Journal of Information Systems Education

Volume 28
Issue 2
December 2017

# Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance

Kenneth J. Knapp, Christopher Maurer, and
Miloslava Plachkinova

Recommended Citation: Knapp, K. J., Maurer, C., & Plachkinova, M. (2017). Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance. *Journal of Information Systems Education,* 28(2), 101-114.

Article Link: http://jise.org/Volume28/n2/JISEv28n2p101.html

| | |
|---|---|
| Initial Submission: | 22 August 2016 |
| Accepted: | 1 June 2017 |
| Abstract Posted Online: | 7 November 2017 |
| Published: | 12 December 2017 |



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

# Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance

**Kenneth J. Knapp**
Department of Information & Technology Management
Sykes College of Business
University of Tampa
Tampa, FL 33606, USA
kknapp@ut.edu

**Christopher Maurer**
McIntire School of Commerce
University of Virginia
Charlottesville, VA 22904, USA

**Miloslava Plachkinova**
Department of Information & Technology Management
Sykes College of Business
University of Tampa
Tampa, FL 33606, USA

**ABSTRACT**

Much has been published about developing a cybersecurity curriculum for institutes of higher learning (IHL). Now that a growing number of IHLs globally offer such programs, a need exists on how to guide, maintain, and improve the relevancy of existing curricula. Just as cybersecurity professionals must hone their skills continually to keep up with a constantly shifting threat landscape, cybersecurity programs need to evolve to ensure they continue to produce knowledgeable graduates. In this regard, professional certifications in the cybersecurity industry offer an opportunity for IHLs to maintain a current curriculum. Governing bodies that manage professional certifications are highly motivated to ensure their certifications maintain their currency in the competitive marketplace. Moreover, employers who hire security professionals look for certifications in assessing a candidate's overall credentials. This paper attempts to fill a void in the literature by exploring the use of professional certifications as helpful input to shaping and maintaining a cybersecurity curriculum. To this end, we offer a literature analysis that shows how changes made to professional certifications are applicable and relevant to maintaining a cybersecurity curriculum. We then provide a case study involving an undergraduate cybersecurity program in a mid-sized university in the United States. Before concluding, we discuss topics such as experiential learning, cybersecurity capstone courses, and the limitations to our approach.

**Keywords:** Cybersecurity, Curriculum design & development, Security, Certifications

## 1. INTRODUCTION

Several scholarly articles have been published concerning developing a cybersecurity or information security curriculum[1] for colleges and universities (Belle, Imboden, and Martin, 2013; Bogolea and Wijekumar, 2004; Endicott-Popovsky and Popovsky, 2014; Hentea, Dhillon, and Manpreet, 2006; Whitman and Mattord, 2004). Furthermore, a multitude of frameworks and learning objectives for cybersecurity are found in the broader literature (e.g. NSA/DHS Centers of Academic Excellence in Cyber Defense (and Operations) (CAE-CD, CAE-CO), NICE Cybersecurity Workforce Framework (NCWF), ACM Joint Task Force on Cybersecurity Education). Yet, a research gap exists regarding how to maintain and update cybersecurity curricula at a practical level. A large and growing number of institutes of higher learning (IHL) offer such programs, and a need exists on how to best guide and improve upon established curricula.

While many disciplines evolve over time, cybersecurity faces a constantly shifting landscape of threats, vulnerabilities, and countermeasures that can impact curricula. Just as cybersecurity professionals must engage in continuous education to ensure they remain current in their skill sets, IHLs with cybersecurity programs must also be prepared to continuously evaluate their curriculum to provide students with the most current and relevant knowledge to succeed in this field.

There is certainly no shortage of new and emerging sources for faculty members to reference when organizing their curricula. Designations like the NSA/DHS CAE-CD/CO, provide a thorough set of "knowledge units" that students are expected to acquire throughout their studies (NSA, 2016). Frameworks such as NCWF provide a detailed listing of knowledge, skills, and abilities that are required to successfully perform various work tasks in a cybersecurity career (NIST, 2016). These sources of material have much validity and are increasingly being recognized in the field for their rigor. However, simply incorporating the minimum baseline requirements or objectives from such frameworks can limit an IHL's ability to fully differentiate itself from other IHLs offering similar cybersecurity degrees. Cybersecurity programs can therefore plan their curriculum initially around such well-accepted frameworks; however, the ongoing maintenance and improvement of a program can be bolstered by considering professional certifications in the cybersecurity field.

Any successful cybersecurity program should consider the needs of the workforce in designing and maintaining its curriculum. A common job title for recent graduates with a cybersecurity degree is the Information Security Analyst. The Department of Labor describes an Information Security Analyst as a person that may

> plan, implement, upgrade, or monitor security measures for the protection of computer networks and information; ensure appropriate security controls are in place that will safeguard digital files and vital electronic infrastructure; respond to computer security breaches and viruses (Bureau of Labor Statistics, 2010).

Information Security Analyst jobs are expected to grow by 18%, and many organizations prefer candidates to have some sort of cybersecurity certification (Bureau of Labor Statistics, 2015a, 2015b). As such, there are over 140 professional certifications from 30 certifying organizations that are relevant to the Information Security Analyst job description (Department of Labor, 2016).

Considering the preference given to job candidates with certifications and the number of certifications available, many argue that it is in the students' best interest to pursue professional certification (McGill and Dixon, 2005; Rob, 2014; Wireschen and Zhang, 2010). Wright states, "Academics should encourage students to pursue certification. There are hundreds of cybersecurity-related certifications, and navigating through the confusing array can be a daunting challenge." Moreover, earning a professional certification is highly useful for promotion in the cybersecurity career field (Wright, 2015). If certifications are so valuable in the workforce, then it would be prudent for IHLs to prepare students for certification exams by incorporating the objectives of those exams into the overall program curriculum.

In 2016, there were more than 200,000 cybersecurity job postings, and some forecast this number to grow to over 1.5 million globally by 2019 (Tittel, 2016). Cybersecurity positions are more likely to require certifications than other information technology (IT) jobs. One-third (35%) of cybersecurity jobs call for an industry certification, compared to 23% of IT jobs overall (Burning Glass, 2015). A survey conducted by the authors in 2014 of 18 local IT business executives shows how they view certifications. The following question was given: "How important are industry certifications to your firm's hiring process?" They responded with a 3.9/5.0 average (1 = not important; 5 = very important) with 12 of the 18 (67%) stating it was either important (4) or very important (5). One respondent commented,

> For an IT security position, we look for certifications because there is a minimum level of knowledge we are looking for… there is nothing wrong with certifications – they can only help. However, just because you have a certification does not mean you will do a great job.

