Intel Security surveyed corporate and government IT professionals, finding that an overwhelming 71% stated that the talent shortage was already starting to cause direct and measurable damage to their organizations[13].

Simultaneously, in 2015, the millennial population surpassed Generation X in the U.S. workforce[6].

Organizations can take actions now, to build the cybersecurity talent ecosystem with the surging population of millennials:

- Partner with community colleges and universities – Strategically target universities in locations aligned with data center buildout plans and vice versa. Invest in the development of curriculum and delivery of training to influence the training of up-and-coming talent. Accenture has formal alliances with academic institutions to conduct joint research and apply cutting edge solutions to tackle real-world business challenges. For example, Accenture has established programs with:
    - Massachusetts Institute of Technology (MIT) – creation of a Analytics Innovation Consortium—an exclusive network of chief analytics officers, subject matter experts at MIT and Accenture, to discuss emerging trends in analytics and shape future alliance research projects[12].
    - Duke University – Duke graduate and undergraduate students who participate in the program closely collaborate on campus with Accenture professionals, and focus on jointly developing new advanced analytics solutions to address real-world business challenges[11].

  In addition, Accenture is also in the beginning stages of forging a relationship with Armstrong State University (ASU) for continued cyber education. ASU provides opportunity to gain competency and skills in cybersecurity through its Center for Applied Cyber Education (CACE). The school offers degrees such as Associate of Science degree with a Certificate in Cyber Security, Bachelor of Science in Criminal Justice with an emphasis on Cyber Crime/Digital Forensics, Bachelor of Information Technology with an emphasis on Cyber Security[10].

- Employ students and transitioning career professionals for internships and apprenticeships – A recent US College Graduate Engagement Study shows that 79% of those surveyed participated in an internship, co-op or apprenticeship; of those who participated, 67% claimed it led to a job post-graduation[4]. Cybersecurity executives can leverage university students or career professionals, who are transitioning from a different background, to gaps in entry-level skills in their current cyber

workforce. High-performers can be coached up the skill curve to fill more complicated and proficient cyber roles as they build their relationship and loyalty to the organization.

- Hold events to crowdsource talent to solve typical problems – hackathons or coding challenges can be a great way to get schools and the community involved in solving even complex security problems. In parallel, it also serves as a source to identify potential talent. Identify one or two critical security challenges within your organization and partner with universities and also high schools to get students engaged in the problem-solving. This serves as an opportunity to build a relationship directly with students and 'sell' them on the organization's mission and culture.
- Partner with state and local governments and communities to create educational and vocational programs for students, working professionals seeking new skills, transitioning or current military family and family members in the area of cybersecurity.
- Find opportunities to cross-train talent with different backgrounds to expand further the talent pool – In the market "certifications" or college degrees in the technical field are often cited as proof of competency, however that is often not the case. The Department of Defense (DoD) is planning on replacing the DoD Directive 8570, which provides a baseline of information assurance certifications and training, with a new directive, DoD 8140, which emphasizes job experience and skills over certifications[7]. This directive change will take the focus off of recruiting for certifications, and allow for more successful recruiting methods such as assessing aptitude and gamification.

3.2 Apply analytics and artificial intelligence to transform the security workforce

70% of CIOs plan to invest significantly more in artificial intelligence than they did in 2013[2].

Data, analytics, and artificial intelligence are fundamentally changing the kinds of work people do and the style of working they adopt as they attempt to keep the company's digital assets safe from encroaching attackers. These trends will have a pronounced impact on the ways security professionals approach their jobs. Understanding the probable implications of these changes will help security leaders position their organizations for success over the next five years.

Accenture's Cyber Defense Platform (ACDP) includes components by Splunk, to gather data for security analytics based on underlying queries that detect malicious activities. In addition, Splunk User Behavior Analytics helps find known and unknown threats through machine learning and peer-group baselining analytics.[9]

Such models will allow security teams to shift from simply detecting risks to actively identifying threats and enabling automated responses to the activity. Essentially analytics and intelligent automation will turn a proficient analyst into a highly skilled one. By combining AI with security function automation, it becomes possible to either fully or partially automate and guide the process—to the point where ancillary tasks become trivial to execute, thus enabling staff to concentrate on major threats instead of minor issues, and scaling the effectiveness of resource-constrained security organizations.

By standardizing excellent performance with automation, companies can begin to get their arms around the growing shortage of skilled security people[3].

3.3 Leverage sourcing partners for standard security operations functions

Keeping pace with best practices and technology in the security industry is a daunting task. According to Accenture's 2016 High Performance Security Research, nearly 1,000,000 variants and vulnerabilities arrive daily. Organizations must find an effective sparring partner to improve security capabilities, and combat challenges such as:

- decreasing the half-life of solutions due to rapidly evolving technology,
- evaporating boundaries, requiring access to resources and data anywhere on the planet,
- declining budgets, and
- typical time to hire, in government agencies, ranging from 6 to 9 months.

