Instructional Perspective: Towards an Integrative Learning Approach in Cybersecurity Education

Sherly Abraham [1], Lifang Shih [2]
[1]Assistant Professor Information Technology
Georgia Gwinnett College
[2]Associate Dean of Technology
Excelsior College
sabraham1@ggc.edu, lshih@excelsior.edu

ABSTRACT: *This paper describes a multifaceted approach to cybersecurity education based on integrative learning theory. We emphasize the need to focus on curriculum, experiential learning techniques, assessment and fostering a community of practice. The need to build conceptual, tactical and practical skills among cybersecurity professionals is highlighted. The paper will include examples of how integrative learning methods can be implemented in cybersecurity education through a number of methods such as curriculum, virtual labs, simulations, cyber student clubs and participation in cyber security competitions.*

Keywords: Cybersecurity education, Integrative learning theory, Experiential learning, Community of practice

Received: 14 June 2015, Revised 15 July 2015, Accepted 26 July 2015

1. Introduction

Cybersecurity data breaches are on the rise and result in monetary and reputational losses to organizations [25]. The recent cyberhack at Sony Pictures reveal the national significance of protecting data systems against cyber threats. In addition, power plants and other critical infrastructure are vulnerable to cyber attacks [33] emphasizing the need for continued and strong protection against cyber threats. Given the rising threat presented by Cybersecurity, organizations are expanding their capital to hire and retain cybersecurity professionals. As the sophistication of attack methods and sources of attacks continue to increase in complexity so does the need to train and educate a competent workforce in cybersecurity[18]. However, a key challenge in the realm of Cybersecurity is the lack of skilled professionals in order to thwart and defend against the rising and looming threat presented by Cyber criminals[5,20,26] .

Cybersecurity is still an immature field and lacks a cohesive intellectual body of activity and clear underlying science [22]. Studies point to the need for a science of cybersecurity that would provide a principled account for techniques that work for building secure systems [28]. A number of efforts have been developed to define curriculum and best practices in cybersecurity education. For example, the designation of Center for Academic Excellence in Information Assurance (CAE/IAE) provides higher educational institutions with standards and criteria to develop cybersecurity curriculum. Similarly, the Cybersecurity

Framework developed by NIST provides a structure for defining cybersecurity program based on industry, academic and government requirements. In the same vein, a number of organizations share resources in utilizing cyber security curriculum and virtual labs (eg. CSSIA, NICCS) and a number of efforts are underway (eg. NICE Challenge Project).

Although, there are a number of growing resources and supporting materials being made available to foster Cybersecurity education, there is a need for a holistic and theoretical approach to Cybersecurity education [21] that considers the development of conceptual, tactical and practical skills in cybersecurity professionals. Also, the dynamic and evolving nature of Cybersecurity calls for fostering a Community of Practice (CoP) among professionals so knowledge can be shared and used to develop protection mechanisms. In this paper, we identify the need for a multifaceted approach to Cybersecurity education that draws on integrative learning theory, experiential learning and community of practice learning theory.

2. Cybersecurity Education

The extant literature in cybersecurity education focuses on specific areas such as the use of virtual labs [11, 24] and gaming and simulation [27]. Other approaches include sharing perspectives on cybersecurity education or examples of curriculum development [11,23,30]. While these studies are important to examine educational approaches to cybersecurity education, there is a need for comprehensive perspectives in order to capture the essential ingredients that assist with developing the conceptual, practical, tactical and soft skills in cybersecurity professionals. Also, there are many information security models and curricula in existence [12] that warrants the need for a holistic view to cybersecurity education.

