An Interdisciplinary Approach to Educating an Effective Cyber Security Workforce

Dr. Jane LeClair
Chief Operating Officer
National Cybersecurity Institute
Excelsior College
7 Columbia Circle, Albany, NY, 12203
(315)4402827
jleclair@excelsior.edu

Dr. Sherly Abraham
School of Business and Technology
Excelsior College
7 Columbia Circle, Albany, NY 12203
(518)6088351
sabraham@excelsior.edu

Dr. Lifang Shih
School of Business and Technology
Excelsior College
7 Columbia Circle, Albany, NY 12203
(518)6088362
lshih@excelsior.edu

ABSTRACT

Organizations and communities are now increasingly dependent on computer networks for their daily operations, which makes the digital world both attractive and lucrative for cyber criminals. Additionally, the volume of banking and monetary transactions that occur across the Internet from devices such as laptops, tablets, and mobile phones has increased immensely, further making the Internet an interesting playground for cyber criminals. Given the evolving landscape of cyber security threats, it is important to provide our workforce with ongoing training in cyber security. The protection of cyber assets requires a multipronged approach that requires the coordination of government, academia and industry. Therefore, the educational methodologies need to evolve and adapt to support the needs of people who are geographically separated and constrained by time. In this paper, the authors propose an interdisciplinary approach to cyber security education and the best practices for integrating advanced instructional technologies to online cyber security education.

Categories and Subject Descriptors

J. 1. [Computer Applications]: Education.

General Terms

Theory

Keywords

Cyber security, Workforce Development, Online Education

1. INTRODUCTION

Cyber security threats are constantly evolving and the need for protecting our national assets has become a great concern. Organizations and communities are increasingly dependent on computer networks for their daily operations, which makes the cyber digital world both attractive and lucrative for cyber criminals. While the importance of protecting our electronic assets has existed for some time, the amount of sensitive and personally identifiable information that is now available and accessible globally calls for increased security measures. For example, Wal-Mart handles more than 1 million customer transactions every hour nationwide. Those transactions feed databases estimated to be the equivalent of 167 times the amount of books in America's Library of Congress (The Economist 2010a). Additionally, the volume of banking and monetary transactions that occur across the Internet from devices such as laptops, tablets, and mobile phones and has increased immensely, further making the Internet an interesting playground for cyber criminals.

In addition to the importance of protecting personally identifiable and monetary information stored and accessed across the Internet, the realm of cyber security is now challenged by threats of cyber warfare. Cyber warfare is defined as "actions by a nation state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (Clarke and Knake, 2010). The cyber spectrum has entered the fifth domain of warfare in addition to land, sea, air and space with President Barack Obama declaring America's digital infrastructure to be a "strategic national asset" (The Economist 2010b). In this context, cyber attacks could target military and national defense systems of a nation in order to pose threats and destruction to national assets for political motivations. Therefore, the protection of cyber assets requires a multipronged approach that requires the coordination of government, academia and industry (Abraham and Chengalur-Smith, 2010). This need for protection is further supported by the increasing sophistication of cyber security threats and attacks. Figure 1 shows the trends in the evolution of cyber security threats over the years in terms of scope and level of sophistication (VanDerwerken and Ubell, 2011). Clearly, it is evident that the threat landscape of cyber security is evolving to become more sophisticated and to be able to counteract protection mechanisms.

Information Security Curriculum Development Conference 2013 October 12, 2013, Kennesaw, GA, USA.

