Journal of Information Technology Education: Innovations in Practice

An Official Publication of the Informing Science Institute InformingScience.org

JITEiip.org

Volume 18, 2019

ENHANCING STUDENT LEARNING IN CYBERSECURITY EDUCATION USING AN OUT-OF-CLASS LEARNING APPROACH

Hwee-Joo Kam	University of Tampa, Tampa, FL, USA	hkam@ut.edu
Pairin Katerattanakul*	Western Michigan University, Kalamazoo, MI, USA	p.katerattanakul@wmich.edu

* Corresponding author

ABSTRACT

Aim/Purpose	In this study, the researchers investigated whether the out-of-class learning approach could help the students to attain any valuable learning outcomes for cybersecurity learning and could enhance the perceived value of cybersecurity education among the students.
Background	Cybersecurity learning poses challenges for its students to learn a complicated subject matter and the students may be intimidated by the challenging courses in cybersecurity programs. Therefore, it is essential for the faculty members to devise some mechanisms to promote cybersecurity learning to increase its student retention. The mechanism suggested by this study was the out-of-class learning approach.
Methodology	The researchers in this study employed a content analysis and adopted a semiotic method to analyze qualitative data. The researchers also conducted crosstabulation analyses using chi-square tests to detect the significant differences in the emerging learning outcomes from the two different out-of-class learning activities investigated in this study.
Contribution	This study addressed the difficulty of cybersecurity education and proposed a viable mechanism to promote the student learning in such a complicated subject matter.
Findings	For cybersecurity education, the out-of-class learning approach is a viable pedagogical mechanism that could lead the students to several learning outcomes, including connecting them to the real-life scenarios related to the cybersecurity profession, guiding them to their career choices and development, stimulating

Accepting Editor Krassie Petrova │ Received: October 8, 2018 │ Revised: January 4, 2019, February 8, 2019 │ Accepted: February 10, 2019.

Cite as: Kam, H-J. & Katerattanakul. P. (2019). Enhancing student learning in cybersecurity education using an out-of-class learning approach. *Journal of Information Technology Education: Innovations in Practice, 18,* 29-47. https://doi.org/10.28945/4200

their intellectual growth, creating their justification of learning, and raising their cybersecurity awareness.

Recommendations for Practitioners The instructors of any cybersecurity programs should incorporate some out-of-class learning activities into the courses in their programs, especially the introductory-level courses. Additionally, it is important to coordinate the out-of-class learning activities with the in-class lessons to enable the students to justify what they have learned in their classrooms and motivate them to learn more.

Recommendation for Researchers Researchers could look beyond in-class learning and laboratory learning to investigate the impacts of out-of-class learning activities on cybersecurity education to help the students to attain better learning outcomes.

Impact on Society By promoting cybersecurity education, universities and colleges could attain a higher retention rate of the students in their cybersecurity programs. The higher retention rate of the students in cybersecurity programs would help to ease the critical shortage of cybersecurity talent.

Future Research Future research could explore the impacts of other out-of-class learning activities on cybersecurity learning; for example: job shadowing, attending cybersecurity conferences, internship, developing cybersecurity systems or tools for actual customers, working on cybersecurity research with faculty members. Additionally, future studies could investigate the effects of the out-of-class learning approach on promoting other academic programs that are characterized by intensely complex and technical nature, similar to cybersecurity programs.

Keywords cybersecurity education, out-of-class learning, learning outcomes

INTRODUCTION

Currently, we are facing the pressing issue of the shortage of cybersecurity talent in both private and public sectors worldwide (Executive Office of the President, 2016; Zadelhoff, 2017). On the other hand, cybersecurity learning poses challenges for its students (Saunders, 2002) to learn a complicated subject matter (Yurcik & Doss, 2001) and thus requires the persistence of the learners. Unfortunately, the students who are "testing the water" may be intimidated by the challenging courses in cybersecurity programs.

It was reported that the dropout rates of the students in information technology programs and in computer science programs were higher than those in other programs (Beaubouef & Mason, 2005; Lang, McKay, & Lewis, 2007; Soh, Samal, & Nugent, 2007). Accordingly, this study argued that the attrition rate of the students in cybersecurity programs would be high as well. Therefore, to improve the attrition rate of the students in cybersecurity programs and ease the critical shortage of cybersecurity talent, it is essential for the faculty members of any cybersecurity programs to devise some mechanisms to promote cybersecurity education. The mechanism suggested by this study was the out-of-class learning approach. The out-of-class learning approach could produce several valuable learning outcomes, including knowledge and subject matter competence, cognitive skills and intellectual growth, psychosocial changes, attitudes and values, moral development, educational attainment, career choice and development, economic benefits, and quality of life after college (Kuh, 1993).

In previous studies related to cybersecurity education, some researchers highlighted the implementation of cybersecurity education in higher education (Conklin, Cline, & Roosa, 2014; Dark & Mirkovic, 2015; Schneider, 2013), while other researchers investigated cybersecurity learning by using simulation (Nagarajan, Allbeck, Sood, & Janssen, 2012; Pastor, Díaz, & Castro, 2010) or discussed the effect of cybersecurity competitions on student learning (Mirkovic, Tabor, Woo, & Pusey, 2015; Tobey, Pusey, & Burley, 2014).

