


Chapter 6

Certifications in Cybersecurity Workforce Development: A Case Study

Ping Wang

 <https://orcid.org/0000-0003-0193-2873>

Robert Morris University, USA

Hubert D’Cruze

University of Maryland, USA

ABSTRACT

The workforce demand for cybersecurity professionals has been substantial and fast growing. Qualified cybersecurity professionals with appropriate knowledge, skills, and abilities for various tasks and job roles are needed to perform the challenging work of defending the cyber space. The certified information systems security professional (CISSP) certification is a globally recognized premier cybersecurity credential and validation of qualifications. This case study analyzes the CISSP certification requirements, domains and objectives and attempts to map them to the cybersecurity industry competencies and the US national cybersecurity workforce framework (NCWF). This research is an extended study with full mapping of all CISSP domain areas to the knowledge, skills, and abilities in NCWF. The extended study aims to discover the in-depth value and role of reputable certifications such as CISSP in competency development for cybersecurity workforce. This article also discusses the value and implications of the CISSP certification on cybersecurity education and training.

1. INTRODUCTION

There has been a significant workforce gap and a fast-growing industry demand for qualified cybersecurity professionals globally and in the United States. According to the (ISC)² Cybersecurity Workforce Study, the shortage of cybersecurity professionals is close to three million globally and about half a million in North America and the majority of the companies surveyed reported concerns of moderate or extreme

DOI: 10.4018/978-1-6684-3554-0.ch006

risk of cybersecurity attacks due to the shortage of dedicated cybersecurity staff ((ISC)², 2018c). An information security analyst is only one of the career titles in the cybersecurity profession. The latest career outlook published by the United States Labor Department Bureau of Labor Statistics shows that the employment of information security analysts is projected to grow 28 percent from 2016 to 2026, much faster and with better pay than the average for all occupations (US Labor Department BLS, 2018).

Education, training, and professional certifications are common solutions for alleviating shortage of professional staff. However, a recent study shows that top universities in the United States were failing at cybersecurity education with a lack of cybersecurity requirements for graduates and a slow change in curriculum and courses (White, 2016). The national Centers of Academic Excellence in Cyber Defense Education (CAE-CDE) designation program jointly sponsored by the US National Security Agency (NSA) and Department of Homeland Security (DHS) has been a reputable standard for certifying and maintaining high quality of cybersecurity education with rigorous requirements for program evaluation and assessment of cybersecurity knowledge units. However, only less than 300 (or about four percent) of the all colleges and universities in the U.S. have achieved the CAE-CDE designation status so far (Wang, Dawson, & Williams, 2018).

Recognizing the need to develop more and qualified cybersecurity professionals to meet the workforce demand, the U.S. National Initiative for Cybersecurity Education (NICE) recently published the NICE Cybersecurity Workforce Framework (NCWF SP800-181), which specifies cybersecurity professional categories, tasks, job roles as well as knowledge, skills, and abilities (KSAs) needed for cybersecurity jobs (NICE, 2017). These KSAs are also mapped to the cybersecurity knowledge units (KUs) for college and university programs with CAE-CDE designations. An initial effort to map the KSAs with limited cybersecurity certification domains was conducted by Wang and D’Cruze (2019).

Professional certifications are an important supplemental credential system to help select talents and guide the training and development of cybersecurity workforce. In hiring information security analysts, for example, many employers prefer their candidates to have some relevant professional certification in the field, such as Certified Information Systems Security Professional (CISSP) in addition to a minimum of a bachelor’s degree in order to validate the knowledge and best practices required for the job (US Labor Department BLS, 2018). Ideally, the certification process used for developing and selecting qualified professionals in the cybersecurity field should incorporate the job tasks and KSAs specified in the NCWF as well.

There are many different types of certifications for the cybersecurity field with various levels of requirements and rigor. The CISSP (Certified Information Systems Security Professional) certification stands out as a challenging but popular vendor neutral certification choice coveted by cybersecurity professionals and employers. Studies show CISSP as a top cybersecurity credential sought after and most valued by employers (Brown, 2019; (ISC)², 2017b; ISCN, 2018; Wierschem, Zhang, & Johnston, 2010). This study is motivated by the urgent need and research efforts for viable solutions to the shortage of cybersecurity talent and by the recent study on the CISSP certification by Wang and D’Cruze (2019).

Based on the recent and initial KSA mapping by Wang and D’Cruze (2019), this paper reviews and evaluates the rigorous requirements of the CISSP certification and continues to explore the significant value and benchmark role of the CISSP certification in developing and maintaining cybersecurity workforce competencies with substantial and extended mapping data. This paper will reveal the value and limitations of the CISSP certification and contribute a thorough mapping of all the CISSP knowledge domains and objectives to the model of competencies of the US cybersecurity industry and knowledge, skills, and abilities (KSAs) in the NICE cybersecurity workforce framework (NCWF). The goal of this

18 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/certifications-in-cybersecurity-workforce-development/292107

Related Content

Understanding, Celebrating and Maintaining the “HBCU Experience”

Tia C. M. Tyree and Christopher D. Cathcart (2016). *Administrative Challenges and Organizational Leadership in Historically Black Colleges and Universities* (pp. 25-43).

www.irma-international.org/chapter/understanding-celebrating-and-maintaining-the-hbcu-experience/156851

Integrating MOOCs in Higher Education: Procedures and Tools for a Mutual Commitment to Quality

Florence Rouveix, Magali Guyon and Rémi Bachelet (2020). *Handbook of Research on Operational Quality Assurance in Higher Education for Life-Long Learning* (pp. 265-290).

www.irma-international.org/chapter/integrating-moocs-in-higher-education/245363

The Experiences and Self-Efficacy of Faculty Members Using Distance Learning for the First Time: A Qualitative Inquiry

Luis Miguel Dos Santos (2022). *Assessing University Governance and Policies in Relation to the COVID-19 Pandemic* (pp. 70-90).

www.irma-international.org/chapter/the-experiences-and-self-efficacy-of-faculty-members-using-distance-learning-for-the-first-time/288200

Faculty Videos of Resilience Narratives at Two Institutions: Residency Resilience Skills Program Innovation

Hedy S. Wald and Brenda Bursch (2020). *International Journal of Innovative Teaching and Learning in Higher Education* (pp. 16-24).

www.irma-international.org/article/faculty-videos-of-resilience-narratives-at-two-institutions/245770

Factors Affecting Malaysian Undergraduate Students' Motivation in Improving English Proficiency in Academic Environments

Ali Sorayyaei Azar and Siti Aisyah Binti Mohd Sahar (2021). *Higher Education Challenges in South-East Asia* (pp. 35-73).

www.irma-international.org/chapter/factors-affecting-malaysian-undergraduate-students-motivation-in-improving-english-proficiency-in-academic-environments/267454