Is Today's Information Systems Curriculum Preparing the Next Generation of Cyber Warriors?

Mathias R. Plass

Lewis University

Table of Contents

Abstract

News headlines are continuously filled with discussions of cyber-attacks, cyber breaches, and losses of individual's personally identifiable information. Equally important and frequently examined is the ever-widening gap of cybersecurity talent which is desperately needed to combat these growing threats. These headlines are increasing the visibility on colleges and universities and what these institutions are doing to help address the problems and shortages in the cybersecurity workforce. This paper will look at the current state of information systems curriculum and discuss the opportunities and challenges they currently present. This conversation will then lead to an outline of new ways which can allow colleges and universities to restructure the current curriculum into a new cybersecurity information systems program. The new cybersecurity information systems program will then be able to address the growing shortage of talent in the cybersecurity workforce and allow these colleges and universities to prepare students as they move into cybersecurity careers by giving them the necessary tools to make a positive impact within their organization starting on day one.

Keywords: Center of Excellence, curriculum development, cyber education, cybersecurity, information systems

Is Today’s Information Systems Curriculum Preparing

the Generation of Cyber Warriors?

News headlines are consistently filled with reminders of black hat hackers, nation-state cyber-attacks and cyber breaches. Equally discussed is the ever-growing shortage of cybersecurity professionals to combat these elements. While government programs have begun looking at ways to fill the cybersecurity gap the question that needs addressing is what are our colleges and universities doing to address the shortage? Another question is which programs are being used to educate cybersecurity professionals and are the currently used information system programs allowing students to gain the necessary competitive cybersecurity edge?

With so many students attending and graduating from these information systems programs, why are employers having such a difficult time trying to fill cybersecurity roles? What are these information systems programs lacking in preparing these next-generation cyber warriors? Can colleges and universities adequately adjust so they can provide the best-prepared graduates and ensure they are meeting employer requirements upon hire? This paper will take a closer look at how current information systems curriculums are meeting employer needs and what deficiencies are prevalent so these information systems programs can be tailored to allow students to fill the cybersecurity professional shortage.

Today’s Information System Curriculum

Today's current information systems programs have been showing declining enrollment numbers while the cybersecurity job gap continues to widen (Akbulut-Bailey, 2012). The primary reason for this issue is that traditional information systems programs and educational institutions are failing to provide students with the necessary skills required by employers (Hentea, Dhillon & Dhillon, 2006). Traditional information systems programs have numerous shortcomings such as an outdated curriculum and not providing the necessary mix of technical and non-technical skills (Akbulut-Bailey, 2012). There is also the issue of information systems programs utilizing a silo approach which fails to create the technically skilled cyber business professional (Baumgartner, 2014). However, some colleges and universities are creating new models which better reflect current standards and guidelines defined by government and other organizations (Hentea, Dhillon & Dhillon, 2006). Even though these colleges and universities are following these models, they are still missing critical skills necessary for the student to make a successful transition to the business world (Hentea, Dhillon & Dhillon, 2006).

Programs Supporting Cybersecurity Adoption

Several programs were originally started to research cybersecurity initiatives and verify the nation's readiness to defend its citizens from cyber threats. These programs and organizations have exposed where there are deficiencies in our nation's cyber posture. They have also presented places where we can build permanent stopgaps to ensure resiliency to future cyber threats. These programs have also revealed where collaborative efforts can be made between government, business, and academia to ensure that the nation builds a highly educated and dedicated cyber workforce. One program started from a presidential directive and the other from a National Science Foundation (NSF) grant which allowed for a collaborative effort between the public and private sector to ensure that students were better prepare for cybersecurity careers.

NIST and NICE Government Programs

The National Institute of Standards and Technology (NIST), founded in 1901, is part of the United States Department of Commerce (NIST, 2017). NIST is one of the oldest physical science laboratories tasked with the challenge of allowing the nation to gain industrial competitiveness with the rest of the world (NIST 2017). Today NIST continues to be tasked with promoting innovation and competitiveness by using measurements, standards, and technology to enhance the economic security of the nation and improve the quality of life to its citizens (NIST, 2017).

