Issues in Information Systems
Volume 17, Issue II, pp. 150-161, 2016

CYBERSECURITY EDUCATION: A HOLISTIC APPROACH TO TEACHING SECURITY

Jason E. James, Robert Morris University, jejst243@mail.rmu.edu.edu
Chris Morsey, Robert Morris University, cmmst47@mail.rmu.edu
Joel Phillips, Robert Morris University, jrpst273@mail.rmu.edu

ABSTRACT

This paper provides a pedagogical analysis of current security courses being taught at Centers of Academic Excellence in Cyber defense education 4-year institutions in the United States and compares that to the ACM IS2010 Model Curriculum and ISC2 Common Body of Knowledge. This study attempts to assess the degree to which security issues are being addressed not only in the model curriculum, but also in the actual curricula being delivered to students compared to the common body of knowledge. In addition, this paper serves as a learning guide for universities for hiring cybersecurity faculty and cybersecurity professionals to teach security and encouraging professional development. It is expected that universities currently offering, or planning on offering, degree programs in cybersecurity, or cybersecurity related degrees could benefit from this pedagogical perspective.

Keywords: Cybersecurity, Security, Higher Education, Professionals, Information Systems, Curriculum

INTRODUCTION

In the last 20 years, computers and networks, particularly the Internet, have become an integral part of everyday life, used for a variety of reasons at home, in the workplace, and at schools. As computer and networks are used for communication and for varieties of online interactions and transactions, cyber security has become the key issue in today's information technology world (Pritchard, 2004).

With the increasing concern for safety and integrity of information against cyber attacks, it has become mandatory that organizations follow strict guidelines and security framework to assure the safety and protection of data and systems (Aviel, 1997; Channel Minds, 2004; Eloff & Eloff, 2005). In order to address these needs, many universities have incorporated information security courses at the undergraduate and graduate levels as part of information systems or computer science majors. The goals of such programs and courses are to reduce vulnerability in National Information Infrastructure by promoting higher education in cybersecurity, and to produce a growing number of professionals with information systems security expertise (Arsenault & White, 1991;Aviel, 1997;Bishop, 1993);Bishop, 2000a; Bishop, 2000b; The NIST Handbook, 2005).

LITERATURE REVIEW

The growth and availability of the Internet has created serious vulnerabilities. In response to this, the Federal Government has created several programs. Significant among those is the National Security Telecommunications and Information Systems Security Policy and the implementing directives that specify training standards for various professional positions related to telecommunications and information systems security. The recommendations from the 1991 National Research Council systems security study include the observation that, computer system security and trustworthiness must become higher priorities for educators (Sharma & Sefchek, 2007). Dr. Richard Spillman (1992), Professor of Computer Science and Computer Engineering at Pacific Lutheran University in Tacoma, WA, noted several reasons that sensitivity to security issues was low and stated that, ''one source of this problem is the

woeful lack of computer security education in computer science departments''. Dr. Matt Bishop (1996), Professor at Department of Computer Science at the University of California at Davis and author of two computer security books, noted that very few computer science students are required to develop robust, thoroughly tested code and that until this problem is addressed, 'security problems will continue to plague computer systems''.

The Clinton administration, through executive order 13010, established the President's Commission on Critical Infrastructure Protection (Clinton, 1996; Leach, 2003). The commission was tasked to address cyber threats as one of the two primary threats to critical infrastructures (the other being physical threats). One of the critical requirements identified by the commission was the need for more information security education. To address these needs, many universities incorporated computer and information security courses into their undergraduate and graduate level curriculum (Bishop, 1993; Bishop, 1999; Bishop, 2000a; Bishop, 2000b). The courses are designed to teach students how to secure an information system from the design stage through the implementation and maintenance stages (Bishop & Heberlein, 1996).

The need for Cybersecurity education was to ensure all efforts to prepare a workforce with the needed knowledge, skills, and abilities for our information systems, especially critical organizational security systems. Cybersecurity education has been growing in importance and activity for the past few several years. In the late 1990's, the National Security Agency (NSA) jointly with the Department of Homeland Security (DHS) developed the National Information Assurance Education and Training Partnership (NIETP) program that includes members from government, academia and industry focused on advancing information assurance education, training and awareness. The NIETP serves in the capacity of national manager for cybersecurity education and training related to national security systems and coordinates this effort with the Committee on National Security Systems (CNSS). The CNSS provides a forum for the discussion of policy issues, sets national policy, and promulgates direction, operational procedures, and guidance for the security of national security systems. CNSS is responsible for the development of principles, policies, guidelines, and standards that concern systems holding or related to national security information. Education and training standards are among the many standards and guidelines that CNSS issues (CNSS Guidelines). CNSSI standards have been deployed to colleges and universities in an effort to also prepare qualified individuals (The NIST handbook, 1995; The NIST handbook, 2005).

