Using Bloom's and Webb's Taxonomies to Integrate Emerging Cybersecurity Topics into a Computing Curriculum

Mark A. Harris
Karen P. Patten
Integrated Information Technology
University of South Carolina
Columbia, SC 29201, USA
markaharris@sc.edu; pattenk@hrsm.sc.edu

ABSTRACT

Recent high profile hackings have cost companies millions of dollars resulting in an increasing priority to protect government and business data. Universities are under increased pressure to produce graduates with better security knowledge and skills, particularly emerging cybersecurity skills. Although accredited undergraduate computing programs recognize the need to solve this problem, these computing programs are constrained by accreditation standards and have limited ability to modify their curricula. This paper discusses a case study on how one Accreditation Board for Engineering and Technology (ABET) accredited undergraduate IT program created a strategy to continue to teach existing security-related topics as well as emerging cybersecurity topics within its IT curriculum without increasing credit requirements. The faculty developed an *IT Security-related and Cybersecurity Curriculum Taxonomy* to identify strategies to move security-related topics taught in the higher level courses to lower and intermediate courses. Thus emerging cybersecurity topics could be added to high-level courses. The faculty also created the *IT Student Learning (Security-related) Taxonomy* by combining *Bloom's Taxonomy's* six levels of thinking with Webb's *Depth of Knowledge Model*. This student learning taxonomy enabled the faculty to review the student learning outcomes for each of the existing security-related core topics and develop new ones for the emerging cybersecurity topics. Challenges, benefits, and application of this strategy to other disciplines are discussed.

Keywords: Cybersecurity, Curriculum design and development, Bloom's taxonomy, Webb's depth of knowledge

1. INTRODUCTION

As high profile hacking incidents increase (e.g., Target and Home Depot), protecting government and business data has become an increasingly critical and strategic priority. However, hiring cybersecurity professionals has proven difficult because of the lack of qualified applicants. Cisco estimates there is currently a shortage of one million qualified cybersecurity professionals worldwide (Cisco, 2014). A common call to solving the shortage problem is for universities to educate new cybersecurity professionals (Conklin, Cline, and Roosa, 2014; Janicki, Cummings, and Kline, 2013; Sauls and Gudigantala, 2014). But the problem goes beyond just educating new cybersecurity professionals. Every student heading into the workforce needs to be educated about cybersecurity to some degree. Research shows that the human element is still the weakest link (Caldwell, 2012; Thomason, 2013). This means all graduates from all disciplines need some form of cybersecurity education.

Many current computer science (CS), information systems (IS), and information technology (IT) programs are attempting to solve the cybersecurity professional shortage problem. Some, such as the Illinois Institute of Technology have developed new cybersecurity or cyber forensics graduate programs (Illinois Institute of Technology, 2015). Other computing programs are adding new courses or concentrations in cybersecurity. However, this push for new cybersecurity education is occurring at the same time some universities are eliminating existing courses and credits to meet other university goals, such as improving student graduation rates. Also, many computing programs are constrained by accreditation standards resulting in limited ability to modify their curricula The recognized accreditation body within the computing discipline is the Accreditation Board for Engineering and Technology (ABET). Within ABET, each of the five computing disciplines has its own curriculum criteria, although there is some overlap.

This paper discusses a case study on how one ABET-accredited undergraduate IT department created a strategy to address the need for all IT students to have increased cybersecurity knowledge and skills. At the same time, we ensured that ABET-required security-related topics continued to be taught, along with emerging cybersecurity topics, without increasing credit requirements. Within an ABET-accredited IT program, the comprehensive IT curriculum covers thirteen Knowledge Areas (KAs), including “information assurance and security (IAS).” Because of university undergraduate credit caps, adding new courses is difficult without dropping an existing course. Prior to this case study, most of the existing security-related IAS topics were taught in a catch-all advanced *Security* course. The IT faculty developed a strategy to teach required IAS core topics throughout the curriculum, integrating these topics into the lower and intermediate level courses, resulting in adding a new security component to several courses. This created room in the existing upper-level security course to add emerging cybersecurity topics. A few IAS core topics were included in several lower level courses, but were not covered in depth. Thus, students now learn security-related topics within each of the IT curriculum KAs rather than in one security course. The new curriculum not only teaches ABET-required IAS topics, but other important emerging cybersecurity topics not included in ABET guidelines. The approach used in this case study is also applicable to other computing disciples.

Considering ABET’s broad IT education standards, our undergraduate ABET program emphasizes breadth of IT knowledge and skills, now including cybersecurity knowledge and skills, for the newly minted entry-level IT professionals. Our undergraduate IT program’s intent is to maximize our graduate’s knowledge of security within the given constraints, by providing them adequate knowledge and skills to succeed in the workforce when seeking entry level positions. Those seeking a more robust, specialized security education are encouraged to investigate graduate programs, on-the-job training, or certifications in security.

We’ve used Bloom’s Taxonomy in the past to identify specific learning outcomes for lower-level, intermediate, and advanced courses within our IT curriculum. While working on this project, we again used Bloom’s Taxonomy along with Webb’s Depth of Thinking Model to create an *IT Security and Cybersecurity Curriculum Taxonomy* to help identify areas where new cybersecurity topics could be added to specific courses within the curriculum. A benefit of this strategy was that the mapping also ensured that all IAS-related topics were actually being addressed within our curriculum. Another benefit of using Webb’s Model is that faculty members realize at what depth each topic is being or should be taught. Every IAS plus new cybersecurity topic was mapped to the six levels of thinking in our adapted *IT Student Learning Taxonomy* (remembering, understanding, applying, analyzing, evaluating, and creating), making it easy for the faculty to identify areas where different levels of instruction may be needed or where topics are duplicated unnecessarily.

Security-related topics within the current Association for Computing Machinery (ACM) *IT2008 Model Curriculum* (Lunt et al., 2008) and emerging cybersecurity topics, identified by IT curriculum experts and industry representatives, are discussed in Section 2. We also include a brief review of Bloom’s Taxonomy and Webb’s Depth of Thinking in that section. In Section 3, we describe our continuous improvement IT curriculum strategy to integrate emerging cybersecurity topics into the IT curriculum. Section 4 discusses the challenges, student learning outcomes, and the benefits of our integration strategy along with the use of the *IT Security Curriculum Taxonomy*. Finally, the paper concludes in Section 5 with our research contributions, limitations, and future directions.

2. LITERATURE REVIEW: SECURITY-RELATED AND EMERGING CYBERSECURITY TOPICS

This section reviews the development of security-related “information and assurance (IAS)” topics within ACM’s *IT2008 Curriculum Model*, the identification of emerging cybersecurity topics, and a review of Bloom’s Taxonomy and Webb’s Depth of Thinking Model.

2.1 IT2008 Model Curriculum Security Development

The ACM Special Interest Group on Information Technology Education (SIGITE) Curriculum Committee covered “computing security” topics in several different ways within the *IT2008 Model Curriculum* (Lunt et al., 2008). Initially, the committee writers were not comfortable considering “computing security” as a separate “Knowledge Area” (Dark, Ekstrom, and Lunt, 2006). Instead, the committee found that “information assurance and security” covered a broader context, better fitting the broader context of the IT computing discipline. Knowledge areas, or KAs, are defined as specific bodies of knowledge within a discipline. The National Information Assurance Education and Training Partnership (NIETP) defines information assurance as a “*set of measures intended to protect and defend information and information systems by insuring their availability, integrity, authentication, confidentiality, and non-repudiation* (Dark, Ekstrom, and Lunt, 2006). As a result, the committee included “information assurance and security (IAS)” as one of the 13 knowledge areas within the IT curriculum. The *IT2008 Model Curriculum* is the first place where IAS is defined within any computing discipline. IAS topics are included in three separate areas within the *IT2008 Model*:

- Within the “IT fundamentals (ITF)” KA targeted for freshmen
- As a ’pervasive theme‘ throughout many courses within the curriculum
- As a separate IAS KA with a course for seniors integrating all concepts learned in earlier core competency courses.