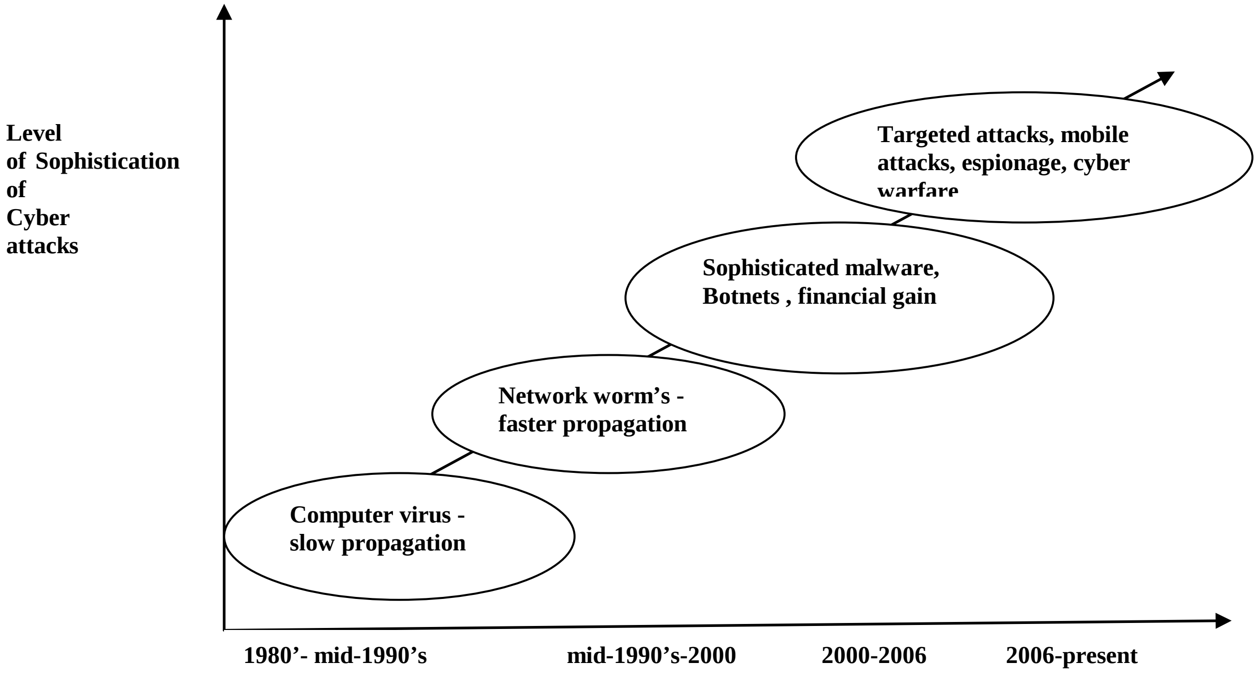

Level
of Sophistication
of
Cyber
attacks
Targeted attacks, mobile attacks, espionage, cyber warfare
Sophisticated malware, Botnets , financial gain
Network worm's - faster propagation
Computer virus - slow propagation
1980'- mid-1990's
mid-1990's-2000
2000-2006
2006-present

Figure 1. Cyber Security Threat Landscape

1.1 A looming challenge in the Cyber security Spectrum

A looming challenge in the realm of cyber security that has been echoed in a number of studies (Assante and Tobey 2011; Locasto et al. 2011; Roew et al. 2011; VanDerwerken and Ubell, 2011) is the lack of a trained and educated cyber workforce in order to meet the challenges presented by a growing cyber attack spectrum filled with cyber criminals of varying motives. For example, a recent study conducted by the world's largest not-for-profit information security professional body, International Information Systems Security Certification Consortium(ISC)2 in partnership with Booz Allen Hamilton with over 12,000 information security professionals worldwide pointed to the shortage of skilled cyber security professionals(The 2013 Global Information Security Workforce Study). The study also reveals that managers are not satisfied with the quality of cyber security job applicants. The shortage of cyber security professionals could lead to organizations compromising their security by tasking individuals that might not be proficient in cybersecurity to adequately perform cyber security functions (VanDerweken and Ubell, 2011).

2. EDUCATING CYBER SECURITY WORKFORCE

At the core of the shortage of cyber security professionals is the need for a commitment to educating the workforce (Locasto et al. 2011). It is important to recognize the importance of university education that builds cyber security professionals with a holistic perspective on cyber education. As Locasto et al. 2011 notes, "Plans for training government cyber security workers should focus on educating a new work force rather than mass certification of existing workers". The National Board of Labor Statistics (BLS) data shows that Network Systems and Data Communication Analysts and Network and Computer Systems Administrators (i.e. the areas that are closely related to cyber security) are projected to experience above average employment growth through 2018, 53% and 23%, respectively. Figure 2 provides the 10-year employment projection for careers related to cyber security from the Department of Labor 2008 report.