The most significant effort to involve colleges and universities has been through the National Centers of Academic Excellence in Information Assurance Education (CAE/IAE) Program, now known as the National Centers of Academic Excellence in Cyber Defense Education (CAE/CDE) The CAE/IAE program was started in 1998 by the National Security Agency (NSA) and is now jointly sponsored by the NSA and the Department of Homeland Security (DHS) in support of the President's National Strategy to Secure Cyberspace (February 2003). The purpose of the program is to recognize colleges and universities for their efforts in information assurance education and also to encourage more colleges and universities to develop courses and programs of study in information assurance (Joseph & Barry, 2005). In order to be eligible to apply for CAE/IAE (CAE/CDE) certification, an institution must first demonstrate that it teaches the content covered in NSTISSI 4011 – The National Training Standard for Information Systems Security Professionals (Leach, 2003).

Teaching information systems security involves a vast variety of areas, including cryptography/cryptanalysis, network protocol vulnerabilities, web application vulnerabilities, firewall/IPsec/VPN/IDS configuration, user access rights administration, Wi-Fi security, Bluetooth security, file system security and so on. Learning how to protect information systems from attacks involves a significant amount of time to be invested into getting familiarized with the relevant tools and/or systems. Unfortunately, academic courses usually span over one to two semesters, thus providing a rather short period of available time for going through all the tools and relevant principles and analyzing them sufficiently (Papanikolaou et al, 2013).

Previous research into the teaching of computer security has revealed various recommendations to include more information security topics (Prichard &MacDonald, (2004); Vaughn & Boggess, 1999). Some studies have looked at the efficacy of particular programs or courses. Anderson and Schwager (2002) found that many of the areas in the Certified Information Systems Security Professional (CISSP) common body of knowledge were considered relevant to the IS curriculum. They concluded that no required IS curriculums covered all of the CISSP security issues. The authors also found that the majority (70%) of respondents wanted security integrated into other courses, although

32% felt that if a security course were available, it should be required. However, they were unable to determine the extent to which these topics are actually being taught (Anderson & Schwager, 2002). Because of the evolving nature of the field, IS faculties often include topics from sources outside of textbooks. Rather than relying on measures of coverage within textbooks, the Foltz & Renwick (2011) study gathered data directly from faculty teaching IS courses.

Foltz & Renwick's (2011) study revealed some significant findings. First, there was an overwhelming consensus that information security needs to be addressed. Second, present curricula are not meeting security needs, especially in the required courses where a majority of the IS faculty agreed security issue coverage should be increased in required IS courses. Lastly, most respondents suggested a need for increased security coverage during the next five years in required, elective and non-IS courses. There is less consensus, however, as to what should actually be included in IS security coverage.

Unfortunately, their study found that present curricula leave little time for additional topics. This lack of time may hinder efforts to add new material to the curriculum. The challenges of information security, however, are an important issue that faculty and students will continue to face. The need for additional instruction in this area cannot be disregarded (Foltz & Renwick, 2011).

They concluded it was perhaps time to look at new teaching methods and approaches to learning to increase both the breadth and depth of our student's educational experience with security in the classroom. Their study extended previous research by providing a glimpse inside IS program classrooms. Whereas previous work looked primarily at external sources such as textbook reviews, catalogs, and external recommendations, Foltz & Renwick (2011) asked faculty directly what was presently being taught, rather than what is covered in textbooks and asked what faculties are including from more up-to-date resources.

In order to fill the void left by the Anderson & Schwager (2002) study as well as add to the findings of the Foltz & Renwick (2011) study, our study involved collecting data about the National Centers of Academic Excellence in Cyber Defense Education 4-Year (CAE/CDE 4Y) regarding security classes being taught and see if any change has taken place over the past 5 years since Foltz & Renwick (2011) performed their study.

