Association for Information Systems
AIS Electronic Library (AISeL)

SAIS 2019 Proceedings | Southern (SAIS)

3-22-2019

A Framework for Cybersecurity Gap Analysis in Higher Education

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

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

A FRAMEWORK FOR CYBERSECURITY GAP ANALYSIS IN HIGHER EDUCATION

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

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

ABSTRACT

The gap between those qualified for jobs in cybersecurity, and the needs of professionals remains an issue, despite the recent emergence of the importance of cybersecurity. Our project develops a holistic framework to perform a gap analysis by which institutes of higher education can start to understand and identify methods through which they can work to address this gap. While most existing frameworks focus purely on the curricular perspective, our framework extends this to also explore program capacity and the pipeline of incoming students.

Keywords

Cybersecurity, Cybersecurity Education, Educational Framework

INTRODUCTION

The importance of cybersecurity education has emerged in recent years as a priority for governments and industry (Bashir et al., 2017; Kam et al., 2018), with educational programs responding to the growing need for professionals in the field (Conklin et al., 2014), however educators continue to struggle (Thompson et al., 2018). Despite increased efforts by governments (Paulsen et al., 2012) with the development of frameworks such as the NICE framework (Newhouse et al., 2017), the gap between the need for professionals in the field and the number of those qualified for those positions remains (Bashir et al., 2017; NeSmith, 2018; Wei et al., 2016). While knowledge of this gap is not new, most research on cybersecurity education seems to focus on a wide variety of piecemeal topics, with an awareness that there is a lack of rigorous research pertaining to educating the cybersecurity workforce (Thompson et al., 2018).

While these areas of research are no doubt valuable, no common framework has emerged for assessing the gap as a whole. Such a framework could assist researchers in identifying focused areas of research which may assist in closing this gap. Our research provides a framework for assessing the cybersecurity education gap, specifically focused on higher education at the state level. Our research is the result of multiple working group discussions with faculty from multiple state universities. The results of these working groups were then summarized into a cohesive framework, and presented to an advisory board and task force for feedback. Finally, we perform an initial literature review on the identified dimensions to connect our findings back to the academic community.

Our findings identify that the cybersecurity gap in higher education has three primary dimensions: program offerings, program capacity and student pipeline. Program offerings focus on the specific contents of educational programs in cybersecurity, such as topics covered, degrees offered, and other educational offerings such as internships and certifications. Program capacity is focused on the capability to produce the needed number of students to fill the gaps, such as class size, class scalability and faculty recruitment. Finally, student pipeline explores options pertaining to the number of students interested and capable of entering into one of the programs.

The rest of this paper will be structured as follows: We will first discuss the methodology by which our framework was derived, and how it will be explored further in this paper. We will then present our framework. After that, we will perform a literature review focusing on recent literature exploring cybersecurity educational frameworks as well as the three areas identified by this framework. Finally, we will provide a discussion of our results and draw conclusions from our work.

METHODOLOGY AND FRAMEWORK

When performing analysis in qualitative methodologies, it is common to draw a clear distinction between information gathering and analysis activities, however, this distinction can often be problematic (Myers, 1997). Specifically, as stated by Myers (1997) "…the questions posed to informants largely determine what you are going to find out. The analysis affects the data and the data affect the analysis in significant ways". Our research falls into this category of qualitative research, as a working group tasked with a specific area of exploration related to cybersecurity education. The data we were provided and the conclusions we drew are closely related. As a result, our discussion of methodology will mention the data that was provided to the working group, but will primarily focus on the members of the working group, the mode of discussion and validation of the resultant

framework to provide evidence of validity for this framework. Additionally, we will perform a literature review on the elements of the framework identified by the working group to better validate and connect the results of the group to the greater academic community.

Working Group Structure

An initial set of faculty from state institutions, and relevant stakeholders from industry were first identified to be part of taskforce tasked with the exploring cybersecurity related issues. From this initial set, an advisory council of 25 members and 4 working groups were formed. Of the working groups that were formed, each group was tasked with a primary goal and given a deadline to report findings back to the entire task force and advisory board. Of the 4 working groups that were formed, the group of interest to this research was the group for exploring Educational Issues in Cybersecurity (EICS)

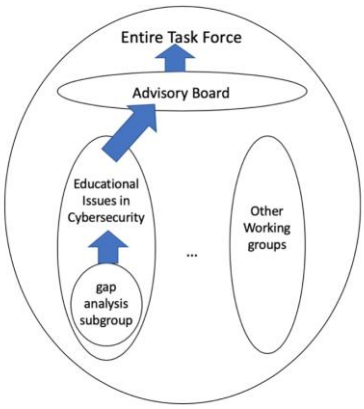

Figure 1. Working Group Reporting Structure

The EICS working group identified multiple subgroups, including the gap analysis subgroup (GASG). The GASG met and generated a report, including a gap analysis framework for cybersecurity education in higher education. The subgroup then reported its findings to the larger working group for Educational Issues in Cybersecurity (EICS). After review and input from this group, it was then presented to the advisory board, and eventually, to the entire task force. The subsequent framework was part of these findings, and was presented both in digital presentations, as well as in person presentations attended by a variety of members. Feedback from these various levels of review was incorporated into the final framework.