In 2010 President Barack Obama tasked NIST with leading the National Initiative for Cybersecurity Education (NICE) (Paulsen, McDuffie, Newhouse & Toth, 2012). This new initiative was derived from the expanding Comprehensive National Cybersecurity Initiative (CNCI) which was a focus of the federal government to bring cybersecurity initiatives to a national endeavor (Paulsen et al., 2012). CNCI was launched by President George W. Bush as National Security Presidential Directive 54/Homeland Security Presidential Directive 23 in January 2008 (US White House, 2010). The CNCI was established to build a frontline defense against cyber threats, to defend against a full spectrum of threats to the nation's key technologies, and to strengthen future cybersecurity initiatives (US White House, 2010). President Obama was looking for NIST to use this initiative to strengthen the nation's cyber capabilities, one of those around cyber education (US White House, 2010).

NICE is tasked with the long-term cybersecurity posture of the nation through programs surrounding cybersecurity awareness, education, training and workforce development (Paulsen et al., 2012). NICE considers "people" the most important resource to combating cyber threats as it is "people" who are on the front lines designing the technology, combating the threats and protecting others in cyberspace (Paulsen et al., 2012). NICE with its collaboration with other federal agencies, academia, industry and other subject matter experts in cybersecurity created the NICE Cybersecurity Workforce Framework (Paulsen et al., 2012). This framework created an organizational structure of cybersecurity work and workers placing them into specialty areas with an associated list of knowledge, skills, and abilities (KSAs) (Paulsen et al., 2012). This framework also allows for the cybersecurity workforce to use a common language to ensure competencies and responsibilities across the discipline (Paulsen et al., 2012). This framework also allows educators to prepare students for these careers, understand the knowledge and skills needed by students to be successful in those cybersecurity careers and assists educators in ensuring classroom instruction matches those KSAs (Paulsen et al., 2012).

National Cyberwatch Center

The National Cyberwatch Center (Cyberwatch) is a national consortium of colleges, universities, businesses and government agencies all focused on a collaborative effort to advance cybersecurity education and build a stronger cybersecurity workforce (Cyberwatch, 2017). Cyberwatch works to fill five main roles as a leader in cybersecurity research and education. These roles are to be, *advocator* in education and workforce development, *builder* of cybersecurity development programs, *collaborator* with cybersecurity entities strengthening education and research programs, *coordinator* ensuring collaboration of cybersecurity programs and *promoter* of developmental models which promote advances in cybersecurity initiatives (Cyberwatch, 2017). In October 2012 Cyberwatch received a grant and funding from the National Science Foundation (NSF) allowing Cyberwatch to mentor over 94 colleges in 29 states (NSF, 2017). Cyberwatch also promotes and mentors K-12 institutions, increases knowledge of cybersecurity careers and assists in expanding the knowledge base of the nation's cybersecurity workforce through education and workforce development (NSF, 2017).

The New Cybersecurity Information Systems Curriculum

The largest appeal to students entering a cybersecurity program is the immediate job prospects available to them upon graduation (Conklin, Cline & Roosa, 2014). However, a major hurdle is that students today can choose to obtain industry certifications allowing them easy access to these coveted job opportunities (Conklin, Cline & Roosa, 2014). The decision to obtain industry certifications presents a significant challenge to the nation and academic institutions in ensuring a highly educated and competitive cybersecurity workforce. This challenge, however, provides an opportunity for colleges and universities to redesign the current information systems program to that which reflects real-world challenges and presents students with hands-on opportunities. These new cybersecurity information systems programs can be blended, so students gain the critical business knowledge needed to be successful throughout the length of their career and provide the skills necessary to enter the workforce and make an immediate difference.

Understanding Employer Needs

When determining what employers are needing from current and future cyber warriors walking through their doors, colleges and universities that are offering information systems programs must make changes to the course topics and how to teach the main concepts. The programs put forth by NICE and Cyberwatch are an excellent baseline for colleges and universities to use in designing these programs. Since the NICE Cybersecurity Workforce Framework outlines KSAs, these also should help colleges and universities to better identify the knowledge and skills for the student to advance in a cybersecurity career (Paulsen et al., 2012). Colleges and Universities may have difficulty trying to match every cybersecurity career field, but the KSAs can still be inserted into core courses ensuring cybersecurity initiatives meet the needs of the NIST Cybersecurity Workforce Framework.

