Journal of Information Systems Education

Volume 35
Issue 3
Summer 2024

A Curriculum Model of Cybersecurity Bachelor's Programs in AACSB-Accredited Business Schools in the US

Samuel C. Yang

Recommended Citation: Yang, S. C. (2024). A Curriculum Model of Cybersecurity Bachelor's Programs in AACSB-Accredited Business Schools in the US. *Journal of Information Systems Education*, 35(3), 313-324. https://doi.org/10.62273/FRJE3390

Article Link: https://jise.org/Volume35/n3/JISE2024v35n3pp313-324.html

Received:	July 30, 2023
First Decision:	October 24, 2023
Accepted:	February 4, 2024
Published:	September 15, 2024

ISSN: 2574-3872 (Online) 1055-3096 (Print)

Journal of Information Systems Education, 35(3), 313-324, Summer 2024
https://doi.org/10.62273/FRJE3390

A Curriculum Model of Cybersecurity Bachelor's Programs in AACSB-Accredited Business Schools in the US

Samuel C. Yang
College of Business and Economics
California State University, Fullerton
Fullerton, CA 92831, USA
syang@fullerton.edu

ABSTRACT

Amid the ever-increasing number of cyberthreats, cybersecurity degree programs represent a potential growth area for business schools. This study examines undergraduate cybersecurity programs offered by AACSB-accredited business schools in the US. It surveyed 503 AACSB-accredited schools and identified 72 cybersecurity programs. Using the IS2020 and CAE-CD standards, this study assessed these programs' core curricula and found that the top three core courses are Cybersecurity Foundations, Application Development and Programming, and IT Infrastructure. A cybersecurity curriculum model is developed based on the survey results. The results are compared with those of a 2017 study to gain insights into the evolution of cybersecurity curricula in business schools.

Keywords: AACSB, IS curriculum, Computing education, Cybersecurity, Information assurance & security, Model curricula

1. INTRODUCTION

The Russia-Ukraine war that began in 2022 has elevated cyber risks (Stupp & Nash, 2023) and highlights the importance of cybersecurity and cyber defense. Because of the war in Ukraine, 29% of organizations increased their focus on business continuity and resiliency, and 22% experienced increased cyberattacks (ISC2, 2022). As organizations depend more on information technology (IT) to conduct business, they are increasingly subject to attacks and breaches. In particular, ransomware has remained the top attack for more than three years, and the most common access vectors for ransomware include phishing and vulnerability exploitation (IBM, 2022). In the future, cyberthreats may be enabled by artificial intelligence (AI). The popular AI tool ChatGPT (OpenAI, 2022) can draft texts for phishing emails and write potentially malicious codes (Check Point Research, 2023); moreover, there are concerns that AI will democratize cybercrime (Keary, 2022). Globally, the cost of cybercrime increased by 80% over two years, from $522.5 billion in 2018 to $945 billion in 2020 (Smith & Lostri, 2020).

In response, 66% of the CIOs surveyed planned to increase their cybersecurity budget, making cybersecurity CIOs' top investment priority—surpassing the 55% who chose business intelligence and analytics (Rosenbush, 2022). However, as the demand for cybersecurity talent increases, there is a shortage of such professionals. Globally, even with a growth of more than 464,000 cybersecurity workers (11.1% year-over-year) from 2021 to 2022, the cybersecurity workforce gap has increased even more by 26.2% year-over-year in the same period (ISC2, 2022). Of those organizations that suffered one or more breaches, 60% reported having trouble recruiting cybersecurity talent (Fortinet, 2022).

These results are consistent with the outlook of the US Bureau of Labor Statistics (BLS). Between 2021 and 2031, the employment of "Information Security Analysts" has the highest growth rate (35%) in the BLS Computer and Information Technology group (BLS, 2022). ("Web Developers and Digital Designers" has the second highest growth rate of 23% in the same group.) In fact, the BLS ranks "Information Security Analysts" as the 8th highest-growth occupation out of *all* occupations (BLS, 2022). Given the lower supply of cybersecurity professionals amid increasing demands from businesses (Duffy, 2021), their pay has also increased. ISC2 found that US cybersecurity professionals with a bachelor's degree earn $130,000 annually (ISC2, 2022). Overall, "cybersecurity workers are in greater demand than they have ever been before and supply cannot keep up" (ISC2, 2022, p. 17).

The persistent gap between supply and demand for cybersecurity professionals creates an opportunity for universities (Tsado, 2019), and the need for managerial, leadership, and soft skills of these professionals creates an opening for business schools. Business schools can help train cyber professionals because cybersecurity is not only technical but also multidisciplinary (Blair et al., 2019). In addition to technical issues, cybersecurity encompasses organizational issues often addressed by business schools, such as social media risks and security compliance, as well as accounting, auditing (Stafford et al., 2018), management, law (Craigen et al., 2014), policy, ethics, and risk management (Joint Task Force on Cybersecurity Education, 2017).

Amidst increasing cyberthreats against organizations, only 6.7% of undergraduate information systems (IS) programs in business schools require a security course (Bohler et al., 2020). While some call for a separate IT security core course in the IS curriculum (Avery & Oakley, 2019), cybersecurity in the

business curriculum (Weiser & Conn, 2017), and even cybersecurity in general education (Redman et al., 2020), this study examines actual cybersecurity curricula in business schools. To gain an inclusive perspective, this study collected data from all undergraduate business schools accredited by The Association to Advance Collegiate Schools of Business (AACSB), not just from a sample of schools. To that end, the objectives of this study are first, to assess the core courses required for their cybersecurity degrees and second, to examine the changes in the core courses required by the institutions over time. The first objective is necessary because core courses reflect peer institutions' view on the discipline's essential body of knowledge, which can help curriculum designers gain insights into and structure their curricula and courses. The second objective is needed because reviewing curricula is an ongoing and continuous process (Leonard et al., 2019); technology-oriented programs operate in a competitive environment, and these programs "need to adopt new courses in response to anticipated market needs" (Elazhary & Morelli, 2016). Because cybersecurity is a dynamic field and threats constantly evolve, a cybersecurity curriculum must meet the changing cyberthreats and ensure that students acquire up-to-date skills. By examining trends in the required core courses, this study elucidates the changing market demands reflected in both the core courses and the resulting empirical curriculum model informed by such demands.