With the exception of the studies on cybersecurity competitions, there has been no literature discussing the impacts of the out-of-class learning approach on cybersecurity learning. There is very little evidence that demonstrates whether the out-of-class learning approach is a viable mechanism for helping the students to attain valuable learning outcomes, promoting cybersecurity learning, enhancing the perceived value of cybersecurity education, and improving the retention rate of the students in cybersecurity education.

Hence, this study filled in the gap by investigating the effectiveness of the out-of-class learning approach on cybersecurity learning. Specifically, the researchers in this study examined whether the out-of-class learning approach could help the students to attain any valuable learning outcomes for cybersecurity learning and could enhance the perceived value of cybersecurity education among the students. The research findings would suggest whether the out-of-class learning approach should be used to improve student engagement in cybersecurity learning. High student engagement would help to increase the student retention for cybersecurity programs.

THEORETICAL FRAMEWORK

CYBERSECURITY EDUCATION

The U.S. National Initiative for Cybersecurity Education (NICE) proposes that cybersecurity education should encompass the core knowledge consisting of securely provision (SP) (i.e., securing IT infrastructure), operate and maintain (OM) (i.e., system administration), oversee and govern (OV) (i.e., leadership and management of information security), protect and defend (PR) (i.e., mitigating cyber threats), analyze (AN) (i.e., specialized reviews of IT infrastructure for cyber intelligence), collect and operate (CO) (i.e., adopting deception operation for developing cyber intelligence), and investigate (IN) (i.e., investigating cybercrimes through digital forensic) (Newhouse, Keith, Scribner, & Witte, 2017). Accordingly, this NICE framework implies that cybersecurity education incorporates the technical learning that requires a high cognitive capacity to master the complex concepts of software and network security. Additionally, cybersecurity education involves the analytical learning that demands a specialized skill to evaluate a high volume of data. Moreover, cybersecurity education includes the managerial learning that links technical knowledge to management's decision-making.

Overall, cybersecurity education is multidisciplinary, relying on computing infrastructure, policies, and people (Kessler & Ramsay, 2014). Cybersecurity education encompasses psychology, sociology, politics, law, computer science, computer engineering, and management (Davis & Dark, 2003). This multidisciplinary nature is reflected in real life. For example, cyberattacks in the present days do not only limit to website defacements but also involve targeting specific organizations, industries, or nations to destroy infrastructure, steal intellectual property, or disrupt the economy motivated by political agenda. With such a complicated subject matter, the learners may experience some difficulties to grasp the multi-faceted, complex concepts of cybersecurity (Saunders, 2002; Yurcik & Doss, 2001).

Because of the high attrition rates of the students in information technology programs and in computer science programs (Beaubouef & Mason, 2005; Lang et al., 2007; Soh et al., 2007) and the challenges in cybersecurity education (Saunders, 2002; Yurcik & Doss, 2001), the researchers of this study argued that the attrition rate of the students in cybersecurity programs would be high as well. Unfortunately, the challenges in cybersecurity education and the presumably high attrition rate of the students in cybersecurity programs do not help to ease the pressing issue of the shortage of cybersecurity talent in both private and public sectors worldwide (Executive Office of the President, 2016; Zadelhoff, 2017).

Out-of-class Learning Approach and College Impact Approach

The assessment of student learning in colleges usually focuses on academic aspects including classrooms, laboratories, studios, libraries (Kuh, 1993). However, some studies suggested that learning well in classrooms does not necessarily translate into doing well outside the classrooms (Resnick, 1987), primarily because in-class learning may be insufficient to prepare the students for real-world challenges.

On the other hand, the out-of-class learning approach encourages the students to transcend the formal classroom, studio, or laboratory settings so that the students can involve the out-of-class learning activities related to their course works. In particular, Kuh posited that:

"Out-of-class experiences presented students with personal and social challenges, encouraged them to develop more complicated views on personal, academic, and other matters, and provided opportunities for synthesizing and integrating material presented in the formal academic program (classes, laboratories, studios)" (Kuh, 1995, p. 146)

Unlike in-class learning identified by symbol-based learning (e.g., conceptual learning of disaster recovery), out-of-class learning openly connects to events and objects in the physical worlds (e.g., how organizations safeguard sensitive data using disaster recovery approach) (Resnick, 1987). Out-of-class learning entails the educational activities that empower the students to interface with and learn about the real-life application (Pearson, 2004). These out-of-class learning activities include, for example: volunteer work, internship, service learning, conducting research with faculty, academic-based peer relationship, involvement in campus organizations, and other co- and extra-curricular activities (McKinney, Saxe, & Cobb, 1998).

In this study, the researchers contended that the out-of-class learning activities for cybersecurity education may include the research project about the real-life incidents of hacking, the interaction with some cybersecurity professionals such as FBI Infragard representatives or banking compliance officers, and the assignments that require solving the real-world problems related to cyber intelligence analysis.

