5-2018

The Significance of Professional Associations: Addressing the Cybersecurity Talent Gap

Calvin Nobles
William Woods University, calvin.nobles@willamwoods.edu

Darrell Burrell
Florida Institute of Technology, dburrell@email.phoenix.edu

The Significance of Professional Associations: Addressing the Cybersecurity Talent Gap

Calvin Nobles, PhD
William Woods University
calvin.nobles@willamwoods.edu

Darrell Burrell, DHEd
Florida Institute of Technology
dburrell@email.phoenix.edu

Abstract

The cybersecurity professional scarcity is endangering organizations from combatting unrelenting cyber threats. The shortage of cyber talent highlights the urgency for entry standards into cybersecurity to enrich the professionalization. Researchers and practitioners provide countless recommendations for improving the cybersecurity workforce by addressing the professionalization issue. Professional associations are the nexus of cybersecurity and possess the expertise, leadership, and sustenance to spearhead efforts to develop national-level strategies to resolve the talent gap and establish professionalization standards. Failure to resolve the cybersecurity workforce shortage perpetuates existing underperformances and prevents organizations from attaining optimal security preparedness. Professional associations have the wherewithal to lead the development of a national-level strategy to increase the number of cybersecurity professionals to meet the workforce demands.

Keywords: Cybersecurity, Professional Associations, Talent, Cyber Threat Landscape, Complex Adaptive System, Professionalization

Introduction

A litany of surveys, reports, and studies have indicated a shortage of cybersecurity professionals, which is a global problem, resulted in energizing extensive recruitment projects and academic partnerships to increase the number of cybersecurity professionals (Cobb, 2016). The dynamic cybersecurity threat environment coupled with the increasing cost of cybercrime is forecasting a cost of $400B a year (Spidalieri, 2016). The continuous development of new technology encourages malicious actors to engage in nefarious activities, which increases unpredictability in the cybersecurity space (Cobb, 2016; Dutta, Geiger, & Lanvin, 2015; Keely, 2017; Spidalieri, 2016). Keely (2017) indicates that phishing, spearphishing, ransomware attacks, social engineering, and malware are primary threat vectors used by malicious cyber actors. Organizations are struggling to find the correct balance between technology, processes and people as malicious cyber actors have the strategic advantage in executing attacks because cybersecurity defense continues as a reactive mechanism to nefarious activities (Henshel, Cains, Hoffman, & Kelley, 2015). Organizations suffer from the shortage of cybersecurity professionals, technological vulnerabilities and dependency, and increasing response times between the attack and initial response (Spidalieri, 2016). Cobb (2016) asserts that the shortage of cybersecurity professionals globally could exceed one million; consequently, resulting in the weakening of security preparedness and distrust in information security capabilities. According to Cobb (2016), the uncertainty surrounding the cybersecurity professional shortage requires

empirical research to assess the problems holistically. Professional associations are centrally positioned within the cybersecurity nexus to lead and strategically identify critical skills shortages, the professionalization of cybersecurity, discover innovative pipelines, and compose an accurate assessment of the talent shortage. The purpose of this paper is to discuss the significant role of professional associations in addressing the talent shortage in cybersecurity.

Complex Adaptive Systems

The cybersecurity domain consists of sociotechnical systems, known as a system of systems; the systems include technology, processes and procedures, people, organizations, compliance, operations, and the threat environment (Eldardiry & Cladwell, 2015; Keely, 2017; Nobles, 2016). Organizations within the system of systems are institutions of higher learning, certifying organizations, professional associations, governments, industry, and non-profit entities (Knapp, Maurer, & Plachkinova, 2017). In question is the educational and academic component that requires transformation to increase the number of cybersecurity personnel. Researchers and practitioners identified the following areas that influence certifying examinations: technology changes, threat landscape, industry standards, workforce requirements, and government and regulations (Knapp, Maurer, & Plachkinova, 2017). The systems are interdependent of other components; therefore, modifying one component could impact other systems. Eldardiry and Cladwell (2015) postulate that any system or the linkages between components are susceptible to vulnerabilities or weaknesses based on changes such as the threat environment is dynamic and capricious (Keely, 2017), resulting in changes to system calculus. From a macro perspective, as organizations adapt to the threat environment, it increases the demand for cybersecurity professionals in which there is a recognizable scarcity of cyber personnel (Cobb, 2016). The paucity of cybersecurity professionals impacts the system and induces complexity. A common practice is for organizations to leverage new technology; however, information technology professionals struggle to maintain pace with the technological changes (Eldardiry & Cladwell, 2015). By using the complexity theory perspective, according to Scioli (2017), one can comprehend the behavior of complex systems and associated components.