2. LITERATURE REVIEW AND MOTIVATION FOR STUDY

For business schools, Yang and Wen (2017) previously reviewed the literature on undergraduate cybersecurity curricula; thus, the present study's literature review focuses on those works published since 2017. Since then, the literature has primarily centered on studies at the program level and the curriculum level. At the program level, Knapp et al. (2017) analyzed a single business school's cybersecurity program and its courses' correspondence to various certifications, including the Certified Information Systems Security Professional (CISSP), the Certified Information Security Manager (CISM), and the Certified Information Systems Auditor (CISA). The authors advocated considering professional certifications to maintain the currency of the cybersecurity curriculum. Clark et al. (2020) described their experience applying for a National Centers of Academic Excellence (CAE)-the designated institution in cybersecurity. They documented the process of mapping the institution's courses to the various knowledge units (KUs) required by the CAE program. Grover et al. (2016) examined security courses offered by IT programs of The University of North Carolina (UNC) system. They compared these security courses with the Information Assurance and Security (IAS) knowledge area of ACM's IT curriculum guideline and found that each UNC campus does not cover all IAS knowledge areas. In an undergraduate cybersecurity program, Payne et al. (2020) reported utilizing high-impact practices, such as learning communities, research, internships, service learning, and e-portfolios. Based on their experience, they made specific recommendations on developing best practices and implementing them. Towhidi and Pridmore (2023) proposed a backward course design process, which was used to design a cybersecurity course for the Bachelor of Business Administration (BBA) in Management Information Systems (MIS) program at a midsize AACSB-accredited business school; the backward course design process aims to align the course with the industry's cybersecurity needs.

Other works focus on cybersecurity coverage in non-IS business programs. Raineri and Fudge (2019) sent surveys to students in undergraduate entrepreneurship programs at 58 universities. They found that these students have some understanding of cybersecurity, but their knowledge may need to be improved given the threats faced. For example, when asked, "I understand at least two precautions regarding social engineering" (Raineri & Fudge, 2019, p. 80), 61% of the students claimed no knowledge or understanding of the question. Small businesses rely on various technologies to run their operations, but because of limited resources available to protect the organization, cyberattacks can severely impact an entrepreneur's business (Raineri & Fudge, 2019). Plachkinova and Pittz (2021) used an inquiry-based approach involving 54 cybersecurity undergraduate students and 26 entrepreneurship graduate students (at a business school) to analyze the risks of startup firms. At the end of the semester, students reported an increase in their understanding of the negative consequences of security threats and their ability to quantify security costs.

At the curriculum level, several studies make recommendations regarding curricula and content based on conceptual rationales or interviews/surveys. Shoemaker et al. (2019) called for including ethics in cybersecurity curricula. Tsado (2019) advocated for a top-driven, multidisciplinary, and school-wide approach to developing cybersecurity education programs, including those in business schools. There have also been calls to align cybersecurity curricula with industry skill demands better. Jones et al. (2018) asked 44 cybersecurity professionals about the relative importance of 32 knowledge, skills, and abilities (KSAs) in the "Protect and Defend" category of the National Initiative for Cybersecurity Education (NICE) Framework (Newhouse et al., 2017). The results can provide "direction for prioritizing KSAs in cyber curricula…" (Jones et al., 2018, p. 11:3). Brooks et al. (2018) developed 20 domain-related skills that are in demand by analyzing 798 cybersecurity job postings. These skills can also provide "curriculum designers with a more robust understanding of employer expectations…" (Brooks et al., 2018, p. 215). Parekh et al. (2018) identified 53 core topics for assessing graduating cybersecurity students by utilizing the Delphi method with 36 experts, and the identified core topics can "provide insights into the core concepts of a curriculum…" (Parekh et al., 2018, p. 17).

This literature review shows that research on undergraduate cybersecurity programs is limited, especially lacking cross-sectional studies of those programs in business schools. There is a gap in the literature on the maintenance of cybersecurity programs (Knapp et al., 2017), as well as a "lack of consensus on the topical content of information security programs" (Cram & D'Arcy, 2016, p. 34). Institutions must continuously evaluate their cybersecurity programs so that their curricula stay relevant (Knapp et al., 2017), and in the context of business schools, there should be a shared understanding of expectations of "skills and knowledge graduating students must have" (Raj & Parrish, 2018, p. 72).

Therefore, this paper will assess the cybersecurity curricula of a cross-section of peer business schools and will formalize the shared understanding of the curricula. This paper will focus on undergraduate cybersecurity programs because 60% of

entry-level cybersecurity jobs require a bachelor's degree (Marquardson & Elnoshokaty, 2020). With this focus, this paper will analyze AACSB-accredited business schools' cybersecurity core courses to gain insight into any emerging consensus on business schools' cybersecurity curricula. Core courses are examined because, as required courses, they represent topics deemed essential by these programs for their students to possess. A descriptive curriculum model for cybersecurity bachelor's degrees in business schools is developed based on surveys of actual core curricula. This curriculum model can then inform other business schools' development of new undergraduate cybersecurity programs.

Furthermore, several years have passed since the publication of a previous curricular survey (Yang & Wen, 2017). The intervening years saw some significant developments, including the popularization of ransomware, a focus on business continuity due to COVID-19, and the Russia-Ukraine war. Given that cybersecurity is dynamic and cyber threats change quickly, it is essential to survey how business schools have adapted their cybersecurity curricula in this rapidly changing environment. In doing so, this study will present the results collected and compare them to those obtained by the previous curricular survey, thus providing a longitudinal view of how the cybersecurity curricula offered by US institutions have evolved in the last several years.

3. RESEARCH FRAMEWORKS

Two curricular frameworks are utilized to examine core courses: one based on cybersecurity and one based on information systems (IS). For cybersecurity-related courses, this study adopts the knowledge units (KUs) published by the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program, which is sponsored by the National Security Agency (NSA) with the Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) as partners. The program's missions include establishing standards for cybersecurity curriculum and academic excellence, developing competency in students and faculty, and integrating cybersecurity practice across academic disciplines (NSA, n.d.). For cybersecurity bachelor's programs, the most applicable designation awarded by the NCAE-C program is the Cyber Defense (CAE-CD) designation. The CAE-CD designation is awarded to regionally accredited schools offering cybersecurity programs at the associate's, bachelor's, master's, and doctoral levels. To be awarded the CAE-CD designation, the school must offer three foundational KUs, five technical or nontechnical core KUs, and 14 optional KUs that can be aligned with courses (NCAE-C, 2022). Albert et al. (2015) called the CAE program "a de facto accreditation standard for the fledgling cybersecurity discipline" (p. 45). The NCAE-C defines a set of learning outcomes and topics for each KU. Thus, each KU is akin to an academic course. This study utilizes CAE-CD KUs to examine cybersecurity-related courses—see Table 1 (NCAE-C, 2020).

The AACSB treats IS as a business-school discipline (AACSB, 2022b), and cybersecurity is related to protecting IS in organizations. For IS bachelor's programs, IS2020 is a major curriculum framework that recommends ten required competency areas—see Table 2 (The Joint ACM/AIS IS2020 Task Force, 2020). IS2020 states that programs offering IS-specific courses "may be able to dedicate a full course to cover each competency area" (The Joint ACM/AIS IS2020 Task Force, 2020, p. 12). Thus, this study utilizes IS2020's competency areas to examine IS-related core courses. Aligning the research framework with IS2020 and CAE enables institutions not only to meet the IS2020 guidelines, but also to leverage their curricula to pursue CAE designation should they choose to do so in the future.

