Journal of Computer Engineering & Information Technology

Research Article

A SCITECHNOL JOURNAL

Examining the Pedagogical Best Practices of Student Mastery of Cyber Security in Higher Education

Abbas Imam*, Samuel Said

Abstract

The intricacy of information security management (ISM) has become a major issue for organizations as Cybercrime is on the rise and cybercriminals are only getting better at what they do. The skills gap is growing between the people who hack and the people who could help protect against cybersecurity vulnerabilities of new technologies, such as drones and autonomous vehicles. As threats that exploit vulnerabilities in our cyber infrastructure grow and evolve, an integrated cybersecurity workforce must be capable of designing, developing, implementing, and maintaining defensive and offensive cyber strategies. The role of higher educational institutions (HEI) preparing students in cyber security workforce development could not have been more important as institutions are finding themselves with the challenge of preparing a workforce for a battle that is apparently hard with which to keep pace. The purpose of this study qualitative research was to determine best practices in cybersecurity competencies and teaching pedagogies in higher education. The study sought to find the best pedagogies being used in cybersecurity programs in institutions designed as Centers of Academic Excellence (CAE) to prepare students. The study also sought to determine specific pedagogical best practices depending upon type of competency. Interviews were conducted with cybersecurity educators from eight (8) colleges and universities in Alabama and Tennessee who are members of the National Centers of Academic Excellence (CAE) program in Cyber Defense (CD). The interviews data collected were kept confidential. The results from this study indicate that while cybersecurity competencies can be achieved through all the four (4) pedagogical themes: hands-on virtual reality online; hands-on with instructor; mixed or blended learning; and flipped classroom learning, hands-on with virtualization led by an instructor stands out as the best pedagogy.

Keywords

Bitcoin, Competency, Cybersecurity, CEA, Cyberterrorism, Digital Age, Education System, Flipped classroom Learning, Hands-on Virtual Reality Online; Hands-on With Instructor; Mixed or Blended Learning, Stakeholders, Vulnerabilities, Workforce

Introduction

At the center of information security is the concept of risk which is encountered by many organizations. While some risks are easily controllable, others can threaten the very survival of the organization [1]. The world faces new threats every moment with the certainty of blooming new technologies that are dynamic in nature. Cybercriminals are only getting better at what they do, which means the skills gap is growing between the people who hack and the people who stop them. Imam [1] stated that in the past numerous organizations took information security threats frivolously, but today threats are well seen as opportunities through which attackers could cripple an organization instantaneously. As cyber threats continue to evolve, the nation's protection against them relies on a steady stream of qualified cybersecurity professionals entering the workforce. Higher education institutions are finding themselves with the challenge of preparing a workforce to stay current with technological developments [2].

All higher education institution faces the demands of cybersecurity realities: An integrated cybersecurity workforce can address the cybersecurity challenges inherent to preparing their organizations to successfully implement aspects of their missions and business processes connected to cybersecurity. An integrated cybersecurity workforce includes technical and nontechnical roles that are staffed with knowledgeable and experienced people.

To keep up with workforce demands over the next decade, it will be imperative for institutions of higher education to keep their fingers on the pulse of competencies and pedagogies to adequately prepare workers to compete in an educationally progressive world. Institutions are cultivating an integrated cybersecurity workforce that is globally competitive from hire to retire and prepared to protect our nation from existing and emerging cybersecurity challenges.

Higher education institutions are facing an explosion of technological threats and a new generation of young people who are addicted to the new technologies, ignoring their consequences that lead to a physical, emotional, psychological, spiritual, and economic hijacking.

Research Questions

The following describes the instrument that was used to answer the two research questions:

Research Question 1: What pedagogies are being used in CAE designated cybersecurity programs to prepare students?

Research Question 2: Are there specific pedagogical best practices depending upon type of competency?

Research Question 3: What factors exist that may either promote or hinder student learning in cybersecurity education?

Description of the Problem

Information security professionals are in demand in both government and private enterprise, and the trend is not expected to change [3]. As the education market exists today, the United States may not be in a position to quickly and adequately train the sizeable security workforce needed to secure critical infrastructure and key resources [4]. In order to meet this increasing need, more cybersecurity degree programs, particularly at the undergraduate level, are required. Currently, only a small number of academic

***Corresponding author:** Abbas Imam, Department of Information Technology, Volunteer State Community College, United States, E-mail: doc.toure13@gmail.com

Received: October 03, 2021 **Accepted:** October 18, 2021 **Published:** October 25, 2021

programs are funded and equipped to formally train cybersecurity professionals, and those few programs cannot train a workforce of thousands in a relatively short period of time [4].