The results of some studies suggested that the out-of-class learning approach could promote student development in college settings (Goodman, 2007; McKinney et al., 1998) and enhance student learning in some disciplines such as sociology (McKinney et al., 1998), outdoor and leadership (Hattie, Marsh, Neill, & Richards, 1997), and language (Guo, 2011; Pickard, 1996).

Additionally, the college impact approach has been used to study what happens (i.e., changes, impacts, or outcomes) to the students during their college years (Pascarella & Terenzini, 1991). This approach focuses less on the internal psychological processes associated with dimensions of change but more on the external environmental and sociological conditions and origins of change (Pascarella & Terenzini, 1991). This approach emphasizes the interactions between the students and the broadly conceived institution's environments (Kuh, 1993). The college impact approach was employed to discover 14 learning outcomes (as shown in Table 1) that college students associated with out-of-class learning (Kuh, 1993).

Given the multidisciplinary nature (Kessler & Ramsay, 2014) and the challenges of cybersecurity learning (Saunders, 2002; Yurcik & Doss, 2001), it is vital to introduce cybersecurity learning as a process where the learners can learn through interactions with the real world as interacting with the real world would enable cybersecurity learners to acquire the first-hand knowledge that promotes cybersecurity learning. That is, the researchers of this study suggested that the out-of-class learning approach could produce valuable learning outcomes for cybersecurity learning and promote cybersecurity education.

Unfortunately, there has been no literature discussing the impacts of the out-of-class learning approach on cybersecurity learning, except the studies on cybersecurity competitions (Mirkovic et al., 2015; Tobey et al., 2014). Cybersecurity competitions seem like a promising tool to boost engagement and attract novices to cybersecurity field; however, the structure and difficulty of cybersecurity competitions may also scare away novices (Mirkovic et al., 2015). Thus, there is very little evidence that demonstrates whether the out-of-class learning approach is a viable mechanism for helping the students to attain valuable learning outcomes, promoting cybersecurity learning, enhancing the perceived value of cybersecurity education, and improving the attrition rate of the students in cybersecurity programs.

Table 1. Learning Outcomes from Out-of-Class Learning (Kuh, 1993)

LEARNING OUTCOMES	EXAMPLES
Practical competence	organizational skills such as time management, budgeting, dealing with systems and bureaucracies
Vocational competence	acquiring attitudes, behaviors, and skills related to post-college employment
Self-awareness	self-examination, spirituality
Autonomy and self-directedness	decision making, taking initiative and responsibility for one's own affairs and learning, movement from dependent to independent thinking
Confidence and self-worth	esteem, self-respect
Social competence	capacity for intimacy, working with others, teamwork, leadership, dealing with others, assertiveness, flexibility, public speaking, communication, patience
Reflective thought	critical thinking, ability to synthesize information and experiences, seeing connections between thinking and experiences, seeing different points of view, examining one's own thinking
Knowledge application	relating theory to practice and using skills learned in the classroom, laboratory, library, and so on in other areas of life, such as using political science theory and research methods when working in a law office
Knowledge acquisition	academic and course-related learning, content mastery
Academic skills	learning how to study, to write, to conduct independent research
Altruism	interest in the welfare of others, awareness of and empathy and respect for needs of others, tolerance and acceptance of people from racial, ethnic, cultural and religious backgrounds different from one's own
Esthetic appreciation	appreciation for cultural matters as in the arts, literature, theater, esthetic qualities of nature
Sense of purpose	clarifying life goals and the work one will do after college, sometimes by discovering what one is not well suited to do
Others	such concepts as movement from conservative to liberal attitudes or vice versa, change in physical features, growing apart from a spouse, and so on

Hence, this study filled in the gap by investigating the effectiveness of the out-of-class learning approach on cybersecurity learning. Specifically, in this study, the researchers examined whether the out-of-class learning approach could produce any valuable learning outcomes for cybersecurity learning and could enhance the perceived value of cybersecurity education among the students.

RESEARCH METHODOLOGY

THE STUDY AND THE PARTICIPANTS

Cybersecurity learning poses challenges for its students (Saunders, 2002) and requires the persistence of the learners; unfortunately, the students who are "testing the water" may be intimidated by these challenges and requirement. Thus, in this study, the researchers focused on the novices; that is, the researchers examined whether the out-of-class learning approach used in an introductory-level course of a cybersecurity program could help the students in this course to attain any valuable learning outcomes and could enhance the perceived value of cybersecurity education among the students.

This study was a qualitative study conducted at a student-centered public university in the Midwest region of the United States. Additionally, this study was exempt from the policy for the protection of human subjects in research as described in 45 CFR 46.101(b)(1). That is, this study was the research on the effectiveness of or the comparison among instructional techniques, curricula, or classroom management methods. In this study, two out-of-class learning group projects were integrated into the regular classroom settings and then the data were collected from two class sessions (i.e., Session A and Session B) teaching "Introduction to Cybersecurity" course in Spring 2016. Session A had 21 students and Session B had 16 students. Both sessions were taught by the same instructor using the same syllabus, lectures, assignments, exams, and delivery method.