As the field of information systems continues to develop, it is important for faculty to remain current in the field and incorporate this knowledge in their teaching. As an evolving field, information systems must continue to examine content and coverage for currency. Furthermore, the inclusion of the various IS security topic (discussed later in the article) areas within the curriculum should continue to be evaluated. Given the limited time available within the existing curricula and the importance of covering IS security, the model curricula needs to be revised to reflect these developments in the field (National Science Foundation, 2014).

The relatively new and rapidly evolving cybersecurity field continues to have significant implications for cybersecurity professionals as well as the role of cybersecurity faculty. First, professional development is imperative. Cybersecurity faculty members need ongoing professional development to ensure they are aware of and teaching the most current and relevant content. Faculty in disciplines where cybersecurity is to be integrated also need professional development that introduces them to the field and partners who can assist curriculum development and content integration. A second important topic with regard to faculty is the utilization of practice-oriented faculty, which includes faculty with practical experience in the field who are able to convey material in the context of the cybersecurity landscape. Faculty expertise and teacher certification is lacking. The main barriers are lack of qualified faculty to staff programs and teach security, professional development opportunities, time, and the unfamiliarity of all the different security topics (National Science Foundation, 2014). However, with more cybersecurity professionals making the move from industry to academia, all of this will hopefully soon change.

RESEARCH QUESTIONS AND METHODOLOGY

This study is part of a larger, ongoing research program, which aims to establish relationships between professional cybersecurity associations and higher education institutions. The goal of this study is to help identify more holistic

approaches to teaching security in higher education institutions. The proposed research method will be a basic qualitative research study and offers a look into how a more holistic approach to teaching that can be established. Our research centered upon the following research questions:

1. Should security courses be taught holistically?

This study used the National Information Assurance Education and Training Programs (NIETP) website (www.nietp.com) to obtain the four-year teaching institutions designated by the NSA and the Department of Homeland Security (DHS) as a National Centers of Academic Excellence in Cyber Defense Education (CAE/CDE). The NIETP website is maintained by the Information Assurance Directorate of the NSA. A two-step process was used to locate four-year teaching institutions designated by NSA and DHS as a CAE/CDE and the security courses being taught. First, institutions designated as CAE/CDE 4Y – National Centers of Academic Excellence in Cyber Defense Education 4-Year ONLY were identified. Finally, the website of the teaching institution was explored to find what security courses are being taught. Specifically, this study looked at bachelors and masters degrees with majors, minors, or concentrations in information systems, information technology, computer science, engineering, information security or assurance, and cybersecurity.

A content analysis of the posted information on courses being taught was then conducted. Any courses with "Security" in the title or in the course description were identified and whether it was a required course or elective. Resultant data was compared to the model curriculum in the field. The most recent model curriculum for Information Systems is IS 2010, which is published jointly by the Association for Computing Machinery (ACM) and the Association for Information Systems (AIS). The resultant data was also compared to the Common Body of Knowledge (CBOK) standard developed by the International Information Systems Security Certification Consortium (ISC2).

WORLD OF CYBERSECURITY

The cybersecurity profession is a complex world with many different career paths as seem in Figure 1.