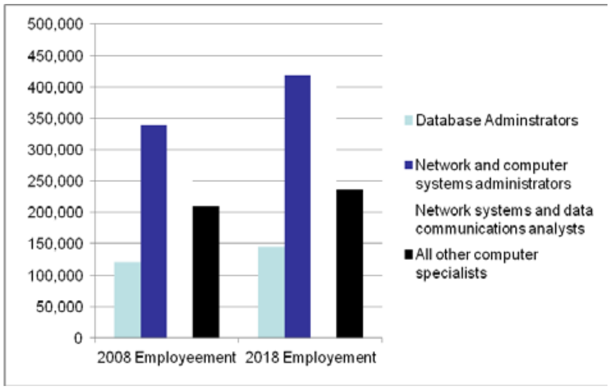


Figure 2: National Long-Term Employment Projection

Similarly, another recent survey showed that 76 percent of the cyber security jobs that were analyzed required a Bachelor's degree (Cyber Security Jobs Report, 2013). It is important to educate the existing workforce, invest in cyber security education, and encourage students to pursue an educational path in cyber security in order to build an effective workforce of cyber security professionals. Ewans and Reeder (2010) allude to the human capital crisis in cyber security in designing security systems and developing the necessary tools to prevent, detect and mitigate risks due to cyber attacks. Ewans and Reeder (2010) identify four major areas to deal with this challenge:

- Promoting and funding the development of more meticulous curriculums in educational environments
- Supporting the development and adoption of technically rigorous professional certifications with thorough educational and monitored practical components
- Employing a combination of the hiring process and the acquisition process to increase the level of technical competence of those involved in building, operating and defending government systems
- Ensuring there is a career path as with other disciplines like medicine to reward and retain those with high-level technical skills

The need to have a well-prepared and trained workforce in cyber security is evident and a pressing issue. Ewans and Reeder (2010) identify two sectors, military and nuclear energy systems, as the two sectors under continuous attack. It seems to be a logistic and effective move to train the existing personnel in these two sectors to address their own need in cyber security. However, most military and nuclear energy personnel do not have the opportunity to attend a traditional college either due to deployments or the demanding work hours. In this paper, the authors begin with identifying the importance of developing effective and affordable educational programs in order to promote educational opportunities in cyber security. The authors will then present a model with a three-pillar domain of an interdisciplinary approach to cyber security education.

In order to educate the current workforce on cyber security, it is imperative to provide learning venues that provide affordable and flexible strategies which cater to the needs of working employees and adult learners. In order to identify the best learning venues for working adults, we need to first look into how adults learn. Andragogical learning approaches learning as a self-directed process that emphasizes the importance of creating a learner-centered rather than an instructor-centered learning environment. Instead of a lecture-based learning environment, learning activities which are task or problem centered and are based on the needs of the learners rather than on a prescribed curriculum based on age level. It values the learner’s prior experience/knowledge which can be used as the building blocks from which all involved can then form a learning community (Maxwell 2012). While the traditional classroom training approach is the most common workforce development strategy, the CERT (Computer Emergency Response Team) approach identifies the shortcomings in the traditional learning approaches. New approaches that consist of knowledge building, skill building, experience building and evaluation in fostering effective, large-scale training to a technical workforce are recommended (Hammerstein and May, 2010). Some of the major shortcomings in the traditional classroom environment which were identified include the weakness in developing skills and experience at a high level of proficiency, time consuming nature, lack of scalability and cost effectiveness, and the challenges in updating curriculum in a rapidly changing environment like cyber security. The CERT approach recommends online training methods in building a cyber security workforce as they offer cost effective, manageable segments, control of the pace of learning, and flexibility. Also, the workforce is not adequately trained in cyber security due to the lack of resources in traditional environments to train and educate large numbers of working professionals (Locasto et al. 2011). Furthermore, a number of studies point to online learning as effective and suitable for professions, and in some cases have shown to produce better results than face-to-face instruction (U.S Department of Education, 2009).

2.1 Adult Learning Theories and Online Learning Environments

The literature indicates that with proper instructional design, the online learning environment can be an effective learning platform for adult learners (Milheim, 2011). A recent research study on the anatomy of the information security workforce revealed that a majority of middle aged cyber security professionals did not process a bachelor’s degree (Lee et al. 2010). Cyber security educational environments need to evolve to cater to this group of professionals so they can earn the necessary degrees that would enable them to excel in their professions. In recent years, the focus of adult education has been shifted from a more behavior (task-oriented) perspective towards a humanistic approach (self-directed and problem based). The various settings in the online learning environment can be integrated to support adult learning from a humanistic perspective of learning, including humanism and critical humanism perspectives (Tisdell and Taylor, 1999). In the next section, we examine how online learning environments support such a perspective.