Organizations employing information security professionals generally base their assessment of an individual's skill level on three main assessment criteria. These include 1) academic qualifications leading to a diploma or a degree, 2) professional and vendor-specific certifications, and 3) job experience, such as internships or full employment (Hentea, Dhillon, and Manpreet, 2006). Hentea, Dhillon, and Manpreet (2006) stated,

> Professional and vendor certifications in information security validate competencies and skills, but they *are not replacing experience or education*. While academic qualifications support broad knowledge and skills in general, professional certifications may be effective in a limited area of operations. Academic programs exposing the students to *theoretical concepts and problem solving experience are critical* for preparing graduates for jobs in the information security (emphasis added).

This same sentiment was conveyed by the respondent from the authors' informal survey noted above. The synergy between content knowledge, critical thinking, and problem solving skills should not be underestimated. Cybersecurity issues are complex, and there is no standard recipe for protecting informational assets within organizations. Therefore, a solid base of content knowledge and technical skill will only take one so far. By immersing students in an engaging environment, challenging them to think about problems from multiple angles, and providing a broad cybersecurity education, IHLs are well-positioned to develop individuals to succeed in the marketplace.

Students pursuing a course of study centered on professional certifications may gain an edge in the marketplace, but should not necessarily do so at the price of finding an internship. Upon graduation, students will be well-

prepared for full-time employment if they've experienced an internship and are equipped to take and pass certification exams. Further, students must demonstrate more than an ability to memorize facts and definitions, often required to pass certification exams – they need to learn how to reason through complex problems and think critically about issues presented to them. Both students and academics need to maintain a balanced outlook of the three assessment criteria discussed by Hentea, Dhillon, and Manpreet (2006).

In sum, we propose an approach that complements other cybersecurity curriculum frameworks. Certifications are commonly referenced as a requirement in job postings and have existed for longer than some newly developed curriculum frameworks. Furthermore, the fact that so many highly specialized cybersecurity certifications exist allows IHLs to develop customized or specialized courses. This can provide an IHL with a competitive advantage in attracting high-caliber students, especially in situations where local organizations are looking for specialized cybersecurity talent. Specialized courses may sit alongside the standard knowledge courses specified in many educational frameworks of this field. The certification marketplace is competitive, and governing bodies will ensure their certifications maintain industry relevancy or else they will lose value. Monitoring updates to certification content areas and adjusting a curriculum accordingly can therefore help IHLs with existing programs and ensure graduates remain in high demand.

In the following section, we offer a literature review exploring the merits of professional certifications for curriculum maintenance and introduce a framework of the considerations certification bodies ought to understand to keep their certifications relevant. Next, we demonstrate with a case study how one IHL is using this approach to maintain a current cybersecurity undergraduate program. Then, we offer a discussion as well as contributions and limitations before concluding the paper.

## 2. LITERATURE ANALYSIS: FACTORS IMPACTING CERTIFICATION RELEVANCY

To maintain the relevancy of their exams, certification bodies need to assess the factors or forces influencing the cybersecurity field and then update their exam content accordingly. These factors may emanate from external forces outside the boundaries of the cybersecurity field or internal forces from within the field. In this section, we briefly discuss five factors that certifying bodies consider when updating their exam coverage, as illustrated in Figure 1. These are important to IHLs because, fortunately, they are the same general factors that impact the content of a cybersecurity curriculum.

To analyze the significant factors that professional certifying bodies consider most important, we reviewed the available literature to answer the question: *what forces do certification bodies consider when updating their exam content?* While the authors evaluated several certifying bodies, we focused on the International Information Systems Security Certification Consortium [(ISC)²] considerations for maintaining their existing certifications and introducing new ones. This organization is a logical choice because of the prominence of the Certified Information System Security Professional (CISSP) credential. Moreover, (ISC)² states that the CISSP was the first certification in the information security field to meet the requirements of ISO/IEC Standard 17024, which requires certifying bodies to maintain a certification scheme for persons that includes the confirmation and relevancy of exam content areas (ISO/IEC, 2012).[2]

Based on our literature analysis, we categorized five major factors that cybersecurity certifying bodies consider in the maintenance of their exam content: threat landscape, technology changes, industry standards, workforce needs, and government and regulation. This list is neither exhaustive nor does it completely represent the actions of every certification body. There may be other factors taken into consideration, and some certifying bodies may not incorporate all five of the forces. We feel, however, that this list justifies why certification curricula provide relevant and timely information that should be incorporated into higher learning curricula.

### 2.1 Threat Landscape

A threat is an indication of an impending undesirable event that may inflict injury or damage to a company's resources (Parker, 1981). This external force is at the top of the list (Shearer, 2015) and understandably so. The EC-Council with its Certified Ethical Hacker (CEH) exam regularly updates exam material on the threat landscape to include the latest attack vectors, tools, and techniques that malicious hackers are using in their environment (EC-Council, 2016). (ISC)² also updated its CISSP and System Security Certified Professional (SSCP) domains of knowledge in 2015 in response to "changes in technology and the evolving threat landscape occurring in the information security field" ((ISC)², 2015a). These updates included a deeper focus on asset security and security assessment given the rapidly changing threat landscape pertaining to these areas.

### 2.2 Technology Changes

Just as changes to the threat landscape present critical challenges to the field, so do changes and evolutions in the technology itself (Shearer, 2015). Technology advances, which refer to society's inexhaustible drive toward technological progression, never stop. For example, the Internet of Things and cloud computing are two relatively new technology paradigms that are having major impacts on the cybersecurity field. Such changes have ushered in updates to many current certifications but also the introduction of new ones, such as the Certified Cloud Security Professional (CCSP) credential in 2015 ((ISC)², 2015b). Demonstrating this influence, this certification was developed in recognition of the market need for cloud security experts in response to changes in technology. Another such example is the Global Information Assurance Certification (GIAC) offering a certification for Python coders. This niche credential responds to the need for penetration testers to rapidly develop their own tools rather than wait for someone else to develop it. The Python programming language is a technology well suited for this task (GIAC, 2016b).