Knowledge Units
Foundational
Cybersecurity Foundations
Cybersecurity Principles
IT Systems Components
Technical
Basic Cryptography
Basic Networking
Basic Scripting & Programming
Network Defense
Operating Systems Concepts
Nontechnical
Cyber Threats
Cybersecurity Planning & Management
Policy, Legal, Ethics, & Compliance
Security Program Management
Security Risk Analysis

Table 1. CAE Required Knowledge Units

Competency Areas
Application Development & Programming
Data/Information Management
Ethics, Use & Implications for Society
Foundations of Information Systems
IS Management & Strategy
IS Practicum
IS Project Management
IT Infrastructure
Secure Computing
Systems Analysis & Design

Table 2. IS2020 Required Competency Areas

4. METHOD

4.1 Population and Scope of Study

The population of this study consists of undergraduate cybersecurity programs in AACSB-accredited business schools in the US. However, cybersecurity programs often have different names. Thus, to improve internal validity, the following criteria are applied to admit cybersecurity programs into the study population:

- Programs that use the terms "security" (e.g., information security or cybersecurity) or "assurance" (e.g., information assurance) in their program names are included. These programs may include concentrations, emphases, options, specializations, and tracks in cybersecurity areas.
- A program's curriculum description and course requirements must be called out and described by the

official university catalog (Elazhary & Morelli, 2016). A simple mention of recommended courses for students interested in cybersecurity (e.g., on the department's website) does not qualify.

- Programs in a related area are not included. For example, a program in a different area or with a narrower aim, such as risk management and insurance, is not included.
- Programs in narrower areas of security, such as computer forensics, are not included. This criterion assesses curricular trends in broad, general cybersecurity programs in business schools.
- Cybersecurity programs offered by computer science departments, even if they reside in business schools, are not included. This is so that the study may examine business-focused cybersecurity programs and capture the implications of their business emphasis rather than the overt technical aspects.

4.2 Data Collection Procedures

Data on business schools' undergraduate cybersecurity programs and their required courses were collected during the summer of 2022. This study adopts the direct survey methodology (Stefanidis & Fitzgerald, 2010, 2014) used by similar prior studies (e.g., Hwang et al., 2015; Osatuyi & Garza, 2014; Yang & Wen, 2017) so that the results obtained by the present study are comparable longitudinally. In this approach, the courses delineated by the research frameworks (i.e., IS2020 and CAE KUs described in the Research Frameworks section) are treated as "course categories" into which the surveyed core courses are mapped. Since 2017 (the starting year of this study's literature review), the same mapping methodology has continued to be utilized for studying curricula in undergraduate business analytics (Ceccucci et al., 2020), categorizing undergraduate and graduate cybersecurity courses and their relationships to the job market (Wang & Wang, 2019), and mapping courses in IS programs (Bohler et al., 2020; Leonard et al., 2019; Yang, 2018). In fact, Richardson et al. (2018) characterized the methodology as "a practical guide to assessing large numbers of programs" (p. 5).

In addition to using IS2020 and CAE, this study also adopts courses utilized and defined by prior studies (e.g., Topi et al., 2010; Yang & Wen, 2017) for conceptual consistency and to facilitate comparison over time. For example, a program may require a capstone course. A capstone is typically taken at the program's end and helps students integrate various skills and experiences gained during the program. Regarding the research framework, IS2020 recommends a practicum, which "can take the form of internships, integrated IS capstone projects, etc." (The Joint ACM/AIS IS2020 Task Force, 2020, p. 30). Thus, this study categorizes internships, capstones (if identified by the institution as a capstone or an integrative experience), and projects under "Practicum/Capstone."

Although a program typically requires students to take a fixed set of core courses, some programs may require students to select a subset of courses from an approved list. For all those programs requiring students to choose a subset of courses, capturing all courses on all approved course lists is not feasible from a data-collection standpoint. So, the present research takes the following approach: If a student must take 50% or more of the courses on the approved list, then all courses on the approved list are considered to be core. If not, then courses on the approved list are not considered core. This approach balances collecting data feasibly and meeting the goal of this study, which is to capture those courses deemed important by the program. The courses and their conceptual foundations are shown in Table 3.

Course Categories	Conceptual Foundations
Application Development & Programming	IS2020 required
Cloud Computing	CAE optional KU
Cybersecurity Foundations	CAE foundational KU
Cybersecurity Planning & Management	CAE core KU
Data/Business Analytics	IS2020 optional
Data/Info Management	IS2020 required
Digital Forensics	CAE optional KU
Foundations of Info Systems	IS2020 required
IT Infrastructure	IS2020 required
IT Systems Components	CAE foundational KU
Network Security	Yang & Wen, 2017
Penetration Testing	CAE optional KU
Policy, Legal, Ethics, & Compliance	CAE core KU
Practicum/Capstone	IS2020 required
Project Management	IS2020 required
Systems Analysis & Design	IS2020 required

Table 3. Course Categories and Their Conceptual Foundations

5. RESULTS

In July 2022, the AACSB website showed 503 undergraduate schools with business accreditation in the US. This study surveyed all 503 schools' official academic catalogs online and identified 72 cybersecurity programs, subject to the criteria described in the Method section. Table 4 shows the numbers and percentages of the programs requiring the courses as delineated by the research frameworks. (The table shows those courses required by more than 15% of the programs. The Appendix shows those courses required by less than 15% of the programs.) The top most-required course is IT Infrastructure (85%). The popularity of the IT Infrastructure course in cybersecurity programs may reflect the continued recognition of the importance of infrastructure in security. Rob Franch, the chief technology officer of the real-estate company Cushman & Wakefield, stated that "modernization of the network is critical for a multitude of reasons, and cybersecurity is one of them" (Rosenbush, 2021). COVID-19 has also prompted companies to emphasize business continuity efforts that require a robust IT infrastructure.

The second most-required course is Application Development and Programming (79%). This result parallels that of Ramezan (2023), who reported that programming knowledge is highly valuable for IS students entering the cybersecurity field, while Bohler et al. (2020) found that 81% of undergraduate IS programs also require programming. The present study, Ramezan (2023), and Bohler et al. (2020) together confirm the importance of programming and application development in cybersecurity and IS programs. The third most-required course is Cybersecurity Foundations

(75%). As defined by the NCAE-C, Cybersecurity Foundations is a required foundational KU and can be a broad course that introduces students to various aspects of the cybersecurity field (NCAE-C, 2020).

Course Category	*n*	%
IT Infrastructure	61	85%
Application Development & Programming	57	79%
Cybersecurity Foundations	54	75%
Data/Information Management	45	63%
Foundations of Information Systems	37	51%
Systems Analysis & Design	37	51%
Cybersecurity Planning & Management	35	49%
Practicum/Capstone	30	42%
Digital Forensics	23	32%
Network Security	22	31%
Policy, Legal, Ethics, & Compliance	22	31%
Project Management	15	21%
Penetration Testing	14	19%
Data/Business Analytics	13	18%
IT Systems Components	12	17%
Cloud Computing	11	15%

Table 4. Core Requirements of Cybersecurity Bachelor's Programs

Table 5 compares the results of the current study and those of a previous study (Yang & Wen, 2017). The three courses with the highest growth are Practicum/Capstone (+23%), Policy, Legal, Ethics, and Compliance (+12%), and Cybersecurity Planning and Management (+8%). The three courses with the largest declines are Foundations of IS (-38%), Systems Analysis and Design (-23%), and Data/Information Management (-12%). Section 6.2 discusses these changes in core requirements in more detail.