Cybersecurity applies to all industries and requires an interdisciplinary approach [18]. Cybersecurity professionals require distinct skills set and need to be considered separately than the general IT workforce [19]. In addition to the technical skills, cybersecurity professionals need business skills [19] and communication skills [8]. Cybersecurity professionals need to work with managers to convince them of the need to invest in cybersecurity. In a similar vein, cybersecurity professionals need to assess risk and ensure compliance with regulations and find the right balance between security and usability [1]. Although, these roles might be separate within organizations, given that the source of a cybersecurity attack can come from within the physical, network, application or human side, a cybersecurity professional needs a holistic understanding of these areas irrespective of their specific role. Next, we identify key theoretical approaches that assist with development of a holistic approach to cybersecurity education.

3. Integrative Learning Theory

Integrative learning can be attributed to fostering the ability among learners to make, recognize and evaluate connections among disparate concepts, fields or contexts [13]. It is important in this approach to center the educational approaches on the real-world context [34] and promote critical thinking and problem solving approaches [6]. Integrative learning approaches encompass analyzing real-world problems through different perspectives and considering different solutions to the problem. Cybersecurity is a practice oriented discipline and requires critical thinking skills and the ability to analyze a situation through multiple perspectives [7]. For example in the context of risk management in cyber security, it is important to consider the cost of mitigating risks and prioritizing risk in the organization. An organization that relies solely on selling products through its online website will face a large loss if the website is attacked as it disrupts the business operations for the organization. On the other hand, an organization that does not sell products through its websites but just provides information on their products does not face the same impact. It is important to consider multiple perspectives such as the likelihood of the threat, the impact of the threat on the business operation of the organization, the methods that can be utilized to prevent the threat and cost associated with mitigating threats. The right combination of cost and survivability needs to be accounted for in mitigating and analyzing cybersecurity risks. Another example for the need of considering multiple perspectives and the ability to draw connections among disparate concepts in Cybersecurity is in threat detection. A number of recent data breaches reveal that hackers had access to the networks of attacked organizations for months before they were detected [16]. Threat detection requires considering a number of factors including unusual outbound network traffic, anomalies in privileged user account activity, geographical irregularities, increase in database read volumes and so on [10]. This requires cyber professionals to think critically, be proactive and consider multiple perspectives.

In addition to fostering critical thinking skills, integrative learning approaches help learners to recollect and apply information obtaining for longer than in other traditional learning situations [13]. The application of concepts learned is very important skill set in the Cybersecurity field. Integrative approaches assist with the development of important soft skills in Cybersecurity such as communication skills [4]. Cybersecurity professionals are required to communicate with other units in the organization and need to promote awareness and obtain a buy-in from management. We identify four dimensions as essential elements in supporting an integrative learning approach in Cybersecurity consisting of curriculum development, experiential learning methods, assessment and building a community of practice. Each of these elements complements the other in supporting an integrated learning approach. Figure 1 illustrates this concept.

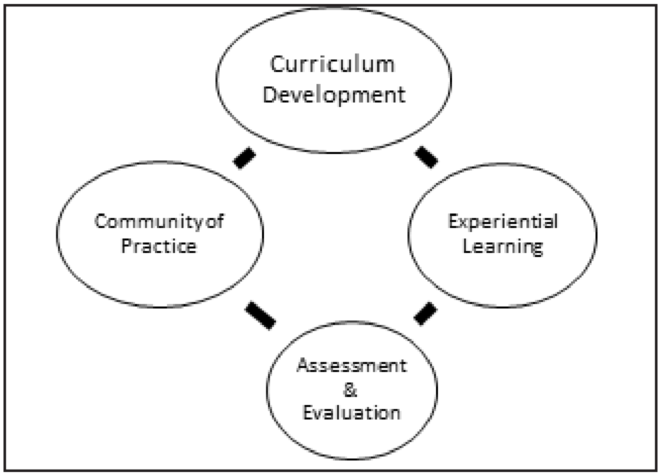


Figure 1. Holistic Cybersecurity Education model

4. Experiential Learning

Experiential learning can be defined as the systematic approach to applied learning facilitated by students extracting from a variety of experiences within and outside the classroom to promote lifelong learning [35]. Studies identify four components that define an activity as experience based – concrete experience, reflective observation, abstract conceptualization and active experimentation [17]. A key dimension of experiential learning is the culmination of knowledge through interactions with the social and learning environment. This is in contrast with learning where the learner only reads about, hears about, or writes about the concept but does not experience them as part of a learning process [15].