None of the students in both sessions had taken any cybersecurity course before this study; so, this "Introduction to Cybersecurity" course was their first course related to cybersecurity. Additionally, in each session, only one student was in criminal justice major and the rest of the students were in cybersecurity major. Furthermore, there were two female students in each session. The average age of the students in Session A and Session B was 25 years old and 21 years old respectively.

The students in each session were randomly arranged into six groups. Each group had two to four students. Each group in Session A was required to work on the out-of-class learning group project that involved interviewing a cybersecurity professional. One cybersecurity professional was randomly assigned to each group in this session. On the other hand, each group in Session B was required to work on the out-of-class learning group project to research a cybercrime topic. Similarly, one cybercrime topic was randomly assigned to each group in this session. Table 2 provides the details of the group assignment for each session.

In Session A, the students in each group had to find the information about the interviewee and were required to prepare the questions for the interview. The interview was recorded after the group received the permission from the interviewee. Then, upon completing the interview, the students had to prepare their group report of the interview. On the other hand, the students in each group in Session B had to prepare their group report providing an overview of the assigned cybercrime topic, at least two real-life incidents of the cybercrime (including the timelines and other details of the two cybercrime incidents), how to prevent the cybercrime, and the negative impacts of the cybercrime on the society.

DATA COLLECTION AND ANALYSIS

Upon completing their out-of-class learning group projects, the students in both sessions were asked to provide their written feedback explaining any learning experiences they may gain from their out-of-class learning group projects. Particularly, the students were asked to share their views about how their out-of-class learning group projects benefited them. The students were also encouraged to share any comments or suggestions they may have regarding their out-of-class learning group projects. Furthermore, the students were asked to describe whether their out-of-class learning group projects led them to perceive the value of cybersecurity education higher. Altogether, this study collected more than 70 pages of written feedback from the 21 students in Session A and more than 50 pages of written feedback from the 16 students in Session B.

Table 2. Group Assignment

GROUP	SESSION A: CYBERSECURITY PROFESSIONAL INTERVIEW PROJECT	SESSION B: CYBERCRIME RESEARCH PROJECT
Group 1	*Interviewee:* Head of Cybersecurity at a Fortune 500 company *Expertise:* application security, security policies and procedures, leadership	Cyberstalking
Group 2	*Interviewee:* IT Security Professional at a local company *Expertise:* mobile devices security, SSL creation and management, and single sign-on	Medical Identity Theft
Group 3	*Interviewee:* Network Security Engineer at a large architectural firm *Expertise:* disaster recovery, risk management, and vulnerability analysis	Online Banking Fraud
Group 4	*Interviewee:* Digital Forensic Consultant *Expertise:* digital recovery, digital forensic, and Xbox hacking	Phishing /Crimes Committed over Social Network
Group 5	*Interviewee:* Senior Fellow for Homeland Security and Defense Issues at Washington, D. C. *Expertise:* cyberterrorism, cybersecurity, and homeland security.	Illegal Hacking
Group 6	*Interviewee:* Director of Information Systems at a local county *Expertise:* business continuity planning, policies compliance, and cybersecurity management	Denial of Service attack

The researchers of this study analyzed the collected written feedback by using a content analysis. A content analysis is a research methodology that makes valid inferences from text and can be used for many purposes; for example: coding open-ended questions in surveys, identifying the intentions and other characteristics of the communicator, determining the psychological state of persons or groups, describing attitudinal and behavioral responses to communications (Weber, 1985). In a content analysis, data are read and categorized into concepts that are suggested by the data rather than imposed from outside (Agar, 1980).

The central idea in a content analysis is that the many words of the text are classified into much fewer content categories (Weber, 1985). As one objective of this study was to examine whether the students experienced any learning outcomes from participating in the out-of-class learning projects, the researchers of this study adopted the 14 learning outcome categories (see Table 1) as the framework for the data analysis in this study.

In classifying words of the text into content categories, researchers must make two fundamental decisions; that is, whether the categories are to be mutually exclusive and how narrow or broad the categories are to be (Weber, 1985). The learning outcome categories were not mutually exclusive as the same written feedback may imply more than one learning outcome; for example:

"My interest was raised as a result of the project....One of the areas I'm most interested in is cryptography, so the focus on SSL and TLS in the interview was thought-provoking."

This written feedback could imply that this particular student developed more interest and curiosity (i.e., intellectual growth – the knowledge acquisition learning outcome) in cryptography and may pursue his career in this area (i.e., career goal – the sense of purpose learning outcome).

On the other hand, each learning outcome category adopted in this study was somewhat broad; that is, each learning outcome may include several different examples (see Table 1). Additionally, the students could express the same learning outcome in many ways using many different words; for example:

"Before the interview, I am not sure that there are many cybersecurity positions available in [this region]. But, with the expanding mobile field, and the numerous threats to come, maybe my fears will be laid to rest."

"After the interview, I learned that I shouldn't ever have to worry about job opportunities because the job market in the field is growing and will continue to grow."

The two students in this example expressed that the in-class lessons taught them the skills that the job market was looking for and they had made the correct choice in deciding to study cybersecurity (i.e., learning justification – the confidence and self-worth learning outcome).