### 2.3 Industry Standards

Certifying organizations also respond to industry forces such as standards and best practices. Over the past decade, numerous industry standards and guidelines have emerged worldwide, such as ISO standards, NIST security frameworks,

and the Payment Card Industry Data Security Standard (PCI-DSS). The ISO 27000-series is a prominent international standard providing both authoritative statements on information security management as well as procedures to be adopted by organizations to ensure information security (Backhouse, Hsu, and Silva, 2006). Numerous NIST standards, such as publication 800-53, were originally intended to serve U.S. Federal Government agencies but have been adopted or used as a benchmark for designing security programs in private industry as well. PCI-DSS was developed by the major credit card issuers to help merchants securely process card payments and store card-related data. Such standards are updated to remain relevant. As such, cybersecurity certifying bodies do not ignore their content and include them in exams such as the CISSP (Stewart, Chapple, and Gibson, 2015).

### 2.4 Workforce Needs

$(ISC)^2$ gauges global workforce needs via regular surveys to understand the trends and changes impacting the constituents in the profession ($(ISC)^2$, 2015d). This is valuable information used in their certification maintenance process. For instance, 70% of survey respondents stated they thought a cloud security certification is either very or somewhat relevant. This feedback helped to justify the CCSP as well as introduce additional cloud security material into the CISSP Common Body of Knowledge (CBK). Similarly, the ISACA organization regularly conducts assessments of tasks performed by currently certified individuals. The Certified Information System Auditor (CISA) content was restructured to reflect the latest responsibilities of IS audit professionals (ISACA, 2015). ISACA has also polled cybersecurity professionals to identify key skills that are lacking in the available workforce. Findings have suggested that a lack of business understanding is more prominent than a lack of technical skills in the field (ISACA, 2016). Additionally, CompTIA updates its Security+ exam using input from subject-matter experts and industry-wide surveys to ensure its exam verifies what an information security professional with two years in the workforce must know (CompTIA, 2013).

### 2.5 Government and Regulation

Laws, regulations, and governments can significantly impact the cybersecurity field of a nation. In the United States, organizations like the Department of Homeland Security (DHS) and the National Security Agency (NSA) significantly influence the field; their impact on cybersecurity education will be discussed later in this paper. Laws such as the Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act (SOX) have also had major impacts on the field. Certification bodies often respond to these governmental pressures by introducing new certifications or adding content to existing ones. For example, $(ISC)^2$ tailored a credential to suit government needs in Japan ($(ISC)^2$, 2009), and the Healthcare Information Security & Privacy Practitioner (HCISPP) credential was introduced to help specialists navigate the growing healthcare regulatory environment.

### 2.6 The Model

Based on our literature review, the framework in Figure 1 illustrates five key factors that certifying bodies consider as they maintain the relevance of their certifications. The output of these factors can help colleges and universities maintain a relevant cybersecurity curriculum.

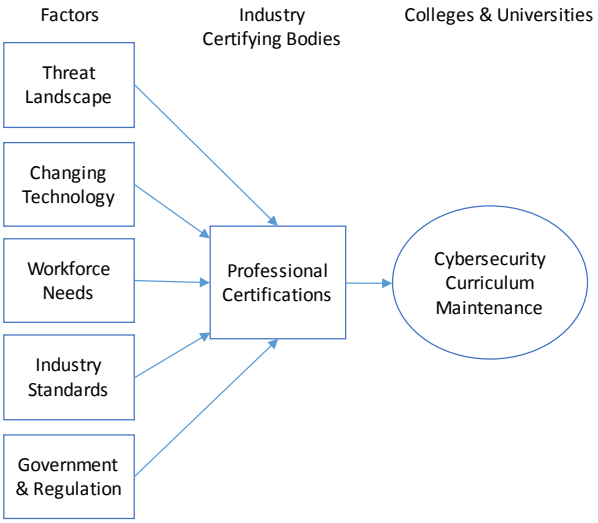


**Figure 1. Factors Impacting the Maintenance of Cybersecurity Certifications**

While overlap naturally exists, these factors represent the significant inputs requiring consideration by a certifying body in maintaining their certifications. This level of research is difficult for academics in IHLs to conduct on their own so it makes sense to leverage the extensive knowledge gathering that goes into certification design to better improve cybersecurity curricula. By looking to professional certifications through organizations like $(ISC)^2$, academics can tap into additional sources of feedback to better ensure the relevance and currency of their own cybersecurity curriculum.

To illustrate the notion that IHLs can use professional certifications as a guide for keeping cybersecurity curriculum current, consider the topic of mobile device security. In 2013, Patten and Harris (2013) proposed that future IT professionals should be aware of and learn how to secure mobile devices. They suggested the topic be integrated into an IT model curriculum. However, for certifying bodies, this topic was already addressed. As it pertains to the CEH, the EC-Council was covering topics relating to mobile devices, and this material was already published in third-party exam preparation texts (Oriyano, 2014). Mobile security was then upgraded into a larger topic for the CEHv9 exam. Official preparation material from the EC-Council contained 147 pages of slides covering the topic of *Hacking Mobile Platforms* (EC Council, 2015). In this case, we can see that the EC-Council was making changes to its exams to adapt to technological changes as IHLs began modernizing their curricula. Generally speaking, certification bodies keep up with technology and industry changes and can therefore be good sources of forward-looking guidance.

## 3. CASE STUDY

To understand the development and maintenance of cybersecurity curriculum, we utilized qualitative methods. Following best practices on qualitative research (Bryman, 2012) and case study applications in education (Merriam, 1998), we examined a case study involving a medium-sized private university in the eastern United States. At this school, the Cybersecurity program is part of the Information & Technology Management department within the College of Business, which is accredited by the Association to Advance Collegiate Schools of Business (AACSB). The department also supports a Management Information Systems (MIS) major, which is accredited by the Accreditation Board for Engineering and Technology (ABET). The Cybersecurity program officially began in August 2015, while the planning began eighteen months prior. Five new courses were proposed, and four existing courses were integrated into the curriculum with minimal adaptation. The entire curriculum was designed to ensure comprehensive coverage of the CISSP CBK. After courses were designed but before the new courses were first offered to students, $(ISC)^2$ updated the CBK by emphasizing certain topics (like asset security and assessment/testing) and re-aligning other topics under a different domain structure. The changes were studied and used as an opportunity to analyze how certification evolution can seamlessly be integrated into curricula. This particular change to the CBK did not impose the need for any significant modifications to the program, but it highlighted an opportunity to review the knowledge domains for other prominent certifications to further improve the relevancy of the proposed curriculum.