Working Group Composition

Of the working groups, the EICS group specifically explored educational programs and experiential learning. This working group was composed of 17 members, of which 12 members were from 11 different public institutions of higher education, 4 were from industry, and 1 was from a state council of higher education. Of the participating members, 4 had a title of provost, assistant provost or similar title; 2 had a tile of dean, assistant dean or similar title, 5 had a title of director, and 5 were instructional faculty.

Title/Role	#
Provost, Asst. Provost or Similar	4
Dean, Asst. Dean or Similar	2
Director	5
Instructional Faculty	5
State Education Council	1

Table 1. Breakdown of EICS Working Group Participants

Additionally, from this set of working group members, the gap analysis sub group (GASG) was identified to specifically focus on the gap analysis. This sub group was responsible for the initial discussion, and generation of the initial framework which was then presented to the parent working group. The subgroup consisted of 9 of the 17 members of the parent working group.

Working Group Format

The working groups, comprised of geographically diverse members of universities and industries, were primarily conducted online. On two occasions, in person meetings were hosted, however, only a subset of the general members was present at the

in-person meetings. Online tools included video/audio conferencing capabilities during scheduled meeting times. Additionally, email was used to communicate among members in the EICS subgroup, and the gap analysis sub group. Summaries of the meetings were delivered via email.

Working Group Data

The working groups were presented with a set of online resources containing data and other relevant information pertaining to cybersecurity in the state. A total of 19 documents were provided in this set of resources, and focused on the following areas: regional analysis of cybersecurity workforce needs for 3 large regions in the state; resources for cybersecurity educational resources and programs provided by the state; resources associated with the National Initiative for Cybersecurity Education (NICE); and resources from a variety of councils, alliances and partnerships pertaining to cybersecurity. In whole, the data was provided from diverse sources exploring various aspects of cybersecurity, employment and education in the state. Additionally, working group members shared additional resources which were available to their respective organizations that were relevant to the discussion. While there is no guarantee that each member of the working group reviewed all relevant data, a common core of data was available for review by all members.

Framework

The framework was developed from the discussions performed by the gap analysis subgroup. The high level concerns and suggestions brought forward by working group members were summarized, and then categorized by a member of the group, and presented back to the group for review. The results of this process identified a model with three broad categories/dimensions being relevant to the gap between education and the needs of the cybersecurity workforce. The exploration of these three dimensions were presented as a graphical model, as well as a textual narrative exploring each dimension, assuming the other two dimensions could be perfectly met, provided in table 2 and figure 2.

Dimension	Narrative
Program Offerings	Assuming an infinite supply of students, and infinite resources with which to educate those students, are we capable of offering a set of programs that are sufficient to close the workforce gap in cybersecurity?
Program Capacity	Assuming an infinite supply of students, and a set of educational comprehensive programs and offerings, would our educational institutions have the necessary resources to close the workforce gap in cybersecurity?
Student Pipeline	Assuming a set of comprehensive educational programs, and infinite resources with which educational institutions could use to implement, would there be enough students willing and capable to engage in such programs?

Table 2. Summary of the Gap Analysis Dimensions in Narrative Form

While the narrative form explored these dimensions from a hypothetical perspective, assuming two of the dimensions can be perfectly met, this is not possible in practice. Given resource constraints, the allocation of resources to address gaps along these dimensions would likely require a compromise or a given focus. As a result, the final graphical model was represented as a triangle, where any point within the triangle can represent the relative allocation of resources to address the overall problem that is trying to be solved.