In the collected written feedback, the students may describe each learning outcome category by using one, several, or many words. The words, phrases, or other units of text describing the same learning outcome were presumed to have similar meanings and this similarity may be based on the precise meaning of the words or the shared similar connotations (Weber, 1985). Thus, a semiotic method (Maasik & Solomon, 2012, p. 9-12) was adopted to analyze the collected written feedback in this study.

A semiotic method supports the analysis of signs and symbols (Manning & Cullum-Swan, 1994). It pertains to the meaning of signs and symbols that could be categorized into main conceptual categories (Myers, 1997). Everyone is already adopting a semiotic method and practicing sophisticated semiotic analyses every day; for example, reading any text is an act of semiotic decoding (words and even letters are signs and symbols that must be interpreted), but so is figuring out just what a friend means by wearing a particular shirt or dress (Maasik & Solomon, 2012). A semiotic method facilitates a richer analysis of text (Manning & Cullum-Swan, 1994) and, based on a semiotic method, researchers could employ a content analysis to draw inferences from words and signs in the text (Myers, 1997).

The researchers of this study analyzed the collected written feedback in a face-to-face manner. They started by reading the written feedback and then discussed the meanings of the written feedback in relating to the 14 learning outcomes (see Table 1). For instance, in the following examples of the collected written feedback, the researchers agreed and interpreted that the students referred to their career choices; thus, the "career goal" learning outcome occurred.

"It helped me to understand different aspects of my career… [and] realize that there is a medical relation to hacking so healthcare security is something I can look into for my future career."

"Before our interview, I was kind of interested in the business and government aspect of cybersecurity. Now after the interview, I'm very interested in both; more so toward the government aspect. I am keenly interested in developing well developed cybersecurity laws that are not limiting, but are more flexible and able to adjust to future developments and may assist victims without chastising them."

"[This project] has shown me different avenues of cybersecurity that I hadn't been aware of and made me refine some of my original cybersecurity goals. I wasn't exactly sure of the field before, but realize that there are a couple specific areas that I would like to pursue."

When any interpretation differences arose in the analysis of the written feedback, the researchers in this study resolved these differences by finding common ground. The researchers also agreed to revisit these differences after analyzing all collected written feedback. In those studies where a consensus among observers or raters is required, interrater reliability may be used to correlate the observations or scores of the raters and render an index of how consistent their ratings are (Cooper & Schindler, 2000). However, as the researchers of this study worked together in a face-to-face manner and discussed with each other to find common ground, the interrater reliability was not calculated. Additionally, working together in a face-to-face manner would allow the researchers of this study to avoid any potential biases each of them may have when analyzing the collected written feedback.

Additionally, the best content analytic studies should utilize both qualitative and quantitative operations on text (Weber, 1985). Thus, how frequently each learning outcome category occurred was recorded. The categories that occurred regularly would be identified as the emerging learning outcomes from the out-of-class learning projects. That is, if the occurrences of a particular learning outcome category were relatively high (i.e., occurring in seven or more students), this learning outcome category would be identified as an emerging learning outcome from the out-of-class learning projects. The frequencies of each emerging learning outcome for both class sessions were recorded. Then, crosstabulation analyses using chi-square tests were conducted to detect any significant differences in the frequencies of the emerging learning outcomes between the two class sessions.

A chi-square test is probably the most widely used nonparametric test of significance and it is particularly useful in the tests involving nominal data (Cooper & Schindler, 2000). Typical are cases where persons, events, or objects are grouped into two or more nominal categories. Researchers could use this technique to test for significant differences between the observed distribution of data among categories and the expected distribution based on the null hypothesis (Cooper & Schindler, 2000).

In this study, the students were also asked to describe whether the out-of-class learning projects led them to perceive the value of their cybersecurity education higher. Then, the students' responses were analyzed by using a content analysis based on a semiotic method as well. In the analysis of the perceived value of cybersecurity education, the students' responses were classified into two groups – the responses expressing enhanced perceived value and the responses not expressing enhanced perceived value. The frequencies of each group for both class sessions were recorded. Then, another crosstabulation analysis using a chi-square test was conducted to detect any significant differences in the frequencies of each group between the two class sessions.

Results

The following subsections present the analysis results. These results suggested five emerging learning outcomes (based on the 14 learning outcomes used as the framework for the data analysis in this study, see Table 1): career goal (i.e., sense of purpose), real-life professional (i.e., vocational competence), intellectual growth (i.e., knowledge acquisition), learning justification (i.e., confidence and self-worth), and cybersecurity awareness (i.e., self-awareness). Additionally, the last subsection presents the analysis results related to the enhanced perceived value of cybersecurity education.

Career goal

Out of the 21 students in Session A, 16 students (76.2%) posited that the cybersecurity professional interview project provided them with a sense of purpose that helped them to realize their career goals. Hence, "Career Goal" emerged as a student learning outcome. For example, some of these students stated that:

"Despite the fact that [the interviewee] is a consultant and I want to actually be a cop, she gave me a good picture of what to expect, what to do and who to talk to. She was knowledgeable about both sides: computers and law enforcement. She advised me on whom to ask and offered numerous ways to achieve my desired career. I greatly appreciate that and the insight she offered into the digital forensics field."