Extending beyond the CISSP, content areas for the Certified Information Security Auditor (CISA), Certified Information Security Manager (CISM), and CEH credentials were compared to the existing curriculum. This set of certifications was chosen for several reasons. First, it helps to incorporate environmental sensing capabilities from three different certifying bodies: $(ISC)^2$, ISACA, and the EC-Council (Table 1). Second, these four certifications were chosen because they are all listed on the ANSI/ISO 17024 certification list and generally cover a broad range of topics related to cybersecurity. Finally, multiple industry surveys indicate that these four certifications are highly requested in job postings. One survey had the CISSP, CISA, and CISM as the top three certifications appearing in job postings within the field (Burning Glass, 2015). Another survey placed the CISSP, CISM, and CEH in the top four of information security certifications across four major job boards (Tittel, 2016). These results demonstrate the value of these certifications in the job market. The reader is encouraged to visit job board sites such as Indeed, LinkedIn Jobs, SimplyHired, and others to explore the value employers place on these and other certifications.

To complete this review, faculty members (who passed the particular certification exam) compared the learning objectives and topics covered in each course to the certification exam objectives. The percentage of a course dedicated to material from each certification exam was identified through this exercise and the results are presented in Table 1. To conduct such a review, faculty members should have earned the certification or be a subject matter expert in the topic.

| Certification[3] | $(ISC)^2$ | ISACA | | EC-Council |
|---|---|---|---|---|
| Undergraduate Course | CISSP | CISM | CISA | CEH |
| Management Information Systems | 5% | 5% | 20% | 5% |
| Application Development | 5% | 5% | 5% | 5% |
| Information Security Principles | 100% | 70% | 50% | 50% |
| Network & Cloud Infrastructure | 90% | 10% | 50% | 65% |
| Info Security Standards, Risk Mgmt, & Compliance | 100% | 100% | 100% | 15% |
| Network Security | 100% | 15% | 40% | 65% |
| Ethical Hacking | 35% | 10% | 20% | 100% |
| Physical and Operational Security | 75% | 10% | 60% | 30% |
| Cybersecurity Capstone | 100% | 40% | 60% | 30% |
| Total Coverage of Exam Objectives | 100% | 100% | 100% | 100% |

**Table 1. Generic Certification-to-Course Coverage Matrix Sample**

To illustrate, the Ethical Hacking course is 100% dedicated to covering CEH objectives, whereas only 10% of the course covers CISM objectives in our case study. Note that this does not imply that all CEH exam material is covered in the Ethical Hacking academic course. To arrive at the "Total Coverage of Exam Objectives" row at the bottom of Table 1, faculty members performed the mapping process in reverse by examining all content areas of each exam and evaluating the extent to which they are covered in each of the nine courses in the curriculum. Appendix A provides an example of this mapping of course material to the CISSP CBK domains. Appendix B provides an example of a more granular mapping using major course topics to one example CBK domain.

The two-way mapping approach was very insightful and allowed faculty members to identify key areas of opportunity. For example, in reviewing CEH content areas, it was determined that feasible changes could be made to the curriculum to achieve two primary outcomes. First, one course title could easily be rebranded as "Ethical Hacking" (it was previously named "Advanced Network Security") and could focus on covering CEH certification material. Second, and more importantly, courses could incorporate additional experiential education opportunities to provide students with hands-on activities meant to develop problem solving and adversarial thinking skills. Given the frequent use of examples

documented in various CEH exam prep books, it was straightforward to identify lab activities that could be used to illustrate the certification exam content areas in action.

While Table 1 and Appendices A and B reflect our case study, any cybersecurity program can replicate this table and adjust it to fit their program. Depending on the focus of a particular school's curriculum, the table can be modified to add or remove certifications as well as updated to reflect changes in individual courses or certification exam objectives over time. IHLs can review available professional certifications on an annual basis and evaluate whether changes to their curriculum should be incorporated. Further, the release of a new exam version or a change to certification objectives by a certification body should trigger a corresponding curriculum review at the IHL.

## 4. DISCUSSION

### 4.1 Appropriateness of Using Certifications for Curriculum Shaping

Using professional certifications as a guide for course development is not new and has been done in the area of accounting systems and control (Walters, 2007). As previously mentioned, 35% of cybersecurity job postings requested a professional certification. While no single certification should be recommended, certifications are currently an important measure that the industry has for regulating professional competency, thus academic programs should work to integrate certifications into their curriculum (Fulton, Lawrence, and Clouse, 2014).

Some academic viewpoints hold that emphasizing professional certifications focuses too much on yesterday's technology and thus IHLs should focus on training a new workforce rather than building one based on certifications (Locasto et al., 2011). This suggestion is valid – any cybersecurity program should not focus too much on professional certifications at the expense of introducing students to emerging developments in the field. Indeed, there is no reason why faculty should focus on certifications without also covering the latest changes that may not have made their way into certification content yet. By taking a strategic approach to selecting a few key certifications to integrate into a curriculum, there should be plenty of room left to incorporate new technologies. At the university described in the case above, the faculty deemed it important to expose students to emerging issues related to critical infrastructure, cyber-physical systems, and the Internet of Things (IoT). Without losing any coverage of certification exam material, these topics were integrated into existing courses.

Further, certification bodies are attempting to combat this challenge by updating their examination criteria and material on a more frequent basis. For example, $(ISC)^2$ has refreshed the CISSP exam material approximately every three years since 2009. Therefore, we recommend faculty should find ways to cover material that includes emerging technology and tools while also promoting certifications so students can develop a rounded and relevant education as they enter the workforce (Kaspersky and Furnell, 2014). Considering input from multiple certifications also helps address this problem as certification exams undergo revisions to their objectives at different times, meaning that each year brings updates to different certifications on an ongoing basis.