The question of incorporating the needs of the employer must be balanced to ensure that the study of theory includes hands-on activities in a laboratory setting (Hentea, Dhillon & Dhillon, 2006). As well as meeting the needs of the employer there also must be an integration of ethics, social, and legal ramifications necessary for all cybersecurity professionals to study in a cybersecurity information sciences curriculum (Hentea, Dhillon & Dhillon, 2006).

Addition of Industry Certification

The addition of industry certification programs into the cybersecurity information systems program of study can help to validate the KSAs needed to satisfy the NICE Cybersecurity Workforce Framework while not substituting or eliminating the educational degree (Hentea, Dhillon & Dhillon, 2006). The academic program of study is still a necessity as this degree aids students by providing theoretical concepts and problem-solving abilities (Hentea, Dhillon & Dhillon, 2006). However, the knowledge and skills that industry certification provides when not combined with a college or university degree fail to provide the necessary experience element that employers are looking for (Hentea, Dhillon & Dhillon, 2006).

Centers of Academic Excellence

To ensure college and universities are meeting the challenge of adding cybersecurity fundamentals into their programs, they need to certify as a Center of Academic Excellence in

Cyber Defense (CAE/CD) or Cyber Operations (CAE/CO) (Paulsen et al., 2012). It is upon gaining this designation that colleges and universities can set themselves apart from more traditional information systems programs. As a CAE, more tools are available to allow colleges and universities to map programs to the NICE Cybersecurity Workforce Framework using a common vocabulary and architecture (Paulsen et al., 2012).

The ability to align coursework to the NICE Cybersecurity Workforce Framework, allows colleges and universities to define course elements surrounding cybersecurity concepts. These colleges and universities also provide opportunities for their students to participate in Collegiate Cyber Defense Competitions (CCDC) which allow students to gain more credit for hands-on scenario-based exercises (Conklin, Cline & Roosa, 2014).

There are also opportunities to be involved in projects which solve unclassified problems presented by the National Security Agency (NSA), government agencies and private business (Sherman et al., 2017). One of these projects is known as the INSuRE Project which is a cybersecurity research course allowing students the opportunity to work on problems of national importance (Sherman et al., 2017). The INSuRE Project has been successful at placing over 350 students into cybersecurity positions (Sherman et al., 2017). The outcomes from this project have also allowed faculty to design better cybersecurity courses into the curriculum (Sherman et al., 2017).

The New Cybersecurity Curriculum

To build the new cybersecurity information science curriculum it needs to incorporate a constant flux of technology, threats and attack vectors (Hentea, Dhillon & Dhillon, 2006). The curriculum also needs to encompass best practice security standards, the newest teaching methods and incorporate gamification of cybersecurity concepts into the course design (Hentea, Dhillon & Dhillon, 2006). This new curriculum needs to ensure it is not one-sided or a contest of computer science versus information systems. The new cybersecurity information systems curriculum must include technical and non-technical aspects which keep pace with the changing security requirements of business and government sectors (Hentea, Dhillon & Dhillon, 2006).

The non-technical curriculum requirements should center around information and risk management concepts (McGettrick, 2013). These concepts need to include how the regulatory environment shapes good cybersecurity design and aids in the determination of the necessary technical skills and tracks for students. These students should also learn management concepts centered around network security, secure coding, and operations. Skills such as those gained by a theoretical understanding of business continuity and disaster recovery help to ensure future cyber warriors can move into security management in the future if that is their path. The inclusion of these cybersecurity concepts and techniques will better prepare students as they become managers, business owners and boardroom executives (Pawlowski & Jung, 2015).

