Community College Cybersecurity Programs: a Proposed Framework

Patrick Ward
patrick.ward@cgu.edu
Center for Information Systems and Technology
Claremont Graduate University
Claremont, CA 91711 US

Abstract

This paper describes a work in progress for developing a cybersecurity program framework. The framework will include factors that affect cybersecurity program development ranging from program accreditation to program designation, industry needs, faculty initiatives, and state guidelines for public community colleges. I have modified an existing framework using action-design research and I am now validating the factors by conducting a Delphi study of faculty responsible for the developing cybersecurity programs.

Keywords: community college, curriculum development, cybersecurity.

1. INTRODUCTION

There are many challenges to training cybersecurity professionals well. Various efforts that mainly address curriculum development have been made in the past with limited success (Mew, 2016; Yates, Frydenberg, Waguespack, McDermott, OConnell, Chen & Babb, 2018; Yang and Wen, 2017), and they all fall short when it comes to training undergraduates in two-year degree programs to be ready to combat the causes of cybersecurity incidents. They may fail to address industry's needs. Thus, this work in progress proposes to not only develop and test a framework and methodology for developing cybersecurity curricula, but to validate the factors, including industry needs, influencing program development by conducting a Delphi study of faculty responsible for developing cybersecurity programs.

Various standards are in use as curriculum development guidelines. The Department of Homeland Security (DHS) in partnership with the National Security Agency (NSA) created a Center of Academic Excellence Cyber Defense (CAE-CD) designation (NSA, 2020) for programs that meet certain standards. Three principal organizations accredit cybersecurity programs: Association of Technology, Management, and Applied Engineering (ATMAE), Accreditation Council for Business Schools and Programs (ACBSP) and Accreditation Board for Engineering and Technology (ABET). There are industry recognized certifications that can be used to guide curriculum development (Knapp, Maurer and Plachkinova, 2017), and a joint task force formed the Cyber Security Education Consortium (CSEC) to produce the CSEC2017 standard (JTF, 2017). The Association of Computing Machinery (ACM) recently released curriculum guidance (Tang, Tucker, Servin, Geissler and Stange, 2020) that relates to both National Initiative for Cybersecurity Education (NICE) and CAE knowledge units (KUs). I found one paper that describes using ATMAE to guide curriculum development (Doggett, 2015). While the paper describes a 2-year undergraduate program, it fails to address the methodology used for curriculum development. Each of the above efforts addresses curriculum development, but they fail to address all the underlying factors that influence that development.

Having established a need for a framework for community college cybersecurity program

development, I outline the rest of this work in progress below. First, a brief literature review showing the factors influencing curriculum development. Then, I discuss the Action Design Research (ADR) method that I used to modify an existing framework (Kim and Beuran, 2018) and how I constructed the framework. Then, I discuss how I plan to validate the factors influencing program development using a Delphi study, my contribution to the field, limitations, and a conclusion.

2. LITERATURE REVIEW

The introduction established the need for a framework to follow when developing an undergraduate cybersecurity program curriculum (the "why" of the design). Prior to discussing the methodology that one could use to develop a curriculum, one must realize that there are many factors influencing curriculum development. Curriculum standards are one such factor. Some curriculum standards include CSEC2017 (Conklin and Bishop, 2018), CAE (Clark and Stoker, 2018), CS2013 (McGettrick, 2013), and NICE (McGinnis and Comstock, 2003). The problem this work in progress tries to solve is the impact that all factors have on curriculum development, not just individual curriculum standards.

Another factor affecting curriculum development is the accreditation of the cybersecurity program itself. Three principal organizations that accredit cybersecurity programs are ABET, ACBSP and ATMAE. While many of the papers discuss ABET (e.g. Harris and Patten, 2015), I have not found a paper that discusses meeting ATMAE accreditation requirements for a 2-year undergraduate cybersecurity curriculum. ABET only offers its Computing Accreditation Commission (CAC) accreditation to 4-year schools. ACBSP has a business orientation, not information technology. However, the ATMAE accreditation is the most appropriate for an IT curriculum at a 2-year college. Table 1 lists the ATMAE standards. This paper looks at the factors influencing program development regarding standards 5, 6, 16, and 17.