### 4.2 Experiential Learning

Different certifications will have different foci. For example, many certification exams stress broad knowledge and concepts such as the CISSP. Other certifications focus on specific technologies or infrastructure (e.g., Certified Cloud Security Professional). Some certifications focus on tools and techniques, like the Certified Ethical Hacker (CEH) credential. The Global Information Assurance Certification (GIAC) offers dozens of specialized certifications aimed to ensure an individual has the skills necessary as a practitioner (GIAC, 2016a). Advanced certifications like the Licensed Penetration Tester (LPT) and Offensive Security Certified Professional (OSCP) require a hands-on penetration test demonstration in a cyber-range. While only a select few certifications require the demonstration of skills, nearly all discuss the use of tools and techniques within the field of cybersecurity. Schools should implement experiential or hands-on material wherever possible. This is advisable as Manson and Pike (2014) argue that changes in technology and security threats require aspiring cybersecurity professionals to set a goal of 10,000 hours of relevant, hands-on skill development over a long-term career. Providing hands-on experience, even if only in a simulated lab environment, instills in students not only the ability to understand *what* must be done to secure systems, but also *how* to go about doing it. This helps to address the concerns from employers that certifications alone do not guarantee competence; experience in applying the topics and techniques is a must.

Thus, in addition to certification, cybersecurity programs should promote hands-on experiential learning. Building and configuring an infrastructure to provide such experience may be challenging for IHLs, but many certification bodies provide environments to teach hands-on skills, such as iLabs from the EC-Council. In addition to cyber competitions and games like capture the flag, hands-on focused certifications can be used to advance the notion that cybersecurity students need such skills development.

### 4.3 Capstone Courses in Cybersecurity

Capstones courses present opportunities to prepare students for entry-level professional certifications. Capstones are typically taken by seniors who are nearing graduation. As cybersecurity majors, they will have taken the full curriculum allowing a capstone class to be taught at a high-level and serve as a certification exam prep course. Further, students are still in "study mode" while in school which presents timely opportunities to take these exams. Once they graduate and are working 40-60 hour weeks, it becomes increasingly difficult to set aside time to study. To overcome time constraints and the lack of motivation to study, many working professionals spend money on exam "boot camps" or other preparation materials. Rather than subjecting recent graduates to additional expenses associated with these materials, it's beneficial to provide current students with the necessary tools to take and pass certification exams before they graduate. While capstone classes traditionally involve "real-world" projects, they may be used as intensive "boot camps" to prepare students to pass certification exams. This approach is helpful considering the

competitive edge certifications can give a job candidate. For faculty considering this approach, we recommend using a quality study guide as a course textbook, such as an official CISSP study guide (Stewart, Chapple, and Gibson, 2015).

While some cybersecurity certifications do not require work experience (e.g., Security+ and GIAC Security Essentials), other certifications require a minimum length of professional experience in the field. In some cases, completing a university degree program reduces the amount of work experience required (e.g., CISA, CISM, and CISSP). Work experience requirements should not, however, discourage IHLs from modeling capstones after certification materials nor should it discourage current students from taking certification exams. Many certifying bodies allow an individual's passing score to be valid for several years, allowing them time to gain the experience required to become fully certified. Further, some certifications offer alternate designations to those who have passed the exam but are still working toward fulfillment of the experience requirement. $(ISC)^2$ awards "associate" status to such individuals, and, while they are not officially certified, this status differentiates graduates from others who have not even prepared for, and passed, a certification exam. Moreover, many certifications have significant overlap in coverage, so if a capstone concentrates on one certification, it will also cover in large measure other major certifications. Finally, faculty who teach a capstone focusing on certifications should assess how well students and graduates perform in passing certification exams. Doing so will help assess the effectiveness of this capstone approach. In summary, undergraduate capstones offer timely windows of opportunity where students can be primed to take entry-level certifications. Thus, consideration should be given to adding a capstone course to a program.

## 5. CONTRIBUTION

Applying our approach should reduce the amount of time spent determining curricula maintenance in an ongoing manner. While we should not limit curricula updates to certification material, staying in tune with certifications can reduce the time needed to research changes in the cybersecurity field. In essence, we are proposing a way to spend less time on figuring out "what" to teach, which allows for more time spent figuring out "how" to teach it.

Many cybersecurity programs in the United States seek designations by the Department of Homeland Security and the National Security Agency (DHS/NSA). These U.S. federal government organizations have been leaders in helping to shape cybersecurity and information assurance curriculum for years and have made significant positive contributions to cybersecurity education. The approach advocated in this paper, however, can be used to maintain any IHL's cybersecurity curriculum whether designated by DHS/NSA or not. This is important because our approach can be applied by any IHL globally since most certifications, such as from $(ISC)^2$, are international in scope whereas DHS/NSA are U.S.-centric.

Finally, based on our extant review of the scholarly literature, a gap exists in the literature regarding maintaining cybersecurity programs. Developing course objectives that are relevant and applicable is of key significance to such a rapidly developing field like cybersecurity. Even highly successful programs can quickly fall behind the curve if their curricula is not adequately modernized to reflect the current state of the field. While the current paper strives to provide guidelines to academicians who wish to update and maintain their existing programs, the same approach can also provide value to those looking to create a brand new program.

## 6. RECOMMENDATIONS

Faculty managing undergraduate cybersecurity curriculum should include an annual review of key professional certifications and monitor them for updates and changes. A great way to stay abreast of changes to these professional certifications is for faculty to become certified themselves. Most certification bodies require annual continuing education credits to ensure that certified individuals remain current on evolving threats and trends in the cybersecurity field. Having access to such training materials provides an effective way for academics to identify potential improvements to their existing curricula. In the case study, the CISSP, CISA, CISM, and CEH served as program benchmarks. The cybersecurity faculty either obtained these certifications or are active members in the societies supporting them. Any changes to these certifications are readily identifiable and can be used to update security courses.

## 7. LIMITATIONS

Besides certification, other inputs are important to maintaining curriculum and are not covered in this paper. These include seeking inputs from stakeholders, employers, graduates, and faculty. Guidance can also come from academic accreditation bodies, such as the developing Cyber Science standards from ABET (Gibson et al., 2015). In keeping curriculum current, faculty can also solicit the help of graduates and local industry leaders to be members of an advisory board. These boards can meet annually to help ensure the relevancy of a program.

Other well-known or possible resources that may be used to guide the maintenance of cybersecurity programs include using international standards, particularly the growing ISO/IEC 27000 series of information security publications. Academics could look to these industry standards as a guide for certain course coverage, such as using ISO 27000 standards in covering Governance, Risk, and Compliance (GRC) topics. IHLs particularly based in the U.S. can look to the US. Government's National Initiative for Cybersecurity Education (NICE). NICE promotes standards of cybersecurity education, training, and workforce development throughout the U.S. This effort publishes the National Cybersecurity Workforce Framework that gives a blueprint to organize and describe cybersecurity work into knowledge, skills, and abilities (KSAs). This comprehensive framework can be used to maintain and update cybersecurity curricula as it is used to help define professional requirements in cybersecurity (DHS, 2016). As of this writing, the framework is being developed into a U.S. standard (NIST, 2016).

