Chapter 4
The Cyber Talent Gap and Cybersecurity Professionalizing

Calvin Nobles
University of Maryland University College, Adelphi, USA

ABSTRACT

Two significant issues loom throughout the cybersecurity domain. The first is the shortage of cybersecurity professionals and the second quandary is the lack of minimum entry standards in cybersecurity. Some organizations' cybersecurity operations are suffering due to the cybersecurity talent gap accompanied by the increasing sophistication and number of cyber-attack attempts. The shortage of cyber talent is rampant in private entities as in public agencies, which highlights the resolve for entry standards into cybersecurity to enhance the professionalization. Researchers and practitioners provide countless recommendations for ameliorating 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.

INTRODUCTION

There is no doubt that the cybersecurity talent gap is taking a toll on private and public organizations as researchers assert that in 2017 there was a shortage of two million cybersecurity professions (Zantua, Dupuis, & Endicott-Popovsky, 2015). There is a multitude of surveys, reports, and studies indicating a shortage of cybersecurity professionals, which is a global problem, inciting extensive recruitment projects and academic partnerships to increase the number of cybersecurity professionals (Cobb, 2016). The tumultuous cybersecurity threat environment coupled with the mounting 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 uncertainty in cybersecurity (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

DOI: 10.4018/978-1-7998-2466-4.ch004

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, 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,