Because of the IAS emphasis, the curriculum committee also included ‘security’ as a sub-topic within the knowledge areas of “networking,” “social and professional issues,” and “web systems and technologies” (Rowe, Lunt, and Ekstrom, 2011).

When topics are considered essential, but do not seem to fit any specific knowledge area, they are included as ’pervasive themes.’ It is intended that pervasive themes should be introduced within the IT fundamentals class and included in many of the courses throughout the IT curriculum. Ekstrom et al. (2006) defined pervasive themes as “*a set of ‘big ideas’ that reside at the heart of the discipline and that cannot be covered directly, but must somehow be grasped by students as they become proficient* *in the discipline.*" Thus, security-related topics are intended to be included in many courses within the curriculum.

2.2 Cybersecurity Curriculum Research

Researchers are investigating ways to both integrate cybersecurity into the existing curricula, but also to create a separate cybersecurity curriculum within higher education, but very few discuss it within the context of ABET accreditation. Andel and McDonald (2013) described a lengthy 132 credit Bachelors of Science degree in Cyber Assurance, providing a "systems-level approach that incorporates cybersecurity skills at both the hardware and software level." The new degree program is so focused on cybersecurity that it would not fit into any of the existing computing curriculum models. Greenlaw, Phillips, and Parrish (2014) addressed this problem by calling for the ABET Accreditation Board to create a new set of cybersecurity criteria for emerging cybersecurity programs, since the current criteria make it difficult for cybersecurity programs to meet accreditation requirements. They discuss how current accreditation criteria fail to differentiate among new cybersecurity programs based on the specifics of a cybersecurity curriculum.

In one study, Patten and Harris (2013) discuss adding mobile device security education to a current ABET-accredited IT curriculum by mapping the new topic learning outcomes across several courses within the curriculum. Another study by Wood et al. (2010) investigated how to use ABET Information Systems (IS) criteria to create a bachelor's degree that also incorporated aspects of forensics and information security. The authors note that the ABET IS criteria are flexible enough to adapt the new courses within the framework although no such mapping was provided for the CS or IT curriculum criteria.

In other research not related to ABET guidelines, Futcher, Schroder, and von Soms (2010) identified an evident "information security gap" within undergraduate IT programs in South Africa. Security appeared to be better represented and more mature within the postgraduate programs. In those few undergraduate programs where information security was included, it was on an ad hoc basis with a few information security aspects covered. These authors concluded that "information assurance and security (IAS)" appears to be a challenge in many undergraduate IT programs. Students will need to have competencies beyond those technical or narrowly defined skills.

Chen, Maynard, and Ahmad (2013) compared security curricula between China and the United States. Both countries include CS security topics and IT IAS topics, but China also emphasizes telecommunications security. The United States programs differed by emphasizing enterprise-level security strategy, security policy, security management, and cyber law. Bicak, Liu, and Murphy (2015) discussed the creation of three specific graduate specialties to handle emerging topics and to prepare students with specific skills employers seek, rather than with broad-based knowledge. The three specialties are cybersecurity data analysis, cyber intelligence, and healthcare information security and privacy. Finally, another paper calls for an infusion of criminal justice and political science into a cybersecurity curriculum to give students skills outside of the typical computing discipline and to better prepare them for careers in government and industry (Stockman, 2013).

2.3 Identifying and Classifying Security-related Topics

A list of topics concerning cybersecurity education were developed at a workshop on cybersecurity education and training, sponsored by the ACM in 2013 (McGettrick, 2013). To provide a visual representation of how various security and cybersecurity topics relate to each other, the workshop attendees developed a classification scheme of nested security categories using "information assurance" and "computer security" core topics and newly identified cybersecurity topics. The definitions used in this classification scheme were first developed at an Innovation in Technology in Computer Science Education (ITiCSE) workshop (Cooper et al., 2010). Information Assurance (IA) refers to the *"set of technical and managerial controls designed to insure the confidentiality, possession of control, integrity, authenticity, availability, and utility of information and information systems"* (Cooper et al., 2010). Since this nearly matches the *IT2008 Model Curriculum* definition of IAS, we modified the classification to use the more familiar IAS. Cybersecurity (CySec) describes *"the ability to protect or defend the use of cyberspace from cyber-attacks"* (Cooper et al., 2010). Computer security (CSec) develops "*measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated"* (Cooper et al., 2010).

Figure 1 shows these nested categories where information assurance and security (IAS) topics are the broadest category, encompassing cybersecurity (CySec) topics, which in turn encompasses the more specialized computer security (CSec) topics (McGettrick, 2013).

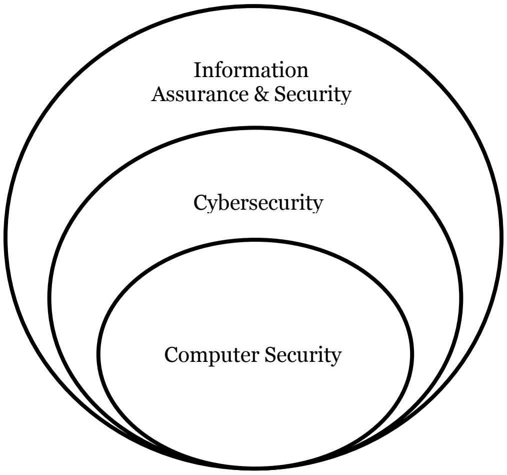

Figure 1. Computer Security, Cybersecurity, and Information Assurance and Security Relationships

Participants at the 2013 workshop brainstormed and created a list of 27 separate security and cybersecurity topics. Each of the 27 security-related and cybersecurity topics were compared and then classified using the nested categories shown in Figure 1. Several topics were classified in more than one category (CSec, CySec, or IAS) because the same topic may have different aspects. For example, *"cryptography"* and *"database administration"* are included in both the computer security (CSec) and information assurance and security (IAS) knowledge areas. Other topics are unique to cybersecurity (CySec) such as *"malware"* or *"botnets."*

2.4 Developing Student Learning Outcomes within an IT Curriculum

Benjamin Bloom, together with a group of scholars, developed a classification of learning levels based on intellectual behavior, known as Bloom's Taxonomy (Bloom and Krathwol, 1956). In 2001, key elements of the taxonomy were updated to reflect more relevance to 21st century educational goals (Anderson and Krathwohl, 2001; Krathwohl, 2002). In 1997, Norman Webb developed a process to analyze the alignment between standards and standardized assessments. This process, referred to as the *Depth of Knowledge (DoK) Model*, is also used to review alignment of curricula with standards and assessments (Webb, 1997). The model assumes that expected student activities within specific courses may be categorized based upon the cognitive demands needed to produce acceptable responses. Each grouping of tasks reflects a different level of cognitive expectation, or depth of knowledge, required to complete the tasks.

Merging the constructs of the updated Bloom's Taxonomy with the depth of knowledge classifications from Webb's DoK Model is useful when developing specific student learning outcomes as shown in Table 1 (Keane et al., 2009; Overbaugh and Schultz, 2015; Perkins, 2008; Starr, Manaris, and Stalvey, 2008).