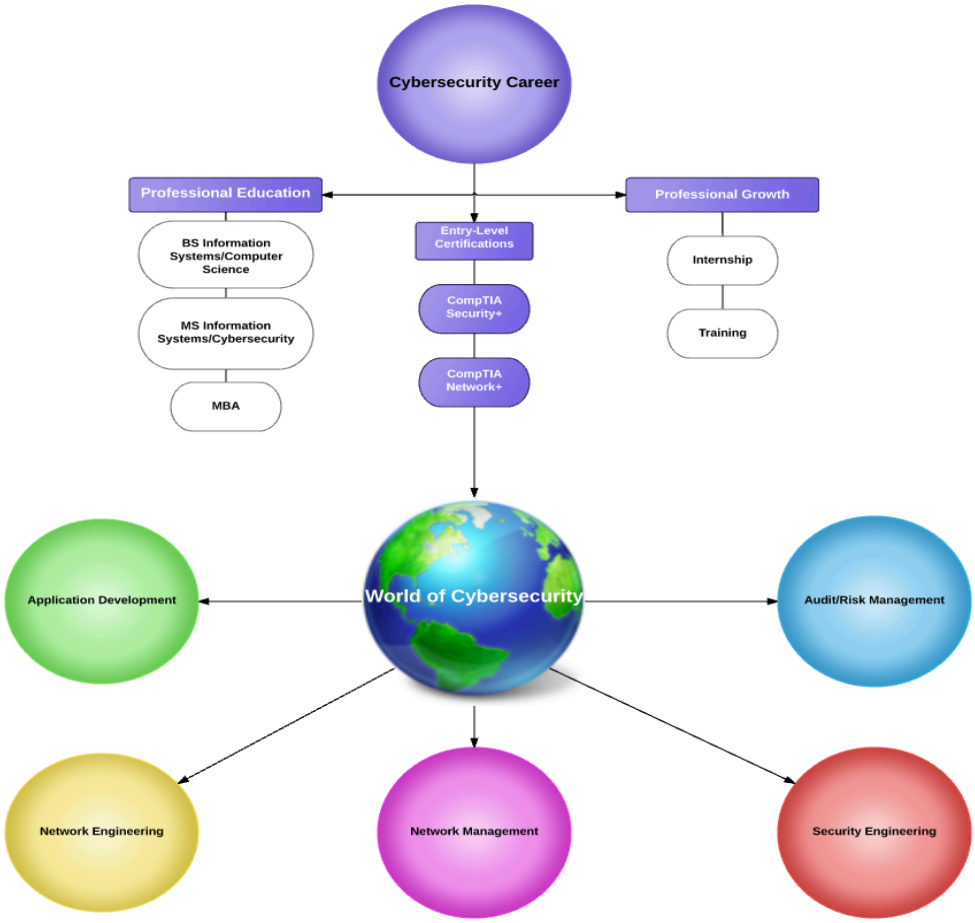

Figure 1. The World of Cybersecurity

The typical cybersecurity student will obtain a Bachelor of Science (BS) in either Information Systems or Computer Science and then obtain their Master of Science (MS) in Information Systems or Cybersecurity. Some students may decide to get an MBA as well. Those typical students also will have an Internship and additional training outside the classroom. Sometimes students want to get ahead and pursue entry-level certifications such as CompTIA Security+ or Network+. After they graduate, the path they choose can be overwhelming and may change over time as many cybersecurity professionals do. Therefore, depending in the path chosen by a cybersecurity student, whether they major in information systems, computer science, or cybersecurity, the courses taught in security may be not be enough or and a deeper dive into information security would be needed as detailed in the next section.

PROFESSIONAL DEVELOPMENT

Although there are many paths cybersecurity professionals can follow, they typically follow a career path with one of 6 specialties as depicted in Figure 1, with each career path broken down into sub-specialties as follows:

Table 1. The World of Cybersecurity Sub-Specialties

Application Development	Network Engineering	Network Management	Security Engineering	Audit/Risk Management
Mobile App Dev. Computer Program	Cloud Network Operating System Storage Virtualization Architecture Data Center	Project Management ITIL	Information Security Forensics Hack/Penetration Test Application Hacking Business Continuity Control System Administrator	Privacy Physical Security Audit Risk PCI Health IT Financial

Many cybersecurity professionals specialize in multiple sub-specialties and many experienced cybersecurity professionals specialize across the six main paths. The sign that a cybersecurity professional is specialized in a certain area is usually denoted by professional certifications. Overall there are approximately 2,000 different cybersecurity certifications across over 150 different vendors (IT Certification, 2016). However, as a cybersecurity professional knows, you cannot just obtain a certification unless you have the proper years of experience and knowledge to pass the exams. Once the amount of years of experience has been met, most vendor-neutral or vendor-specific require a certain amount of training each year to maintain that certification and knowledge.

How do cybersecurity professionals stay up-to-date in the cybersecurity world? They have to participate in facilitated learning opportunities including credentials, academic degrees, formal coursework, conferences, webinars, live training, etc. This is what is known as professional development and is the continuous process of acquiring new knowledge and skills that relate to one's profession, job responsibilities, or work environment. Professional development plays a key role in maintaining trained and informed experts. It is the process of improving and increasing capabilities of one's expertise through access to education and training opportunities in the workplace, through outside organizations, or online opportunities.

Cybersecurity faculties who teach security attend much of the same conferences and training, except a lot of it is related to academia well. The same standards that apply for professional development that cybersecurity professional have to abide by, the same holds true for cybersecurity faculty. Faculties that were employed in the cybersecurity industry bring a much different perspective to teaching cybersecurity than those that do not.