"Before our interview, I was kind of interested in the business and government aspect of cybersecurity. Now after the interview, I'm very interested in both; more so toward the government aspect. I am keenly interested in developing well-developed cybersecurity laws that are not limiting, but are more flexible and able to adjust to future developments and may assist victims without chastising them."

"[This project] has shown me different avenues of cybersecurity that I hadn't been aware of and made me refine some of my original cybersecurity goals. I wasn't exactly sure of the field before, but realize that there are a couple specific areas that I would like to pursue."

In the same token, nine out of the 16 students in Session B (56.3%) mentioned that the out-of-class cybercrime research project made them realize their career goals. For example, some of the students in this session stated that:

"I believe this group project helped me [to see that] if I do not get a job in law enforcement and decide to go into a homeland security profession I will have a strong background of [cybersecurity]."

"It helped me realize what type of security I wanted to go into and security type of computers. I would like to go into penetration testing or tracking of the networks that have been hacked."

"It helped me to understand different aspects of my career… [and] realize that there is a medical relation to hacking so healthcare security is something I can look into for my future career."

Real-life profession

From the 21 students in Session A, 17 students (81.0%) stated that the interview project shed light on the real-life cybersecurity profession. That is, the students realized the learning outcome related to vocational competence. For example, some of these students mentioned that:

"Classes and books about cybersecurity are informative, but it is very interesting to get a peek into the day-to-day world of a security professional…[The interviewee] spreads most of his working time between reviewing projects for security concerns and keeping up with current security knowledge. It is the latter that consumes most of his free time."

"[The interviewee] was asked to explain the interplay between government and the private sector in relation to [the] critical infrastructure and he admitted that it is a work in progress with some higher priorities on some industries than others... [The interviewee] also admitted that the most valuable lesson he has learned about cybersecurity is that the legal and regulatory issues are much harder 'nuts to crack' than the technical ones."

"Through this project I was able to get a better understanding of the demands of the modern cybersecurity professional, as well as the current threats that face them every day. I had always had a feeling that most IT personnel were a jack of all trades, so to speak, but this confirmed that even further. [Our interviewee] is asked to do scripting, employee training, data redundancy implementations, among other things on an almost-daily basis."

In contrast, none of the students in Session B suggested that the cybercrime research project provided any insight into the real-life cybersecurity profession.

Intellectual growth

Results of the content analysis discovered that intellectual growth was another emerging learning outcome. In the context of intellectual growth, the students from both sessions showed that their out-of-class learning projects had increased their interests in cybersecurity and thus they would like to acquire more knowledge related to cybersecurity. From the 21 students in Session A, 14 students (66.7%) suggested that the interview project helped them to increase their intellectual curiosity about cybersecurity. For example:

"This interview project did raise my interest and curiosity in cybersecurity. Penetration testing is something I'm very interested in. Every operating system has bugs and I grow a very big interest in being able to exploit them"

"My interest was raised as a result of the project....One of the areas I'm most interested in is cryptography, so the focus on SSL and TLS in the interview was thought-provoking."

"Not only was the information that my group learned and researched interesting but so was all the information the rest of the groups presented. It highlighted areas that I'm not well versed in which sparked my interest in learning more about them."

Similarly, 13 out of the 16 students in Session B (81.3%) mentioned that the cybercrime research project raised their intellectual curiosity about cybersecurity. For example:

"It made me more curious on what you can do to protect yourself or you can do to prevent attacks from happening to you. I also like learning how to do all of the hacking and stuff it is very interesting."

"After the [group project] I feel more interested in cybersecurity subjects….I will probably end up doing some research on my own to find out more about the topics I was very interested in."

"This project definitely sparked my interest in learning more about cybersecurity. I have realized that there is an endless amount of concepts and things to learn about the field. I am looking forward to learning more next semester."

Learning justification

The analysis results suggested another emerging learning outcome related to justification of learning. Some of the students participating in this study gained the confidence and self-worth that the lessons they learned in the classrooms would be useful and relevant to their cybersecurity profession. That is, seven of the students in Session A, but none of the students in session B, suggested that they developed the justification of learning. For example, some of these seven students revealed that a peek into the cybersecurity profession made them realize that the in-class lessons taught them the sought-after skills.

"The work that we do here at [the class] directly corresponds to tasks that a cybersecurity professional might carry out. Whether it is using the command line to diagnose a networking problem, or preparing an entire enterprise for disaster recovery, the skills we are learning today are helping us to prepare for a future in cybersecurity."

"[The interviewee] confirmed that the majority of what we are currently learning, [the interviewee] utilizes in his current workplace, or has utilized, seeing as he's pretty much 'top-dog'."

"[The interviewee] also said that he had seen some network administrators that had no command line skills and really shouldn't have been the network administrators in the first place. So, the Command line we learn so far does payoff"

Additionally, part of the learning justification came from the students' beliefs that they would have many job opportunities upon graduation.

"Before the interview, I am not sure that there are many cybersecurity positions available in [this region]. But, with the expanding mobile field, and the numerous threats to come, maybe my fears will be laid to rest."