The next section describes a case study on how faculty at one large southeastern public ABET-accredited undergraduate IT department developed an integration strategy using Bloom's – Web's taxonomy to move security-related core topics into lower-level courses, freeing up space in the senior-level *Security* course to add emerging cybersecurity topics without adding new credits to the curriculum.

3. CASE STUDY: INTEGRATING EMERGING CYBERSECURITY TOPICS

As part of the initial ABET accreditation process, the faculty considered many factors including the *ACM IT2008 Model Curriculum* (Lunt et al., 2008) as a guide for mapping specific technology topics to existing IT courses, making changes to courses and the curriculum to meet the ABET guidelines, establishing student learning outcomes for each of the courses, and then going through the formal accreditation process. The existing IT curriculum also included experiential learning goals (1) to insure that students are graduating with necessary knowledge, skills, and abilities, including ethical and moral values, (2) to demonstrate that students are able to integrate their knowledge into real projects in complex organizational settings, and (3) to insure that students understand the organizational needs of businesses (Keane and Patten, 2010; Keane et al., 2009).

Keeping an undergraduate IT curriculum relevant and timely is a well-known challenge for faculty because an IT curriculum is an evolutionary process due to the continuous change in technology and continual shifting of workplace requirements (Surendra and Denton, 2009). Issues include: keeping emerging technology topics up-to-date; keeping the faculty's emerging technology knowledge up-to-date; providing students with in-depth knowledge and relevant hands-on experiences, and developing specific learning outcomes that reinforce earlier student learnings.

Once an undergraduate IT program becomes ABET-accredited, the IT faculty must demonstrate continuous improvement to maintain its program's accreditation. Student learning outcomes are continuously assessed to insure students are learning the necessary topics. Courses must continuously be evaluated to insure that current and emerging technologies are included or, if the analysis shows core topics are missing, determine how these core and emerging topics can be added to the curriculum. This case study involved mapping the student learning outcomes for each of the current security-related topics to all levels of the curriculum and how key gaps, in this case, emerging cybersecurity student learning outcomes, can be added to the updated curriculum.

3.1 Current Student Learning Levels within the IT Curriculum

The first step in this case study was to analyze the current ABET-accredited integrated curriculum within the IT program. The faculty had previously established continuous improvement process goals incorporating experiential learning theories within the curriculum, determining the level of expertise required by each student within each course, and insuring that the delivery of the technical courses results in a rich environment, where students are able to learn at a high level. As described in the previous section, the faculty combined *Bloom's Taxonomy* and Webb's *Depth of Knowledge (DoK) Model*, Table 2, to determine to what degree each student is expected to understand and use concepts as well as demonstrate particular skills in each course. This helped the faculty determine at what level each course fits within the curriculum. Thus, the faculty documented that course goals are aligned with instructional methods and assessment techniques for each course.

Within the lower level courses in the IT curriculum, the learning outcomes "remembering" and "understanding" best aligned with the *Introduction to IT* course as well as business foundation courses. Students within the IT core courses should be using "applying" and "analyzing" levels of thinking. Once students reach the higher level courses, their learning outcomes best address the "evaluating" and "creating" cognitive areas.

3.2 Security and Cybersecurity Gaps within the IT Curriculum

The second step was to follow the recommendations of Rowe, Lunt, and Ekstrom (2011) to carefully analyze the current IT curriculum to determine where security-related topics currently are taught as well as where emerging cybersecurity

Level of Learning	Bloom's Updated "Six Levels of Thinking" (Webb's Four "Depth of Knowledge" Concepts)	Student Learning Outcomes: "Student is able to…"	IT Security Student Learning Examples
Higher Level (Expert)	**6. Creating (Extended Thinking)** Can the student create a new product or point of view? Requires investigation, complex reasoning, planning, developing, and thinking, probably over an extended period of time.	• Put elements together to form a coherent or functional whole; • Reorganize elements into a new pattern or structure through generating, planning, or producing.	• Create a security risk assessment and disaster recovery plan.
	5. Evaluating (Strategic Thinking) Can the student justify a stand or decision? Requires reasoning, developing plans or a sequence of steps, some complexity, more than one possible answer.	• Make judgments based on criteria and standards.	• Evaluate threats and countermeasures based on a risk assessment.
	4. Analyzing (Strategic Thinking) Can the student distinguish between the different parts? Requires reasoning, developing plans or a sequence of steps, some complexity, more than one possible answer Higher level of thinking than previous two levels.	• Break down material into component parts so that its organizational structure may be understood.	• Identify and analyze project risk and perform qualitative and quantitative analyses.
Intermediate Level	**3. Applying (Skill / Concept)** Can the student use the information in a new way? Engages mental process beyond habitual response using information or conceptual knowledge. Requires two or more steps.	• Use learned material in new and concrete situations.	• Apply appropriate physical vs. logical and centralized vs. decentralized access control in various scenarios.
Lower Level- (Beginner)	**2. Understanding (Recall and Reproduction)** Can the student explain ideas or concepts?	• Grasp the meaning of the material.	• Understand and explain auditing, asset management, standards, and enforcement when managing networks.
	1. Remembering (Recall and Reproduction) Can the student recall or remember a fact, information, or procedure?	• Recall appropriate information.	• Discuss encrypting user account passwords.

Table 1. IT Student Learning Taxonomy (Security-Related)

topics can be integrated into existing courses or into newly created courses. Given the constraint that a new cybersecurity course could not be added without dropping an existing technical course, the faculty evaluated the current security student learning outcomes on a course-by-course basis. As mentioned earlier, the ACM 2013 Cybersecurity Workshop identified 27 security topics (McGettrick, 2013), classified as more specialized computer security (CSec) topics, emerging cybersecurity (CySec) topics, and broader information assurance and security (IAS) topics.

After reviewing each topic compared to our existing curriculum, our faculty determined that several of the topics were closely linked and could be combined, while others should be separated. For example, *"mobile and cloud"* were listed as a single security-related topic, but we decided these technologies should be separate topics within our curriculum. "*Malware and intrusion detection systems"* were considered one topic, however, our faculty decided that *"intrusion detection systems"* detect more than just *"malware." "Botnets,"* originally listed as a separate topic, were instead combined with *"malware."* Based on our curriculum, the faculty decided not to include "*sociology"* and *"economics."* We determined that *"web"* and *"programming"* topics were part of our programming courses and not topics. We also removed the *"applications"* since many other applications besides healthcare and finance are included in our courses. After separating, condensing, and removing the security-related topics, a list of 24 security-related and cybersecurity topics, as classified by the workshop participants, was approved by the IT faculty and shown in table 2. Of these 24 items, the faculty concluded that 19 were already included in the ACM *IT2008 Curriculum Model* (Lunt et al., 2008) as well as covered to some extent within our curriculum. Five additional topics were defined as emerging cybersecurity topics not included in the *IT2008 Model.* The IT faculty, based on their own research interests, industry experiences, and relationships with IT professionals, identified four additional topics, to be added to the IT curriculum. These faculty-identified topics were *"Internet of Things (IoT)," "personal security," "security culture,"* and *"security training."* The final list, shown in Table 2, includes 28 security-related and cybersecurity topics.