The technical and operational nature of cybersecurity requires educational approaches to integrate experience based learning. Specifically, cybersecurity practitioners require technical skills sets and experience working with a variety of tools and technologies. For example, vulnerability detection is a basic skill set for most of cybersecurity professionals. Often vulnerabilities need to be discovered in versatile environments from web, database, networks, and operating systems. This requires hands-on-knowledge in using these technologies and deep understanding of technical concepts. Experiential learning opportunities in the form of virtual labs, simulations, and outside classroom experiences in the form of cyber competitions and internships can assist with facilitating these types of learning.

Virtual labs provide a safe environment to test ethical hacking skills as well. For example, we developed a network topology in our network communications security course that enables student to work in real-time environment to solve network security problems and configure technologies. Figure 2 illustrates the topology of the network setup for the virtual lab.

The students login in to the landing virtual machine and then remotely connect to other machines on the network. Students work on completing and acquiring real-time experience in network vulnerability assessment, packet sniffing, configuring firewalls, server hardening and a number of other activities that provides them with experience to simulate real-world network attacks. In addition to performing these hands-on-experiences, students reflect on their experience in completing the lab and address questions that require them to think critically.

Likewise simulations that mimic real-world problems in the cybersecurity realm provide opportunities for students to think critically and analyze a problem from multiple perspectives. For example, we have developed a simulation activity in our capstone course that requires students to apply the concepts and experience gained in the program to deal with the kind of issues that cybersecurity professionals face every day. The simulation requires learners to manage their time, delegate effectively, work well with colleagues and understand the ethical and legal issues related to information technology and privacy. Figure 3 provides a screenshot of the simulation activity.

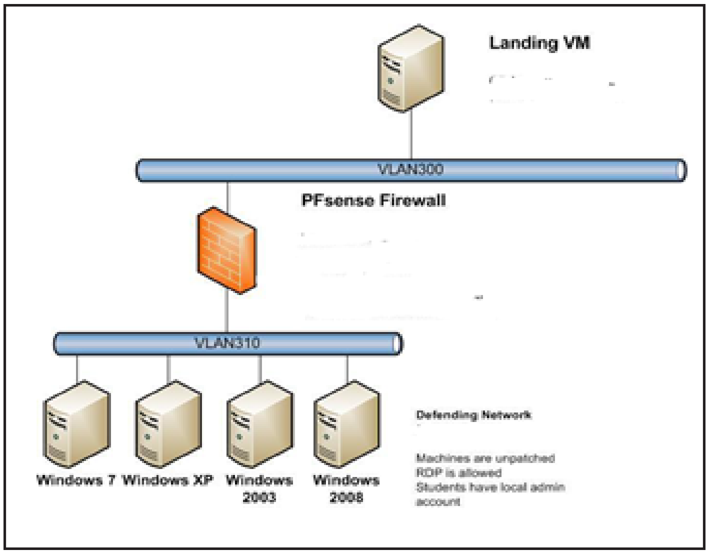
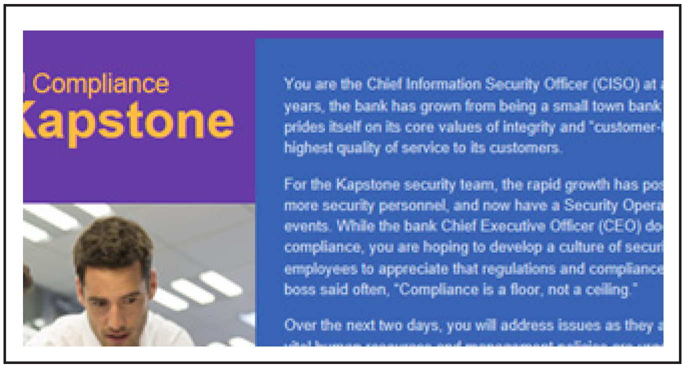


Figure 2. Network Topology of Virtual Lab in Network Communications Security



You are the Chief Information Security Officer (CISO) at
years, the bank has grown from being a small town bank
prides itself on its core values of integrity and "customer-
highest quality of service to its customers.