6. DISCUSSION

This section discusses developing a cybersecurity curriculum model using empirical results collected from actual cybersecurity programs. Then, in the context of this new model, it considers the evolution of undergraduate cybersecurity programs, opportunities for IS programs and business schools, limitations, and future research.

6.1 New Cybersecurity Curricular Model

Figure 1 shows the resulting curriculum model for undergraduate cybersecurity programs in business schools. This descriptive model is developed using empirical results on the most-required core courses. Of the 72 cybersecurity programs, the average number of core courses is 8.9, or nine rounded. Thus, the curriculum model contains the top nine most-required core courses (from Table 4). Cybersecurity Foundations, Cybersecurity Planning and Management, Digital Forensics, and IT Infrastructure are more closely related to cybersecurity. In contrast, Foundations of IS, Application Development and Programming, Systems Analysis and Design, and Data/Information Management are related to IS. (IT Infrastructure is applicable to both cybersecurity and IS.) In this curriculum, students can start with an introductory course to cybersecurity (i.e., Cybersecurity Foundations), then continue to the technically-oriented IT Infrastructure and Digital Forensics and the organizationally-oriented Cybersecurity Planning and Management. Students would also take the Foundations of IS, then move on to Application Development and Programming, Systems Analysis and Design, and Data/Information Management. Taken toward the program's conclusion, Practicum/Capstone integrates the learning and experiences gained throughout the curriculum. Based on the actual courses required by cybersecurity programs, this curriculum model effectively represents these programs' collective view on the essential topics and concepts to impart to students.

Course Category	Yang & Wen (2017)	Current	Change
Practicum/Capstone	19%[a]	42%	23%
Policy, Legal, Ethics, & Compliance	19%	31%	12%
Cybersecurity Planning & Management	41%[b]	49%	8%
IT Infrastructure	78%	85%	7%
Network Security	26%	31%	5%
Digital Forensics	30%	32%	2%
Application Development and Programming	81%	79%	-2%
Cybersecurity Foundations	78%[c]	75%	-3%
Project Management	26%	21%	-5%
Data/Info Management	74%	63%	-12%
Systems Analysis and Design	74%	51%	-23%
Foundations of Information Systems	89%	51%	-38%
Penetration Testing	N/A[d]	19%	N/A
Data/Business Analytics	N/A[d]	18%	N/A
IT Systems Components	N/A[d]	17%	N/A
Cloud Computing	N/A[d]	15%	N/A

[a]Reported as "Capstone/Project".
[b]Reported as "IT Risk Management/Managerial Issues".
[c]Reported as "IT Security".
[d]No data reported.

Table 5. Comparison Between the Current and Yang & Wen (2017) Results

Institutions do not have to implement this study's exact curriculum model when adopting a curriculum. Rather, the model (Figure 1) can serve as a baseline curriculum. At the same time, the study's ranked results (Table 4) can enable an institution to customize its final curriculum.

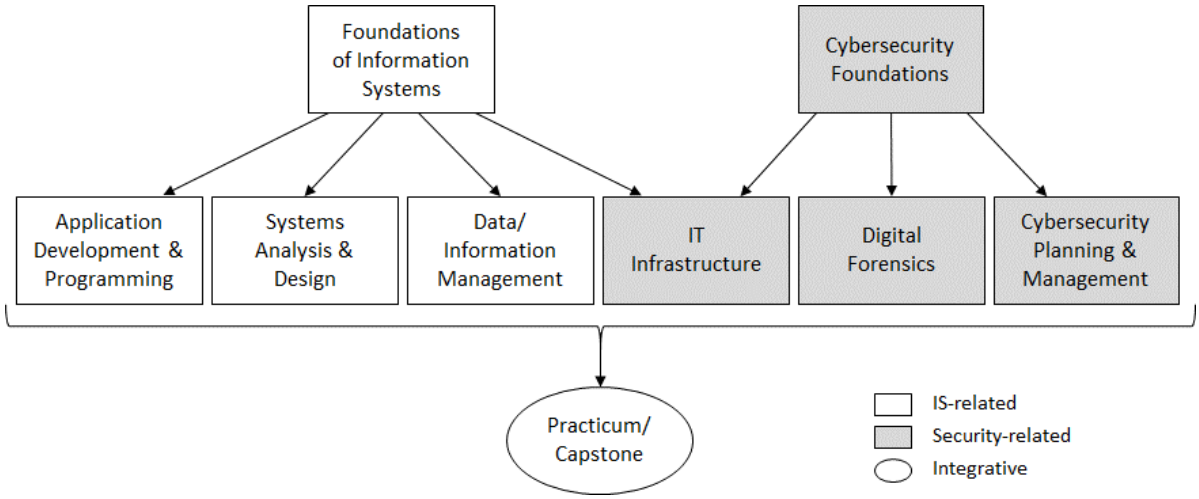


Figure 1. Curriculum Model of the Cybersecurity Bachelor's Program: Core Courses

For example, Digital Forensics ranks higher than Network Security on the ranked list of courses (Table 4), but Network Security exhibited a higher growth than Digital Forensics (Table 5). For this reason, an institution may elect to substitute Digital Forensics with Network Security in its curriculum, especially if the department has greater expertise in network/infrastructure than in forensics. Thus, this study's model (Figure 1) can form the foundation for customizing an institution's own curriculum.

Nevertheless, this research contributes by developing an empirical curriculum model based on programs' actual course requirements. As such, it puts less emphasis on the conceptual rationale behind a curriculum. Other works, such as the Joint Task Force on Cybersecurity Education (2017) and ABET (2023), present extensive discussions on what conceptually should belong in a cybersecurity curriculum.

6.2 Evolution of the Cybersecurity Curriculum

To examine cybersecurity curricular evolution, this study compares the current core requirements with those found in a previous study (Yang & Wen, 2017). Table 5 depicts the results of both studies and the changes. The course with the highest growth rate in requirements is Practicum/Capstone (from 19% to 42%). Such growth may reflect business schools' increasing attention to students acquiring practical and integrative experiences before graduation. In addition to traditional design projects and seminar-based capstones, practical and integrative experiences can include cybersecurity apprenticeships (Armistead et al., 2018) and service learning in information security (Spears, 2018). In particular, getting cybersecurity students out of classrooms and into organizations exposes them to the people aspects of managing security (Spears, 2018). Such training in soft skills is a value-added aspect of business schools' cybersecurity programs.