Higher education institutions are slow to change. They cannot simply start offering more courses in cybersecurity. It is not easy to alter a curriculum, especially when you have students who are advanced in the program, with new students entering the program regularly [5]. Curricula are not updated as often as technology changes because of politics, staffing difficulties, and lack of budget. Many factors are at play in program development, but the focus on enabling higher education to provide their students with needed tools to be professionally successful is dynamic [6].

Literature Review

The rapid changes that are taking place in the world of work today call for higher education to play a stronger role in better preparing college graduates to transition into the global economy and to be ready to contribute to the economic bottom line. Colleges and universities are the hubs through which citizens, educators, practitioners, and policymakers reveal the value and significance of the role of higher education in the world today. The essential role that colleges and universities play in students' preparation requires leaders of higher education institutions to accept responsibility for students' post graduate performance [7]. According to Nicholas [8], preparing students for the challenges of the industry is a central role for higher education.

The idea of teaching cybersecurity concepts is not new but started to become more relevant in the 1980s. Forcht [9] related some observations about education and industry where security when she wrote "*Educators have long struggled with the issue of whether to ignore the data security issue in order to avoid opening a Pandora's Box or whether to face the issue head-on in the hope that the students preparing for business or industry will be cognizant of the problem and will be acquainted through college coursework with the basis of approaching and analyzing the situation*" [9-11].

Theoretical Foundations in Adult Learning

Central to human beings is the need to learn. This desire results from a realization that what we are, the environment within which we exist, and what we know are all in a constant state of flux [10]. In the absence of a severe deficiency, stagnation (the inability to advise or develop) is counter to human nature. The ways by which humans understand what learning is, and the ways in which it takes place, are multivariate relative to individual historical context, philosophical tradition, and cultural point of view. The act of learning is the process by which knowledge is acquired [11]. In the course of this study, the researchers explored the interrelationships between these aspects of learning relative to how the study participants, as contemporary learners, engaged in a dynamic field of practice, as they acquired and maintained the competencies perceived as necessary to perform their duties successfully. Theoretical perspectives of adult learning, including experiential learning, situated cognition, and expertise development, were used to create the content of the study.

Experiential Learning: Much of the foundational work on the process of cognitive development was done by Jean Piaget. Although he focused entirely on children, his theory has provided the foundation of work completed with adults [12]. Piaget identified two processes that are employed by individuals who support adaptation: simulation (using or transforming one's environments to relate to prior mental constructs) and accommodation (changing mental constructs to account for, and relate to, changes in the environment). Piaget identified how these processes are used throughout life, simultaneously and alternately, as individuals mature [13].

As a process, learning focuses on what happens when the learning takes place and causes changes that are persistent and measurable by enabling everyone to formulate or revise his or her mental construct over time [14]. Bloom [15] divided the learning process into a hierarchical taxonomy with the six levels shown in Figure 1.

Figure 1 illustrates [15]'s cognitive taxonomy, as revised by Anderson and Krathwohl in 2001. The layers represent the levels of learning with each layer representing increasing complexity. Presented with each layer are sample verbs and products that describe actions or creations at that level of cognitive development.

Situated Cognition: Situated cognition has its roots in anthropology, sociology, and cognitive science and represents a departure from traditional views that learning is behavioral and individualistic to the perspective that it is emergent and social [17,18].

Expertise Development: It is generally accepted that professionals in a chosen field may progress along a continuum from early entrant to a position of recognition as a member of an elite group of practitioners. Traditionally, career progression has resulted by demonstrating the ability to leverage formal, theoretical learning along with firsthand knowledge of the causes and effects of decisions made in the performance of duties and supplemented with self-initiated activities and the insights offered by others [19].