Since information security is not a subject like mathematics where the materials relied upon today will be timely in five years or even next semester, the faculty must be motivated to update existing materials, assignments, and

course requirements that reflect events of the changing field (Belle, Imboden, and Martin, 2013). While in this paper we argue for the value of using professional certifications as input for curriculum review, other inputs obviously exist and must be considered as well.

Lastly, the current paper is limited in scope and is not intended to explain how to use certification content to make changes to individual course curricula and course syllabi. Instead, we merely suggest that IHLs should look to professional certifications for valuable guidance in their curriculum maintenance process.

## 8. CONCLUSION

The complexity of the cybersecurity landscape provides a number of opportunities and challenges. While industry has been making progress to address the latest developments in cybersecurity, higher education is always in danger of lagging behind in adapting to changes in a timely manner. Understanding the broad spectrum of professional certifications is helpful in order to better incorporate changes to cybersecurity curricula and prepare students for the highly competitive field. The current paper offers a review of literature on cybersecurity certifications and provides practical recommendations to IHLs interested in updating their cybersecurity programs. The presented case study showcases how a variety of certificates can be integrated in the curriculum and demonstrates the benefits of such an approach.

## 9. ENDNOTES

[1] Although definitions differ between cybersecurity and information security, for this paper, we use the terms interchangeably. For a related discussion, see von Solms and van Niekerk (2013).

[2] Since then, ISACA, GIAC, EC-Council, CompTIA, and others have earned this designation for various certifications. For an expanded list, visit www.ansi.org (ANSI, 2017).

[3] (ISC)², CISSP, SSCP, and CBK are registered trademarks owned by (ISC)², Inc. (visit www.isc2.org). ISACA, CISM, and CISA are registered trademarks owned by ISACA (visit www.isaca.org). EC-Council and CEH are registered trademarks owned by the EC-Council (visit www.eccouncil.org). All other trademarks mentioned in this article are the property of their respective owners.

## 10. REFERENCES


(ISC)². (2009). (ISC)² Launches First Country-Specific Credential to Meet Growing Demand for Qualified Information Security Professionals. Retrieved June 25, 2016, from http://www.isc2.org/pressreleasedetails.aspx?id=5206.

(ISC)². (2015a). (ISC)² CISSP and SSCP Domain Refresh FAQ. Retrieved July 5, 2016, from https://www.isc2.org/cissp-sscp-domains-faq/default.aspx.

(ISC)². (2015b). Certified Cloud Security Professional (CCSP) FAQs. Retrieved June 25, 2016, from https://www.isc2.org/ccsp-faqs/default.aspx.

(ISC)². (2015c). *CISSP Exam Outline Candidate Information Bulletin (CIB).* Clearwater, FL: (ISC)².

(ISC)². (2015d). The 2015 (ISC)² Global Information Security Workforce Study. Retrieved June 25, 2016, from https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf.

(ISC)². (2017). (ISC)² International Academic Program (IAP). Retrieved June 5, 2017, from https://www.isc2.org/international-academic-program.

AWS. (2016). *Amazon Web Services Overview of Security Processes*. Amazon Web Services, Inc.

ANSI. (2017). ANSI/ISO/IEC 17024 (Accredited). Retrieved June 3, 2017, from https://www.ansi.org/accreditation/credentialing/personnel-certification/Directory.

Backhouse, J., Hsu, C. W., & Silva, L. (2006). Circuits of Power in Creating de jure Standards: Shaping an International Information Systems Security Standard. *MIS Quarterly*, 30(Special Issue), 413-438.

Belle, W., Imboden, T., & Martin, N. L. (2013). An Undergraduate Information Security Program: More than a Curriculum. *Journal of Information Systems Education*, 24(1), 63-70.

Bogolea, B. & Wijekumar, K. (2004). Information Security Curriculum Creation: A Case Study. *1st Annual Conference on Information Security Curriculum Development.* (pp. 59-65). Kennesaw, Georgia: ACM.

Bryman, A. (2012). *Social Research Methods.* (4th, Ed.) Oxford, England: Oxford University Press.

Bureau of Labor Statistics. (2010). 15-1122 Information Security Analysts. Retrieved June 21, 2016, from http://www.bls.gov/soc/2010/soc151122.htm.

Bureau of Labor Statistics. (2015a). Occupational Employment Statistics Query System. Retrieved June 23, 2016, from https://data.bls.gov/oes/#/home.

Bureau of Labor Statistics. (2015b). Occupational Outlook Handbook, 2016-2017 Edition. Retrieved June 25, 2016, from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-1.

Burning Glass. (2015). *Job Market Intelligence: Cybersecurity Jobs, 2015.* Boston, MA: Burning Glass Technologies.

CompTIA. (2013). Security+ Certification Exam Objectives: SY0-401. Retrieved August 12, 2016, from https://www.comptia.jp/pdf/comptia-security-sy0-401.pdf.

Department of Labor. (2016). *Certification Finder, Search Keyword 15-1122*. Retrieved June 21, 2016, from http://www.careeronestop.org/toolkit/training/find-certifications.aspx?keyword=15-1122.

DHS. (2016). Department of Homeland Security (DHS). Retrieved June 21, 2016, from https://niccs.us-cert.gov/training/tc/framework.

EC-Council. (2015). Hacking Mobile Platforms - Module 15. In *Certified Ethical Hacker - Exam 312-50.* EC Council.

EC-Council. (2016). What is New in the CEH Version 9 Course? Retrieved June 28, 2016, from https://www.eccouncil.org/Certification/certified-ethical-hacker.

Endicott-Popovsky, B. E. & Popovsky, V. M. (2014). Application of Pedagogical Fundamentals for the Holistic Development of Cybersecurity Professionals. *ACM Inroads*, 5(1), pp. 57-68.

Fulton, E., Lawrence, C., & Clouse, S. (2014). White Hats Chasing Black Hats: Careers in IT and the Skills Required to Get There. *Journal of Information Systems Education*, 24(1), 75-80.