Designation is another factor. There are two main designation options for an undergraduate cybersecurity program. Because cybersecurity is a blend of the computer science and information technology disciplines (NIST, 2014), the designations stem from both computer science (CS20123, CSEC2017) and information technology (NSA, 2020). There are four types of computer science requirements for the computer science designation: knowledge areas, crosscutting concepts, application areas, and disciplinary lenses (JTF, 2017). The information technology designation requires similar knowledge units (KUs) that cover the above topic areas via the CAE-CD designation.

Standard 1	Preparation of Self Study
Standard 2	Program Definition
Standard 3	Program Title & Mission
Standard 4	Program Goals
Standard 5	Program Learning Outcomes Identification & Validation
Standard 6	Program Structure & Course Sequencing
Standard 7	Student Admission & Retention Standards
Standard 8	Transfer Course Work
Standard 9	Student Enrollment
Standard 10	Administrative Support & Faculty Qualifications
Standard 11	Facilities, Equipment & Technical Support
Standard 12	Program/Option Operation
Standard 13	Graduate Satisfaction with Program/Option
Standard 14	Employment of Graduates
Standard 15	Job Advancement of Graduates
Standard 16	Employer Satisfaction with Job Performance
Standard 17	Advisory Committee Approval of Overall Program
Standard 18	Outcome Measures Used to Improve Program
Standard 19	Program Responsibility to Provide Information to the Public

Table 1: ATMAE Standards (ATMAE, 2021)

These factors influencing curriculum development are relevant when developing an undergraduate cybersecurity program curriculum. There are even more factors that we discover in the next section when we review an existing framework.

3. EXISTING FRAMEWORK

(Kim and Beuran, 2018) propose a conceptual methodology for designing a cybersecurity education program for higher education. Their paper focuses on the steps applied at a four-year university, but they do not actually implement a

ISSN: 2473-4901
v8 n5824

program, so there are no empirical data on which to assess their methodology. The authors outline the steps required to design a cybersecurity curriculum including reviewing existing programs, defining an educational framework, designing a program curriculum, selecting appropriate pedagogical methods, developing curriculum content, and testing and revising the content. Kim and Beuran (2018) cite the NIST Cybersecurity Framework (NICE), but they ignore the CAE-CDE designation requirements, and other relevant frameworks like CSEC2017 and ACM2013. The authors reference the use of integrative learning theory in developing a holistic cybersecurity education model encompassing curriculum development, experiential learning methods, assessments, and building communities of practice (CoPs). The authors also cite two pedagogical models and methods: Kuzmina-Bespalko-Popovsky (KGP) and Process Oriented Guided Inquiry Learning (POGIL). Kim and Beuran (2018) present their educational program design methodology in Figure 1 of their paper that helps to visualize their model.

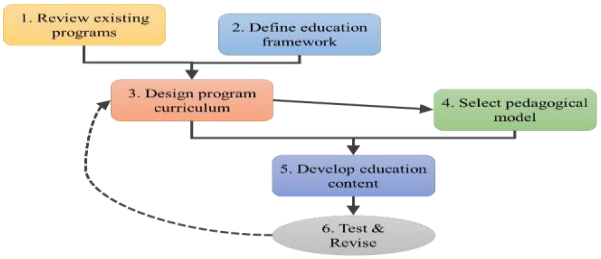

Figure 1: Educational program design methodology

The authors further clarify what they mean by defining the educational framework in dimensions: institutional, users: learners and stakeholders, and external. The authors also propose a curriculum design outline in very broad terms, but the more specific examples in other papers provide more guidance. The authors do have a relatively thorough discussion on choosing pedagogy, which is helpful in analyzing the various discussions of pedagogy in other papers. It also helps to put the various pedagogical methods in the context of a cybersecurity program. In developing educational content, the authors recommend holding a workshop. The final step of revising and testing would occur once a program has been in existence for several years.

I propose to modify the above educational program design methodology specifically to accommodate the design of an ATMAE-accredited cyber security program at a 2-year community college that prepares students to become cybersecurity professionals that the local industry needs.

My proposed solution as outlined at EDSIG 2020 follows:
This is an ongoing effort with a community college cybersecurity program for six years. The program has been steadily increasing in enrollment from 20 in the fall 2016 semester to 54 in the fall 2022 semester. We use ATMAE standards for accreditation. Local industry is consulted twice yearly for their inputs regarding the program and for suggestions for improvement. We review various certification organizations for the different certifications offered, their relevance to the program, and local industries' desire for them. I specify the proposed framework in Figure 2.