The humanism perspective of learning focuses on the identification of learner needs and how these needs can be fulfilled through the learning experience (Knowles, 1950). A humanistic approach in an online learning environment will focus on learners’ motivation and self-development. It sees the role of the instructor as a person who facilitates the learning process but does not direct it. With the flexibility of anytime and anywhere access to the learning environments, online learning allows the students to participate on their own time and direct their own learning following the provided course guidelines. To support the humanism approach of learning, the online learning environment will need to be set up in a way that motivates learners and allows opportunities for the learners to set up their own goals and the strategies to achieve them. Project based learning activities in the online environment, for an example, is where the student can identify a relevant topic of their interests and students can then use their own strategies to search for credible resources to complete the project.

The concept of “critical thinking” can be considered as the starting point for us to understand critical humanism. According to Brookfield, critical thinking is an integral part in adult education (Brookfield, 1987). A critical humanism approach to learning focuses on developing students’ ability to think independently and recognizes individual differences among the learners. It emphasizes the importance of the role of the instructor in recognizing the student differences and facilitating consensus among the group through discussion and cooperation (Tisdell & Taylor, 1999). To support the critical humanism approach to learning, it is crucial to implement well crafted discussion topics that challenge, acquire, and build knowledge among the learners in the learning community. The online learning environment has been identified as a global bonding approach in promoting cyber security education (VanDerweken and Ubell, 2011). With the introduction of advanced technologies into the online learning environments, online learning has enabled learners to apply their daily use of technology into meaningful educational activities. The combination of using commonly used online communication tools such as discussion boards and emails as well as other novel communication tools such as the online chat and video conferencing provides a holistic "communication network" among the learners and enhances the learners' sense of community (West, 2010). Additionally, recent studies show that integrating advanced technologies such as simulations and virtual laboratories into the online environment enables working adults access to the cutting-edge technologies to acquire the required knowledge and skills so they can be successful in their future careers (Maxwell, 2012).

In summary, it is recognized that working adults need a more flexible learning environment that the traditional education settings won't be able to offer (Morris, 2005). With the promise of overcoming the time and distance barriers, it is well documented in the literature that with sound andragogical design, online learning can provide a meaningful educational experience that is equivalent to or sometimes even better than that in the traditional learning environment.

3. INTERDISCIPLINARY APPROACH TO CYBER SECURITY EDUCATION

A number of studies on cyber security education have focused on specific approaches such as utilizing gaming techniques (Cone et al. 2007), laboratory based hands-on courses (Naf and Basin 2008) and integrating virtualization platforms (Stewart et al. 2009). Other studies have focused on providing perspectives on cyber security education or specific examples of curriculum developed for cyber security programs (Irvine 1997; Michael and Mattord, 2004; Sharma and Sefcheck 2007). While these approaches are important in order to shed light on effective educational techniques it is also important to provide a holistic approach to examining cyber security education. Likewise, there are numerous information security educational models and curricula in existence (Hentea et al. 2006) that necessitates the need for a holistic view to cyber security education. Additionally, given that the current cyber workforce has developed without a concentrated and standard view of cyber security, it is important to utilize a holistic perspective in analyzing cyber security education (Dodge et al. 2012).

Unlike other disciplines, cyber security approaches apply to all industries and require an interdisciplinary approach (Hentea el at. 2006) in order to obtain the right skills in the field. Also, studies indicate that the cyber security workforce requires a distinct skill set and should be considered separately than the general IT workforce (Lee et al. 2010). Specifically, Lee et al. (2010) showed that cyber security professionals required higher IT and business skills than the general IT area. For example, within an organization, cyber security awareness needs to reach all employees in an organization and each employee has a role to play in the cyber security program. Similarly, the implementation of cyber security policies requires the coordination of various units within the organization. This requires a cyber security professional to have the skills required to work with diverse groups as well as being able to apply the required the technical measures to find the right balance between security and usability (Abraham and Chengalur-Smith, 2011). We identify three major pillars of domain consisting of people, process and technology that need to be integrated into cyber security education programs. Andress (2003) emphasizes the importance of integrating the components of people, process and technology in implementing security solutions and provides recommendations for creating such security solutions. Figure 2.1 identifies the three pillars that integrate to form an effective cyber security program in organizations.