GIAC. (2016a). GIAC - Information Security - Program Overview. Retrieved July 17, 2016, from http://www.giac.org/about/program-overview.

GIAC. (2016b). GIAC Launches New Certification for Python Coders, GPYC. Retrieved July 17, 2016, from http://www.prnewswire.com/news-releases/giac-launches-new-certification-for-python-coders-gpyc-300265014.html.

Gibson, D., Hawthorne, B., Buck, S., Fitzgerald, S., & Lingafelt, S. (2015). Toward Curricular Guidance in the "Cyber Sciences." *The Colloquium for Information Security Education (CISSE)*. Las Vegas, NV. Retrieved June 25, 2016, from www.cybereducationproject.org.

Hentea, M., Dhillon, H. S., & Manpreet, D. (2006). Towards Changes in Information Security Education. *International Journal of IT Education*, 5, 221-233.

ISACA. (2015). ISACA to Update CISA Exam in 2016 to Reflect Changes in Job Requirements - Press Release. Retrieved from http://www.isaca.org/About-ISACA/Press-room/News-Releases/2015/Pages/isaca-to-update-cisa-exam-in-2016-to-reflect-changes-in-job-requirements.aspx.

ISACA. (2016). State of Cybersecurity: Implications for 2016. Retrieved July 7, 2016, from http://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf.

ISO/IEC. (2012). *ISO/IEC 17024 - General Requirements for Bodies Operating Certification of Persons.* Geneva, Switzerland: ISO/IEC.

Kaspersky, E. & Furnell, S. (2014). A Security Education Q&A. *Information Management & Computer Security*, 22(2), 130-133.

Locasto, M. E., Ghosh, A. K., Jajodia, S., & Stavrou, A. (2011). The Ephemeral Legion: Producing an Expert Cyber-Security Work Force from Thin Air. *Communications of the ACM*, 54(1), 129-131.

Manson, D. & Pike, R. (2014). The Case for Depth in Cybersecurity Education. *ACM Inroads*, 5(1), 47-52.

Marsh, N. (2015). *Nmap 6 Cookbook: The Fat Free Guide to Network Scanning*. Fat Free Publishing.

McGill, T. & Dixon, M. (2005). Information Technology Certification: A Student Perspective. *Information International Journal of Information and Communication Technology Education*, 1(1), 19-30.

Merriam, S. B. (1998). *Qualitative Research and Case Study Applications in Education. Revised and Expanded from Case Study Research in Education.* San Francisco: Jossey-Bass Publishers.

NIST. (2016). NICE Cybersecurity Workforce Framework (NCWF), NIST Special Publication 800-181 (draft). (B. Newhouse, Ed.) Retrieved December 17, 2016, from http://csrc.nist.gov/nice/.

NSA. (2016). Information Assurance Directorate at the NSA. Retrieved June 25, 2016, from https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_Knowledge_Units.pdf.

Oriyano, S. P. (2014). *Certified Ethical Hacker (CEH) Version 8 Study Guide.* Indianapolis, IN: Sybex.

Parker, D. B. (1981). *Computer Security Management.* Reston, Virginia: Reston Publishing Company.

Patten, K. P. & Harris, M. A. (2013). The Need to Address Mobile Device Security in the Higher Education IT Curriculum. *Journal of Information Systems Education*, 24(1), 41-52.

Rob, M. A. (2014). IT Certification: Demand, Characteristics and Integration into Traditional University MIS Curriculum. *Communications of the IIMA*, 14(1), 20-44.

Shearer, D. (2015). Maintaining the Relevancy of (ISC)² Certifications: CISSP and SSCP Credential Enhancements. Retrieved June 21, 2016, from http://blog.isc2.org/isc2_blog/2015/01/maintaining-the-relevancy-of-isc%C2%B2-certifications-cissp-and-sscp-credential-enhancements.html.

Stallings, W. (2016). *Network Security Essentials, 6e*. Essex, England: Pearson Education Limited.

Stewart, J., Chapple, M., & Gibson, D. (2015). *Certified Information Systems Security Professional (CISSP) Official Study Guide* (7th ed.). Indianapolis, IN: Sybex.

Tittel, E. (2016). Best Information Security Certifications for 2017. Retrieved December 17, 2016, from http://www.tomsitpro.com/articles/information-security-certifications,2-205.html.

von Solms, R. & van Niekerk, J. (2013). From Information Security to Cyber Security. *Computers & Security*, 38, 97-102.

Walters, L. M. (2007). A Draft of an Information Systems Security and Control Course. *Journal of Information Systems*, 21(1), 123-148.

Whitman, M. E. & Mattord, H. J. (2004). Designing and Teaching Information Security Curriculum. *1st Annual Conference on Information Security Curriculum Development* (pp. 1-7). ACM.

Wireschen, D. & Zhang, G. (2010). Information Technology Certification Value: An Initial Response from Employers. *Journal of International Technology and Information Management*, 19(4), 89-109.

Wright, M. A. (2015). Improving Cybersecurity Workforce Capacity and Capability. *ISSA Journal*, 14-20.

**AUTHOR BIOGRAPHIES**

**Kenneth J. Knapp** is an Associate Professor at The University of Tampa. He is a twenty-year veteran of the U.S. Air Force and received his PhD at Auburn University. Dr. Knapp has published in journals such as Computers & Security, Communications of the Association for Information Systems, Journal of Organizational & End User Computing, International Journal of Information Security & Privacy and Government Information Quarterly. He is a Certified Information Systems Security Professional (CISSP) and Certified Ethical Hacker (CEH).

**Christopher Maurer** is an Assistant Professor in the McIntire School of Commerce at the University of Virginia. He received his PhD from the University of Georgia and was previously an Assistant Professor at the University of Tampa. His research interests include cybersecurity controls, the impact of cybersecurity breaches, enterprise systems, and IT-business alignment. His previous research has appeared in journals and conference proceedings including MIS Quarterly Executive, the International Conference on Information Systems (ICIS), the American Conference on Information Systems (AMCIS), and the Hawaii International Conference on System Sciences (HICSS).

**Miloslava Plachkinova** is an Assistant Professor of Cybersecurity in the Sykes College of Business at the University of Tampa, FL. She holds a PhD in Information Systems and Technology from Claremont Graduate University, CA. She is a Certified Information Security Manager (CISM) and a Project Management Professional (PMP). Dr. Plachkinova's research focuses on information security and healthcare. She investigates how human behavior leads to data breaches and her work in the healthcare field investigates security and privacy issues in mobile health (mHealth) and electronic health records (EHR) on the cloud. Dr. Plachkinova also has extensive industry experience working for both the private and the public sectors.