Competency Model Framework

To assist businesses, educators, and workforce development professionals in identifying the industry-specific skills and

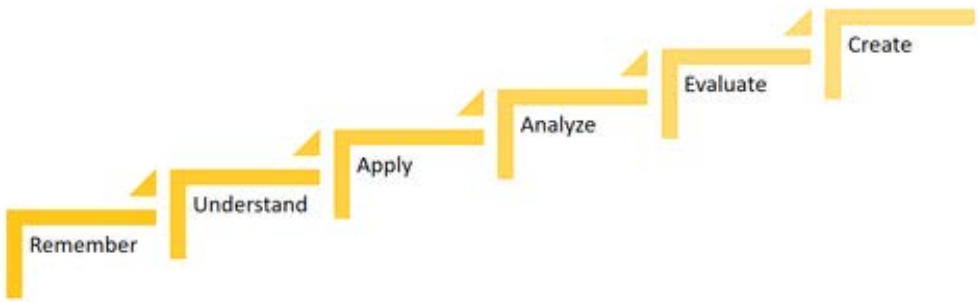

Figure 1: Bloom's hierarchical taxonomy.

competencies that workers will require the U.S. Department of Labor's (DOL) developed Competency Model Clearinghouse public toolkit in an organizing framework on a national level [20]. The framework consists of a set of building blocks arranged into nine tiers containing specific sets of related competencies. The model borrows heavily from the National Initiative for Cybersecurity Education's (NICE) National Cybersecurity Workforce Framework. The framework is designed to provide a common understanding of, and lexicon for, cybersecurity work, and many of the knowledges, skills, and abilities (KSAs) framework and reproduced in the cybersecurity industry model. In the framework, the nine tiers are grouped into three clusters: foundational competencies, industry-related competencies, and occupation-related competencies.

Competencies are recognized by the industry as significant predictors of employee performance and success, which is equally as important as an individual's academic aptitude and content knowledge. A competency is the capability of applying or using knowledge, skills, abilities, behaviors, and personal characteristics to successfully perform critical work tasks, specific functions, or operate in a given role or position. Competencies are the bridge between traditional credit hour measures of student achievement and student learning. For the purpose of this study, a competency was defined as a combination of skills, abilities, and knowledge needed to perform a specific task. Competency-based initiatives are those purposeful actions directed at defining, teaching, and assessing competencies across their programs.

Cybersecurity in Education: Information security analyst is the eighth best job in the United States, according to U.S. News and World Report's Top 100 Jobs in 2015 list. Job openings in the field are expected to increase 36.5% by 2022, and median pay is $88,890 per year, the Bureau of Labor Statistics reported in 2009. However, despite all these benefits, successful hiring in cybersecurity careers is lagging [21]. American employers have realized the importance of cybersecurity, but that realization has created a near-term shortage of workers that may require long-term solutions.

As technology and computing disciplines developed, more time and energy was given towards researching security concepts. In the late 1990s, [22] work explored the idea of providing a lab where students could learn computer science concepts in a quasi-hostile environment. The lab was designed in such a way that as students tested algorithms or operating systems, they did so knowing that Transmission Control Protocol/Internet Protocol snooping could be in use. Prior to September 11, 2001, educators recognized that there that there was a significant lack of security concepts in computing. However, the events of September 11, 2001, triggered a new surge in cybersecurity development in computing education beyond what Yang and others had anticipated [23].

In the United States, the National Security Telecommunications and Information Systems Security Committee (NSTISSC) was established under National Security Directive 42 and re-designated as the Committee on National Security Systems (CNSS) in 2001 and developed a set of standards that accredited national security systems as well as security programs. As reported by Papanikolaou [24], the result is that educators now see a set of expectations that public industries have for cybersecurity professionals. Another contribution to the surge in cybersecurity education development was the result of funding from the National Science Foundation (NSF) for educating professionals in information assurance [25] to entice students to pursue studies in this domain include the Cybercops: Scholarship for Service (SFS) program and the Information Assurance Scholarship Program (IASP) from the Department of Defense.

Even with this effort, researchers are indicating that government officials and industry leaders are not seeing cybersecurity graduates who have problem-solving skills or out-of-the-box thinking abilities [26]. One of the areas of research concerned with cybersecurity education is the improvement of practical hands-on exercises. Cybersecurity courses are appropriate topics for lab-based instruction as many labs are unscripted and open-ended, allowing multiple correct solutions [27]. Others have revealed in research that hands- on experience is essential in order to integrate the topics [28]. Anderson noted that students learn most effectively at the highest levels of analyzing, evaluating, and creating solutions. Experience in these areas makes students better prepared to use the competencies they have in the real world [16].

Methodology

This study involved a case study and qualitative research method to test the hypotheses and answer the research questions. The purpose of qualitative interview, Mason [29] alluded, is not only merely the harvesting of information but the constructing of knowledge in context as well.