2013 ACM Cybersecurity Workshop Security-Related Topics (and Classifications) Currently in IT Curriculum		
(1). Access Control (CSec)	(8). Forensics (CySec)	(15). Risk Management (CySec)
(2). Cryptography (CSec, CySec)	(9). Intrusion Detect / Prevention Sys (CySec)	(16). Secure Software Design & Engineering (IAS)
(3). Database Admin (CSec, CySec)	(10). Legal Framework (CySec, IAS)	(17). Security Policy (CSec, IAS)
(4). Database Governance (IAS)	(11). Malware & Botnets (CySec)	(18). Threats/ Attacks/ Defenses (CSec, CySec)
(5). Database Mining (CySec)	(12). Network Security (CSec, CySec)	(19). Wireless Security (CSec, IAS)
(6). Embedded Systems (CSec)	(13). Operating Sys (CSec)	
(7). Ethics - Security & Privacy (IAS)	(14). Operational Issues (CSec, IAS)	
2013 ACM Cybersecurity Workshop Emerging Security-Related Topics (and Classifications) not in IT Curriculum		
(20). Big Data (CySec)	(22). Cyberwarfare (CSec, CySec)	(24). Security Architecture (CSec, CySec, IAS)
(21). Cloud Security (CySec)	(23). Mobile Security (CySec)	
New Faculty Identified Security / Cybersecurity Topics		
(25). Internet of Things	(27). Security Culture	
(26). Personal Security	(28). Security Training	

Table 2. Final List of Topics for Case Study (Adapted from McGettrick, 2013).

3.3 Integrating New Cybersecurity Topics into the IT Curriculum

The IT faculty next determined which of the 28 topics were currently being taught, in what courses, and at what depth of knowledge. Faculty agreed where to add the new or missing topics into specific courses at specific levels of instructional depth. The result of this analysis is shown in Table 3, the *IT Security-related and Cybersecurity Curriculum Taxonomy.* The integration of security-related topics and emerging cybersecurity topics impacted eleven core courses: *Introduction to IT, Introduction to Hardware, Introduction to Networking, Advanced Networking, Database, Management* *of IT, HCI, Programming I, Programming 2, Project Management,* and *Security*; and two technical elective courses: *Advanced Database* and *Telecommunications*. The faculty then mapped each topic within each course against the "Level and Depth of Learning" from Bloom's - Webb's six categories ranging from the lower level remembering, understanding, applying, to the higher level analyzing, evaluating, and creating.

The final part of the project was to implement the revisions to the curriculum using the *IT Security-related and Cybersecurity Curriculum Taxonomy.* The following discussions and conclusions section describes faculty observations about the curriculum impacts from the changes, challenges faced by the faculty to implement the changes, as well as impacts on student learning.

<table>
<tr><th>Bloom's-Webb's Taxonomy/
Security Related Topics</th><th>1. Remembering</th><th>2. Understanding</th><th>3. Applying</th><th>4. Analyzing</th><th>5. Evaluating</th><th>6. Creating</th></tr>
<tr><td>Access Control (CSec)</td><td colspan="2">Intro to IT</td><td colspan="3">Security</td><td></td></tr>
<tr><td></td><td colspan="2">Intro to Hardware</td><td colspan="3">Advanced Networking</td><td></td></tr>
<tr><td></td><td colspan="2">Intro to Networking</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="3">Database</td><td colspan="2">Advanced Database (Elective)</td><td></td></tr>
<tr><td></td><td colspan="2">Management of IT</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="3">HCI</td><td></td><td></td><td></td></tr>
<tr><td>Big Data (CySec)</td><td colspan="2">Database</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Cloud Security <b>(NEW)</b></td><td colspan="2">Intro to Hardware</td><td colspan="2">Telecommunications (Elective)</td><td></td><td></td></tr>
<tr><td></td><td colspan="2">Intro to Networking</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="2">HCI</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="2">Management of IT</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="4">Advanced Networking</td><td></td><td></td></tr>
<tr><td>Cryptography (CSec,CySec)</td><td colspan="2">Intro to IT</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="3">Intro to Networking</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="2">Programming 1</td><td colspan="4">Programming 2</td></tr>
<tr><td></td><td></td><td></td><td colspan="4">Advanced Database (Elective)</td></tr>
<tr><td></td><td colspan="6">Security</td></tr>
<tr><td>Cyberwarfare <b>(NEW)</b></td><td colspan="2">Intro to IT</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Database Admin (CSec, CySec)</td><td colspan="2">Intro to IT</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="3">Database</td><td></td><td></td><td></td></tr>
<tr><td>Database Governance <b>(NEW)</b></td><td colspan="2">Database</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Database Mining (CySec)</td><td colspan="2">Database</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Embedded Systems (CSec)</td><td colspan="2">Advanced Networking</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Ethics - Security & Privacy (IAS)</td><td colspan="2">Intro to IT</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="3">Management of IT</td><td colspan="3">Project Management</td></tr>
<tr><td>Forensics (CySec)</td><td colspan="3">Security</td><td></td><td></td><td></td></tr>
<tr><td>Internet of Things <b>(NEW)</b></td><td colspan="3">HCI</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="2">Security</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Intrusion Detect / Prevention Sys (CySec)</td><td colspan="2">Intro to Networking</td><td colspan="2">Telecommunications (Elective)</td><td></td><td></td></tr>
<tr><td></td><td colspan="5">Advanced Networking</td><td></td></tr>
<tr><td>Legal Framework (CySec, IAS)</td><td colspan="2">Intro to IT</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="5">Management of IT</td><td></td></tr>
<tr><td></td><td colspan="3">Security</td><td></td><td></td><td></td></tr>
<tr><td>Malware (CSec, CySec)</td><td colspan="2">Intro to IT</td><td colspan="2">Telecommunications (Elective)</td><td></td><td></td></tr>
<tr><td></td><td colspan="2">Intro to Hardware</td><td></td><td colspan="2">Advanced Networking</td><td></td></tr>
<tr><td></td><td colspan="2">Intro to Networking</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Mobile Security (CySec) <b>(NEW)</b></td><td colspan="2">Intro to IT</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="5">Advanced Networking</td><td></td></tr>
<tr><td></td><td colspan="3">Telecommunications (Elective)</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="5">Security</td><td></td></tr>
</table>

Table 3. IT Security-related and Cybersecurity Curriculum Taxonomy

<table>
<tr><th>Bloom's-Webb's Taxonomy/ Security Related Topics</th><th>1. Remembering</th><th>2. Understanding</th><th>3. Applying</th><th>4. Analyzing</th><th>5. Evaluating</th><th>6. Creating</th></tr>
<tr><td rowspan="3">Network Security (CSec, CySec)</td><td colspan="2">Intro to IT</td><td colspan="2">Telecommunications (Elective)</td><td></td><td></td></tr>
<tr><td colspan="2">Intro to Networking</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="4">Advanced Networking</td><td></td><td></td></tr>
<tr><td rowspan="2">Operating Sys (CSec)</td><td colspan="3">Intro to Hardware</td><td></td><td></td><td></td></tr>
<tr><td colspan="6">Advanced Networking</td></tr>
<tr><td rowspan="3">Operational Issues (CSec, IAS)</td><td colspan="6">Management of IT</td></tr>
<tr><td colspan="3">Advanced Networking</td><td colspan="3">Project Management</td></tr>
<tr><td colspan="4">Security</td><td></td><td></td></tr>
<tr><td rowspan="2">Personal Security <b>(NEW)</b></td><td colspan="2">Intro to IT</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">Intro to Networking</td><td>security</td><td></td><td></td></tr>
<tr><td rowspan="2">Risk Management (CySec)</td><td colspan="3">Management of IT</td><td colspan="3">Project Management</td></tr>
<tr><td colspan="6">Security</td></tr>
<tr><td rowspan="2">Secure Software Design & Engineering (CSec, CYSec, IAA)</td><td colspan="3">Programming 1</td><td></td><td></td><td></td></tr>
<tr><td colspan="6">Programming 2</td></tr>
<tr><td>Security Aritecture <b>(NEW)</b></td><td colspan="3">Security</td><td></td><td></td><td></td></tr>
<tr><td rowspan="3">Security Culture <b>(NEW)</b></td><td colspan="2">Database</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">Management of IT</td><td></td><td></td><td></td></tr>
<tr><td colspan="3">Security</td><td></td><td></td><td></td></tr>
<tr><td rowspan="4">Security Policy(CSec, IAS)</td><td colspan="2">Database</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="2">HCI</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="4">Management of IT</td><td></td><td></td></tr>
<tr><td colspan="5">Security</td><td></td></tr>
<tr><td rowspan="2">Security Training <b>(NEW)</b></td><td colspan="3">HCI</td><td></td><td></td><td></td></tr>
<tr><td colspan="3">Security</td><td></td><td></td><td></td></tr>
<tr><td rowspan="5">Threats/ Attacks/ Defenses (CSec, CySec)</td><td colspan="2">Intro to IT</td><td colspan="2">Security</td><td></td><td></td></tr>
<tr><td colspan="2">Intro to Networking</td><td colspan="3">Advanced Networking</td><td></td></tr>
<tr><td colspan="3">Database</td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td colspan="4">Advanced Database (Elective)</td></tr>
<tr><td colspan="3">Programming 1</td><td colspan="3">Programming 2</td></tr>
<tr><td rowspan="3">Wireless Security (CSec, IAS)</td><td colspan="2">Intro to IT</td><td colspan="2">Telecommunications (Elective)</td><td></td><td></td></tr>
<tr><td colspan="2">Intro to Networking</td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="6">Advanced Networking</td></tr>
</table>