For the Kapstone security team, the rapid growth has pos
more security personnel, and now have a Security Opera
events. While the bank Chief Executive Officer (CEO) do
compliance, you are hoping to develop a culture of secur
employees to appreciate that regulations and compliance
boss said often, "Compliance is a floor, not a ceiling."

Over the next two days, you will address issues as they

Figure 3. Screen shot of simulation activity in Capstone course

5. Assessment

Assessment and evaluation is a very crucial source of input to the program's continuous improvement. It provides a metric against which the institution can assess its performance. It provides metrics to assure all stakeholders, students, faculty, and prospective employers, of the value of this form of education. Most importantly, it serves a continuing reminder to the faculty of the professional goals of technology education, and provides a guidepost for the degree of rigor needed in coursework. Overall, there are two forms of direct assessment used to assess student learning, formative assessment and summative assessment. The purpose of formative assessment is to provide ongoing feedback on student learning to provide information on the strengths and weakness in the student learning so both the faculty and student to make necessary adjustment to improve their teaching and learning. The formative assessments can be done in various ways including but not limited to class discussions, textbook assignments, and multiple-choices quizzes.

The goal for summative assessment is to evaluate student's competency at the end of an instructional unit by comparing it against the intended learning outcomes. Capstones are cited in the Characteristics of Excellence in Higher Education [9] as an effective summative assessment of student learning (p.64) [32]. The capstone experience/end of course assessment serves several critical functions in the process of assessment of the program outcomes. First, it is the assessment tool that directly measures the achievement of student learning outcomes, a vital indicator of a program's performance. Second, it also serves as a mechanism through which the institution can ensure that all its graduates have passed all the benchmarks for acceptance in their fields. Third, it provides a crucial source of input that drives the continuous improvement of the program.

In addition to direct measure of student learning, indirect measures of students are also useful indicators of program effectiveness. Indirect data can be gathered using surveys and questionnaires delivered within the relevant courses or upon graduation in order to collect data on student engagement in and satisfaction with the course and the program as a whole. A sound program assessment plan should collect both direct and indirect evidence to improve the curriculum of the program and to identify areas of strength and weakness in student learning [31]

6. Community of Practice (COP)

An integrative approach to learning is also connected to building a community among the learners. This is a highly relevant area that needs to be built in to cybersecurity education. Community of practice can be defined as consisting of "members that are informally bound by what they do together from engaging in lunchtime discussions to solving difficult problems and by what they have learned through their mutual engagement in these activities" [36]. A number of studies have attributed communities of practice to the learning environment [29]. Communities of practice are instrumental in fostering the development of tactical knowledge [2]. There are a number of advantages to COPs that promotes learning and is relevant in the context of cybersecurity education. These include the exchange and interpretation of information, knowledge retention, steward competencies and homes for identities. COPs are great resources to promote lifelong learning and this is an important skill set to develop in cybersecurity professionals. "*The learning community is a very structured introduction to the integrative learning experiences that student participate in throughout their education*" [29].