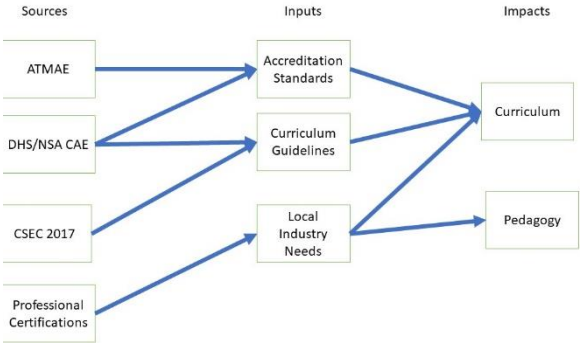

Figure 2: Program Development Factors

Table 2 lists only the computer information technology courses in the current program curriculum. We updated these courses, including sequencing and content, based on the factors listed in Figure 2. Some examples include having CITC 1302 offered prior to CITC 1351 because CITC 1351, the intro cyber course, requires a fundamental understanding of networking taught in the CITC 1302 course. Requiring the CITC 1332 Linux course early in the curriculum becomes necessary to learn command line interfaces on routers in CITC 2351 and other command line tools in CITC 2358. The command line skills taught in the CITC 1332 Linux course also become necessary in the CITC 2356 Penetration Testing course as we use many Kali Linux command line tools in the course.

We changed our curriculum based on industry input via our industry advisory board and added the CITC 2351 CCNA Security course and the CITC 2358 Cybersecurity Operations course replacing existing courses that local industry indicated that they no longer needed skills sets. We also updated student-learning outcomes for courses based on industry input.

Term/Year	Course	Course Name
Fall/1st	CISP 1010	Computer Science 1
	CITC 1302	Introduction to Networking
	CITC 1351	Principles of Info Assurance
Spring/1st	CISP 1020	Computer Science 2
	CITC 1303	Database Concepts
	CITC 1332	UNIX/Linux Operating System
	CITC 2326	Network Security
Fall/2nd	CITC 2335	Systems Analysis and Design
	CITC 2351	CCNA Security
	CITC 2352	Digital Forensics
	CITC 2358	CCNA Cybersecurity Operations
Spring/2nd	CITC 2354	Advanced Digital Forensics
	CITC 2356	Penetration Testing and Network Defense
	CITC 2391	Special Topics in CIT
	CITC 2399	CIT Internship

Table 2: Proposed Program Curriculum (updated from (Ward, 2020)

4. METHOD (ADR)

I considered Takeda's design cycle (Takeda, Veerkamp and Yoshikawa, 1990) because it is an early adoption of using design science research (DSR) as a research paradigm for IS research projects as outlined in Hevner's MISQ 2004 paper (Hevner, March, Park, and Ram, 2004). I also looked at Action Design Research (ADR) (Sein, Henfridsson, Purao, Rossi and Lindgren, 2011). ADR seemed more relevant for this paper than DSR because ADR considers the organizational context.

In this case, the organizational context contributes prospective employers for the students, accreditation requirements, a setting as in a trade school or a 4-year university to the cybersecurity program's development. The effect that the organizational context has on the program's development cannot be understated, and hence the need to recognize the organizational context's contribution necessitates the use of an approach that considers the organizational context.

In ADR, researchers develop innovative artifacts (such as models, theories, or prototype systems) that solve a general set of problems. In this study, I develop a framework to use to develop a cybersecurity program at a community college. ADR defines an appropriate approach to this complex problem. This proposal's "ensemble artifact" (Orlikowski & Iacono, 2001) is the cybersecurity program itself. I will use the ADR method itself to justify its use in this case. I adapt ADR as the research methodology for this study. I chose this approach because of the influence that the organizational context has on the development of the college's cybersecurity program.

The central activity in ADR is building and evaluating the designed artifacts and theories (Sein, et al., 2011). During this stage, the theorist creates an early design of an artifact. Artifacts can be in the form of frameworks, models, or systems. In the present study, I design an artifact in the form of a framework to identify cybersecurity program development prerequisites. The designed artifact will be tested and further modelled during the interventions.