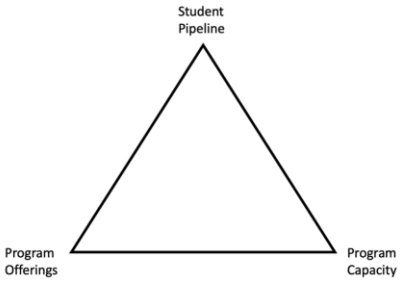

Figure 2. Graphical Representation of Cybersecurity Education Gap Analysis Framework

The first dimension we will discuss, program offerings, focused on whether universities were providing what the workforce was expecting in terms of skills and other educational outcomes. This dimension identified several areas of exploration such as: additional courses, additional degrees, certificates and certifications. The addition of new courses could be used to focus education on specific areas needed by the workforce, while being quicker and easier to do by both smaller and larger universities. The addition of new degrees, while accompanied with overhead from an accreditation perspective, could generate

cohorts of students capable of fulfilling a large variety of cybersecurity jobs. Finally, exploring custom combinations of skills, either through the use of a certificate program or certification program could signal to industry that students are specifically qualified for work in a specific area and reduce the time necessary for them to enter the work force in the cybersecurity arena from time of graduation. The second dimension, program capacity, explored the problem through the lens of what an established university could do to increase their ability to generate qualified graduates through options such as: additional faculty, additional facilitates, online offerings. The group identified that larger universities would be uniquely positioned to pursue this strategy as compared to smaller schools. Finally, the third dimension, student pipeline, identified areas including: high school recruitment, 2 to 4 year opportunities, marketing and scholarships.

Framework Literature Review

The final component of this research paper is a brief literature review exploring each of the dimensions identified in the framework. This is done to connect the qualitative research that is presented here back to the greater community of research that exists in this area. The literature will primarily explore technical journals and conferences in the computer science and information systems arenas. The research that was explored is primarily limited to the past 4 years to ensure that recent research in these areas was captured and was relevant to recent updates in the need for qualified cybersecurity professionals. However, in certain cases, if a relevant research is located in an exceptionally high-quality journal and/or is well cited, it may be included in the subsequent analysis.

LITERATURE REVIEW

While the working groups and sub group developed a framework that received review and feedback of the greater task force, this methodology lacked rigor in that the distinction between the data and the analysis is often blurred with this type of qualitative study (Myers 1997). To strengthen the rigor of this framework, we took the findings, suggestions, and resultant framework of the working group, and chose to extend it through an initial literature review. The purpose of this literature review was to explore the relevant literature related to the 3 proposed dimensions, thus placing the framework in the greater context of relevant research in this area. This literature review will explore relevant frameworks that exist in the area of cybersecurity and education, as well as the three dimensions identified in the framework presented.

Frameworks in Cybersecurity

When exploring frameworks pertaining to cybersecurity and education, a recent and comprehensive framework, the National Initiative for Cybersecurity Education or NICE has been developed by the National Institute of Standards and Technology (NIST) (Newhouse et al., 2017). The purpose of this framework was to better define and assess the cybersecurity workforce, resulting in a common and consistent lexicon for the categorization and description of cybersecurity related work. The NICE framework has been utilized in a variety of academic works such as the creation of new academic disciplines (Trilling, 2018). Wei et al. (2016) develop a framework for classifying the level of education, categorizing them into 3 levels, modeled as a pyramid. At the top of the pyramid are the management and decision/policy makers. The middle level os comprised of the cybersecurity technicians and practitioners, with the base of the pyramid being cybersecurity literate general masses. Finally, Hallett et al. (2018) develop Cybersecurity Body of Knowledge (CyBOK) with the purpose of providing a common basis for the comparison of various curricular frameworks in the area. The common theme among these frameworks is the focus on the knowledge and skills that be included in cybersecurity educational programs.

Program Offering

As the gap between the unfilled positions in cybersecurity and the number of graduates in related fields grows, universities need to work on changes in curriculum and courses to narrow this gap. Many cybersecurity curricular frameworks exist to guide universities and organizations in implementing courses (Hallett et al., 2018), which should provide a starting point for this challenge. Despite available frameworks, recent discussions identified that out of 32 top U.S. universities for computer engineering and computer science only three of the schools required at least one class in cybersecurity. As the interest in opening new programs for cybersecurity increases, the Accreditation Board for Engineering and Technology (ABET) has developed specific criteria for cybersecurity (ABET, 2018), to ensure the quality of cybersecurity programs. Such accreditation programs should increase the quality of the programs, but decrease the ease and time with which they can be implemented. One final area that was discussed in the generation of the frameworks was certifications, which have been identified as being relevant to organizations who are looking for to close the jobs gap (Brooks et al., 2018).