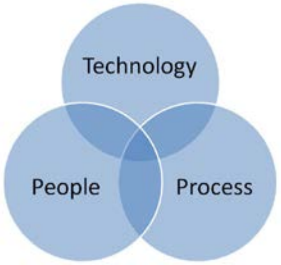


Figure 2.1. The Three Major Pillars of a Cyber Security Program

In order to demonstrate the importance of people, process and technology in cyber security, let us consider a simple security precautionary method of requiring employees to change their passwords every 3 months. Table 1 shows the dependence and role of these three elements needed in an organization in order to successfully implement the password policy.

Table 1: Technology, Process and People in Cyber Security

Element	Role
Technology	The right technology, configuration, maintenance, integration in to existing environment.
Processes	The policies that define the scope and usage, applicability, exceptions.
People	Awareness and end user acceptance, the technical personnel required to maintain the system.

This view is applicable to almost all security procedure implementations in organizations and, therefore, it is important for cyber security personnel in organizations to know the dependence and integration of these elements. A purely technical perspective is often characterized in the cyber security domain; however, this view does not consider the importance of people and process in the successful implementation of security policies. A number of studies identify the challenges in implementing security policies due to the people and process factor. In order to leverage the important role of these elements, it is important to ensure that cyber security education curriculums incorporate learning methods and content that addresses the three major elements of cyber security. In the next section we look at the role of people, process and technology and the required skills that are needed in these areas for effective cyber security education. We will then look at the different methods that can be employed in online environments in order to provide such a balanced skill set in cyber security education.

3.1 People Element

Cyber security professionals are dependent on people in a number of different dimensions. A cyber security professional in an organization cannot work on an island, but requires building bridges with various units in the organization in order to successfully implement policies. This requires good communicative and management skills. The various stakeholders involved in the implementation process need to capture the importance of cyber security and this needs to be illustrated and communicated in terms that are comprehensive to employees in different levels in the organizations. Communications skills are very important in the information systems field in general and a number of studies point to the ineffective communications skills of information systems staff as a possible cause of failed projects (Miller and Luse, 2004). In a different dimension, cyber security professionals need to design security solutions and policies keeping the end user in mind. This includes considering the aspects of human computer design and end user design of technology and processes. If a security solution is too complicated or erroneous for an end user to use, it will not be successful. Also, cyber security professionals require building awareness of cyber security policies and best practices among people. Human beings are considered the weakest link in a security plan (Mitnick and Simon, 2002). Human error continues to be a major cause of security breaches in organizations which makes it important to design security programs to effectively build awareness among users. Finally, cyber security requires protecting assets against hackers and criminals, and it is important to understand the psychology, behavior and motives of hackers in order to help prevent cyber attacks. A recent study showed that schools, colleges and universities can help thwart hacking attempts among the younger generation by adopting a zero tolerance attitude towards hacking. That, combined with early intervention to address hacking activity, offering courses in computer ethics and organizing competitions for cyber defenses (Xu et al. 2013) can go a long way in developing stronger moral values against illicit behavior.

3.2 Process Element

In addition to people, cyber security policies and strategies require integrating the solutions into existing procedures of the organization. This requires a preplanned and highly organized process (Bayuk et al. 2012) that is governed and streamlined to fit the business objectives of the organizations. It is important for the procedures to be well documented and established in the organization. Similarly, the procedures need to be revised on a regular basis to fit the evolving pattern of cyber security attacks. Cyber security requires planning, documenting and integrating policies into the culture, and structure of the organization. Some of the noted areas where the process element gains importance in cyber security include policies, risk analysis, incident handling and response, project management, laws, business continuity and disaster recovery.

3.3 Technology Element

Finally, technology plays an integral role in cyber security and requires professionals to possess a diverse set of technical skills ranging from programming, system architecture, networking, telecommunications, server administration, and system design. While the technical roles in cyber security require expertise in different areas, it is also important to have a basic understanding of the core technical areas in order to have a holistic view of cyber security. Some of the examples of the core technical areas include programming, computer architecture, operating systems, database concepts, data communications and networking, and software system analysis and design. The mastery of technical concepts in online environments can be leveraged with the aid of virtual labs that facilitate opportunities to simulate cyber attacks and defense mechanisms. The employment of virtual labs enables a large number of students to obtain practical exposure to technical competencies required in the cyber security area which can be challenging to offer in traditional environments to a large number of students.