Cyber competitions provide excellent avenues to build hands-on-skills and also promote a community of learning among students, faculty and industry peers. For two years, our Cybersecurity students have participated in the National Cyber League (NCL) competition and ranked in the top ten among the specific brackets assigned. Students work on completing individual competitions based on the skill level and finally participate in a team based effort. The experiences shared and knowledge gained assists with building a strong community and peer network among students. Also the team competition exercise tremendously assists in building connections among students. Specifically, the use of a team name and identifying members by the team name helps to create a team spirit among the group. During the competition, it is important for faculty and coaches to keep the students motivated and focused. Another example of an excellent avenue to build a community among students is through student clubs. We have a cybersecurity club that helps students to participate in common discussion topics. Some of the discussion topics students participate in includes experiences attending conferences, completing professional certifications, resources for professional certifications, job fairs, and cyber competitions. In our online environment this is facilitated through the development a course shell that includes a number of discussion threads and resources in an informal setup. The informal setup assists with students sharing experiences and connecting and relating to each other. Table 1 summarizes the strategies to implementing integrated curriculum in cybersecurity education

Integrated Learning Area	**Strategies**
Curriculum	InterdisciplinaryStandards Industry Focused Professional CertificationsOngoing Review
Experiential Learning	Virtual LabsCyber CompetitionsInternships
Assessment & Evaluation	Course Embedded AssessmentCapstone Course Outcomes AssessmentProgram and Curriculum ReviewStudent SurveysExit Surveys
Community of Practice	Cyber CompetitionsStudent AssociationsStudent Clubs

Table 1. Integrated curriculum strategies in cybersecurity education

7. Conclusion

Cybersecurity education needs to emphasize an interdisciplinary approach to learning that fosters learners to think critically and draw connections from disparate disciplines. The evolving and dynamic nature of cybersecurity also calls for the need to build strong connections with the industry in order to develop a competent workforce. We find integrative learning approaches to be an effective framework to develop cybersecurity education programs. The integrative learning approach utilizes interdisciplinary approaches and is centered on the application of real-world scenarios. Also, integrative learning approaches supports building a community of learners. A holistic approach that centers on curriculum, experiential learning, assessment and community of practice is essential in cybersecurity.

References

[1] Abraham, S., Chengalur-Smith, I. (2011). The Role of Conflict Resolution in Designing and Implementing Information Security Policies: An Institutional Perspective. Proceedings of AMCIS (America's Conference on Information Systems), Detroit, MI.

[2] Allee, V. (2000). Knowledge Networks and Communities of Practice. OD Practitioner, Fall/Winter 2000.

[3] Andress, A. (2003). Surviving Security: How to Integrate People, Process, and Technology. Boca Raton, FL: Auerbach Publications

[4] Anema, I. (2014). Integrative Learning and Evidence-Based Practice: Mastering the Process. Contemporary Issues in Communication Science and Disorders. (41). 1-11.

[5] Assante, M. J., Tobey, D.H. 2011. Enhancing the cybersecurity workforce, IEEE IT Professional, (13). 12–15.

[6] Birenbaum, M., Breuer, K., Cascallar, E., Dochy, F., Dori, Y., Ridgway, J., et al. (2006). A learning integrated assessment system. *Educational Research Review* 1(1) 61-67

[7] Bishop, M. and Irivine, C. (2010). Demythifying Cybersecurity. *IEEE Computer and Reliable Societies.* May/June 2010

[8] Caldwell, T. (2013). Plugging the cyber-security skills gap. Computer Fraud and Security, July 2013.

[9] Characteristics of Excellence in Higher Education (2006), Middle States Commission on Higher Education, PA.

[10] Chickowski, E. (2013). Top 15 Indicators of Compromise. Dark Reading. Retrieved from http://www.darkreading.com/attacks-breaches/top-15-indicators-of-compromise/d/d-id/1140647?

[11] Cone,D. B., Irvine, E. C., Thompson, F., M., Nguyen, T. (2007). A Video game for cyber security training and awareness, *Computers & Security,* (26) 63-72.

[12] Hentea, M., Dhillon, H. (2006). Towards Changes in Information Security Education. Journal of Information Technology Education. (5) 221-233.

[13] Huber, M. T., Brown, C., Hutchings, P., Gale, R., Miller, R., Breen, B. (Eds.). (2007). Integrative Learning: Opportunities to Connect. Association of American Colleges and Universities and The Carnegie Foundation for the Advancement of Teaching.