Table 3 Continued. IT Security-related and Cybersecurity Curriculum Taxonomy

4. DISCUSSION

When recommending changes to the curriculum, affecting multiple courses, faculty members need to first understand the reason for the changes and then agree to implement the changes within their courses. In the early part of this project, we collected and then reviewed with our faculty the final list of 28 security-related and cybersecurity target topics (Table 2). During the analysis of our existing curriculum, we identified security-related gaps in our various courses, but we also found considerable duplication of topics. For example, *"malware"* and *"wireless security"* were discussed in detail in multiple courses at the same level of student learning. Sometimes, teaching specific topics within a curriculum changes over time, especially with instructor or text book changes. Reducing this duplication also made room in the curriculum to add the emerging cybersecurity topics.

4.1 Benefits of the IT Security-related and Cybersecurity Curriculum Taxonomy

The IT faculty realized that the *IT Security-related and Cybersecurity Curriculum Taxonomy* could be very useful when integrating any new topic into the IT curriculum, not just security-related and cybersecurity topics. The *Curriculum Taxonomy* helps faculty to determine the expected level of student learning and depth of student thinking across relevant courses within the curriculum. We also found from our faculty analysis that *"cryptography"* is taught in six different courses. Students are introduced within the *Introduction to Information Technology* course to the concept of *"cryptography,"* including understanding the terms 'encryption' and 'decryption,' and how these processes are used to send secure messages and protect data. Within the *Introduction to Networking* course, students review the basic terms again and then learn more advanced topics, such as the ‘public key infrastructure,’ ‘symmetric keys,’ and ‘asymmetric keys.’ They also learn under which circumstances various technologies are applied. In the two programming courses, students learn about ‘securing accounts’ and ‘passwords’ using ‘hashing functions’ and ‘salting’ while completing a class project using the techniques. The *Security* course is offered in the student’s senior year where basic terms are revisited once more. For example, ‘encryption’ is discussed in more detail and from a broader view. Other topics are also discussed in more detail, such as the in-depth understanding of ‘digital signatures,’ ‘digital certificates,’ ‘certificate authorities,’ etc.. Hands-on exercises are assigned utilizing a commercial product.

Based on the faculty analysis, nine of the 28 topics are taught covering all six levels of the learning taxonomy. On the other hand, eleven of the topics are only covered in the lower / intermediate level courses. Although the higher level courses such as *Project Management* and *Securit*y usually cover material where student learning outcomes are mapped to Bloom’s analyzing, evaluating, and creating categories, some security-related topics are only introduced and not covered in depth in the advanced courses. For example, *“embedded systems”* is included in *Advanced Networking*, but covered only at an introductory level, where students are expected to only be able to remember and understand the key concepts. Another example is *“legal frameworks”* introduced in the *Security* course, but not covered in depth.

Without using the new *Curriculum Taxonomy*, the networking and security faculty would have struggled to add to the existing *Security* course the five cybersecurity topics not included in the *ACM IT2008 Curriculum Model* plus the four new faculty-identified security-related topics. To make room in the curriculum, lower-level courses were modified using the *Curriculum Taxonomy* to include security-related and cybersecurity topics in any and all courses where appropriate. For example, the new *“cloud security”* topic was initially taught in the *Security* course, but was moved to the *Advanced Networking* and the *Telecommunications* courses, freeing-up space in the *Security* course. *“Intrusion detection and prevention systems”* topic was also moved from the *Security* course to the *Advanced Networking* course.

Interestingly, the new *“personal security”* topic covers student learnings from level one to level six in the Curriculum Taxonomy. The IT faculty believes all graduating students should have the knowledge to secure their own personal environments. The *Introduction to Networking* course goes a little further and teaches how to secure mobile data, such as Wi-Fi security and VPN security. The *Security* course goes further by utilizing hands-on projects to teach students concepts such as encrypting data on personal cloud storage, creating digital signatures, and using hashing function checksum software to verify file transfers. The strategy to integrate more security content into existing courses created room in the senior-level *Security* course for many of the additional security-related topics. However, not all of the new topics were added to the *Security* course. For example, *“database governance”* security issues were added to the *Database* course. It was only coincidence that many of the new topics fit better in the *Security* course than in other courses.

4.2 Challenges Implementing New Topics into an Existing Curriculum

Naturally, faculty members were concerned with adding more content to their existing courses. We identified several ways to free-up space within existing courses. The faculty agreed that introductory material for each of the introductory and intermediates courses would be taught in the *Introduction to IT* course, allowing these topics to be reviewed in the first course of networking, database, programming, etc. Some faculty members were not covering any security topics in their courses and assumed these topics were covered in the *Security* course. Secondly, the faculty made decisions where duplications could be reduced, again freeing up some space.

Our university recently introduced hybrid or “flipped” courses. Within the “flipped” course model, rather than covering specific topics in class with lectures, faculty create videos and other learning material, which students study and review outside of the class time. This frees up class time for more in-depth discussion on newer, emerging topics. Because flipped courses are encouraged at our university, it made acceptance from faculty easier.

In addition to the above difficulties, adhering to ABET’s continuous improvement guidelines also proved to be challenging. All ABET-accredited programs have a set of learning outcomes that are assessed and evaluated on a rotating basis as a part of continuous improvement. In our case, each student learning outcome is formally assessed and evaluated during one semester every two years using specific measurements for assessing that outcome. When topics are moved from one course to other courses, student learning outcomes must also be moved. If these student learning outcomes are also ABET’s continuous improvement or university assessment items, then those topics become the responsibility of the new faculty members teaching that content. This did happen during our case study. Several ABET continuous improvement learning outcomes were moved from the *Security* course to other courses. The faculty members teaching those courses needed to become familiar with those learning outcomes to ensure they would be evaluated properly for ABET. Our ABET student learning outcome guidelines also had to be modified to reflect the changes. In addition, the faculty for each course adding new topics had to update his or her syllabus to reflect the new content. After overcoming the challenges described above, our undergraduate IT program was able to increase its emphasis on cybersecurity providing our IT graduates an introductory foundation of cybersecurity knowledge and skills.