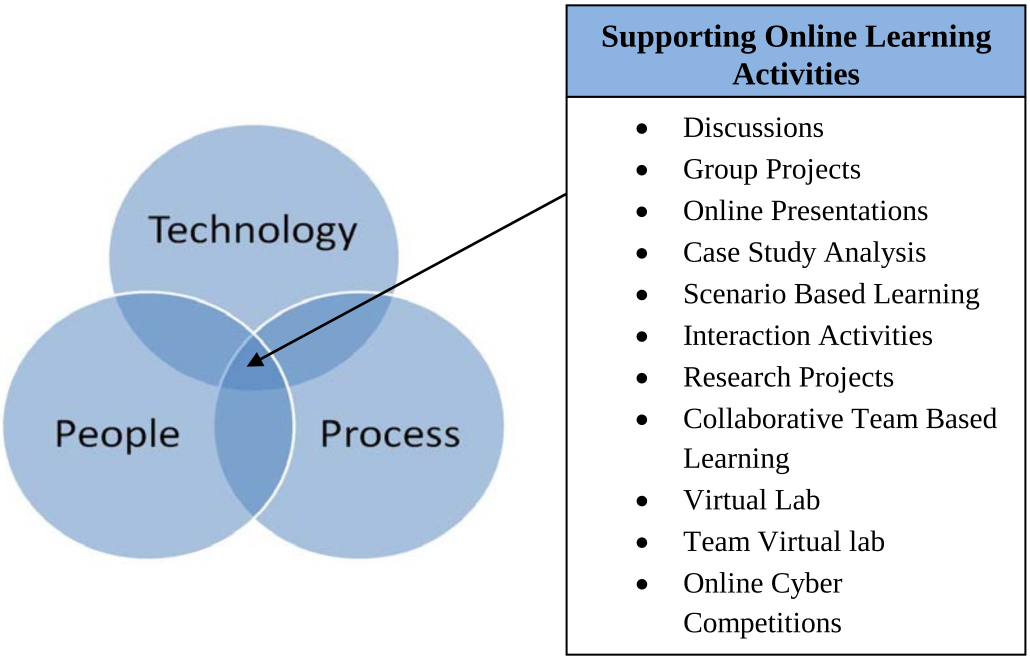
It is important to note that the cyber security profession includes a variety of job titles and the varying roles might require varying levels of interactions with people, process and the technology element. For example, a malware analyst will be more involved with analyzing malware, writing scripts and monitoring security logs in the organization. On the other hand, a security policy officer will be more involved in creating and developing security policies in the organization. Irrespective of the specific role, all cyber security professionals should be required to have proficiency in the three pillars of people, process and technology in the organization, which is why it is important to build these skills among cyber security professionals. Table 2 provides information on aligning the the generally needed skills into each major element. In Figure 3, we present a framework of how online learning activities can be integrated into online cyber security education with the elements of people, process and technology to develop the general skills required in these areas. We further illustrate the online learning activities that support the development of the skills.

4. CONCLUSION

In this we paper we bring forward the numerous challenges in the cyber security field which, among others, include the lack of a skilled workforce to fill the growing demand for cyber security professionals. We also identify the need for education that is flexible and affordable for working professionals. The online environment is identified as an ideal learning environment for working professionals in order to be educated and trained in cyber security. The humanistic perspective on learning is analyzed in order to draw on the advantages of online learning for adults. Additionally, the need for an interdisciplinary approach that focuses on people, process and technology is brought forward and support provided for the application of this approach to cyber security education. The study concludes by identifying the various online methods that can be employed in order to promote an effective interdisciplinary approach to cyber security education.

Table 2: General Required Skills by the Elements

Element	General Skills Desired	
People	• Communication • Management • Collaboration	• Team Work • HCI (Human Computer Interaction) • Criminal Psychology
Process	• Technical Writing • Project Management	• Critical Thinking • Team Work
Technology	• Programming • Computer Architecture • Operating Systems • Data Communications and Networking	• Database Concepts • Computer Security • Security Tools • System Analysis and Design



Supporting Online Learning Activities

- Discussions
- Group Projects
- Online Presentations
- Case Study Analysis
- Scenario Based Learning
- Interaction Activities
- Research Projects
- Collaborative Team Based Learning
- Virtual Lab
- Team Virtual lab
- Online Cyber Competitions

Figure 3: Framework for Cyber security Online Education

5. REFERENCES

[1] Abraham, S. & Chengalur-Smith, I. (2010), "Social Engineering Malware: Trends, Tactics and Implications", Technology in Society, 32 (3), 183-196.