After considering using the three design science research cycles of relevance, design, and rigor (Hevner, 2007) to perform each of the Takeda, et al., process steps, the author chose to modify them to conform to the ADR methodology leading to the final proposed framework. The iterations will consist of changes made to the curriculum because of industry input or student performance against learning objectives. Additional iterations may be necessary to accommodate industry certifications, academic program accreditation or other external inputs. Iterations may also include both formative and cumulative assessments of student work, major field competency tests at graduation, and feedback from employers on recent graduates' knowledge.

4. PROCESS

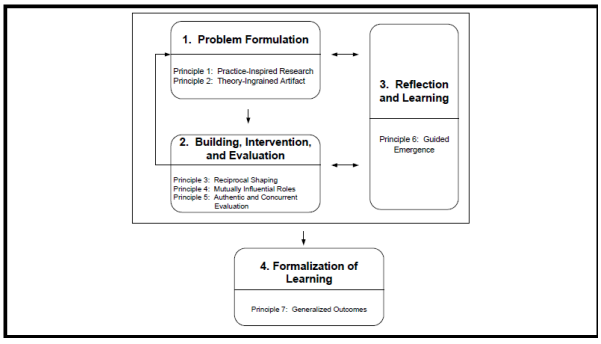

Figure 3: Action Design Research (ADR) Method: Stages and Principles

The author will also use the ADR stages reflected in Figure 3 (Sein, et al., 2011).

The first stage of ADR is problem formulation. The introduction introduced the problem of developing a program that meets the needs of various stakeholders. These stakeholders are all part of the organizational context. The initial scope of the problem is to develop a program that meets the needs of faculty, students, and cybersecurity professionals representing Kim and Beuran's (2018) three dimensions in the Existing Framework section above. This problem posed a unique research opportunity using the existing theories as discussed in the Existing Framework section to develop a cybersecurity program fitting the college's organizational context. The formulation of the problem relies on practice-inspired research in which I create knowledge through revising and testing a new cybersecurity program to meet the college's changing organizational context. The "ensemble artifact," i.e., the program itself, in ingrained in Kim and Beuran's (2018) framework as a Gregor (2006) Type V design theory.

Kim and Beuran's (2018) three dimensions of the institution, the users, and external are useful in describing the situation at the college. Both the current and the prospective students, i.e., both the students who are currently seeking employment after graduation and the students who are considering attending the college's cybersecurity program to gain employment in the industry after graduation, represent the users. The users of the program are also represented by the faculty themselves that provide input based on their own IT and cyber experience into the cybersecurity programs' development. The college and its various regional and program accreditations represent the institutional dimension. The Existing Framework section mentions the ATMAE accreditation and the college itself needs a SACS accreditation. The local industry advisory board (IAB), which is composed of hiring managers from some of the local companies employing students in the cybersecurity and IT industries, represent the external dimension.

The second stage is building out, intervening in, and evaluating the artifact, i.e., the program. The organizational context dominates the program. First, the academic publisher's textbook offerings with courses formed around each textbook's 15 or so chapters corresponding to 15-week semesters. The program initially held an AACSB accreditation, but the requirements for that accreditation changed, and the faculty elected to pursue a new accreditation with ATMAE. Initially, the faculty, representing IT nationwide, deemed the curriculum adequate. However, after conferring with the local IAB the faculty determined that the program needed to have some basis in nationally recognized industry accredited certifications. Each iteration of the program's build-out bases itself on recursive cycles of decisions made by the stakeholders as the organizational context changes. Even the IAB members themselves changed as either needs changed and the IAB member no longer came, or new needs arose, and a different company would participate in the IAB to help influence the faculty's decisions.

Another input at this second stage is the curriculum committee process of developing, submitting, discussing, and approving curriculum changes. The process of modifying the courses is essentially the same at each iteration as curriculum committee reviews each change to the curriculum, but how those changes come about varies depending on industry input, accreditation changes, or industry-recognized certification changes. Initially, faculty created the cybersecurity program because there was no previous program and there was an industry need. However, as industry needs change, so must the curriculum. Since the IAB meets once a semester (twice a year), there exist ample evaluation opportunities to ensure that the program is meeting those needs. One change to the evaluation process itself is to elicit input from key industry stakeholders to ensure that needs are being met. One such example was a dialogue with representatives of the local utility company and their corresponding staffing agency to ensure that the college's cybersecurity program was meeting their needs. Because of this, faculty added student preparation for additional industry certification exams to the existing courses by modifying those courses to be more comprehensive in their coverage of topics on the exams. As we update the exams themselves every few years, there is now a periodic curriculum evaluation for those certification courses to ensure that they meet current certification exam requirements (Ward, 2021).

