Cybersecurity and Information Assurance in Information Science Curricula

Unal Tatar and Abebe Rorissa
University at Albany, State University of New York, USA
utatar@albany.edu, arorissa@albany.edu

ABSTRACT

As a newly emerging and one of the fastest growing fields of study, cybersecurity/information assurance has plenty to offer in terms of teaching and research. If Library and Information Science (LIS) schools are to take advantage of this fast growth in the field by expanding their program and/or course offerings, thereby increasing their enrollments, and, indeed, provide their students with opportunities to be able to take advantage of the demand for skilled manpower in cybersecurity/information assurance, it is imperative for them to systematically approach the inclusion of courses and/or programs to their curricula. A component of this systematic approach is a closer examination of programs, concentrations, and courses in cybersecurity/information assurance currently offered at similar or peer LIS schools in order to identify best practices and gaps. The study reported here is a small but important part of this effort.

TOPICS

Information security; Cybersecurity; Education; Curriculum

INTRODUCTION

While the two domains, cybersecurity and information assurance, cannot be considered synonymous, they have enough overlap in terms of problems and issues addressed. For the purposes of this paper, we will use the two interchangeably. Where one of them is mentioned, it should be considered that we are referring to both, notwithstanding the fact that information assurance is not a new field and may be broader in scope.

As not only one of the newly emerging and fastest growing fields of study, cybersecurity, although narrower in focus than LIS, has plenty to offer in terms of teaching and research. Because of its novelty, several problems and issues have not yet been addressed adequately through research and teaching. It also suffers from the lack of an interdisciplinary perspective which emphasizes human, social, and economic aspects of society alongside technical ones. In most cases, cybersecurity programs put the emphasis on technologies rather than people or human factors.

What is more, cybersecurity is an emerging field with close to zero unemployment. In 2016, the National Initiative for Cybersecurity Education (NICE), which is led by the U.S. Commerce Department's National Institute of Standards and Technology (NIST), funded the CyberSeek website (Cyberseek, 2019) to provide detailed & actionable data about supply and demand in the

cybersecurity job market. Based on that data, there are an estimated 301,873 active cybersecurity job openings in the United States as of October 2018. The November 2018 *Cybersecurity Workforce Development* report of the New America Foundation contained the following data for specialists in cybersecurity: "In 2015, the anticipated global shortfall was expected to reach 1.5 million unfilled jobs by 2020; in 2017, the estimate was 1.8 million by 2022; and the estimated current-day gap is close to 3 million." (Bate, 2018).

A much broader and interdisciplinary discipline such as information science, with its focus on information, people, technology, and their interactions, is a logical place for cybersecurity - the same way data science/analytics became an integral part of LIS curricula in recent years. While cybersecurity is relatively new, information science has reasonably well-established methods, theories, processes, tools, and the knowledge base that can be leveraged to find comprehensive solutions to problems in the cybersecurity domain. However, it is not clear the extent to which programs, especially those offered by LIS schools, are incorporating cybersecurity topics, issues, and problems in their courses and whether LIS schools are expanding their enrollments by offering cybersecurity focused programs or concentrations. Hence, there is a need for the current study. To guide the study, the following research questions were considered: To what extent do LIS schools cover cybersecurity in their courses/concentrations/programs at both the undergraduate and graduate (MS and Ph.D.) levels?

METHODS

Websites of all LIS schools in the United States of America (USA) were searched for courses, concentrations, and programs in cybersecurity and/or information assurance. With the help of two undergraduate and a graduate student, the two authors collected and conducted content analysis of the descriptions of each of the programs, concentrations, and courses with cybersecurity and/or information assurance as their main focus. We utilized the *specialty areas* and *knowledge/skills/abilities* identified in the NICE Cybersecurity Workforce Framework [1] (Newhouse, Keith, Scribner, and Witte, 2017) to guide our content analysis of descriptions of cybersecurity programs, concentrations, and courses. With respect to coding consistency or reliability, the two authors coded the entire set of descriptions independently first and then resolved any differences until a 100% agreement was reached.

PRELIMINARY FINDINGS

We are still at the initial stages of our data analysis. However, based on coding conducted on descriptions of programs, concentrations, and courses, we found that LIS schools in the USA have started to offer courses on cybersecurity, but the number of cybersecurity focused programs and concentrations are still low, and there is room for growth given the potential demand for graduates. The first stage of our analysis showed that the offered cybersecurity programs and concentrations are mostly at the graduate (master's, Ph.D., and graduate certificate) level while there are more

[1] https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

courses offered on cybersecurity at the bachelor's level. The courses cover a broad area of cybersecurity from network security and cryptography to cybercrime, law, and privacy – which also reflects the interdisciplinary perspective of LIS schools.

A gap remains in terms of the topics that need to be covered if graduates of cybersecurity programs at LIS schools are to enjoy a competitive advantage in their search for positions that require acceptable levels of skills and knowledge in cybersecurity and/or information assurance.

IMPLICATIONS AND RECOMMENDATIONS

Findings of the current study will have curricular implications for LIS schools and career implications for students. LIS schools could use the findings to either revise their programs, concentrations, and courses (if they already have existing ones) and/or design new and more competitive as well as state-of-the-art ones that meet the needs of students and their potential employers. Although it is a field with a long history, like any dynamic discipline, Information Science itself is still evolving. Consequently, LIS schools are continuously adapting their programs to address new areas of research, teaching, and learning, such as cybersecurity, data science, and AI. We believe that our research will help LIS schools in their efforts to adapt as well as benchmark their current cybersecurity programs and set out a road map.

REFERENCES

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *NIST Special Publication, 800*, 181.

Bate, L. (2018). *Cybersecurity Workforce Development: A Primer*. New America Foundation. Retrieved from https://www.newamerica.org/cybersecurity-initiative/reports/cybersecurity-workforce-development/.

Cyberseek. (2019). Retrieved from https://www.cyberseek.org/.