To adequately build the new cybersecurity information systems program the curriculum must include strong foundational technical knowledge and be hands-on with exposure to practical concepts (Sauls & Gudigantala, 2013). The technical elements are necessary so that students can gain the "fingers to keyboard and appliance" skills that employers require (Conklin, Cline & Roosa, 2014). These classes should center on securing operating systems, cryptology, forensics and physical security concepts and techniques. There should be courses taught using both the free tools and appliances used to secure modern environments such as intrusion detection prevention systems (IDS/IPS), firewalls, next-generation firewalls and content filters. Understanding these concepts will allow students to understand where to implement these devices, what data is at risk, what systems are vulnerable and most importantly how does it all tie into the success and profitability of the business. By combining these courses with industry certifications, students are using skills obtained in the classroom and are demonstrating to employers how they can make an immediate impact in the organization upon hire. The benefits of aligning these courses to industry certifications such as CompTIA Network+, Security+, ISC^2 CISSP, ISACA CRISC to name just a few well-known certification pathways enhances the new cybersecurity information systems curriculum.

These programs must include an opportunity for students to gain industry internships or collaborative avenues with interdisciplinary areas (Sauls & Gudigantala, 2013). These interdisciplinary areas can include collaborative programs with healthcare, aviation, or business programs within the college or university. This collaboration can open additional avenues for cybersecurity students that may not have been previously available since cybersecurity touches all business and government sectors. Faculty designing these next-generation courses and programs should be working towards grants which aid with curriculum design innovations allowing faculty to bring more real-world techniques, applications, and security devices into the classroom (Sauls & Gudigantala, 2013).

Finally, these new cybersecurity information systems curricula must include a concept that most industry certifications and classroom instruction miss, the concepts of cyber ethics. Cyber ethics refers to the ethical concerns surrounding property rights, privacy, and acceptable usage of individual and business information (Alvarez, Silva, and Correia, 2015). Cyber ethics is a technique that must be taught at the collegiate level as it is an effective practice necessary for students to learn before moving into the cybersecurity workforce

(Chukuka & Locasto, 2015). Cyber ethics is also necessary as there are many opportunities in this career field that can have unintended consequences with negative outcomes if proper procedures or practices are not followed (Chukuka & Locasto, 2015). The teaching of offensive and defensive hacking techniques, malicious attacks and illegal use of proprietary data can cause several unintended outcomes (Alvarez, Silva & Correia, 2015). The skills students are acquiring will be necessary to be successful in their new careers but can also be very lucrative if used in a negative way (Pawlowski & Jung, 2015). An irresponsible or malicious student without ethical training could use these newly acquired skills and attempt illegal attacks outside of the isolated lab environment (Trabelsi & McCoey, 2016). If these cybersecurity techniques fail to include cyber ethics, it can leave students with a sizable knowledge gap (Chukuka & Locasto, 2015). If these techniques include cyber ethics, then the new cybersecurity information systems curriculum will adequately address the ethical pitfalls that can arise throughout the student's cybersecurity career (Chukuka & Locasto, 2015).

Recommendations for Future Research

When looking to what future research can be conducted to help get the new cybersecurity information systems curriculum running, three main points appear. The first looks at the creation of one single curriculum description to aid students in finding the right program, the second is ensuring the new curriculum does not become stagnate and continues to evolve, and third that real-world concepts and hands-on skills fill the coursework while still ensuring that theory and ethics are embedded within.

The first recommendation revolves around the need to remove the confusion of multiple programs across disciplines. Instead of having a Management Information Systems (MIS), Computer Information Systems (CIS), Information Systems (IS), Computer Science (CS) and Information Technology (IT) focused cybersecurity program, the adoption of a single program such as a Cybersecurity Information Systems needs to be established (Conklin, Cline & Roosa, 2014). This new program would remove some of the confusion that students are experiencing in determining the right degree program.

A second recommendation is, as educators, there is a need to embrace and be aware of the quickly changing cybersecurity landscape so that courses and curriculum can be easily modified to ensure students meet the changing needs of employers (Bicak, Liu, & Murphy, 2015). To help adjust the program to rapid changes in the world, the new cybersecurity information systems program should be located within the college or university allowing for collaboration between departments (Bicak, Liu, & Murphy, 2015).