"After the interview, I learned that I shouldn't ever have to worry about job opportunities because the job market in the field is growing and will continue to grow."

"At times I wonder if I made the right choice but after interviewing [the interviewee] I see more and more that I did make the right choice…I know I could get a job…"

Cybersecurity awareness

Furthermore, nine students in Session B and two students in Session A posited that, upon completing their out-of-class learning projects, they learned the danger of cybercrime and how to protect their personal data. That is, these students developed their self-awareness about cybersecurity and thus cybersecurity awareness emerged as another student learning outcome. For example, some of the students stated that:

"..Illegal hacking...is a topic that I now believe everyone should be aware of because it can affect anybody and anytime. By doing this research it makes me think more about how I can protect my personal information better, especially online"

"I never would have thought that seemingly unimportant information such as my hometown and family relations could make my facebook profile more vulnerable for cybercrimes such as phishing...Needless to say, I made some minor chang-

es to my Facebook profile and security choices after finding out my settings were not as secure as I had originally thought."

"I learned a lot about Online Banking Fraud...The two examples that we found, the one stole $100,000 and the other stole $150,000!...I also had no idea that a hacker could get your information so easily...Hackers can get my information without even breaking a sweat. It definitely made me want to change my passwords more often and to check my online banking statements more too."

Enhanced perceived value of cybersecurity education

Majority of the students from both sessions expressed that their out-of-class learning projects did not change their perceived value of cybersecurity education. Specifically, 19 out of the 21 students (90.5%) in Session A stated that their perceived value of cybersecurity education was not changed, but they appreciated their out-of-class learning experiences. For example:

"Not in any particular way really. It was very cool that we were given the honor of speaking to someone so high up in the IT Security field when this is just the beginning of our college career…"

"Not exactly, I knew cybersecurity was pretty broad and this project showed that through what each group presented. It definitely helped me learn more about it though."

"No it didn't change my perception of [the cybersecurity program]. It was nice however to talk to someone in the industry. He was very helpful."

Likewise, 14 out of the 16 students (87.5%) in Session B mentioned that the out-of-class learning project did not affect their perceived value of cybersecurity education. Nonetheless, their out-of-class learning experiences increased their knowledge about cybersecurity. For example:

"No it didn't. I only learned a different aspect of [cybersecurity] program. It was a very informative project."

"No I knew [the program] was good. I just had no idea how good [the program] really was but now I know"

The students also posited that they had already formed a preconceived notion about the cybersecurity program and that the out-of-class learning experiences did little to change their perception; nevertheless, their out-of-class learning experiences enhanced their understanding of the program. For example:

"This interview project did not change my perspective of the cybersecurity. The reason for this is the fact that I think highly of this program. But now I learn that this program provides the skills and information need to protect the national security and a company's infrastructure."

"I don't think it changed my perception per say because I always knew [the university] had a very good program. It did make me realize how thorough our education and experience will be when we graduate because we seem to learn about all aspects relating to the field."

The analysis results showed that many students attained at least one of the five emerging learning outcomes (see Table 3). That is, from both sessions and across the five emerging learning outcomes, on average 46.1% of the students posited that the out-of-class learning projects helped them to attain some of the five emerging learning outcomes. Similarly, on average only 11.0% of the students from both sessions stated that the out-of-class learning projects enhanced their perceived value of cybersecurity education.

Table 3. Emerging Learning Outcomes and Enhanced Perceived Value

EMERGING LEARNING OUTCOMES / ENHANCED PERCEIVED VALUE	SESSION A: INTERVIEW PROJECT (N = 21)	SESSION B: CYBERCRIME RESEARCH PROJECT (N = 16)
Career Goal	16 (76.2%)	9 (56.3%)
Real-Life Profession	17 (81.0%)	0 (0%)
Intellectual growth	14 (66.7%)	13 (81.3%)
Learning Justification	7 (33.3%)	0 (0%)
Cybersecurity Awareness	2 (9.5%)	9 (56.3%)
	Overall average: 46.1%	
Enhanced Perceived Value	2 (9.5%)	2 (12.5%)
	Overall average: 11.0%	

Then, crosstabulation analyses using chi-square tests were conducted to test whether the two out-of-class learning projects provided any significant differences in each of the five emerging learning outcomes and the enhanced perceived value of cybersecurity education. The results in Table 4 show the significant differences in "Real-Life Profession," "Learning Justification," and "Cybersecurity Awareness" emerging learning outcomes between the cybersecurity professional interview project and the cybercrime research project.

DISCUSSION

Based on the results of this study, the students from both sessions expressed that their out-of-class learning experiences helped them to realize their career goals and stimulated their intellectual growth. The chi-square test results showed no significant differences in these two emerging learning outcomes between the students in the two sessions. These results suggested that the cybersecurity professional interview project and the cybercrime research project were equally effective in enabling the students to recognize their career goals and stimulating their intellectual growth. Intellectual growth would provoke curiosity to seek more knowledge; thus, the students would be motivated to take more cybersecurity courses.

