Fall 9-11-2020

Quantifying Program Offerings with a Cybersecurity Education Maturity Model

Christopher Kreider
Christopher Newport University, chris.kreider@cnu.edu

Mohammad Almalag
Christopher Newport University, mohammad.almalag@cnu.edu

QUANTIFYING PROGRAM OFFERINGS WITH A CYBERSECURITY EDUCATION MATURITY MODEL

Christopher Kreider
Christopher Newport University
chris.kreider@cnu.edu

Mohammad Almalag
Christopher Newport University
mohammad.almalag@cnu.edu

ABSTRACT

The jobs gap is a problem in cybersecurity whereby there are insufficient number of qualified individuals to fill the jobs in this burgeoning area. Work has been done to understand this gap and close it. A framework for this gap analysis has been identified with 3 key dimensions: program offering, student pipeline and program capacity. This paper seeks to further explore the program offering dimension, developing a model for measuring academic program offerings. The purpose of this framework is to enable further research on efforts to decrease the jobs gap, specifically through state level initiatives and funding.

KEYWORDS

Cybersecurity, Cybersecurity Education, Educational Framework

EXTENDED ABSTRACT

Cybersecurity education has become an important priority for a variety of stakeholders including government and industry, with educational programs struggling to respond to this growing need for professionals in the field (Bashir, Wee, Memon, & Guo, 2017; Conklin, Cline, & Roosa, 2014; Thompson & Thompson, 2007). Progress has been made in through the development of the National Initiative for Cybersecurity Education (NICE) framework, which was developed by the National Institute for Standards and Technology (NIST). This framework develops a common lexicon for cybersecurity related work including skills necessary. Despite this progress, the jobs gap remains, with many states introducing state-wide initiatives to increase the number of graduates in this field, such as Virginia's Commonwealth Cyber Initiative CCI. Kreider and Almalag (2019) developed a holistic framework to better assess this gap, identifying three key dimensions: program offering, student pipeline and program capacity. Their work provides an initial framework and evidence to support the inclusion of the three dimensions, but does not go into detail on how to quantify these dimensions. This paper seeks to extend the work of Kreider and Almalag (2019) by developing a framework for quantifying the program offering dimension of cybersecurity education. This framework will utilize an ordinal numbering scheme, assigning numeric values to various levels of cybersecurity offerings that may be available at a university, or across a system of universities. This scale is assumed to be ordinal, with the assumption that higher values represent greater progress towards generating graduates qualified to fill jobs requiring cybersecurity knowledge. This is referred to as a maturity model, as higher scores indicate a more mature cybersecurity ecosystem, with the highest scores representing the ability to not only potentially fill the jobs gap, but the generation of qualified faculty capable of teaching and increasing values along other dimensions, such as program capacity. The scale generated spans the values of 0 to 10, with 0 being no university level offerings pertaining to cybersecurity with 10 being doctoral level programs.

0	1	2	3	4	5	6	7	8	9	10
No offerings	Class(es) as part of an elective	Associates degree	Minor or area of emphasis	Single Bachelors Degree/ Majors	Multiple Bachelors Degrees/ Majors	Single Masters Degree	Multiple Masters Degrees	Single Doctoral Degree	Multiple Doctoral Degrees	Postdoc Options

This framework will then be used to assess the cybersecurity offerings across a set of universities in states that instituted state-wide initiatives in cybersecurity education, along with associated investment cost to better assess impact of such programs.

REFERENCES

1. Bashir, M., Wee, C., Memon, N., & Guo, B. (2017). Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Computers & Security, 65*, 153-165.
2. Conklin, W. A., Cline, R. E., & Roosa, T. (2014). *Re-engineering cybersecurity education in the US: an analysis of the critical factors.* Paper presented at the System Sciences (HICSS), 2014 47th Hawaii International Conference on.
3. Kreider, C., & Almalag, M. (2019). A Framework for Cybersecurity Gap Analysis in Higher Education.
4. Thompson, C., & Thompson, D. (2007). Identity Management. *IEEE Internet Computing*, 82-85.