The cybersecurity foundation described in this case study benefits all IT graduates regardless of the specific IT area in which they choose to work. For those graduates choosing a career in cybersecurity, the new security strategy provides a solid foundation for an entry level position as well as prepares the graduate to further pursue a Master’s degree and\or certification programs in cybersecurity. For those choosing other areas, such as database or networking, the revised IT program provides those students with a basic security foundation for their entry level positions.

Appendix A, *Mapping Security-related / Cybersecurity Topics by IT Course Concepts*, gives more detail about specific concepts taught in each course with examples of student activities to support the expected student learning outcomes. Each of the 28 security-related / cybersecurity topics are mapped to the appropriate course level, the levels of the student learning taxonomy the instruction covers, and example concepts being taught. These examples of the security-related topics taught in each course were provided by each faculty member. These example course concepts are in no way all-inclusive of everything being taught for each topic, but are provided as a reference only, to give the reader a better understanding of the depth of learning across the topics.

5. CONCLUSIONS

Our IT undergraduate curriculum is not designed to teach any one particular subject in great depth, but instead to provide a broad breadth of the knowledge and skills, resulting in a well-rounded entry-level IT professional. As with many undergraduate IT programs, it is expected that students will continuously learn new technologies, receive more training from their employers, and, if interested, seek additional training through master's degrees and/or certifications.

5.1 Research Contributions

Integrating *Bloom's Taxonomy* with Webb's *Depth of Knowledge Model* (Table 1) provided two important contributions for curriculum development. First, faculty may use it as a rubric to decide how to determine desired student learning outcomes and how to assess the learning activities for any course. Secondly, it provided specific examples for analyzing security-related and emerging cybersecurity topics in an ABET-accredited IT curriculum.

The *IT Security-related and Cybersecurity Curriculum Taxonomy* may also be used by faculty at other universities to map their own security-related / cybersecurity topics to their own courses (see Table 3). As in this study, they may find some topics are taught in excess, some too little, and some topics may be missing entirely. Accountability of learning topics included in the curriculum is important for ABET-accredited institutions. Secondly, mapping the topics to the student learning taxonomy can help faculty determine the level of thinking and depth of knowledge being taught for each topic. Based on that outcome, it may be desirable to increase depth where appropriate to better prepare students for the workforce. Thirdly, the topic to course mapping can help faculty determine the best way to add emerging cybersecurity topics to the curriculum without adding additional credits.

5.2 Limitations and Future Research Directions

The primary limitation of this study is that it is a case study from one ABET-accredited undergraduate IT program. Generalizing to other institutions is difficult because not all institutions have identical IT curricula, not all IT curricula are ABET-accredited, and not all IT programs have the need or desire to add emerging cybersecurity topics to their curriculum. However, the tables and taxonomies may be easily reviewed, modified, and adapted by faculty to review other IT-related Knowledge Areas topics and content. The taxonomy can also be used by non-ABET institutions and other disciplines.

We plan to extend the work completed in this case study on cybersecurity to use the integrated *Bloom's Taxonomy* and Webb's *Depth of Knowledge Model* (Table 1) to analyze learning outcomes in each IT course. Then we plan to map specific topics to specific courses within out IT curriculum. Mapping other areas of IT can be used to increase our students' level of thinking and depth of knowledge.

6. REFERENCES

Andel, T. & McDonald, J. (2013). A Systems Approach to Cyber Assurance Education. *Proceedings of InfoSecCD'13: Information Security Curriculum Development Conference*.

Anderson, L. & Krathwohl, D. (Eds.) (2001). *A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives.* Boston: Allyn & Bacon, Pearson Education Group.

Bicak, A., Liu, X., & Murphy, D. (2015). Cybersecurity Curriculum Development: Introducing Specialties in a Graduate Program. *Information Systems Education Journal*, *13*(3), 99.

Bloom, B. & Krathwohl, D. (1956). *Taxonomy of Educational Objectives: The Classification of Educational Goals. Handbook I: Cognitive Domain*. New York: Longmans, Green.

Caldwell, T. (2012). Training – The Weakest Link. *Computer Fraud & Security,* 2012(9), 8-14.

Chen, H., Maynard, S., & Ahmad, A. (2013). A Comparison of Information Security Curricula in China and the USA. *Proceedings of the 11th Australian Information Security Management Conference*, Perth, Australia.

Cisco (2014). Cisco 2014 Annual Security Report. Retrieved October 21, 2015, from http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

Conklin, W., Cline, Jr., R., & Roosa, T. (2014). Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors. *Proceedings of 47th Hawaii International Conference on System Science*.

Cooper, S., Nickell, C., Perez, L., Oldfield, B., Berynielsson, J., Gokce, A., Hawthorne, E., Klee, K., Lawrence, A., & Wetzel, S. (2010). Towards Information Assurance (IA) Curricular Guidelines. *Proceedings of the 2010 ITiCSE Working Group Reports*, Atlanta, GA.

Dark, M., Ekstrom, J., & Lunt, B. (2006). Integration of Information Assurance and Security into Education: A Look at the Model Curriculum and Emerging Practice. *Journal of Information Technology Education,* 5(5), 389-403.

Ekstrom, J., Gorka, S., Kamali, R., Lawson, E., Lunt, B., Miller, J., & Reichgelt, H. (2006). The Information Technology Model Curriculum. *Journal of Information Technology Education,* 5(5), 343-361.

Futcher, L., Schroder, C., & von Solms, R. (2010). Information Security Education in South Africa. *Information Management and Computer Security,* 18(5), 366-74.

Greenlaw, R., Phillips, A., & Parrish, A. (2014). Is it Time for ABET Cybersecurity Criteria?. *ACM Inroads*, 5(3), 44-48.

Illinois Institute of Technology (2015). *Graduate Program in Cyber Forensics and Security*. Retrieved September 13, 2015, from http://www.appliedtech.iit.edu.

Janicki, T., Cummings, J., & Kline, D. (2013). Information Technology Job Skill Needs and Implications for Information Technology Course Content. *Proceedings of the Information Systems Educators Conference*, San Antonio, TX.

Keane, L. & Patten, K. (2010). Information Technology Education: Experiential Learning Benefits. *Communications of Global Information Technology,* 2, 89-100.

Keane, L., Patten, K., Brookshire, R., Cardon, P., Gerdes, J., & Norris, D. (2009). Toward Developing an Experiential Learning Curriculum Model in Information Technology. *Proceedings of the Fifteenth Americas Conference on Information Systems*, San Francisco CA.

Krathwohl, D. (2002). A Revision of Bloom's Taxonomy: An Overview. *Theory into Practice,* 41(4), 212-218.

Lunt, B., Ekstrom, J., Gorka, S., Hislop, G., Kamali, R., Lawson, E., LeBlanc, R., Miller, J., & Reichgelt, H. (2008). *Information Technology 2008: Curriculum Guidelines for Undergraduate Degree Programs in Information Technology*. Association for Computing Machinery (ACM) and IEEE Computer Society.

McGettrick, A. (2013). Toward Curricular Guidelines for Cybersecurity. *Report of a Workshop on CyberSecurity Education and Training*. Association for Computing Machinery (ACM).