There is no question that information security is an issue. The importance of information security has grown in tandem with the importance of information systems in all aspects of business. The Internet has provided the basis for the implementation of innovative business applications such as e-commerce and electronic data interchange. These major changes to the information technology infrastructure are producing new information security challenges every day (Wellner, 2000). Faculties who were employed in industry and attend professional development conferences and training in cybersecurity are able to keep up to date and can develop or integrate information security into new and better security courses.

MODEL SECURITY CURRICULUM and CBOK

This study attempted to assess the degree to which IS security issues are being addressed not only in the model curriculum and the common body of knowledge, but also in the actual curricula being delivered to students. In trying to evaluate present security curriculum, we looked at the model curriculum in the field. The most recent model curriculum for Information Systems is IS 2010. Published jointly by the Association for Computing Machinery (ACM) and the Association for Information Systems (AIS), it is used for guidance by colleges and universities offering information systems as an undergraduate major.

ACM IS 2010 has seven core courses, which include, Foundations of Information Systems, Data and Information Management, Enterprise Architecture, IS Project Management, IT Infrastructure, Systems Analysis and Design, and IS Strategy, Management and Acquisition. Security is listed as a topic area in all seven-core courses but with very little coverage. In fact, only IT Security and Risk Management, which is an elective, is the only course that goes in

depth in covering security.

As for the CBOK, this is the standard in the industry as defined by the Certified Information Systems Security Professional (CISSP) examination and is an indication of expertise in the area of information systems security and is highly regarded in the computing industry. The CBOK includes security and risk management, asset security, security engineering (including cryptography), communications and network security, identity and access management, security assessment and testing, security operations, and security in the system development life cycle. With the exception of identity and access management, the CBOK title all have security in their title and even though identity and access management may not have security in the title, it is the most pervasive and omnipresent aspect of information security since access controls encompass all operational levels of an organization. No wonder the CBOK has become the standard in the security industry since every aspect of the eight domains is comprised of only IS security topics.

SECURITY IN THE CLASSROOM

Gene Spafford, Director for of the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University, testified before congress in 1997 and argued the significance of security education:

> To ensure safe computing, the security (and other desirable properties) must be designed in from the start. To do that, we need to be sure all of our students understand the many concerns of security, privacy, integrity, and reliability.'' As Spafford testified, ''our students and soon-to-be students will be designing our information technologies of the future. We are endangering them and ourselves because the majority of them will receive no training in information security (Sharma & Sefchek, 2007; Sousa, MacDonald, & Fougere, 2005).

Since 1997, there have been universities in the United States that have introduced numerous types of information security courses under different departments as part of various IT related programs (Bishop, 2000a;Bishop, 2000b). These universities have also incorporated security courses into their undergraduate and graduate level curriculum (Edward, 1993; Higgins, 1989; Highland, 1982). The courses are designed to teach students how to secure an information system from the design stage through the implementation and maintenance stages using various approaches ranging from purely theory based to a good mix of hands-on and theory based (Frinke &Bishop, 2004; Horrocks, 2001).

Currently, there are 127 CAE/IAE 4Y- National Centers of Academic Excellence in Information Assurance Education 4-Year and/or CAE/CDE 4Y – National Centers of Academic Excellence in Cyber Defense Education 4-Year. However, only 61 of those are CAE/CDE 4Y (Table 2).

Table 2. Sixty-One-CAE/CDE 4Y

Jacksonville State University (AL)	Armstrong State University (GA)	Capitol Technology University (MD)	Excelsior College (NY)	The University of Tennessee at Chattanooga
The University of Arizona, Tucson	Idaho State University	Towson University (MD)	Rochester Institute of Technology (NY)	Southern Methodist University (TX)
University of Arkansas at Little Rock	University of Idaho	United States Naval Academy (MD)	Utica College (NY)	Texas A&M Univ.-Corpus Christi
California State Polytechnic University, Pomona	DePaul University (IL)	University of Maryland University College	East Carolina University (NC)	University of Dallas
California State University, San Bernardino	Illinois Institute of Technology	Eastern Michigan University	North Carolina A&T State University	University of Texas at El Paso
National University (CA)	Illinois State University	Walsh College (MI)	The Ohio State University	James Madison University (VA)
San Jose State University (CA)	University of Illinois, Springfield	Metropolitan State University (MN)	East Stroudsburg University (PA)	Marymount University (VA)
Colorado Technical University	Purdue University Calumet	St. Cloud State University (MN)	Indiana University of Pennsylvania	Norfolk State University (VA)
United States Air Force Academy (CO)	Fort Hays State University (KS)	Walden University (MN)	Pennsylvania State University	City University of Seattle
University of Denver	University of Kansas	University of Nebraska, Omaha	West Chester University of Pennsylvania	
Florida International University	Northern Kentucky University	Fairleigh Dickinson University (NJ)	Polytechnic University of Puerto Rico	
Nova Southeastern University (FL)	University of Louisville (KY)	New Jersey City University	Fountainhead College of Technology (TN)	
University of South Florida	University of Maine System	New Jersey Institute of Technology	Tennessee Tech University	