Policy, Legal, Ethics, and Compliance shows the second-largest increase in the percentage of programs requiring it (from 19% to 31%). As part of their due diligence before investing and writing policies, investors and insurers now require companies to show that cybersecurity controls, policies, and governance are in place (Rundle & Nash, 2023). Because cyber risks constitute part of the broader set of business risks organizations face (Department of Homeland Security, 2013), it is unsurprising that business schools increasingly require this course in their cybersecurity programs. With their multidisciplinary competencies in management, business law, accounting, and auditing, business schools are in an ideal position to offer such a course. Not coincidentally, Cybersecurity Planning and Management—the course with the third largest increase (from 41% to 49%)—is also within the academic competencies of business schools. From an organizational standpoint, cybersecurity solutions implemented by people and processes are necessary (Culp & Thompson, 2016) in addition to technical safeguards. Research has consistently shown that management and various managerial activities significantly affect information security (Soomro et al., 2016).

In contrast, the three courses with the largest declines in the percentages of programs requiring them are Foundations of IS (89% to 51%), Systems Analysis and Design (74% to 51%), and Data/Information Management (74% to 63%). These three courses are the traditional core courses in IS programs. While cybersecurity programs often reside in IS departments in business schools, the data show that fewer cybersecurity programs now require their students to take these IS-related courses. These declines may be because a cybersecurity bachelor's program, like other majors in computing, has a fixed allocation for the number of core courses (McGettrick, 2013). A bachelor's program also has institution-level and college-level distribution requirements, resulting in a fixed number of core courses allocated to the cybersecurity program. A business school's cybersecurity program typically originates in the IS department. As the cybersecurity program builds up its competency and offers additional cybersecurity courses, given the fixed allocation of core courses, it must reduce its IS course requirements to require more cybersecurity courses. The implication of this shift is that cybersecurity is moving toward becoming its own discipline and specialization in business schools.

Overall, despite the declines and growth in various core courses, the top three most-required courses (described in the Results section) have remained relatively stable in terms of the percentages of programs requiring them: IT Infrastructure

(from 78% to 85%), Application Development and Programming (from 81% to 79%), and Cybersecurity Foundations (from 78% to 75%). The stability of these courses over time suggests a steady consensus on their importance in business schools' cybersecurity programs.

On the whole, the results show the following curricular trends:

- Continued requirements of the top three core courses (IT Infrastructure, Application Development and Programming, and Cybersecurity Foundations).
- Growing emphases on practical and integrative experiences (Practicum/Capstone) and organizationally-oriented cybersecurity courses (Policy, Legal, Ethics, and Compliance and Cybersecurity Planning and Management).
- Declining emphases on traditional IS courses (Foundations of IS, Systems Analysis and Design, and Data/Information Management).

These trends, particularly the growth in integrative experiences and organizationally-oriented cybersecurity courses, suggest that business cybersecurity programs increasingly gain their identities with their core requirements in business schools.

6.3 Opportunities for IS and Business Schools

The cybersecurity programs offered by business schools have gained popularity. The number of cybersecurity programs in undergraduate business schools has grown from 27 programs (Yang & Wen, 2017) to 72 programs (identified by the present study). This increase of 167% in the number of cybersecurity programs is occurring at the same time that the number of IS programs in the US has declined (Bohler et al., 2020). Because of this growth, business schools may want to invest in offering their own cybersecurity programs, especially to meet the rising secular demand from businesses for cybersecurity talent (Stupp, 2022). If a school already has an IS program, then out of the nine core courses in the curriculum model (Figure 1), only three additional security-related courses—Cybersecurity Foundations, Digital Forensics, and Cybersecurity Planning and Management—are needed to start a program (assuming that the IT Infrastructure course already exists). When a program acquires additional teaching resources and capabilities, it can develop those increasingly popular courses, such as Policy, Legal, Ethics and Compliance, and Network Security (see Table 5). The return could be substantial as cybersecurity is commonly recognized as a growth area.

Cybersecurity programs also afford opportunities for cooperation between IS and other departments. For example, accounting has a much-vested interest in cybersecurity, especially in light of the AACSB International Accounting Accreditation Standard. In particular, AACSB Accounting Accreditation Standard A5 expects that "learner experiences integrate real-world business strategies, business acumen, privacy and security concerns, ethical issues, information systems and processes, and data management and data analytics tools" (AACSB, 2022a, p. 22). Accounting academics also agree that accounting graduates should understand the "basics of safeguarding electronic accounting records, including backup media, network security, and disaster recovery" (Winstead & Wenger, 2015, p. 18). The A5 standard, which is IS- and cybersecurity-related, exists for accounting programs but can serve as a guide for all business programs (Weiser & Conn, 2017) because the performance of business departments, such as operations, finance, and marketing, is "…inextricably linked to cybersecurity" (Blair et al., 2019, p. 62). For example, the IS faculty can teach the introductory cybersecurity course Cybersecurity Foundations. The management faculty can teach Cybersecurity Planning and Management, and "developing an organizational culture of security through awareness" (Endicott-Popovsky & Popovsky, 2014, p. 61) is also an area in which the management department can excel. The business law faculty can teach courses such as Policy, Legal, Ethics, and Compliance. Because cybersecurity is multidisciplinary (Blair et al., 2019), offering cybersecurity programs in business schools opens up new opportunities for interdisciplinary cooperation and innovation among departments.

Overall, in an environment of increasing cyberthreats, universities are responsible for addressing cybersecurity (White, 2016). "Just as we have integrated sustainability, ethics, and global responsibility into our curricula, we now must incorporate cybersecurity" (Weiser & Conn, 2017, p. 50). Thus, it is critical for business schools to take on roles in providing cybersecurity education in the same way that they impart foundational skills in accounting, marketing, and finance to their graduates.

6.4 Limitations and Future Research

The empirical basis of this paper's results could also be a limitation. While the paper gains an important perspective based on programs' actual core requirements, a reality of cybersecurity programs may be undetectable by this study. This is because many cybersecurity programs in business schools originate from IS departments. These departments may initially build their curricula on existing IS courses while offering a few cybersecurity courses to the extent possible. As a result, the cybersecurity core may consist of more IS courses than cybersecurity courses (The author wishes to thank one of the reviewers who provided this important perspective). Thus, a possible future research avenue is to examine cybersecurity-only majors distinct from IS majors in business schools.

Another limitation of this study is its focus on US institutions. While US institutions represent a large sample size and data from these institutions can be informative, the study needs to pay attention to the curricular perspectives of institutions outside the US. Those perspectives outside the US may very well reflect their region-specific assessments of the cybersecurity landscape. For example, Europe and the US have different approaches to cybersecurity, with the US focusing on national security and the European Union (EU) focusing on privacy and economics (Center for European Policy Analysis, 2023). Thus, another avenue for future research is to assess cybersecurity curricula in institutions in the EU or other regions. Such studies may present important insights into the emphases of universities, businesses, and government policies in those regions.