Overbaugh, R. & Schultz, L. (2015). Bloom's Taxonomy. Retrieved August 27, 2015, from http://ww2.odu.edu/educ/roverbau/Bloom/blooms_taxonomy.htm

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

Perkins, D. (2008). Levels of Thinking in Bloom's Taxonomy and Webb's Depth of Knowledge. Retrieved September 5, 2015, from http://www.paffa.state.pa.us/PAAE/Curriculum%20Files/7.%20DOK%20Compared%20with%20Blooms%20Taxonomy.pdf

Rowe, D., Lunt, B., & Ekstrom, J. (2011). The Role of Cyber-security in Information Technology Education. *Proceedings of the 2011 Conference on Information Technology Education,* 113-122.

Sauls, J. & Gudigantala, N. (2014). Preparing Information Systems (IS) Graduates to Meet the Challenges of Global IT Security: Some Suggestions. *Journal of Information Systems Education,* 24(1), 71-73.

Starr, C., Manaris, B., & Stalvey, R. (2008). Bloom's Taxonomy Revisited: Specifying Assessable Learning Objectives in Computer Science. *Proceedings of SIGCSE 08,* Portland, OR.

Stockman, M. (2013). Infusing Social Science into Cybersecurity Education. *Proceedings of SIGITE/RIIT'13,* Orlando, FL.

Surendra, N. & Denton, J. (2009). Designing the IS Curricula for Practical Relevance: Applying Baseball's "Moneyball" Theory. *Journal of Information Systems Education,* 20(1), 77-86.

Thomason, S. (2013). People - The Weak Link in Security. *The Global Journal of Computer Science & Technology*, 13(11), 6-12.

Webb, N. (1997). *Research Monograph no. 6: Criteria for Alignment of Expectations and Assessments in Mathematics and Science Education.* Washington, DC: Council of Chief State School Officers.

Wood, K., Kohun, F., Ali, A., Paullet, K., & Davis, G. (2010). Cyber Forensics and Security as an ABET-CAC Accreditable Program. *Information Systems Education Journal,* 8(60).

AUTHOR BIOGRAPHIES

Mark A. Harris is an assistant professor in the Integrated Information Technology Department at the University of South Carolina, Columbia, SC. He has a Ph.D. in Information Systems from Virginia Commonwealth University, a MS in E-commerce and a BS in Information Technology from Old Dominion University. His research interests include security policy management, awareness training, human factors of security, health IT security, and mobile device security. He has authored multiple papers in well-respected refereed information systems journals and conferences. Before academia, Mark was a senior network engineer for a large university, where he oversaw an extensive computer network.

Karen P. Patten is an assistant professor in the Integrated Information Technology Department at the University of South Carolina, Columbia, SC. She earned her Ph.D. from the New Jersey Institute of Technology and her M.S. in Civil Engineering from the University of Minnesota. She teaches IT project management, hospitality and tourism IT, and telecommunications and networking. Her research interests include agile and flexible IT management, small business mobile telecommunications management, and IT curriculum development. She is the author of *Data Networking Made Easy* and co-author of Information Technology for Small Business. She has published articles in *Communications of the Association for Computing Machinery, Communications of the Association for Information Systems, Cutter IT Journal, and the International Journal of Computers, Systems and Signals.* Prior to her academic career, Dr. Patten was a Senior Manager for Emerging Technologies at AT&T Bell Laboratories.

Appendix A: Mapping Security-related / Cybersecurity Topics by IT Course Concepts

Security-related / Cybersecurity Topics (Bloom's Levels of Learning)	IT COURSES (Order in Curriculum) / Examples of Specific Concepts Being Taught
1. Intro to IT	
Access Control (1-2)	Define and conceptualize basic terms (e.g., restricting access to sensitive data).
Cryptography (1-2)	Define and conceptualize basic terms (e.g., sending secure messages, protecting data).
Cyberwarfare (1-2) **(NEW)**	Define and conceptualize basic terms with examples (e.g., top nations involved, potential risks).
Database Admin (1-2)	Define and conceptualize basic terms (e.g., limiting access to data).
Ethics – Security & Privacy (1-2)	Define and describe ethics in relations to security and privacy. Conceptualize basic terms (e.g., ethical behavior while working with corporate users and data, ethical hacking).
Legal Framework (1-2)	Define and conceptualize basic terms (e.g., hacking, acceptable use).
Malware & Botnets (1-2)	Define and conceptualize basic terms (e.g., mobile device and PC malware, loss of data or privacy).
Mobile Security (1-2) **(NEW)**	Define and conceptualize basic terms (e.g. malware, privacy concerns).
Network Security (1-2)	Define and conceptualize basic terms with examples (e.g., confidentiality, integrity, and availability of information, firewalls).
Personal Security (1-2) **(NEW)**	Define and conceptualize basic terms with examples (e.g., mobile security, cloud security, passwords, multifactor authentication).
Threats/Attacks/Defenses (1-2)	Define and conceptualize basic terms with examples (e.g., malware, human threats, DDOS attacks, social engineering, firewalls, and antivirus).
Wireless Security (1-2)	Define and conceptualize basic terms with examples (e.g., WPA2, VPN).
2. Intro to Hardware	
Access Control (1-2)	Discuss physical security for servers, client PCs, and components.
Cloud Security (1-2) **(NEW)**	Discuss infrastructure as a service (IaaS) and basic security considerations.
Malware & Botnets (1-2)	Discuss the impact of malware on misconfigured equipment.
Operating Systems (1-3)	Install and configure Linux and Windows PCs. Discuss basic security hardening (e.g., patches, antivirus, admin, root, guest accounts).
3. Intro to Networking	
Access Control (1-2)	Define and explain differences between authentication and authorization.
Cloud Security (1-2) **(NEW)**	Define and conceptualize basic terms (e.g., private and public clouds, private and public data).
Cryptography (1-3)	Discuss cryptography in more detail (e.g., public key, private key, PKI, certificate authority) and understand when to apply.
Intrusion Detection/Prevention Sys (1-2)	Define and conceptualize basic terms (e.g., intrusion detection system, intrusion prevention system).
Malware & Botnets (1-2)	Define and conceptualize basic terms (e.g., malware, worms, viruses, Trojan horses, rootkits).

Network Security (1-2)	Define and conceptualize basic terms (e.g., Firewalls, demilitarized zones, IDS, IPS, subnets).
Personal Security (1-3) **(NEW)**	Define and conceptualize basic terms (WPA2 at home, personal VPNs, encrypting personal data).
Threats/Attacks/Defenses (1-2)	Define and conceptualize basic terms (e.g., malware, denial of service, firewalls, IDS, IPS, subnets).
Wireless Security (1-2)	Define and conceptualize basic terms (e.g., WEP, WPA, WPA2, RADIUS server, VPN).
4. Database	
Access Controls (1-3)	Demonstrate how to authorize access at the object level (roles, privileges, and permissions).
Big Data (1-2) **(NEW)**	Define and discuss big data, the benefits of big data, and the problems with big data. What tools are used to analyze big data?
Database Admin (1-3)	Demonstrate ability to draw tables with users, constraints, foreign and primary keys, and check constraints to enforce business and logic rules.
Database Governance (1-2) **(NEW)**	Apply business rules to databases. The database management system contains features that can enforce a particular security framework.
Database Mining (1-2)	Define and discuss data mining and what commercial tools are used to mine data.
Security Culture (1-2) **(NEW)**	Discuss how roles and responsibilities fit into the corporate security culture.
Security Policy (1-2)	Discuss how security policy drives roles, privileges, and permissions.
Threats/Attacks/Defenses (1-3)	Discuss passwords, authorizations, and permissions.
5. Management of IT	
Access Controls (1-2)	Define and conceptualize basic terms (e.g., authentication mechanisms).
Cloud Security (1-2) **(NEW)**	Cover a cloud security model at a data governance level.
Ethics - Security & Privacy (1-3)	Case studies on applying security privacy and ethics to a business situation.
Legal Framework (1-5)	Explain the following concepts: Regulatory compliance using COBIT policy and governance (Sarbanes Oxley, HIPPA, FISMA, FIPS, and others). Use a framework to evaluate a case study.
Operational Issues (1-6)	Explain the following concepts: Cost/benefit analysis, return on investment (ROI), total cost of ownership (TCO), auditing processes, asset decision making, procurement, managing and accounting for IT assets. Create ROI and TCO models.
Risk Management (1-3)	Explain security risk assessment and disaster recovery plans.
Security Culture (1-3) **(NEW)**	Discuss IT culture with a subset of security culture.
Security Policy (1-4)	Design policies to protect assets based on a risk assessment and legal framework. Intel IT Manager Duel game.
6. HCI	
Access Control (1-3)	Explain basic terms. Identify and explain biometric access control in interface design (ABET).
Cloud Security (1-2) **(NEW)**	Explain security and privacy issues with cloud interactions with apps.
Internet of Things (1-3) **(NEW)**	Design Internet of Things (IoT) interfaces. Demonstrate how to link IoT devices to social media.
Security Policy (1-2)	Design apps to match organizational security policies.
Security Training (1-3) **(NEW)**	Design interfaces that makes training easier and effective.

