Chapter 17
Opportunities and Challenges of Cybersecurity for Undergraduate Information Systems Programs

Shouhong Wang
https://orcid.org/0000-0002-4634-8833
University of Massachusetts Dartmouth, Dartmouth, USA

Hai Wang
https://orcid.org/0000-0002-2860-1954
Saint Mary's University, Halifax, Canada

ABSTRACT

This article investigates the opportunities and challenges of cybersecurity for information systems (IS) programs and proposes a curriculum structure of cybersecurity track for IS programs. The study has collected data from eighty-two course websites of thirteen institutions at the graduate level and sixteen institutions at the undergraduate level as well as twenty descriptions of cybersecurity jobs posted on the internet. The collected qualitative data has been analyzed from the from the perspective of IS education. The findings indicate that the topics of cybersecurity management and essential cybersecurity technology are relevant to the IS discipline. The article suggests that these topics can be the components of two cybersecurity courses offered by IS programs to meet the demands and challenges of cybersecurity.

1. INTRODUCTION

Protection of information in business and government organizations in the global digital environment has become an urgent and current issue. The U.S. cybersecurity market size is estimated to grow from $1.8 billion in 2017 to $22 billion by 2022. ("Market Research Media," 2018). Given the increasing cyberattacks through the Internet, the need for highly trained cybersecurity professionals is acute. A

DOI: 10.4018/978-1-6684-3554-0.ch017

projected shortfall of cybersecurity professionals is significant (Nelson, 2016). U.S. News and World Report ranked a career in information security analysis eighth on its list of the 100 best jobs for 2015, and cybersecurity jobs are expected to grow at a rate of 36.5 percent annually through 2022 (South, 2015).

Given the increasing demand for the cybersecurity professionals across the world, it is clear to all disciplines related to information technology (IT) that strategic innovation of the IT curricula for cybersecurity is imperative. The information systems (IS) area in business education has expressed great concern about the stable low enrollments and career skills oriented undergraduate information systems curriculum (Harris et al., 2012; Khoo, 2012). The IS community has curriculum guidelines, IS 2010 (Topi et al. 2010), for undergraduate degree programs in IS and IT in general. The IS 2010 curriculum guidelines, established in a collaborative effort by ACM (The Association for Computing Machinery) and AIS (The Association for Information Systems), contain a set of model curricula for undergraduate degrees in IS. The IS 2010 curriculum guidelines are not directly linked to any degree structure in a specific environment but provide guidance regarding the core contents of the curriculum that should be present in various career tracks in the IS field. There is a wide range of adherence to the IS 2010 curriculum guidelines in business schools (Bell et al., 2013). As all aspects of the global computing field continue to face rapid and continuous changes, IS programs need to maintain currency of curricula to meet the dynamic needs of the job market of post-secondary IS/IT graduates. Whilst cybersecurity has been identified as one of the most serious challenges over the past several years (Agamba and Keengwe, 2012; Gill, 2016), the curriculum of cybersecurity in the IS discipline has not fully established yet. This study investigates how IS programs can contribute to cybersecurity education and how cybersecurity curriculum should be embedded in IS programs. The objective of the article is to propose a curriculum structure of cybersecurity track for IS programs to collaborate with other disciplines for cybersecurity education.

The rest of the paper is organized as follows. Section 2 is a review of literature of related work. Section 3 provides an overview of data collection through reviews of web documents related to cybersecurity education. The collection of qualitative data about cybersecurity programs and cybersecurity job requirements were used for this study. Section 4 describes the qualitative data analysis process used in this study. Section 5 presents the findings of the qualitative data analysis and recommendations. Section 6 discusses the limitations of the study. Finally, section 7 concludes the study.

2. LITERATURE REVIEW

Most studies of cybersecurity education emphasize on technical aspects of cybersecurity and suggest that operating systems, telecommunication, networking, cryptography, malware analysis, and computer forensics are important technical skills for cybersecurity students (Beznosov and Beznosova, 2007; Fulton et al., 2013; Trabelsi and McCoey, 2016). Given the board coverage of technical topics in cybersecurity, there is no standard set of learning outcomes associated with technical aspects of cybersecurity (Slusky and Partow-Navid, 2012). Some cybersecurity programs use professional certification standards (e.g., CISSP (Certified Information Systems Security Professional)), and others use curriculum guidelines (e.g., NSA (National Security Agency) and NHS (National Health Service)).

Research into cybersecurity has suggested that the process of cybersecurity requires much more than mere technical controls, and demands human-centered approaches (Noluxolo et al., 2017) and organizational development approaches (Stanciu & Tinca, 2017). From an organizational perspective,