7. CONCLUSIONS

Business schools play a role in cybersecurity because organizations look for a broader set of skills—technical and nontechnical (ISC2, 2021). Public, private, and government organizations seek cybersecurity professionals who are critical thinkers with good communication skills and hands-on

experience (Brooks et al., 2018). However, many traditional cybersecurity programs do not emphasize soft skills such as business, compliance, ethics, troubleshooting, and general management (McQuaid & Cervantes, 2019). The present study examines cybersecurity programs offered by business schools and sets out two study objectives. The first objective is to assess the core courses of cybersecurity degrees, and the second is to examine the changes in the core courses over time. The study meets its first objective by analyzing comprehensive data from *all* undergraduate cybersecurity programs in US AACSB-accredited business schools. The resulting curriculum model (Figure 1) reflects a collective view of these institutions on the essential topics and courses for these programs, and the model can be a valuable tool for business schools developing new cybersecurity programs. This study also meets its second objective by comparing the current results with those of a previous 2017 study. The comparison shows that the core courses exhibit a growing emphasis on integrative experiences, organizationally oriented cybersecurity courses, and a declining emphasis on traditional IS courses. While the presence of IS courses in the curriculum model could be due to IS department resources, the results provide an empirically-based curriculum model built on actual core requirements. As such, this study hopes to engage the business cybersecurity community—teachers, researchers, and practitioners—to "inform a shared understanding of the curriculum" (Richardson et al., 2018, p. 2), and offering a business-oriented cybersecurity degree at the undergraduate level contributes to developing effective future business leaders.

8. REFERENCES

AACSB (2022a, July 1). *2018 Standards for Accounting Accreditation, Updated July 1, 2022*. https://www.aacsb.edu/educators/accreditation/accounting-accreditation/aacsb-accounting-accreditation-standards

AACSB (2022b, July 1). *2020 Interpretive Guidance for AACSB Business Accreditation, Updated July 1, 2022*. https://www.aacsb.edu/educators/accreditation/business-accreditation/diversity/standards

ABET. (2023). *Criteria for Accrediting Computing Programs, 2023 – 2024*. ABET Computing Accreditation Commission. https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2023-2024/

Albert, R. T., Bennett, C., Briggs, D., Ebben, M., Felch, H., Kokoska, D., Lovewell, L., MacDonald, C., Markowsky, G., Markowsky, L., Murphy, J., Sihler, E., & Wilson, G. (2015). Experiences With the Establishment of a Multi-University Center of Academic Excellence in Information Assurance/Cyber Defense. *Proceedings of the International Conference on Security and Management (SAM)* (pp. 45-50). Las Vegas, NV: The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Armistead, E. L., Guess, R. C., & Blevins, S. R. (2018). Cyber Apprenticeship: A Traditional Solution to a Vexing New Problem. *Journal of Information Warfare*, 17(1), 87-98.

Avery, A., & Oakley, R. L. (2019). The Business Case for IT Security as a Core Course in IS Curriculum. *Proceedings of the Twenty-fifth Americas Conference on Information Systems*, 32. https://aisel.aisnet.org/amcis2019/is_education/is_education/32

Blair, J. R. S., Hall, A. O., & Sobiesk, E. (2019). Educating Future Multidisciplinary Cybersecurity Teams. *Computer*, 52(3), 58-66. https://doi.org/10.1109/MC.2018.2884190

Bohler, J. A., Larson, B., Peachey, T. A., & Shehane, R. F. (2020). Evaluation of Information Systems Curricula. *Journal of Information Systems Education*, 31(3), 232-243.

Brooks, N. G., Greer, T. H., & Morris, S. A. (2018). Information Systems Security Job Advertisement Analysis: Skills Review and Implications for Information Systems Curriculum. *Journal of Education for Business*, 93(5), 213-221. https://doi.org/10.1080/08832323.2018.1446893

Bureau of Labor Statistics (BLS). (2022, September 8). *Occupational Outlook Handbook*. https://www.bls.gov/ooh/home.htm

Ceccucci, W., Jones, K., Toskin, K., & Leonard, L. (2020). Undergraduate Business Analytics and the Overlap With Information Systems Programs. *Information Systems Education Journal*, 18(4), 22-32.

Center for European Policy Analysis. (2023). *Injecting Security into European Tech Policy*. https://cepa.org/wp-content/uploads/2023/03/Injecting-Security-Full-Report.pdf

Check Point Research. (2023, January 6). OPWNAI: Cybercriminals Starting to Use ChatGPT. https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-use-chatgpt/

Clark, U., Stoker, G., & Vetter, R. (2020). Looking Ahead to CAE-CD Program Changes. *Information Systems Education Journal*, 18(1), 29-39.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 4(10), 13-21. https://doi.org/10.22215/timreview/835

Cram, W. A., & D'Arcy, J. (2016). Teaching Information Security in Business Schools: Current Practices and a Proposed Direction for the Future. *Communications of the Association for Information Systems*, 39, Article 3. https://doi.org/10.17705/1CAIS.03903

Culp, S., & Thompson, C. (2016). The Convergence of Operational Risk and Cyber Security. Accenture. https://www.accenture.com/t20160212T030611__w__/us-en/_acnmedia/PDF-7/Accenture-Cyber-Risk-Convergence-Of-Operational-Risk-And-Cyber-Security.pdf

Department of Homeland Security. (2013). *Cyber Risk Culture Roundtable Readout Report*. https://www.dhs.gov/sites/default/files/publications/cyber-risk-culture-roundtable-readout_0.pdf

Duffy, C. (2021, May 28). Wanted: Millions of Cybersecurity Pros. Salary: Whatever You Want. *CNN*. https://www.cnn.com/2021/05/28/tech/cybersecurity-labor-shortage/index.html

Elazhary, M., & Morelli, F. (2016). Digital Transformation of Information Systems Master's Curriculum. *Academic Journal of Science*, 6(1), 523-532.

Endicott-Popovsky, B. E., & Popovsky, V. M. (2014). Application of Pedagogical Fundamentals for the Holistic Development of Cybersecurity Professionals. *ACM*

Inroads, 5(1), 57-68. https://doi.org/10.1145/2568195.2568214

Fortinet. (2022, April). 2022 Cybersecurity Skills Gap: Global Research Report. https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf

Grover, M., Reinicke, B., & Cummings, J. (2016). How Secure Is Education in Information Technology? A Method for Evaluating Security Education in IT. *Information Systems Education Journal*, 14(3), 29-44.

Hwang, D., Ma, Z., & Wang, M. (2015). The Information Systems Core: A Study From the Perspective of IS Core Curricula in the U.S. *Information Systems Education Journal*, 13(6), 27-34.