Building and managing a security infrastructure is costly in terms of both resources and time, as it requires both complex and rapidly outdated technology infrastructure and applications and significant management resources. Organizations typically also do not view security capabilities as a business differentiating, value-added service.

Managed security operations reduces both the cost and complexity associated with security solutions by delivering effective managed operations in partnership with top specialty providers—freeing up resources so organizations can focus on the core business.

Managed security providers maintain a large capacity of adept professionals with deep knowledge and experience, combined with key alliances with best-in-class vendors.

Accenture Security and its partners such as, Amazon Web Services (AWS) and Microsoft Azure, solely differentiate based on security capabilities. These organizations focus resources on security capabilities in a way that is unmatched by the companies they serve (e.g., through investments in advanced machine learning, proactive hunting, etc.). By leveraging the cloud, elastic computing, and software defined networking, managed security operations open the door for a reality where a proactive security posture and concepts such as scaling up and down, pay per use, are possible.

Federal agencies must make bold decisions to focus resources on the core mission work to deliver business outcomes while forging alliances with technology providers who excel daily at defending and protecting the vast enterprise. More specifically, federal agencies must take advantage of cloud computing's standardization and automation to create more secure, defensible environments for mission systems and data.

4.0 Conclusion

To prepare for this security workforce of the future, organizations need to assess where they stand today. Despite the cybersecurity investments public and private sector organizations are making, attack sophistication is increasing and costs in the aftermath are steeply rising. A reactive approach is not enough to keep pace with threats. Organizations need to proactively design and deploy mission-oriented cybersecurity strategy that is forward-looking as well as an aligned operating model that is robust and responsive. When considering intelligent automation applications, companies should determine which security functions are currently staff time-sinks—repetitive and low-impact activities that nonetheless help to sustain security and which functions address the most significant

cybersecurity threats to their business, and align skills to those core capabilities in order to target cybersecurity talent with those skills in their recruitment efforts.

They can evaluate the areas of security where the organization has traditionally struggled to find sufficient staff; those parts of security that require short-term but highly skilled professionals; or, those that would benefit greatly from access to a larger perspective of the data. Leaders should also actively pursue partnerships with local communities and universities to identify and recruit talent early-on through short-term programs/events, internships, and apprenticeships.

5.0 About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology, security, and operations. We combine unmatched experience and specialized skills across all industries and all business functions, underpinned by the world's largest delivery network. With more than 401,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. In the U.S. Federal space alone, Accenture has over 9,000 resources dedicated to serving the specific needs of government agencies to deliver mission outcomes and to serve our nation.

Accenture understands the U.S. Department of Commerce, its work, and its mission, having supported the Department since 1994. Accenture is the lead integrator on the Department of Commerce's Shared Service Human Resources Initiative providing an innovative, flexible, and extensible human resources information technology and operations platform. Accenture also provides software development and product implementation to integrate Commerce's eight financial systems into the Departmental Core Financial Management System, to be accessed with a single graphical user interface. In addition, Accenture supports the U.S. Census Bureau by providing innovative digital transformation capabilities, advanced analytics, dissemination services, and technical integration solutions supporting the upcoming 2020 Census. Like the National Institute of Standards and Technology (NIST), we aim to provide advanced technologies to enhance the U.S. government and the quality of life of citizens and residents. We are committed to bringing U.S. government agencies to the forefront of technology and innovation, and we welcome the opportunity to help NIST realize and advance their priorities and values.

6.0 References

[1]Accenture Being Digital Survey 2015

[2]Accenture Technology Vision 2016

[3]Accenture Security Technology Vision 2016

[4]Accenture Strategy 2016-2017 U.S. College Graduate Employment Study

[5]S. Olyaei, M. Coleman, M. Stamper, Gartner, Adapt Your Traditional Staffing Practices for Cybersecurity, January 10, 2017

[6]Pew Research, U.S. Labor Force by Generation, 1995 – 2015

[7]GovTech Works, New Directive Could Redefine Cybersecurity Certification, June 22, 2016

[8]FCW, https://fcw.com/articles/2016/11/29/cyber-talent-gap-comment.aspx, November 29, 2016

[9]Accenture Cyber Defense Platform Architecture Overview 2016

[10]Scheidt, Scott C., Center for Applied Cyber Education, Armstrong State University

[11]Accenture LLP, Press Release, Accenture and Duke University Collaborate on Analytics Research, August 13, 2016

[12]Accenture and MIT Alliance in Business Analytics, 2014, https://go.accenture.com/AccentureMITalliance

[13]Frost & Sullivan, The 2015 (ISC)2 Global Information Security Workforce Study