[2] 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.

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

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

[5] Bayuk, L.J., Healey, J., Rohmeyer, P., Sachs, M.m and Schmidt, J. (2012). Cyber Security Policy Guidebook. Hoboken, NJ: John Wiley and Sons

[6] Brookfield, S.D. (1987). Developing Critical Thinkers: Challenge Adults to Explore Alternative Ways of Thinking and Acting. San Francisco, CA: Jossey-Bass

[7] Clarke, A.R. and Knake,K.R. (2010). Cyber War: The Next Threat to National Security and What to Do about It, New York: HarperCollins.

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

[9] Cybersecurity Jobs report (2013). The Abell Foundation and CyberPoint International, LLC. Retrieved from http://www.ctic-baltimore.com/reports/Cyber%20Security%20Jobs%20Report-010813.pdf

[10] Cynthia, E.I. (1997). Computer Security Education Challenges. IEEE Software, (14:5).110–111.

[11] Dodge, C. R., Toregas, C., and Hoffman, L. (2012). , Cybersecurity Workforce Development Directions, Proceedings of the Sixth International Symposium on Human Aspects of Information Security and Assurance.

[12] Ewans, K., and Reeder, F. (2010). A Human Capital Crisis in Cybersecurity. CSIS Commission on Cybersecurity for the 44th Presidency

[13] Hammerstein, J and May, C. (2010). The CERT Approach to Cybersecurity Workforce Development. Technical Report CMU/SEI-2010-TR-045 ESC-TR-2010-110

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

[15] Irvine, E.C. (1997). Computer Security Education Challenges, IEEE Software, (14:5), 110-111. Knowles, M. (1950). Informal Adult Education. Chicago, IL: Association Press.

[16] Knowles, M.S. (1950). Informal Adult Education. New York: Association Press.

[17] Lee, J., Bagchi-Sen, H. Rao, R. and Upadhyaya. (2010). Anatomy of the Information Security Workforce. IEEE IT Professional, (12:1), 14-23.

[18] Locasto, E.M., Ghosh, K.A., Jajodia, S., and 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.

[19] Maxwell, A. (2012), Technological Advancements in Methods of Training with Reference to Online Training: Impact and Issues for Organizations, Journal of Arts, Science & Commerce, (3:2).

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

[21] Milheim, K. L. (2011). The Role of Adult Education Philosophy in Facilitating the Online Classroom. Adult Learning, 22(2). 24-31.

[22] Miller, A. R., and Luse,W., D. (2004), Advancing the IS Curricula: The identification of Important Communication Skills Needed by IS Staff During

[23] Mitnick, K.D., and Simon, W.L. 2002. The Art of Deception: Controlling the Human Element of Security. Indianapolis, IN: Wiley.

[24] Morris, L. (2005) Challenges of Access, Affordability, and Persistence. Innovative Higher Education, (30:3).147-148.Systems Development, Journal of Information Technology Education. (3). 117-131.

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

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

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

[28] Stewart, E,K., Humphries, W., J., and Andel, R., T . (2009). Developing a Virtualization Platform for Courses in Networking, Systems Administration and Cyber Security Education. Proceedings of the 2009 Spring Simulation Multiconference, March 22-27, 2009, San Diego, California.

[29] Tisdell, J. & Taylor, W. (1999). Adult Education Philosophy Informs Practice. Adult Learning, (11:2). 6-10.

[30] The 2013 Global Information Security Workforce Study, A Frost and Sullivan Market Study in Partnership with Booz Allen Hamilton. Retrieved from https://www.isc2.org/GISWSRSA2013

[31] The Economist. (2010a). Data, data everywhere. Retrieved from http://www.economist.com/node/16478792

[32] U.S. Department of Education, Office of Planning, Evaluation, and Policy Development. Evaluation of Evidence-Based Practices in Online Learning: A Meta-Analysis and Review of Online Learning Studies. Washington, DC,2009.

[33] VanDerwerken, J. and Ubell, R. (2011). Training on the Cybersecurity Frontlines, T+D, (65:6). 46-50.

[34] West, R .(2010). A Student's Guide to Strengthening an Online Community. Tech Trends, (54:5). 69-75.

[35] Xu, Z., Hu, Q., and Zhang, C. (2013). Why Computer Talents Become Computer Hackers. Communications of the ACM. (56:4). 64-74.