5. VALIDATION USING DELPHI

My work in 2020 was to develop the framework that you see in Figure 2, and I have since updated the curriculum you see in Table 2. The next step in the process is for me to validate the factors that I represent in Figure 2 with a Delphi study.

I propose to use a Delphi study to validate the

factors that I used for cybersecurity program development and to answer the following research questions:

- What do experts identify as important to the development of cybersecurity programs?
- What do experts identify as important to the development of assessments and rubrics in cybersecurity programs?
- What do experts identify as important to the development and implementation of learning resources in cybersecurity programs?
- What curriculum standards guided the experts in developing their cybersecurity programs?

I chose a qualitative research design because it provides an opportunity to explore the thought processes of cybersecurity education practitioners. The goal of this research is to determine effective practices for building cybersecurity programs. Using questionnaires allows for determining various effective practices.

The Delphi method is well suited for understanding effective practices in developing academic programs that acknowledges the input from experts in the field understanding individual viewpoints. A high response rate is essential to the validity of the results. The Delphi method is a preferred qualitative approach for this work in progress because there are multiple cybersecurity curriculum models available, and each institution has its own unique approach. The Delphi method allows the opportunity to examine multiple perspectives to find a broader consensus related to cybersecurity program development.

Since the process of developing cybersecurity programs is challenging, this method is particularly appropriate to ensure consideration of multiple perspectives. The goal is to find where these individual perspectives converge, and what commonalities may exist. These commonalities may inform an emerging set of best practices that institutions can use to develop cybersecurity programs.

In this study, I plan on three rounds of e-mail and/or telephone/online interviews. The participants will remain anonymous. The process is an iterative one that requires evaluation and re-evaluation of data by determining possible themes and common ideas from the participants. After round one, questions for round two will ask participants to identify areas of agreement, areas of disagreement, and any additional relevant factors. Round three questions will follow the same format until consensus.

I will recruit initial participants from my professional network of peers who have developed or are teaching in cybersecurity programs. I will recruit more participants by snowball sampling. I will verify the existence of the cybersecurity program. Since the research topic is narrow (factors influencing the development of cybersecurity programs), the field of potential participants is limited to those with experience developing or teaching in these programs. To manage the results of the research study and obtain enough information to make conclusions, I will recruit 25 participants with the goal of obtaining a minimum sample size of 10.

6. CONTRIBUTION

I hope that this work in progress of developing a framework will help other community colleges as they develop their cybersecurity programs. As the curriculum development process is constantly in flux, it is essential that educational institutions adapt to meet those needs. As I am now working on developing such a framework for a community college, and I plan to gather the insight of other community college cybersecurity program developers, I hope that the guidance that they provide can help guide colleges as they both develop new and modify existing programs.

7. LIMITATIONS

I only plan to conduct the Delphi study with community college cybersecurity program developers, so the factors influencing them may not be similar to those factors influencing people that develop cybersecurity programs for 4-year universities or training specific to certain jobs. However, as community colleges exist as both a bridge to immediate employment and as a transition from secondary education to 4-year universities, the colleges have the potential to influence both curriculum development at the 4-year universities and at the high schools as the students' transition to college.

8. CONCLUSION

This work in progress hopes to explore those factors influencing community college cybersecurity program development. Certain factors influence my curriculum development, and hopefully, other people use these factors at other public community colleges and they can use these factors at 4-year universities as they create and/or modify programs to keep pace with the changing field of cybersecurity and industry needs.

9. REFERENCES

Association of Technology, Management, and Applied Engineering (ATMAE) ATMAE Accreditation Handbook (2021) downloaded from https://cdn.ymaws.com/www.atmae.org/resource/resmgr/accred_2018/2021_accreditation_handbook_.pdf

Clark, U., & Stoker, G. (2018). Reflections on Applying for CAE-CDE Designation. In Proceedings of the EDSIG Conference ISSN (2473) 3857.

Conklin, W., & Bishop, M. (2018). Contrasting the CSEC 2017 and the CAE Designation Requirements. In 2018 51st Hawaii International Conference on System Sciences (pp. 2435-2441). IEEE.