A final recommendation encompasses course design so that new cybersecurity information systems courses are designed incorporating case studies based on real-world examples where students will be able to apply their theoretical and hands-on knowledge to solve issues and then compare solutions with how the issues were actual solved (Pawlowski & Jung, 2015). The courses also need to be designed allowing students to increase their security awareness while promoting the growth of best practices. It must include the ethical implications of the privileges they hold within an organization as well as the ethical uses of the skills they have acquired. It is this task-centered focus of course design which will allow students to fill the in-demand cybersecurity roles (Pawlowski & Jung, 2015).

Summary

In summation, what is needed is one single program that allows students to navigate to the right cybersecurity program easily. This cybersecurity program must include a design that embeds hands-on concepts, real-world case studies, industry certification options, and ethical studies. It should also align with the common cybersecurity verbiage of the NICE Cybersecurity Workforce Framework. The coursework, while embracing the technical hands-on concept, must also include non-technical skills necessary for cybersecurity students to easily move into management roles if that career path is made available to them in the future. By creating a new cybersecurity information security curriculum with these parameters, students will be provided the necessary skills to be prepared to enter the cybersecurity workforce. These new curriculum changes will allow students to make an immediate difference in the organization and help close the cybersecurity job gap.

References

Akbulut-Bailey, A. (2012). Improving IS Enrollment Choices: The Role of Social Support. *Journal of Information Systems Education, 23(3),* 259-271.

Alvarez, I. B., Silva, N.S.A., & Correia, L.S. (2015). Cyber Education: towards a pedagogical and heuristic learning. *SIGCAS Computers & Society, 45*(3), 185-192.

Baumgartner, I. (2014). A Set of Best Practices to Design Face-to0face Teaching Sessions for Technology-centered University-level Computing Courses. *International Journal of Engineer Pedagogy, 4*(4), 59-67.

Bicak, A., Liu, M., & Murphy, D. (2015). Cybersecurity Curriculum Development: Introducing Specialties in a Graduate Program. *Information Systems Education Journal, 13,* 1-12.

Chukuka, B., & Locasto, M. (2015). A Survey of Ethical Agreements in Information Security Courses. *Proceedings of the 47th ACM Technical Symposium on Computing Science Education – SIGCSE 16'*, 479-484.

Conklin, A W., Cline, R.E., & Roosa, T. (2014). Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors. *4ih Hawaii International Conference on System Science,* 2006-2014.

Cyberwatch (2017). National Cyberwatch Center website. Retrieved from https://nationalcyberwatch.org/about/

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

McGettrick, A. (2013). Toward Effective Cybersecurity Education. *IEEE Security & Privacy,* 11(6), 66-68.

NIST (2017). National Institute of Standards and Technology website. Retrieved from https://www.nist.gov/about-nist/our-organization/mission-vision-values

NSF (2017). National Science Foundation website. Retrieved from https://www.nsf.gov/awardsearch/showAward?AWD ID=1204533

Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012). NICE: Creating a cybersecurity workforce and aware public. *IEEE Security and Privacy, I0(3),* 76- 79.

Pawlowski, S.D., Jung, Y. (2015). Social Representations of Cybersecurity by University Students and Implications for Instructional Design. *Journal of Information Systems Education, 26(4),* 281-294.

Sauls, J. & Gudigantala, N. (2013). Preparing Information Systems (IS) Graduates to Meet the Challenges of Global IT Security: Some Suggestions. *Journal of Information systems Education, 24(1),* 71-73.

Sherman, A., Dark, M., Chan, A., Chong, R., Morris, T., Oliva, L., Springer, J., Thuraisingham, B., Vatcher, C., Verma, R., & Wetzel, S. (2017). The INSuRE Project: CAE-Rs Collaborate to Engage Students in Cybersecurity Research. *CoRR, abs/I703.08859.*

Trabelsi, Z. and McCoey, M. (2016). Ethical Hacking in Information Security Curricula. *International Journal of Information and Communication Technology Education, 12*(1), 1-10.

US White House. (2010). Comprehensive National Cybersecurity Initiative. https://www.hsdl.org/?view&did=28609