The research identified numerous security classes taught at those 61 institutions, both required and elective. After analyzing the security courses being taught at these 61 CAE/CDE 4Y institutions is that a majority of the security courses are being taught as electives and not a required course. In addition, even if the security courses are required, the courses are introductory courses and do not take a deeper dive that one would expect when teaching security to cybersecurity students. Security remains being taught in pieces rather than a whole class. This is consistent with the ACM Information Systems 2010 Model Curriculum that does not have security as a topic built into core courses. So why is security courses not being built into Model Information Systems curriculum outside of computer science. The authors feel obligated to propose the reasons why.

Teaching information systems security has to cover certain aspects (networking, operating systems, viruses, cryptography, access control, authentication and so on) and follow certain principles, such as with penetration testing and ethical hacking. Moreover, the fast pace at which new developments initiate in the wider area of computers and networks, increases the probability of unforeseen flaws to appear, which can be exploited by malicious adversaries in the form of zero-day attacks. Therefore, a well-trained information systems security expert should not only be able to apply well-established rules and guidelines, but also be rather intuitive in order to protect the system against unforeseen attacks too (Papanikolaou et al, 2013).

The framework for the development of an educational environment on information systems security for the

academic community is not currently being created as a standalone framework just for the information systems community. Information systems security, however, is an important area in Computer Science education, as this is documented by the proposals of organizations such as the ACM and IEEE (Papanikolaou et al, 2013). The development of an educational framework on information security possesses unique qualities compared to other scientific areas. Information security, apart from understanding the basic mechanisms and technologies, you must be able to face security incidents that do not follow specific rules and learn to think and adapt by thinking out-of-the-box (Papanikolaou et al, 2013).

Several frameworks have been developed and proposed for training on information systems security outside of the computer science realm. Most notably NIST , National Security Agency (NSA), and the Department of Homeland Security (DHS), in addition to ISO 27002, which defines the wider framework for conducting training and awareness on information systems security(Papanikolaou et al, 2013). One thing to keep in mind is that the development of information systems security framework to use in the academic community has additional requirements than the previous standards and guidelines contain. They need to integrate with online education and due to time constraints imposed by the duration of the academic teaching periods; the syllabus may have to cover quite a wider range of topics, or even the overall workload that the students have to cope with (Papanikolaou et al, 2013).

DISCUSSION

Information system security courses are not the only courses that pose difficulties to academia to teach but we speculate that information systems security is unique because of the wide range of domains involved as seen in Table 1 (Sousa, MacDonald, & Fougere, 2005).It is not uncommon for an instructor to take 10 or more hours to prepare a two-hour security lecture. This is a function of not only the sheer amount of diverse information but also the dynamic nature of the rapidly moving field. Instructors are even using significant security events that have occurred, such as the Home Depot breach, or even software used by experts for mobile and computer forensics, during their courses. Even though this presents both a positive relevance to students it also is a challenge to the instructor if he or she did not previously cover the topic in their course (in which case the instructor and class learn together) (Irvine, 1997).

Security courses are still not being taught holistically in undergraduate courses. As the research above showed, security is being taught as a topic within a non-security course and not a separate course. Just being taught as a topic within an IS course will only provide nothing more than a high level view. Security should be taught in depth so it would add to the knowledge, skills, and abilities relevant for cybersecurity students entering the workforce. On a positive side, more majors are being offered in cybersecurity and more security courses are being taught at the graduate level. In undergraduate IS, the focus still remains on basic IS requirements while graduate is more focused on specifics of IS such as security.