**APPENDIX A.** *Matrix of CISSP Common Body of Knowledge to Undergraduate Cybersecurity Curriculum.* From our case study example, the following matrix shows the results of an analysis of the CISSP CBK compared with a university's Cybersecurity undergraduate program. The percentage in each cell shows how much of each course is included in the CISSP CBK per domain. In total, the entire CISSP CBK is covered in this undergraduate program. The assessment used the CISSP Candidate Information Bulletin (CIB) of April 2015. The CIB lists the key areas of knowledge for all eight CBK domains. Course descriptions and syllabi were used for assessing the courses. The percentages were established by the faculty member teaching the actual course.

| Course<br><br>CBK Domain | Mgt Info Systems | Network & Cloud Infrastr. | Appl. Develop | Info Sec Principles | Network Security | Risk Mgt | Physical & Ops. Security | Ethical Hacking | Cyber Capstone. | TOTAL Coverage of CISSP CBK per domain |
|---|---|---|---|---|---|---|---|---|---|---|
| Security & Risk Mgt | <5% | <5% | <5% | 40% | <5% | 80% | <5% | <5% | 40% | 100% |
| Asset Mgt | <5% | <5% | <5% | 25% | 10% | 20% | 40% | <5% | 50% | 100% |
| Security Engineering | <5% | 20% | <5% | 15% | 20% | <5% | 25% | <5% | 40% | 100% |
| Comm. & Network Security | <5% | 70% | <5% | 20% | 80% (see Apdx B) | <5% | 15% | 20% | 20% | 100% |
| Identity & Access Mgt | <5% | 15% | <5% | 20% | <5% | <5% | 20% | <5% | 50% | 100% |
| Security Assessment & Testing | <5% | <5% | <5% | <5% | <5% | 15% | 20% | 30% | 60% | 100% |
| Security Ops | <5% | <5% | <5% | 10% | 15% | 20% | 30% | 20% | 60% | 100% |
| Software Dev. Security | <5% | <5% | 15% | 20% | <5% | <5% | 40% | <5% | 60% | 100% |

**APPENDIX B**. *Example Matrix of Communication and Network Security Domain to the Undergraduate Network Security Course*. From our case study, the following matrix is an example of the type of analysis that can attain the percentages found in Appendix A. Ultimately, this analysis should be used as a guide for the faculty member to ensure that certification knowledge requirements are covered. The left column lists the Key Areas of Knowledge found in the CISSP CIB ((ISC)², 2015c, pp. 16-17). The title row across the top indicates major lesson topics covered in the Network Security course syllabus. These topics were derived from three substantial texts used in the course: 1) Network Security Essentials, 6th edition (Stallings, 2016), 2) Nmap 6 Cookbook (Marsh, 2015), and 3) Amazon Web Services Overview of Security Processes (AWS, 2016). A check box indicates that the knowledge area received full (100%) coverage in the course textbook material and/or in a course assignment. Partial coverage is identified where the topic is only briefly covered. It is also possible to use course objectives instead of lesson topics, depending on the level of granularity of the course objectives. The final row provides the approximate coverage of the Communications & Network Security CISSP Domain in the Network Security course; as this is a guide, exact precision of the percentage is not necessary here.

| Network Security Course Major Topics / Network Security Key Knowledge on CISSP | Network Introduction & Review | Network Scanning using Nmap | Cryptography | User Auth. & Key Distribution | Network Access Control | Cloud Security & AWS | Transport Layer Security | Wireless Security | Malware | IDS, IPS & Firewalls | Design Secure Network Arch. | Coverage of Key Knowledge on CISSP |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Network Archit. (A) | | | | | | | | | | | | |
| OSI & TCP/IP models (A.1) | √ | √ | | | | | | | | | | 100% |
| IP networking (A.2) | √ | √ | | | | | √ | | | √ | | 100% |
| Multi-layer protocols (A.3) | Partial | Partial | | | | | | | | | | 25% |
| Converged protocols (e.g. MPLS) (A.4) | Partial | Partial | | | | | | | | | | 25% |
| Software-defined networks (A.5) | Partial | | | | | | | | | | Partial | 25% |
| Wireless networks (A.6) | | | | | √ | | | √ | | | | 100% |
| Cryptography (A.7) | | | √ | √ | | | √ | √ | | | | 100% |
| Secure Network Components (B) | | | | | | | | | | | | |
| Hardware Operations (e.g. routers, WAPs) (B.1) | √ | | | | | | | √ | | √ | √ | 100% |
| Transmission media (B.2) | √ | | | | | | | | | | √ | 100% |
| Network access control (e.g. firewalls) (B.3) | | √ | | | √ | | | | | √ | | 100% |
| Endpoint security (B.4) | | √ | | √ | | | | √ | √ | √ | √ | 100% |

| Network Security Course Major Topics<br>Network Security Key Knowledge on CISSP | Network Introduction & Review | Network Scanning using Nmap | Cryptography | User Auth. & Key Distribution | Network Access Control | Cloud Security & AWS | Transport Layer Security | Wireless Security | Malware | IDS, IPS & Firewalls | Design Secure Network Arch. | Coverage of Key Knowledge on CISSP |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Content-distribution networks (B.5) | | | | | | √ | | | | | √ | 100% |
| Physical devices (B.6) | | √ | | | √ | | | | | | | 100% |
| Secure Comm. channels (C) | | | | | | | | | | | | |
| Voice (C.1) | √ | | | | | | | | | | √ | 100% |
| Multimedia collaboration (C.2) | | | | | | | | | | | | 0% |
| Remote access (e.g. VPN) (C.3) | | | √ | | | √ | √ | √ | | | √ | 100% |
| Data communication (e.g. VLANS) (C.4) | | | | | | √ | | | | | √ | 100% |
| Virtualized networks (C.5) | | | | | | √ | | | | | √ | 100% |
| Prevent or mitigate network attacks (D) | | | √ | √ | √ | √ | √ | √ | √ | √ | √ | 100% |
| Approximate Coverage of Communications & Network Security CISSP Domain in Network Security Course | | | | | | | | | | | | 80% |


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