IBM. (2022, February). X-Force Threat Intelligence Index 2022 Report. https://www.ibm.com/security/data-breach/threat-intelligence/. https://doi.org/10.12968/S1361-3723(22)70561-1

International Information System Security Certification Consortium (ISC2). (2021). *A Resilient Cybersecurity Professional Charts the Path Forward: (ISC)² Cybersecurity Workforce Study, 2021*. https://www.isc2.org/Research/Workforce-Study

International Information System Security Certification Consortium (ISC2). (2022). *2022 Cybersecurity Workforce Study*. https://www.isc2.org/Research/Workforce-Study

Joint Task Force on Cybersecurity Education. (2017). *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. ACM, IEEE, AIS, IFIP. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf. https://doi.org/10.1145/3422808

Jones, K. S., Namin, A. S., & Armstrong, M. E. (2018). The Core Cyber-Defense Knowledge, Skills, and Abilities that Cybersecurity Students Should Learn in School: Results From Interviews With Cybersecurity Professionals. *ACM Transactions on Computing Education*, 18(3), 11:1-11:12. https://doi.org/10.1145/3152893

Keary, T. (2022, December 14). How ChatGPT Can Turn Anyone Into a Ransomware and Malware Threat Actor. *VentureBeat*. https://venturebeat.com/security/chatgpt-ransomware-malware/

Knapp, K. J., Maurer, C., & Plachkinova, M. (2017). Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance. *Journal of Information Systems Education*, 28(2). 101-113.

Leonard, L. N. K., Jones, K., & Lang, G. (2019). Information System Curriculum versus Employer Needs: A Gap Analysis. *Information Systems Education Journal*, 17(5), 32-38.

Marquardson, J., & Elnoshokaty, A. (2020). Skills, Certifications, or Degrees: What Companies Demand for Entry-Level Cybersecurity Jobs. *Information Systems Education Journal*, 18(1), 22-28.

McGettrick, A. (2013, August 30). Toward Curricular Guidelines for Cybersecurity: Report of a Workshop on Cybersecurity Education and Training. Association for Computing Machinery. https://www.acm.org/education/TowardCurricularGuidelinesCybersec.pdf. https://doi.org/10.1145/2538862.2538990

McQuaid, P. A., & Cervantes, S. (2019). How to Achieve a Seasoned Cybersecurity Workforce. *Software Quality Professional*, 21(4), 4-10.

National Centers of Academic Excellence in Cybersecurity (NCAE-C). (2020). *Centers of Academic Excellence in Cyber Defense (CAE-CD) 2020 Knowledge Units*. https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_ku.pdf

National Centers of Academic Excellence in Cybersecurity (NCAE-C). (2022). *National Centers of Academic Excellence in Cybersecurity NCAE-C 2022: Designation Requirements and Application Process*. https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_designation_requirements.pdf

National Security Agency (NSA). (n.d.). *National Centers of Academic Excellence*. https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf. https://doi.org/10.6028/NIST.SP.800-181

OpenAI. (2022, November 30). ChatGPT: Optimizing Language Models for Dialogue. https://openai.com/blog/chatgpt/

Osatuyi, B., & Garza, M. (2014). IS 2010 Curriculum Model Adoption in the United States. *Proceedings of the Twentieth Americas Conference on Information Systems (AMCIS 2014)*, 8. https://aisel.aisnet.org/amcis2014/ISEducation/GeneralPresentations/8

Parekh, G., DeLatte, D., Herman, G. L., Oliva, L., Phatak, D., Scheponik, T., & Sharman, A. T. (2018). Identifying Core Concepts of Cybersecurity: Results of Two Delphi Processes. *IEEE Transactions on Education*, 61(1), 11-20. https://doi.org/10.1109/TE.2017.2715174

Payne, B. K., Mayes, L., Paredes, T., Smith, E., Wu, H., & Xin, C. S. (2020). Applying High Impact Practices in an Interdisciplinary Cybersecurity Program. *Journal of Cybersecurity Education, Research and Practice*, 2020(2), Article 4. https://doi.org/10.62915/2472-2707.1071

Plachkinova, M., & Pittz, T. (2021). Assessing the Awareness of Cybersecurity Within Entrepreneurship Students: The Cyberpreneurship Project. *Entrepreneurship Education and Pedagogy*, 4(3), 564-582. https://doi.org/10.1177/2515127420913056

Raineri, E., & Fudge, T. (2019). Exploring the Sufficiency of Undergraduate Students' Cybersecurity Knowledge Within Top Universities' Entrepreneurship Programs. *Journal of Higher Education Theory and Practice*, 19(4), 73-92. https://doi.org/10.33423/jhetp.v19i4.2203

Raj, R. K., & Parrish, A. (2018). Towards Standards in Undergraduate Cybersecurity Education in 2018. *Computer*, 51(2), 72-75. https://doi.org/10.1109/MC.2018.1451658

Ramezan, C. A. (2023). Examining the Cyber Skills Gap: An Analysis of Cybersecurity Positions by Sub-Field. *Journal of Information Systems Education*, 34(1), 94-105.

Redman, S. M., Yaxley, K. J., & Joiner, K. F. (2020). Improving General Undergraduate Cyber Security Education: A Responsibility for All Universities? *Creative Education*, 11, 2541-2558. https://doi.org/10.4236/ce.2020.1112187

Richardson, J., Burstein, F., Hol, A., Clarke, R. J., & McGovern, J. M. (2018). Australian Undergraduate Information Systems Curricula: A Comparative Study. *The 27th International Conference on Information Systems Development, ISD2018*. Lund, Sweden: Lund University. https://aisel.aisnet.org/isd2014/proceedings2018/Education/2

Rosenbush, A. (2021, December 7). To Thwart Hackers, Companies Should Focus More on Modernizing Their Networks. *The Wall Street Journal*. https://www.wsj.com/articles/companies-should-focus-on-modernizing-networks-to-thwart-hackers-11638824980

Rosenbush, A. (2022, October 17). Cybersecurity Tops the CIO Agenda as Threats Continue to Escalate. *The Wall Street Journal*. https://www.wsj.com/articles/cybersecurity-tops-the-cio-agenda-as-threats-continue-to-escalate-11666034102

Rundle, J., & Nash, K. S. (2023, January 16). Private-Equity Firms Tighten Focus on Cyber Defenses at Portfolio Companies. *The Wall Street Journal*. https://www.wsj.com/articles/private-equity-firms-tighten-focus-on-cyber-defenses-at-portfolio-companies-11673643373

Shoemaker, D., Kohnke, A., & Laidlaw, G. (2019). Ethics and Cybersecurity Are Not Mutually Exclusive. *The EDP Audit, Control, and Security Newsletter*, 60(1), 1-10. https://doi.org/10.1080/07366981.2019.1651516

Smith, Z. M., & Lostri, E. (2020, December). The Hidden Costs of Cybercrime. McAfee. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information Security Management Needs More Holistic Approach: A Literature Review. *International Journal of Information Management*, 36(2), 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Spears, J. L. (2018). Teaching Tip: Gaining Real-World Experience in Information Security: A Roadmap for a Service-Learning Course. *Journal of Information Systems Education*, 29(4), 183-202.

Stafford, T. F., Gal, G., Poston, R., Grossler, R. E., Jiang, R., & Lyons, R. (2018). The Role of Accounting and Professional Associations in IT Security Auditing: An AMCIS Panel Report. *Communications of the Association for Information Systems*, 43, Article 27. https://doi.org/10.17705/1CAIS.04327

Stefanidis, A., & Fitzgerald, G. (2010). Mapping the Information Systems Curricula in UK Universities. *Journal of Information Systems Education*, 21(4), 391-409.