Purpose of the Study

The purpose of this study was to examine pedagogical best practices for student mastery of cybersecurity competencies. The researchers needed to know if the conversion of students to professionals was reliant on the course content of higher education institutions. Higher education institutions educate students by providing a curriculum-related theoretical knowledge of each discipline, which may not necessarily align with the requirements of the present-day employers in a highly competitive world [30]. In addition to the knowledge- based pedagogy used in the classroom, it is imperative for the support services in universities, such as career development centers and academic advising centers, to serve as significant partners in enhancing the positive connections between the skills learned by the students in educational institutions to the requirements for skills and competencies of the 21st century workforce.

Cybercrime is on the rise, and the types of attacks are becoming more aggressive, sophisticated, and dangerous. There are more frequent and critical breaches, and there is a trajectory towards attacks on both critical infrastructures and high-profile individuals [31]. The researcher determined the needed pedagogies for Higher Education Institutions (HEI) that would enable students to gain the competencies required to successfully resolve these problems.

Formative Evaluation Materials/Instruments

Within instructional design, the use of formative evaluation ensures that lab activities are delivered efficiently and effectively [32]. The goal of formative assessment is to monitor student learning, allowing for student feedback during the developmental phase, and utilizing it to improve the educational delivery methods [33]. posited that formative evaluation has two primary functions when working with cybersecurity, to examine the educational value and to verify the underlying logic of the exercise [33].

Three stages involved in the instructional design model were outlined by [34]. The first phase of instructional design involves the use of the Subject Matter Expert (SME) and members from the field study. The instructional designer works through the intended

material with the assistance of students, which aids in the discovery of errors in the content. Traditionally instructional designers are not well versed in IT technology studies, so it is up to the SME to provide the most accurate lab materials. Any revisions take place at the end of this phase. The next stage involves a small group evaluation of the instructional material. The instructional designer is an observer in this phase, gathering learners' interactions to the new material. Once created, assessment of the labs occurs to determine if they are compatible with the instructor to finalize additional changes. The final stage of the model involves an actual test in the learning management platform. Implementing the lab into the educational environment examines the feasibility and usability of the design. The instructional designer acts as an observer and undertakes any revisions necessary to create the finished product.

Unfortunately, because of the diversity involved with information technology [35], the steps outlined by [34] are rarely carried through in the design of practical labs used in IT security. As described by [36], universities face a shortage of qualified IT security professionals, which leads to a modified approach to instructional design. Poorly designed computer labs hinder understanding of the security concepts, potentially preventing students from gaining the skills required for the field [37]. Universities that prescribe to the theory only presentation of security materials ultimately impede students' ability to learn the tactile skills required to be an IT security professional. Courses that only offer term papers not only will discourage students, but also these students will find themselves lacking the skills to gain employment [38], suggested four areas associated with a formative evaluation of a computer-based program: the presentation, ease of use, interactive components, and appropriateness to the subject. Evaluating both the written and graphic presentation ensures that the course is readable and appropriate. Providing a learning environment that is easy to navigate, with the directions explicitly available, creates ease of use for the students. Using a variety of interactive components allows for different learning styles, making the content more interesting. Lastly, maintaining the appropriateness of the subject ensures completion of all objectives [38]. Conducted a study that used formative evaluation to measure the effectiveness of a Web-based course by administering questionnaires to students, specifically asking about ease of use and course content. By evaluating ease of use, [32] were able to determine if the navigation hindered student learning. Well-written material and labs allow students to concentrate on the course objectives rather than its presentation. A properly created and executed security lab should increase student knowledge, providing the tactile skills and confidence to understand the subject material.

Research Procedures and Data Collection

In accordance with qualitative research traditions [39], data from multiple sources were collected. Various approaches to data collection have been suggested to ensure the credibility of the data. The type of data collected was in the form of paper notes or memos, online notes, and video files of interviews. The research resulted in numerical data to be downloaded in a variety of formats.

The interviews were used to allow the researcher to get historical and contextual information about the participants' experience in cybersecurity research while controlling the line of questioning [40]. During the interviews, the researcher detached from focusing on the participants [41] and focused attention on the discussed issues for garnering an understanding of the topic [42]. The interviews were recorded so that an accurate record of the participants' views and comments were used in the analysis. Interviewees were provided with an advance copy of the interview protocol. This protocol included heading information about the interview (time, place, participant), as well as the questions to be asked. The ongoing reviews took place to ascertain key facets of the role of cybersecurity professionals.