Program Capacity

With the increased need for qualified graduates in cybersecurity, universities are struggling to increase the number of graduates in the field, as well as hiring of qualified cybersecurity faculty (White, 2016). Additionally, a critical need exists for cybersecurity test beds to enable education and testing without overly complex environments (Tunc and Hariri, 2015), which

can lead to a need for additional resources for universities seeking to increase their capacity. One area that has emerged is the use of online educational programs (Kreider 2017). Online programs have had mixed outcomes in the research, with one meta-analysis of 45 studies exploring online and blended learning environments, found that the online and face-to-face instruction were equivalent in terms of effectiveness (Means et al., 2013). Despite this, only 77 percent of academic leaders rated online learning the same or superior when compared to face-to-face options, and even though these numbers are increasing, a gap still exists (Allen and Seaman 2013). Despite these concerns, recent programs, such as Georgia Tech's Online Masters of Science in Computer Science (OMSCS) have identified many pedagogical benefits of large scale online programs (Joyner et al., 2016). The success of the OMSCS has led Georgia Tech to develop additional programs in this style, including an Online Masters of Science in Cybersecurity starting Fall 2018 (Agarwal, 2018) .

Student Pipeline

The student pipeline explores the flow of students into academic programs that will prepare them to for a qualified for a job in cybersecurity. Wei et al (2016) specifically identify 5 potential sources of entrants into cybersecurity programs including: high school students, two-year college students, university students from other majors, existing workforce and laid off workforce. Other areas explored identified the role of competitions in recruiting students into cybersecurity related careers. For example, Bashir et al. (2017) identified several personality types likely to participate in competitions, and from their personalities, which were more likely to enter cybersecurity fields. Their suggestion is to target this demographic to increase like likelihood that students will carry their interest forward to a full career. Additionally, studies of competitions and cybersecurity educational outcomes go on to explore concepts such as how they are designed, and the implications for underrepresented populations (Pusey et al., 2016).

DISCUSSION

Research identified regarding program offerings generally focused on the many cybersecurity curricular frameworks that exist (Hallett et al., 2018), one of which that has recently emerged and risen to prominence, the NICE framework (Newhouse et al., 2017). These curricular frameworks provided a common lexicon serve as tools for programs looking to increase their cybersecurity course offerings. Apart from research in the category of curricular frameworks, most of the identified research explored smaller areas such as the role of competitions and personality in student recruitment, and explorations of underrepresented populations.

Research identified regarding program capacity highlights some of the challenges of increasing capacity, such as faculty recruitment (White, 2016) and the need for specialized resources specific to cybersecurity related disciplines (Tunc and Hariri, 2015). One possible solution that enables benefits to be achieved for large classes with remotely distributed students is online programs, which have been identified to provide pedagogical benefits (Joyner et al., 2016). Such large programs such as the OMSCS have seen success, and resulted in the development of additional similar programs, with one specifically targeted towards cybersecurity(Agarwal, 2018). It is our belief that this is an area that may have the greatest impact in being able to increase program capacity.

Research identified on the student pipeline was either secondary to another focus of the research, as was the case with Wei et al. (2016), or focused on niche areas such as capture the flag competitions and underrepresented populations (Bashir et al., 2017; Pusey et al., 2016). Performing a more rigorous assessment of the current inbound students in the area with respect to the needs of industry should enable the community to have a better understanding if there are enough current inbound students to meet future needs, and if not, what can and should be done to increase deficiencies in this dimension of the framework.

CONCLUSION

Based on our initial exploration of the literature, we conclude that our framework provides a unique contribution to the problem of the jobs gap in cybersecurity. While a variety of frameworks exist to assess the curricular related knowledge and skills needed to close this gap, these frameworks do not take a holistic approach to the problem. Specifically, while our frameworks recognizes that knowledge and skills are part of the problem, categorized in the *program offerings* dimension, we go on to identify that it is just part of the problem. Specifically, that there are different ways in which programs can alter what they are offering, and this is contingent on the capacity and interested students willing to enter into such a program, complete it, and finally end up in the workforce in the cybersecurity area.

This paper has several limitations. The first limitation is that, the quantitative approach to this study focused more on the qualifications and structure of the working group, as opposed to the data that they were presented. Additionally, the literature review section is exceptionally brief, and lacked the systematic exploration of a thorough literature review. Articles were selected from a small range of dates, and were selected to provide evidence for the framework that was developed. Finally, while this study identifies three major dimensions of the problem, little effort is done to operationalize these concepts. Given

these limitations, future work could explore objective mechanisms for validation of this framework, expand the literature review around this framework to include a more complete and comprehensive review of the literature, as well as provide a more comprehensive exploration and operationalization of each of these dimensions.

ACKNOWLEDGMENTS

We would like to thank other members of the task force and the working group who contributed to the materials and discussion used to generate this framework. Additionally, we would like to thank members of our university who made this possible providing nominations/recommendations of members to join the task force.