The complexity theory was used by scientists to understand mathematical construct to determine system behavior (Scioli, 2017). Researchers indicate that complexity leadership is capable of initiating scholarship and education, modernism, and transformation of institutions and systems (Geer-Frazier, 2014). Drack (2009) and Iosim (2016) highlight a principal objective in the complexity theory, emergence, which emphasizes to the ability to reduce complex entities in the natural world from the most basic form to the high hierarchical and complex structures (Mazzocchi, 2012). Researchers identified another critical aspect of emergence, the notion of feedback, which serves as the energy to propel the systems away from equilibrium; therefore, not aligning with previous research regarding system theory (Arsenault, Clayton, Peng, 2013). Complex adaptive systems are distinctive unrestricted systems that behave and act nonlinearly in an associated construct, which illustrates learning and evolving abilities (Kuziemsky, 2016). The system of systems in cybersecurity is non-linearly. The shortage of cybersecurity professionals is garnering negative feedback as Arsenault, Clayton, and Peng (2016) indicate and as depicted in Cobb's (2016) study.

The Shortage of Cybersecurity Professionals

In a recent study, Cobb (2016) referred to the many studies, reports, and surveys indicating a scarcity of cybersecurity professionals. There were 200,000 cybersecurity job vacancies in 2016 (Knapp, Maurer, & Plachkinova, 2017). Researchers forecast that by 2019 there will be a global deficiency of 1.5 million cybersecurity professionals (Knapp, Maurer, & Plachkinova, 2017; Wright, 2016) and Teoh and Mahmood (2017) postulate that the cyber personnel deficiency will exceed 3 million by 2021. A Ponemon Institute's research project surveyed 504 participants in which 70% of the respondents indicated a scarcity in cybersecurity talent while a 2015 ISACA study involving 3,439 participants from129 countries revealed that 90% reported cybersecurity personnel scarcities as a national-level issue (Wright, 2016). The National Initiative for Cybersecurity Education (NICE) led the National Institute of Standards and Technology and directly supported by 21 agencies is a body charged with increasing the cybersecurity workforce pool and manifesting an international competitive cyber workforce (Wright, 2016). To illustrate the complexity associated with cybersecurity jobs, the Department of Labor (2016) reported that "there are over 140 professional certifications from 30 certifying organizations that are relevant to the Information Security Analyst job description" (Wright, 2016, p. 102). Wright (2016) avows that cybersecurity is unique and unlike other domains that are concreted in long-standing practices while the cyber area is evolving at an unprecedented pace preventing routines and procedures from becoming ubiquitous. The implications of a rapidly changing field compel government, industry, academia, and professional associations to continually revamp existing education programs based on impacts to the threat landscape, technology, regulations, and processes and procedures. Another factor amassing the demand for cybersecurity professionals is cybercrime, resulting in a $400B industry for cybercriminals (Teoh & Mahmood, 2017) because organizations need additional personnel to safeguard against the mounting cybersecurity threats. The shortage of cybersecurity professional is burdensome to the other components; therefore, illustrating the need for professional associations to lead efforts in solving the talent gap.