[14] Irvine, E.C. (1997). Computer Security Education Challenges, *IEEE Software*, 14 (5) 110-111.

[15] 15 .Keeton, M.T., Tate, P. J. (1978). Editors note:The boom in experiential learning (p. 1–8). In M. T. Keeton & P. J. Tate (Eds.), Learning by experience—What, why, how. New directions. for experiential learning. San Francisco: Jossey-Bass.

[16] Kirk, J. (2014). Hackers accessed Goodwill hosting provider for 18 months before card breach. TechWorld. Retrieved from http://www.techworld.com/news/security/hackers-accessed-goodwill-hosting-provider-for-18-months-before-card-breach-3572469/

[18] Kolb, D. A. (1984). Experiential learning: Experience as the source of learning and development. Engelwood Cliffs, NJ: Prentice-Hall.

[19] LeClair, J., Abraham,S., Shih, L. (2013). An Interdisciplinary Approach to Educating an Effective Cybersecurity Workforce. Proceedings of the on InfoSecCD' 13 Information Security Curriculum Development Conference

[20] Lee, J., Bagchi-Sen, H. Rao, R., Upadhyaya. (2010). Anatomy of the Information Security Workforce. *IEEE IT Professional,*

12 (1) 14-23.

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

[22] Martini, B., Choo, K. (2014). Building the next generation of cybersecurity professionals. Proceedings of Twenty Second European Conference on Information Systems, Tel Aviv, 2014. 1

[23] McGettrick, A. (2013). Toward Curricular Guidelines for Cybersecurity. Report of a Workshop on Cybersecurity Education and Training. Retrieved from http://www.acm.org/education/TowardCurricularGuidelinesCybersec.pdf

[24] Michael, E.W., Mattord, H. J. (2004). A draft model curriculum for programs of study in information security and assurance, *In*: Proceedings of the eighth colloquium for information systems security education. 77–83.

[25] Naf, M., Basin, D. (2008). Two Approaches to an Information Security Laboratory. *Communications of the ACM*, 51 (12) pp. 138-142

[26] Ponemon Institute. (2014). 2014 Cost of Data Breach Study: United States. Retrieved from http://www.accudatasystems.com/assets/2014-cost-of-a-data-breach-study.pdf

[27] Roew, C. D., Lunt, M.B., Ekstrom, J. J (2011). The Role of Cyber-security in Information Technology Education. ACM SIGITE'11, West Point, New York, USA

[28] Ryoo, J., Techatassanasoontorn, A., Lee, D., Lothian, J. (2011). Game-based InfoSec Education Using OpenSim. *In* : Proceedings of the 15th Colloquium for Information Systems Security Education. Fairborn, Ohio.

[29] Schneider. (2012). Blueprint for a science of cybersecurity. The Next Wave. (19:2). 47-57

[30] Schultz. (2013). Learning Communities as a First Step in an Integrative Learning Curriculum. About Campus. September-October.

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

[32] Suskie, L. (2004). Assessing Student Learning. Anker Publishing Company, Inc. Bolton, MA.

[33] Thinger, B., Memon, A., Shih, L. (2006). Non-Traditional Learning and Assessment Approach to Nuclear Engineering Technology Education. *In*: Proceedings of ASEE Annual Meeting, Chicago, IL. . Retrieved September 21, 2009 from http://soa.asee.org/paper/conference/paper-view.cfm?id=2167

[34] Tucker, P. (2014). Forget the Sony Hack, This Could Be the Biggest Cyber Attack of 2015. Defense One. Retrieved from http://www.defenseone.com/technology/2014/12/forget-sony-hack-could-be-he-biggest-cyber-attack-2015/101727/

[35] Walker, D. (1996). Integrative Education. Eugene OR: ERIC Clearinghouse on Educational Management.

[36] Weinstein, N. (2008). Experiential Learning. Experiential Learning- Research Starters Education.

[37] Wenger, E. (1998). Communities of Practice: Learning, Meaning, and Identity. Cambridge: Cambridge University Press