7. Programming 1	
Cryptography (1-2)	Discuss encrypting user account passwords.
Secure Software Design & Engineering (1-3)	Introduce a secure software design methodology.
Threats/Attacks/Defenses (1-3)	Discuss threats and attacks (e.g., SQL injection) and how a secure software design methodology can help.
8. Advanced Networking	
Access Control (3-5)	Evaluate a Windows client/server network using Dynamic Access Control.
Cloud Security (1-4) **(NEW)**	Explain how to protect virtual machines, virtual networks, and virtual storage. Demonstrate how to locate data, share cloud resources with others, conduct data backups, and determine availability.
Embedded Systems (1-2)	Define embedded systems with examples (e.g., digital watches, hybrid cars, factory controllers) and why securing them is important.
Intrusion Detection/Prevention Sys (1-5)	Define and explain in detail how and when to use. (e.g., IDS, IPS, host-based IDS, network-based IDS, anomaly detection, signature detection, SIEM).
Malware & Botnets (4-5)	Analyze, evaluate, and mitigate malware threats using appropriate enterprise malware software.
Mobile Security (1-5) **(NEW)**	Introduce and evaluate a Mobile Device Management (MDM) solution.
Network Security (1-4)	Secure network design, VLANS, access control lists (ACL), network hardening, SNMP, ICMP, logging.
Operating Sys (1-6)	Evaluate best OS for the situation. Install, configure, and secure (harden) server and client operating systems.
Operational Issues (1-3)	Understand and explain Auditing, asset management, standards, and enforcement when managing networks.
Threats/Attacks/Defenses (3-5)	Apply appropriate IDS/IPS, MDM, network, wireless, and cloud security to mitigate threats and attacks.
Wireless Security (1-6)	Configure a Remote Authentication Dial In User Service (RADIUS) server. Discuss cloud-based RADIUS service.
9. Programming 2	
Cryptography (3-6)	Encrypt user account passwords using hashing functions and salt.
Secure Software Design & Engineering (1-6)	Follow a secure software design methodology during a software development project.
Threats/Attacks/Defenses (4-6)	Use commercial product to test for software vulnerabilities. Use output to fix security flaws.
10. Security	
Access Control (3-5)	Apply appropriate physical vs. logical and centralized vs. decentralized access control in various scenarios. Role-based (RBAC), Discretionary (DAC), Mandatory (MAC), and Control Lists (ACL). Select appropriate access control methodology based on risk assessment.
Cryptography (1-6)	Explain basic terms. Apply, analyze, and evaluate concepts such as public key, private key, PKI, digital signatures, digital certificates, certificate authorities, encryption algorithms, SSL, TLS, hashing, salting, and checksums. Hands-on exercises utilizing a commercial product.
Forensics (1-3)	Discuss collection, examination, analysis, and reporting. Forensic backups, hidden data, SAN data, deleted data, encrypted or compressed data.

Internet of Things (1-2) **(NEW)**	Define and discuss Internet of Things (IoT) with examples. Discuss the security implications of IoT.
Legal Framework (1-3)	Explain the following concepts: Sarbanes Oxley, HIPPA, Acceptable use policies, standards of conduct, and access to networks.
Mobile Security (1-5) **(NEW)**	Explain the following concepts: Mobile OS security, jailbreaking, rooting. Analyze and evaluate Enterprise Mobility Management (EMM), Mobile Device Management (MDM), Mobile Application Management (MAM), and Mobile Content Management (MCM) practices.
Operational Issues (1-4)	Evaluate threats and choose from available countermeasures given budget constraints.
Personal Security (1-6) **(NEW)**	Use a commercial product to harden mobile devices and PCs and to encrypt personal data on local and cloud drives. Personal VPNs, multi-factor authentication, password management, social engineering concepts, backup & recovery, digital signatures, checksums, and encrypted email.
Risk Management (1-6)	Create a security risk assessment and disaster recovery plan.
Security Architecture (1-3) **(NEW)**	Discuss with security policy and planning. A layered onion model security architecture. Authorization rules influence firewall and ACL rules.
Security Culture (1-3) **(NEW)**	Discuss the importance of creating a security culture. Top management support, relationship with security policy and security training.
Security Policy (1-5)	Understand how to create a security policy. Contributors, audience, frameworks, regulatory concerns, awareness and education program.
Security Training (1-3) **(NEW)**	Discuss the importance of creating a security awareness and training program. Top management support, relationship with security policy and security culture.
Threats/Attacks/Defenses (3-5)	Evaluate threats and countermeasures based on the risk assessment.
11. Project Management	
Ethics – Security & Privacy (4-6)	Explain and evaluate differences in Habernas’s l discourse ethics, federal and state government regulations on security and privacy, ethics of accuracy and intellectual property disputes within projects, outsourcing issues, cybersecurity concerns within international projects.
Operational Issues (4-6)	Evaluate project vendor management issues concerning the security and privacy of related data and information necessary to meet contractual obligations; internal monitoring and control to limit or mitigate security and privacy issues during project implementation.
Risk Management (4-6)	Identify and analyze project risk and conduct qualitative and quantitative analyses. Create a risk mitigation and response plan as referring to potential technology-related security issues both during the design and during the implementation.
12. Advanced Database (Elective)	
Access Control (4-5)	Use commercial product to analyze data access.
Cryptography (3-6)	Use commercial product to encrypt data.
Threats/Attacks/Defenses (3-6)	Use commercial product to analyze compliance risk and stop data loss in real time.
13. Telecommunications (Elective)	
Cloud Security (3-4) **(NEW)**	Identify and analyze access control for cloud services, insider threats and prevention.
Intrusion Detection/Prevention Sys (3-4)	Identify and analyze VoIP intrusion detection / VoIP denial of service, MPLS intrusion detection in various scenarios.
Malware & Botnets (3-4)	Identify and analyze malware vulnerabilities for cellular networks, mobile malware protections.

Mobile Security (1-3)	Explain mobile security frameworks.
Network Security (3-4)	Explain NIST security guidelines and national telecommunications security issues.
Wireless Security (3-4)	Apply appropriate remote monitoring of Wi-Fi security issues in various scenarios.

aitp Association of Information Technology Professionals

No matter how sophisticated the technology, it still takes people! ™

EDSIG

Serving Information Systems Educators

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 1055-3096