These examinations provided a broad sense for what the role expectations were at the various levels of proficiency as well as what competencies were required. Care was taken to ensure that the documents examined and used in the course of the study were authentic and relevant to the research purpose [43].

Once the data were collected, the next step was to categorize the information. The objective was to identify any patterns representing concepts the participants represented during the data collection phase. Specific phrases were developed allowing the researcher to categorize the responses, while identifying emergent themes. During this data aggregation phase, subcategories were identified, which were not identified during the initial development of the research project. These subcategories were identified and coded such that this new information was assimilated into the research's findings. The idea presented by [44] was that the method of analysis in a qualitative study is one that evolves based on small increments of investigation throughout data collection. This is the premise on which the analysis of data was performed for this research.

Findings and Discussion

The summary of these pedagogies are as follows:

- Hands-On Labs Virtual Reality Online
- Hands-On Labs with Instructor
- Mixed Learning Methods
- Flipped Classroom Learning

The themes reflect the experiences of the participants and are significant to the phenomenon. The experience using the pedagogy by the participant is the phenomena. Collecting data and information regarding participants' perceptions on cybersecurity pedagogy will help to understand the phenomenon [40]. He also posited that, phenomenological research elucidates the importance of capturing people's shared experiences and the choices made to accomplish personal goals.

The four themes were repeated throughout the context of the interviews. The data collected consisted of six typewritten transcripts. The use of an inductive data reduction process allowed for the summarization of raw data to establish a clear link between the researcher's objectives and findings. The resultant themes center on two primary areas denoted by the participants' remarks: the importance of hands-on labs, and the need for more frequent opportunities to apply their knowledge. The data extracted from each theme indicated that most of the participants agreed that hands-on virtual labs provide valuable skills that apply to the job market. They expressed the need for more hands-on labs to show students how to hone their tactile skills, and to recognize the importance of hands-on labs.

Fourteen questions from the participants' interviews were used to examine the pedagogical best practices of student mastery of cyber security.

The six issues discovered from the interviews provided the following conclusions:

1. Many of the participants mentioned the use of auditory/visual learning, but all indicated kinesthetic as the preferred method of learning.
2. Participants found their students more confident with their knowledge when applying skills using a virtual machine environment.
3. Participants stressed the need for additional hands-on labs, which they would like to start sooner in the course.
4. Participants indicated, in the specific feedback concerning the virtual lab, a common troubleshooting area should be added to the lab instruction.
5. All participants emphasized the usefulness of video lectures, stating that they often referred to them when working with the hands-on virtual labs using a flipped classroom concept.
6. Participants promoted the instructor-led hands-on approach with more detailed problems.

All participants insisted that translating tactical skills into practical, viable labs for cybersecurity students is becoming an essential aspect of the computer security curriculum. The field of cybersecurity is a subset field of information technology (IT), which focuses strictly on any security issues that could lead to the tampering, destruction, or loss of data or information. The goal of all higher education institutions is to provide training to learn how to mitigate potential threats. All participants reported IT security instructor's ability to create and deliver relevant labs is a critical job requirement in producing a well-versed security technologist. Designing labs with tangible lessons provides an environment to enhance conceptual learning and skills. The goal is to produce technologists with industry-comparable skills.

The development, deployment, and distribution of labs can be created to support a community of contribution and reusability [45]. The challenge in providing a reusable platform starts with the supporting operating system or developer software. Are the students able to access the material from anywhere, or does the school have the hardware to support the demand for virtual labs so it does not adversely affect student ability to conduct their experiments? Distributed labs could offer blended learning [46] and allow instructors to create content that would be stored and reused for later classes [45] suggested that the time spent in devolvement and standardizing could alleviate issues with the quality of the course and labs [47].

The researchers believe that the use of hands-on labs in security training can enhance a student's ability to learn a new subject, especially those involving tool usage. With all the delivery methods available, what tools become the best lab delivery method for security students so he or she can gain the skill sets? To teach cybersecurity courses, schools must be equipped with mainstream technology found in the majority of network infrastructures. These cost-prohibitive equipment labs provide the best learning platform for students. Other viable solutions involve the use of virtualization, which can provide an environment similar to the costly labs at a fraction of the cost.