Security courses should also be taught together between cybersecurity faculty and cybersecurity professionals. Why? Cybersecurity faculties are experts in teaching students in higher education while cybersecurity professionals are experts in security. Together, they can teach students the necessary knowledge about information security so they can better prepare themselves for the workforce. However, as discussed earlier, over the past several years, many cybersecurity professionals have transitioned to the academia world and thus have a great deal of knowledge in both and they are to keep up to date in the latest security trends and they can develop or integrate all types of information security into new and better courses.

Information security is taught in a separate class or, if students are lucky, classes; and these courses are usually electives. Educators spend a lot of time focusing on getting students to cover all the basics. Security is treated in any area as a topic that is added on at the end of the semester and not a lot of time is spent on it in lectures or in labs. The field is so vast and so many different areas to specialize in, students are allowed to focus on the details of a language, building hardware, or learning algorithms. Information security is placed in a silo, instead of incorporating it into every class we teach. Some students specialize in information assurance or information security as part of their majors, and they need specific courses that focus on security topics. But, for the general computer student population, a more holistic approach to teaching security needs to be taken: it needs to be part of every course and

included from the first day (Jacobson & Rursch, 2013).

We believe that we could take a page from our colleagues in the English department, who have over the course of the past 10 years, pushed through a concept of "writing across the curriculum." The point this faculty made was that English 101 and 102, or their equivalents at various universities, had historically been taught as the two basic courses that every freshman endured. And, then the computer engineering, computer science, and software engineering students could forget about writing (Jacobson & Rursch, 2013).

Just as English departments have pushed the concept of "writing across the curriculum", we believe "security across the curriculum" would be a wiser approach for information security education. It would incorporate security as a topic from the beginning of every course, and we would continue to refer to it as we teach students about the basic concepts in each course. This would then carry over to their work as network engineers, programmers, and mobile application developers. When sitting down to work on a new project, we always start at the beginning and lay out the landscape. We should include security as part of the design plan. And, the security of the project should be considered at every revision and stage (Jacobson & Rursch, 2013).

FUTURE RESEARCH

Future empirical research can employ developing an updated model curriculum and how to assess the student's knowledge of security. Additionally, future research can explore faculty knowledge of those with cybersecurity certifications and professional development versus those with none.

CONCLUSIONS

So, let's change the way we traditionally teach students security. We need to teach security as a whole rather than in parts in different cybersecurity classes. Cybersecurity faculty and cybersecurity professionals partnering to teach security holistically can address the need where curriculum is not meeting the security desires, particularly in required courses. There is less consensus, however, as to what should actually be included in IS security coverage.

Whether someone is a cybersecurity faculty or cybersecurity professional, they should be encouraged to treat their job the same way: improving and increasing capabilities of one's expertise through access to education and training opportunities in the workplace, through outside organizations, or through online opportunities and professional credentials.

If we teach students using a holistic approach, it will only follow that they can take this same perspective when they reach the business world. In addition to dedicated cybersecurity programs, majors/minors, certificates, and concentrations, security classes cannot continue to be only electives in the computer science programs, which allows students to enter workforce with little-to-no knowledge or awareness of security issues, thus possibly contributing to security problems. Cybersecurity should be viewed as foundational knowledge, analogous to the manner in which other topics such as programming, operating systems, networking, and computer architectures, etc., are viewed as fundamental topics. In addition, every organized profession (accounting, law, medicine) is governed by its respective professional body and has specialties within the degree that students choose to specialize in

REFERENCES

Anderson, J., Schwager, P. (2002). Security in the information systems curriculum: Identification and status of relevant issues. *Journal of Computer Information Systems*, *42*(3), 16–23.

Arsenault A., White G. (1991). Teaching computer systems security in an undergraduate computer science curriculum. In: Fourteenth national computer security conference, 582–597.

Aviel, R. (1997). An experience teaching a graduate course in cryptography. *Cryptologia*.

Baggett, W., O. (2003). Creating a culture of security. *Internal Auditor*, *60*(3), 37.

Bishop, M. (1993). Teaching computer security. Ninth IFIP international symposium on computer security (IFIP SEC), 43–52.

Bishop, M. (1999). What do we mean by ‘‘computer security education’’? 22nd National information systems security conference, 604.

Bishop, M., Heberlein, L., T. (1996). An isolated network for research. 19th National information systems security conference, Baltimore MD, 349–360.