Professional Associations Advocacy

There is a dearth of applied and theoretical research on cybersecurity-based professional associations advocating for cybersecurity professionals. Shaw (2014) defines advocacy as public support on a specified cause or a proxy to pursue an issue on behalf of a constituent. A key aspect of advocacy is developing relationships with associations to comprehensively achieve a greater influence to advance initiatives (Shaw, 2014). Strong advocacy mandates confirmation such as providing statistics and facts (Shaw, 2014) as in the case with cybersecurity, numerous studies and surveys provide statistical data on the current state personnel shortages (Cobb, 2016). Professional associations are responsible for articulating the data to large audiences addressing the critical concerns and matters of the concerned parties (Shaw, 2014). In the cybersecurity realm, professional associations play a vital role in addressing certification and training for information security professionals (Wight, 2016). Wright (2016) indicates that there are 30 certifying organizations with 140 training certification demonstrating the number of professional associations and the vast number of certifications. Cybersecurity professional associations should increase advocacy and lead efforts to address the talent shortage in cybersecurity. Within the cybersecurity domain, there are many components; however, the dearth of personnel is endangering and preventing organizations from achieving maximum security. Professional and certifying associations provide extensive certifications that illustrate competence in

cybersecurity; however, there is no shortage of education programs whether through certifications or college programs (Knapp, Maurer, & Plachkinova, 2017). Advocating for initiatives to address the cybersecurity talent gap requires professional associations to take an unprejudiced role with a judicious approach when unifying different organizations to address the talent gap. Professional associations aligned to the cybersecurity domain can collaborate with associations in the healthcare industry for lessons learned in previous advocacy developments endeavors and strategizing techniques to lead a unified conglomerate. Each professional association has an organizational agenda; however, the associations are centrally positioned within the cybersecurity nexus to work with public and private entities to lead efforts to resolve the talent chasm. Wright (2016) articulates that current training and development programs in cybersecurity are practical; however, the programs lack focus and application the current environment.

Professionalizing Cybersecurity

Spidalieri (2015 and 2016) writes extensively about professionalizing cybersecurity analogous to efforts the American Medical Association (AMA) undertook to professionalize of medicine in 1847. The AMA defined the minimum standard to be a medical profession to counter self-taught medical practitioners (Spidalieri, 2016). The deficiency in cybersecurity professionals is mounting annually because the industry lacks consistent approaches to assess training, experience, and education (Spidalieri, 2016). Existing initiatives aim to improve cybersecurity education; however, most of the programs are limited in scope and lack a consistent approach (Spidalieri, 2016). One policy expert expounds that colleges and universities are not teaching cybersecurity fundamentals; thus, preventing institutions from contributing to the cyber workforce development (Spidalieri, 2016). Spidalieri (2016) notes that cybersecurity education programs at all collegiate levels require vast improvements and the need for a framework standardizing best practices, core curriculums, and minimum standards provisions. Professional associations with the assistance of government funded entities must take the lead in professionalizing the cybersecurity profession not only to eradicate the self-taught viewpoint but to help guide efforts during the constant changes and chaos (Spidalieri, 2016). Professional associations can organize efforts to develop the baseline for standardizing and professionalizing cybersecurity (Spidalieri, 2016). Oppositionists of professionalizing cybersecurity argue that such efforts could implement arduous standards and further exacerbate the talent gap (Spidalieri, 2016). Professionalizing cybersecurity might affect some cybersecurity professional associations especially the certifying organizations because standardizing the minimum requirements for entry into the cybersecurity domain will infringe on existing certifications.

Recommendations and Conclusion

Thematic analysis revealed that cybersecurity is becoming increasingly complex, there is an existing talent shortage, and a lack of standardization for professionalizing cybersecurity (Cobb. 2016; Spidalieri, 2016; Wright, 2016). The cybersecurity domain needs the advocacy, leadership, and expertise of professional associations to work collaboratively to standardized professionalization and led efforts to address the talent shortage (Spidalieri, 2016; Wright, 2016) and avert the widening personnel chasm (Teoh & Mahmood, 2017.) Professional associations are

vital to lead efforts to develop solutions to eradicate the talent shortage and professionalizing entrance standards in cybersecurity (Cobb. 2016; Spidalieri, 2016; Wright, 2016):

a. Professionalization and standardization requirements for cybersecurity
b. Conduct empirical research to capture an accurate reflection of the cybersecurity professional shortage
c. Develop a national-level strategy for the cybersecurity workforce
d. Partner with academia to develop cybersecurity curriculum
e. Minimizing uncertainties in the industry
f. Create strategies to hire more women and minorities in cybersecurity