REFERENCES

1. ABET (2018) ABET Criteria for Accrediting Computing Programs, *ABET*, Baltimore.
2. Agarwal, A. (2018) How Is Higher Ed Helping to Close the Global Knowledge Gap? Retrieved 12/18/2018, from https://www.forbes.com/sites/anantagarwal/2018/12/10/how-is-higher-ed-helping-to-close-the-global-knowledge-gap/#2d3e928a2830.
3. Allen, E. and Seaman, J. (2013) Changing Course: Ten Years of Tracking Online Education in the United States, Sloan Consortium, Newburyport.
4. Bashir, M., Wee, C., Memon, N. and 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.
5. Brooks, N., Greer, T. and Morris, S. (2018) Information Systems Security Job Advertisement Analysis: Skills Review and Implications for Information Systems Curriculum, *Journal of Education for Business*, 93, 5, 213-221.
6. Conklin, W., Cline, R. and Roosa, T. (2014) Re-Engineering Cybersecurity Education in the Us: An Analysis of the Critical Factors, *Proceedings of the 47th Hawaii International Conference on System Sciences*, January 6 - 9, Waikoloa, HI, USA, IEEE.
7. Hallett, J., Larson, R. and Rashid, A. (2018) Mirror, Mirror, on the Wall: What Are We Teaching Them All? Characterising the Focus of Cybersecurity Curricular Frameworks, *2018 {USENIX} Workshop on Advances in Security Education ({ASE} 18)*.
8. Joyner, D., Goel, A. and Isbell, C. (2016) The Unexpected Pedagogical Benefits of Making Higher Education Accessible, *Proceedings of the Third ACM Conference on Learning @ Scale*, Edinburgh, Scotland, UK, ACM, 117-120.
9. Kam, H., Menard, P., Ormond, D. and Katerattanakul, P. (2018) Ethical Hacking: Addressing the Critical Shortage of Cybersecurity Talent, *Proceedings of the Pacific Asia Conference on Information Systems*, July 8 - 12, Yokohama, JA.
10. Kreider, C. (2017) Applying the Technology Acceptance Model (Tam) to Automatic Grading Technology for Large Projects, *Southern Association for Information Systems*, March 24 - 25, St. Simons Island, GA, AIS.
11. Means, B., Toyama, Y., Murphy, R. and Baki, M. (2013) The Effectiveness of Online and Blended Learning: A Meta-Analysis of the Empirical Literature, *Teachers College Record*, 115, 3, 1-47.
12. Myers, M. (1997) Qualitative Research in Information Systems, *MIS Quarterly*, 21, 2, 241-242.
13. NeSmith, B. (2018) The Cybersecurity Talent Gap Is an Indsutry Crisis. Retrieved 2/14/19 from https://www.forbes.com/sites/forbestechcouncil/2018/08/09/the-cybersecurity-talent-gap-is-an-industry-crisis/
14. Newhouse, W., Keith, S., Scribner, B. and Witte, G. (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, *NIST Special Publication*, 800, 181-182.
15. Paulsen, C., McDuffie, E., Newhouse, W. and Toth, P. (2012) NICE: Creating a Cybersecurity Workforce and Aware Public, *IEEE Security & Privacy*, 10, 3, 76-79.
16. Pusey, P., Gondree, M. and Peterson, Z. (2016) The Outcomes of Cybersecurity Competitions and Implications for Underrepresented Populations, *IEEE Security & Privacy*, 14, 6, 90-95.
17. Thompson, J., Herman, G., Scheponik, T., Oliva, L., Sherman, A., Golaszewski, E., Phatak, D. and Patsourakos, K. (2018) Student Misconceptions About Cybersecurity Concepts: Analysis of Think-Aloud Interviews, *Journal of Cybersecurity Education, Research & Practice*, 1, 5.
18. Trilling, R. (2018) Creating a New Academic Discipline: Cybersecurity Management Education, *Proceedings of the 19th Annual SIG Conference on Information Technology Education*, October 3 - 6, Ft. Lauderdale, FL, USA, ACM, 78-83.
19. Tunc, C. and Hariri, S. (2015) Claas: Cybersecurity Lab as a Service, *Journal of Internet Services and Information Security*, 5, 4, 41-59.
20. Wei, W., Mann, A., Sha, K. and Yang, T. A. (2016) Design and Implementation of a Multi-Facet Hierarchical Cybersecurity Education Framework, *IEEE Conference on Intelligence and Security Informatics*, September 28 - 30, Tuscon, AZ, USA, 273-278.
21. White, S. K. (2016) Top U.S. Universities Failing at Cybersecurity Education. (2018), Retrieved 12/18/2018 from https://www.cio.com/article/3060813/it-skills-training/top-u-s-universities-failing-at-cybersecurity-education.html