Bishop, M. (2000a). Academia and education in information security: four years later. Fourth national colloquium on information system security education, Washington, DC, 249–55.

Bishop, M. (2000b). Education in information security. *IEEE Concurrency*, *8*(4), 4–8.

Channel Minds. (2004). Survey shows: organizations need to develop information security culture. *Channel Minds*. Available: http://www.channelminds.com/article.php3?id_article.1582

Clinton, W. (1996). Executive order 13010 – critical infrastructure protection, 1–6.

Edward, G., A. (1993). A graduate course in computing security technology. ACM technical symposium on computer science education (SIGCSE), 251–255.

Eloff, J., H., P., Eloff, M., M. (2005). Information security architecture. *Computer Fraud & Security, 1*(11), 10–16.

Foltz, C., Bryan, Renwick, J. (2011). Information systems security and computer crime in the IS curriculum: A detailed examination, *Journal of Education for Business, 86*(2), 119-125.

Frinke, D., Bishop, M. (2004). Joining the security education community. *IEEE Security & Privacy*, 61–63.

Higgins, J. (1989). Information security as a topic in undergraduate education of computer scientists. 12th National computer security conference, 553–557.

Highland, H. (1982). A college course in cryptography and computer security. *Security and Audit Control Review*, *1*(2), 34–37.

Horrocks, I. (2001). Security training; education for an emerging profession? *Computers & Security*, *20*(3), 219.

Irvine, C. (1997, October). Challenges in computer security education. *IEEE Software*, 110- 111.

Jacobson, D., Rursch, J. (2013, March). Why information security education isn’t making the grade. Techtarget.com. Retrieved March 19, 2016 from http://searchsecurity.techtarget.com/opinion/Why-information-security-education-isnt-making-the-grade

Joseph, J., Barry, M. (2005). Integration of information assurance and security into IT2005. Ninth colloquium for information systems security education, Atlanta, Georgia, 7–14.

Leach, J. (2003). Improving user security behavior. *Computers & Security*, *22*(8), 685.

Marsh, R. (1999). Critical foundations: Protecting America’s infrastructure. *President’s Commission on Critical Infrastructure Protection*.

National Science Foundation Directorates of Computer & Information Science & Engineering (CISE) and Education and Human Resources (EHR) Cybersecurity Education Workshop (2014) accessed March 21, 2016 from https://research.gwu.edu/sites/research.gwu.edu/files/downloads/CEW_FinalReport_040714.pdf

New Updated List of IT Certifications accessed March 21, 2016 from http://itcertificationmaster.com/updated-list-certifications-2304-160-companies/

Papanikolaou, A., Vlachos, V., Venieris, A., Ilioudis, C. (2013). A framework for teaching network security in academic environments. *Information Management & Computer Security, 21(4), 315-338.*

Prichard, J., MacDonald, L. (2004). Cyber terrorism: A study of the extent of coverage in computer security textbooks. *Journal of Information Technology Education*. (3), 279–289.

Sharma, S., Sefchek, J. (2007). Teaching information systems security courses: A hands-on approach. *Computers & Security,* (26), 290-299.

Sousa, K., MacDonald, L., Fougere, K. (2005). Computer security in the introductory business information systems course: An exploratory study of textbook coverage. *Journal of Education for Business*. *81*(1), 15.

Spafford, E. (1997). One view of a critical national need: support for information security education and research, Testimony before the US House of Representatives Committee on Science, Washington, DC, 1–11.

Spafford, E. (1998). Teaching the big picture of InfoSec. Second national colloquium for information system security education. James Madison University, 1–8.

Spillman, R. (1992). A computer security course in the undergraduate computer science curriculum. Collegiate Microcomputer, (10), 91–96.

The NIST handbook. (1995). SP 800-12. An introduction to computer security. *The NIST handbook*.

The NIST handbook. (2005). SP 800-84. Building an information technology security awareness and training program. *The NIST Handbook*.

Vaughn, J., Boggess, J. (1999). Integration of computer security into the software engineering and computer science programs. *The Journal of Systems and Software*, (49), 149–153.

Victor, M., Corey, D., Daniel R., Don W. (2001). A model for information assurance: an integrated approach. *Proceedings of the 2001 IEEE workshop on information assurance and security*. West Point, NY: United States Military Academy.

Wellner, A. (2000). TrustUS.com. *American Demographics, 22(11), 47.*