Hands-on labs can be costly, and time restrictive, but provide the best learning environment for students [48]. Creating a practical security lab to conduct live experiments may ultimately improve the student's comprehension concerning security. Cost-effective solutions include many of the open- source platforms such as BackTrack or Kali Linux, designed for digital forensics or penetration testing. Some argue that many live experiments are based strictly on attack and defense techniques instead of allowing students to experience real-world business needs [49]. Instead of using a cyber-war approach, create labs using real scenarios so students can apply the skill to pertinent business tasks.

Conclusions

This study provides the participants' perspective about pedagogies used in cybersecurity classes. It adds to the body of knowledge and addresses a specific concern with teaching cybersecurity to ensure that students achieve the needed competencies using the appropriate pedagogy.

By examining cybersecurity participants' shared experiences with virtualization, the findings show that participants perceived the usefulness of virtual labs in gaining the tactile skills in the field of cybersecurity. Hands-on virtual labs are the results of several years of effort, in which capabilities have evolved as new challenge, and student demands have been identified. However, the struggle needed to replicate any of these environments is significantly less, and as such similar labs could be deployed in a short time frame to meet similar needs at other institutions. The technical challenges are solvable with off-the-shelf technology through securing and isolating lab infrastructure, which requires significant and ongoing effort.

Higher education institutions faced with the challenges of furnishing the facility with all of the needed equipment should review the variety of virtualization software that is available. Virtualization offers a flexible platform used in face-to-face classes or online, as long as the students' computers meet the hardware requirements. There is no definitive information that virtual labs are better than any other lab, but the consensus is that hands-on labs are a necessity. How schools achieve that goal will determine if viable security labs are provided to the students. This study shows that participants have recognized the usefulness of hands-on labs and indicated that their students preferred the virtual lab to straight lecture.

References

1. Imam AH (2014) The Role of Top Leadership in the Management of Organizational Information Security Strategies: Review of Management Innovation and Creativity (RMIC), 7(22).
2. Restuccia D (2015) Job market intelligence: Cybersecurity jobs, 2015.
3. Frost L, Sullivan D (2015) Agents of Change: Women in the Information Security Profession. The ISC2 Global Information Security Workforce Subreport, 2013.
4. Locasto M, Ghosh A, Jajodia S, Stavrou A (2011) The ephemeral legion: Producing an expert cyber-security work force from thin air. Communications of the ACM, 54(1): 129-131.
5. Corps Information Systems Control Officer (2014) Cisco 2014 annual security report. San Jose, CA: Cisco Corps.
6. Bittle S (2015) Demand for cybersecurity workers outstripping supply. Retrieved from Burning Glass Technologies.
7. Bok D (2015) Higher Education in America. Princeton: Princeton University Press. Booz.
8. Nicholas P (2010) Try a little harder.
9. Forcht KA (1986) The Need for Including Data Security Topics in the College Business Curriculum. New York: ACM.
10. Decade of Education for Sustainable Development (2005) Learning to Live Together Sustainably.
11. Kyriacou C (1989) Active learning in secondary school mathematics. British Edu Res J 18(3): 309-318.