Stefanidis, A., & Fitzgerald, G. (2014). IS Education Research: Review of Methods of Surveying the IS Curriculum to Support Future Development of IS Courses. *7th SIGSAND/PLAIS EuroSymposium 2014 Proceedings* (pp. 1-11). Cham, Switzerland: Springer International Publishing. https://doi.org/10.1007/978-3-319-11373-9_1

Stupp, C. (2022, October 20). Corporate Cybersecurity Teams Struggle to Fill Jobs. *The Wall Street Journal*. https://www.wsj.com/articles/corporate-cybersecurity-teams-struggle-to-fill-jobs-11666270802

Stupp, C., & Nash, K. S. (2023, January 3). Ukraine War and Upcoming SEC Rules Push Boards to Sharpen Cyber Oversight. *The Wall Street Journal*. https://www.wsj.com/articles/ukraine-war-and-upcoming-sec-rules-push-boards-to-sharpen-cyber-oversight-11671723827

The Joint ACM/AIS IS2020 Task Force. (2020). *IS2020: A Competency Model for Undergraduate Programs in Information Systems*. ACM, AIS, and ISCAP. https://is2020.hosting2.acm.org/2021/06/01/is2020-final-draft-released/. https://doi.org/10.1145/3460863

Topi, H., Valachic, J. S., Wright, R. T., Kaiser, K., Nunamaker, J. F., Sipior, J. C. Jr., & de Vreede, G. J. (2010*). IS 2010: Curriculum Guidelines for Undergraduate Degree Programs in Information Systems*. Association for Computing Machinery and Association for Information Systems. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/is-2010-acm-final.pdf. https://doi.org/10.17705/1CAIS.02618

Towhidi, G., & Pridmore, J. (2023). Aligning Cybersecurity in Higher Education with Industry Needs. *Journal of Information Systems Education*, 34(1), 70-83.

Tsado, L. (2019). Cybersecurity Education: The Need for a Top-Driven, Multidisciplinary, School-Wide Approach, *Journal of Cybersecurity Education, Research and Practice*, 1, Article 4. https://doi.org/10.62915/2472-2707.1050

Wang, S., & Wang, H. (2019). Opportunities and Challenges of Cybersecurity for Undergraduate Information Systems Programs. *International Journal of Information and Communication Technology Education*, 15(2), 49-68. https://doi.org/10.4018/IJICTE.2019040104

Weiser, M. & Conn, C. (2017). Into the Breach: Integrating Cybersecurity Into the Business Curriculum. *BizEd*, 16(1), 49-53. https://www.aacsb.edu/-/media/publications/bized-archives/2017/jf16-bized.pdf

White, S. K. (2016, April 25). Top U.S. Universities Failing at Cybersecurity Education. *CSO*. https://www.csoonline.com/article/3060878/top-u-s-universities-failing-at-cybersecurity-education.html

Winstead, J., & Wenger, M. (2015). Skills vs. Concepts: A Comparison of Practitioners' and Educators' Preferences for Accounting Information Systems Proficiencies. *AIS Educator Journal*, 10(1), 5-25. https://doi.org/10.3194/1935-8156-10.1.5

Yang, S. C. (2018). A Curriculum Model for IT Infrastructure Management in Undergraduate Business Schools. *Journal of Education for Business*, 93(7), 303-313. https://doi.org/10.1080/08832323.2018.1490686

Yang, S. C., & Wen, B. (2017). Toward a Cybersecurity Curriculum Model for Undergraduate Business Schools: A Survey of AACSB-Accredited Institutions in the United States. *Journal of Education for Business*, 92(1), 1-8. https://doi.org/10.1080/08832323.2016.1261790

AUTHOR BIOGRAPHY

Samuel C. Yang is a professor of information systems and decision sciences in the College of Business and Economics at California State University, Fullerton in California. He has authored three books and more than 25 journal articles. Before entering academia, he was a systems engineer at Hughes Space and Communications (now part of Boeing) and a network planning manager at Verizon Wireless. Samuel Yang holds a Ph.D. in management of information systems from Claremont Graduate University. His current interests are in enterprise wireless networks and information systems education.

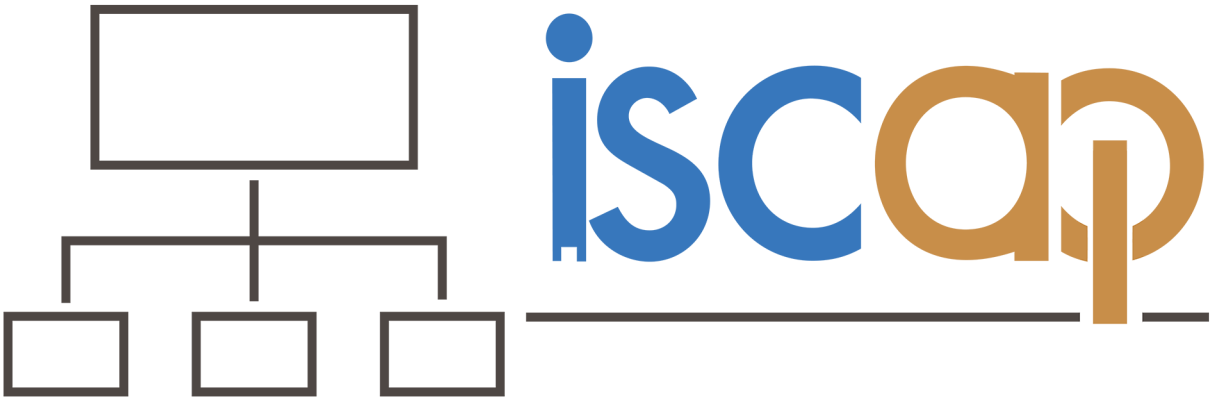
APPENDIX

Other Core Requirements of Cybersecurity Bachelor's Programs

The table below shows those courses required by less than 15% and greater than 5% of the programs. The total number of programs is 72.

Course Category	*n*	%
Advanced Programming	10	14%
Network Defense	9	13%
IT Audit & Controls	7	10%
Security Risk Analysis	7	10%
System Administration	7	10%
Advanced Network Technology & Protocols	6	8%
Data Structures	6	8%
Object-Oriented Paradigm	6	8%
Operating Systems Administration	6	8%
Operating Systems Concepts	6	8%
Web Development	5	7%
Advanced IT Security	4	6%
Algorithms	4	6%
Basic Cryptography	4	6%
Basic Scripting & Programming	4	6%
Intro to CS	4	6%
Intrusion Detection/Prevention Systems	4	6%
Secure Programming Practices	4	6%

INFORMATION SYSTEMS & COMPUTING ACADEMIC PROFESSIONALS



STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the ***Journal of Information Systems Education*** have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN: 2574-3872 (Online) 1055-3096 (Print)