Doggett, M. (2015). Defining the technology management body of knowledge for ATMAE-accredited programs. Technology Interface International Journal, 16(1), 87-99.

Gregor, S. (2006). "The Nature of Theory in Information Systems," MIS Quarterly (30:3), pp. 611-642.

Harris, M. A., & Patten, K. P. (2015). Using Bloom's and Webb's Taxonomies to Integrate Emerging Cybersecurity Topics into a Computing Curriculum. Journal of Information Systems Education, 26(3).

Hevner, A., S. March, J. Park, and S. Ram (2004) Design Science in information systems research, MIS Quarterly, 28 (1), pp. 75-105.

Hevner, A. (2007) A three-cycle view of design science research. Scandinavian Journal of Information Systems 19 (2), pp. 87-92.

Joint Task Force (JTF) on Cybersecurity Education, CyberSecurity Curricula 2017 (CSEC 2017) downloaded from https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf.

Kim, E., & Beuran, R. (2018, October). On designing a cybersecurity educational program for higher education. In Proceedings of the 10th International Conference on Education Technology and Computers (pp. 195-200). ACM. https://dx.doi.org/10.1145/3290511.3290524.

Klašnja-Milićević, A., M. Ivanović, B. Vesin, and Z. Budimac (2018), "Enhancing e-learning systems with personalized recommendation based on collaborative tagging techniques," Appl. Intell., (48)6, 1519–1535.

Knapp, K., Maurer, C., & Plachkinova, M. (2017). Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance. Journal of Information Systems Education, 28(2), 101-113.

McGettrick, A. (2013). Toward effective cybersecurity education. IEEE Security & Privacy, 11(6), 66-68. doi:10.1109/MSP.2013.155.

McGinnis, D. R., & Comstock, K. (2003). The implications of information assurance and security crisis on computing model curricula. Information Systems Education Journal, 1(9), 1-12.

Mew, L. (2016). The Information Security Undergraduate Curriculum: Evolution of a Small Program. In Proceedings of the EDSIG Conference ISSN (Vol. 2473, p. 3857).

NIST SP 800-181 National Initiative for Cybersecurity Education (NICE) Framework (2014) downloaded from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

NSA, National Centers of Academic Excellence (CAE) Resource Guide (2020) downloaded from https://www.iad.gov/NIETP/documents/Requirements/20201019_CAE2021_Proposed_CDE_Designation_Requirements.pdf

Orlikowski, W. J., and Iacono, C. S. 2001. "Research Commentary: Desperately Seeking the 'IT' in IT Research—A Call to Theorizing the IT Artifact," Information Systems Research (12:2), pp. 121-134.

Sein, M. K., O. Henfridsson, S. Purao, M. Rossi, and R. Lindgren (2011), "Action design research," MIS Q. Manag. Inf. Syst., 35 (1), 37–56.

Takeda, H., Veerkamp, P., & Yoshikawa, H. (1990). Modeling design process. AI magazine, 11(4), 37.

Tang, C., Tucker, C., Servin, C., Geissler, M., & Stange, M. (2020, February). Curricular Guidance for Associate-Degree Cybersecurity Programs. In Proceedings of the 51st ACM Technical Symposium on Computer Science Education (pp. 1285-1285).

Ward, P. (2020). "Development of a Small Cybersecurity Program at a Community College." In Proceedings of the EDSIG Conference ISSN (Vol. 2473, p. 4901).

ISSN: 2473-4901
v8 n5824

http://proc.iscap.info/2020/

Ward, P. (2021). "Constructing a Methodology for Developing a Cybersecurity Program." In Proceedings of the 54th Hawaii International Conference on System Sciences (p. 44). https://scholarspace.manoa.hawaii.edu/handle/10125/72125

Yang, Samuel C. & Bo Wen (2017). Toward a cybersecurity curriculum model for undergraduate business schools: A survey of AACSB-accredited institutions in the US, Journal of Education for Business, 92:1, 1-8, DOI:10.1080/08832323.2016.1261790.

Yates, D. J., Frydenberg, M., Waguespack, L. J., McDermott, I., OConnell, J., Chen, F., & Babb, J. S. (2018). Dotting i's and Crossing T's: Integrating Breadth and Depth in an Undergraduate Cybersecurity Course. Information Systems Education Journal, 17(6), 41.