12. Jacoby B (1996) Service learning in higher education concepts and practices. San Francisco, CA: Jossey Bass.
13. Huitt W, Hummel J (2006) Educational psychology interactive. Information Security Forum (2011). Information security governance: Raising the game.
14. Merriam SB, Caffarella RS (1999) Learning in adulthood. San Francisco, CA: Jossey-Bass.
15. Bloom BS (1984). Taxonomy of educational objectives: The classification of educational goals. Boston, MA: Allyn and Bacon.
16. Anderson LW, Krathwohl DR (2001) A Taxonomy for Learning, Teaching, and Assessing. New York: Longman.
17. Dewey J (1938) Experience and Education. New York: Collier Books, Macmillan.
18. Lave J, Wenger E, Dewey J (1991) Situated Learning: Legitimate Peripheral Participation. New York, NY: Cambridge University Press.
19. Ausubel DP, Novak JD, Hanesian H (1978) Educational Psychology: A Cognitive View (2nd ed). New York, NY: Holt, Rinehart and Winston.
20. U.S. Department of Labor (2014). Introduction to the tools. Retrieved from Competency Model Clearinghouse.
21. Nelson K (2015) Cybersecurity Jobs Are Hard to Fill. Retrieved from the high Beam research.
22. Mayo J, Kearns P (1999) A secure unrestricted advanced systems laboratory. New York: Special Interest Group ON Computer Science Education.
23. Yang TA (2001) Computer Security and Impact on Computer Science Education. NY: Consortium for Computing Sciences in Colleges. 16(4): 233-246.
24. Papanikolaou AV (2011) A hacker's perspective on educating future security experts. New York: Panhellenic Conference.
25. Yasinsac AJ, Frazier J, Bogdanov M (2002) Developing an Academic Security Laboratory. Washington, DC: Redmond.
26. Endicott-Popovsky B, Popovsky V (2014) Application of pedagogical fundamentals for the holistic development of cybersecurity professionals. ACM Inroads, 5(1): 57-68.
27. Rowe DC, Lunt BM, Ekstrom JJ (2011) The role of cyber-security in information technology education. In Proceedings of the 2011 Conference on Information Technology.
28. Albert R, Contis D, Grizzard J, Owen H (2006) Georgia Tech Information Security Center hands on network security laboratory. IEEE Transactions in Education, 49(1): 82-87.
29. Mason J (2002) Qualitative researching (2nd ed.). Thousand Oaks, CA: Sage.
30. Dua A (2013) Voice of the graduate. Retrieved from McKinsey & Company.
31. Setalvad A (2015) Demand to fill cybersecurity jobs booming.
32. Phelps J, Reynolds R (1999) Formative evaluation of Web-based course in meteorology. Computers & Education, 32(2): 181-193.
33. Flagg B (1990) Formative evaluation for educational technologies. Hillsdale: Lawrence Erlbaum Associates, Publishers.
34. Dick W, Carey L (1996) The systematic design of instruction. New York: Harper Collins College Publishers.
35. Carlson D (2004) Teaching computer security. SIGCSE Bull, 36(2): 64-67. Carlton M (2016) Development of a Cybersecurity Skills. Fort Lauderdale: Nova Southeastern University.
36. Du W, Wang R (2008) A Suite of Instructional Laboratories for Computer Security Education. SEED, 8(1): 1-24.
37. Vaughn RB, Dampier DA, Warkentin MB (2004) Building an information security education program. In Proceedings of the 1st annual conference on Information security curriculum development, 41-45.
38. Oliver R (1996) Measuring users' performance with interactive information systems. Journal of Computer Assisted Learning, 12(2): 89-102 O'Reilly K (2005) Ethnographic Methods. New York: Routledge.
39. Yin RK (2014) Case study research: Design and methods (5th ed.). Los Angeles, CA, Sage.
40. Creswell JW (2008) Research design: Qualitative, quantitative, and mixed methods approaches. Thousand Oaks, CA: Sage.
41. Caldwell K, Atwal A (2005) Non-participant observation: Using video tapes to collect data in nursing research. Nurse Researcher, 13(2): 42-54.
42. Polkinghorne DE (2005) Language and meaning: Data collection in qualitative research. J Counseling Psychology, 52(2): 137-145.
43. Lincoln YS, Guba EG (1985) Naturalistic inquiry. Beverly Hills, CA: Sage. Locasto M, Ghosh A, Jajodia S, Stavrou A (2011). The ephemeral legion: Producing an expert cyber-security work force from thin air. Communications of the ACM, 54(1): 129-131.
44. Corbin J, Strauss A (2008) Basics of qualitative research: Techniques and procedures for developing grounded theory (3rd ed.) Thousand Oaks, CA: Sage.
45. Choppella V, Brahmajosyula VK, Vutpala M, Kole S (2011) Process Models for Virtual Lab Development, Deployment and Distribution. 2011 IEEE International Conference, 14-16.
46. Safar A, Alkhezzi F, (2013) Beyond Computer Literacy: Technology Integration and
47. Curriculum Transformation. College Student Journal, 47(4): 614. Seiler S, Ptasik D, Sell R (2012) Lab Description Language - A framework approach for describing and mediating remote and virtual labs. 194-198.
48. Abu Shanab, S., Odeh, S., Hodrob, R., & Anabtawi, M. (2012). Augmented reality Internet Labs versus hands-on and virtual: A comparative study. Paper presented at the Interactive Mobile and Computer Aided Learning (IMCL), 2012 International Conference.
49. Najjar M (2008) On scaffolding adaptive teaching prompts within virtual labs. Int J Distance Edu Tech, 6(2): 35-54.

Author Affiliation

Top

Department of Information Technology, Volunteer State Community College, United States