Failure to standardized the professionalization of cybersecurity and resolve the talent scarcity perpetuate the existing shortfalls and struggles (Wright, 2016). The abovementioned recommendations are critical for ameliorating the talent shortage and enhancing organization's ability to combat the perplexing cybersecurity threat environment. Cybersecurity is a matter of national security; therefore government, industry, and academia need to support professional associations in leading efforts to create strategies to improve the talent situation and professionalizing cybersecurity as the AMA did in 1847 (Spidalieri, 2016).

References

Arsenault, M., Clayton, J., & Peng, L. (2013). Mortgage fund flows, capital appreciation, and real estate cycles. *The Journal of Real Estate Finance and Economics*, *47*(2), 243-265.

Cobb, S. (2016). Mind This Gap: Criminal Hacking and the Global Cybersecurity Skills Shortage, a Critical Analysis.

Drack, M. (2009). Ludwig von Bertalanffy's early systems approach. *Systems Research and Behavioral Sciences, 26*, 563-572. doi:10.1002/sres.992

Dutta, S., Geiger, T., & Lanvin, B. (2015). The global information technology report 2015. In *World Economic Forum* (Vol. 1, No. 1, pp. P80-85).

Eldardiry, O. M., & Caldwell, B. S. (2015, January). Improving information and task coordination in cyber security operation centers. In *IIE Annual Conference. Proceedings* (p. 1224). Institute of Industrial and Systems Engineers (IISE).

Geer-Frazier, B. (2014). Complexity leadership generates innovation, learning, and adaptation of the organization. *Emergence: Complexity and organization*, *16*(3), 105.

Henshel, D., Cains, M. G., Hoffman, B., & Kelley, T. (2015). Trust as a human factor in holistic cyber security risk assessment. *Procedia Manufacturing*, *3*, 1117-1124.

Iosim, M. (2016). The simplicity of complex systems: The inquiry into the nature of life, mind, and death phenomena. *The Universal Journal of Psychology, 4*, 27-42. doi:10.13189/ujp.2016.040103

Knapp, K. J., Maurer, C., & Plachkinova, M. (2017). Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance. *Journal of Information Systems Education*, *28*(2), 101-113.

Kuziemsky, C. (2016, January). Decision-making in healthcare as a complex adaptive system. In *Healthcare management forum* (Vol. 29, No. 1, pp. 4-7). Sage CA: Los Angeles, CA: SAGE Publications.

Mazzocchi, F. (2012). Complexity and the reductionism–holism debate in systems biology. *Wiley Interdisciplinary Reviews: Systems Biology and Medicine*, *4*(5), 413-427.

Neely, L. (2017). 2017 Threat Landscape Survey: Users on the front line. Sans Institute. Retrieved on February 17, 2018, from https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910

Nobles, C. (2016). Cyber threats in civil aviation. *Security Solutions for Hyperconnectivity and the Internet of Things*, 272.

Scioli, A. G. (2017). Leadership Strategies for Addressing US Pharmaceutical Drug Shortages and Supply Chain Disruptions (Doctoral dissertation, Walden University).

Shaw, D. (2014). Advocacy: the role of health professional associations. *International Journal of Gynecology & Obstetrics*, *127*(S1).

Spidalieri, F., & Kern, S. (2014). Professionalizing cybersecurity: A path to universal standards and status. *Newport, RI: Pell Center for International Relations and Public Policy, Salve Regina University*.

Spidalieri, F. (2016). Understanding cyber threats: Lessons for the boardroom. *Newport, RI: Pell Center for International Relations and Public Policy, Salve Regina University*.

Teoh, C. S., & Mahmood, A. K. (2017). Cybersecurity Workforce Development for Digital Economy. The Educational Reviewing, USA,2(1), 136-146. http://dx.doi.org/10.26855/er.2018.01.003

Wright, M. A. (2015). Improving cybersecurity workforce capacity and capability. *ISSA Journal*, 14-20.