When compared to the cybercrime research project, the cybersecurity professional interview project demonstrated larger effects on the real-life profession and the learning justification outcomes. These results could stem from the interactive contact embedded in the cybersecurity professional interview project; that is, an interview incorporates effective professional socialization that exposes the interviewer to the industry's ethics, standard, and expectation (McKinney et al., 1998). In the cybersecurity professional interview project, the students directly socialized and engaged in face-to-face interactions with the cybersecurity professionals who played the mentoring role to impart knowledge and provide guidance. That experience was authentic (McKinney et al., 1998) and helped the students to gain the first-hand knowledge about the cybersecurity profession.

Additionally, that professional socialization helped the students to justify the resources spent in their cybersecurity education. After the students learned from the cybersecurity professionals that they had been receiving the knowledge and skills relevant to cybersecurity and that the cybersecurity job market was promising, the students established a career-centered rationale (Much & Mentkowski, 1982) for their cybersecurity education. That is, with a good job market, the students conceived that they could practice the skills learned from classrooms in their careers after college. This realization helped the students to justify the time, efforts, and monetary investment they had spent in their cybersecurity education and thus engendered the justification of learning (Much & Mentkowski, 1982).

Table 4. Cross-tabulation and Chi-Square Test Results

EMERGING LEARNING OUTCOMES / ENHANCED PERCEIVED VALUE	STUDENT RESPONSES	SESSION A: INTERVIEW PROJECT	SESSION B: CYBERCRIME RESEARCH PROJECT	TOTAL
Career Goal:	No	5	7	12
	Yes	16	9	25
	Total	21	16	37
			Significant level of chi-square score: 0.199	
Real-Life Profession:	No	4	16	20
	Yes	17	0	17
	Total	21	16	37
			Significant level of chi-square score: < 0.001	
Intellectual Growth:	No	7	3	10
	Yes	14	13	27
	Total	21	16	37
			Significant level of chi-square score: 0.322	
Learning Justification:	No	14	16	30
	Yes	7	0	7
	Total	21	16	37
			Significant level of chi-square score: 0.010	
Cybersecurity Awareness:	No	19	7	26
	Yes	2	9	11
	Total	21	16	37
			Significant level of chi-square score: 0.002	
Enhanced Perceived Value:	No	19	14	33
	Yes	2	2	4
	Total	21	16	37
			Significant level of chi-square score: 0.773	

On the other hand, the cybercrime research project showed a larger effect on the cybersecurity awareness than that of the cybersecurity professional interview project. This result could be from the reason that the conscious learning (Schmidt, 1994) about the cybercrimes fostered the awareness of the subject matter on which the students were focusing. Overall, conscious learning refers to learner's intention to learn, maintain a high awareness of learning, and manage the learning process (Schmidt, 1994). In this respect, the students' intention to delve into the real-life cybercrime incidents produced a high awareness of cybersecurity. For example, the students who had never heard of medical identity theft came to grasp its devastating effects, learned how to, and then intended to safeguard their medical data.

Despite all the emerging learning outcomes, the analysis results showed that the out-of-class learning approach did not lead the students to perceive the value of cybersecurity education higher. That is, the high average percentage of students (89.0%) from both sessions demonstrated that their out-of-class learning experiences did not reshape their perceived value of cybersecurity education. Besides, there was no significant difference in the enhanced perceived value of cybersecurity education between the students in both sessions. This result could be from the reason that the students had already formed their preconceived notion about the cybersecurity program before their enrollment. Although the out-of-class learning approach did not lead the students to enhance the perceived value of cybersecurity education, this approach engendered the students' appreciation of and increased their knowledge about cybersecurity learning. Overall, the out-of-class learning approach encouraged the students to look at cybersecurity learning in a favorable light.

The analysis results of this study showed that, for cybersecurity education, the out-of-class learning approach could help the students to attain several valuable learning outcomes. The researchers of this study argued that these valuable learning outcomes would help to improve student engagement in cybersecurity learning and the students would develop their interest and purpose that would sustain them throughout their cybersecurity programs.

Implications

Working on the out-of-class learning projects, the students gained several valuable learning outcomes. For instance, the students realized that the in-class lessons provided them the sought-after skills they could practice in their future careers. This realization would make their learning worthwhile. As the students acknowledged that their learning was worthwhile, they would then justify their learning and find a motivation to learn (Brophy, 1999). Additionally, the students developed higher cybersecurity awareness. Raising awareness about a subject matter's real-life events improves the perceived relevance about the subject matter; thus, cybersecurity awareness led the students to realize the criticality of cybersecurity and believe that cybersecurity education would deliver relevant knowledge. Perceived relevance also engenders motivation in learning (Keller, 1987).

Accordingly, the main practical implication of this study is that the instructors of any cybersecurity programs should incorporate some out-of-class learning activities into the courses in their programs, especially the introductory-level courses. These out-of-class learning activities would help the students to attain several valuable learning outcomes. Overall, the out-of-class learning approach could expose the students to the job market potential, the opportunities for future success, and the nature of the cybersecurity profession. Additionally, the out-of-class learning approach could help the students to increase their intellectual growth and curiosity related to cybersecurity and to justify their learning. Finally, the out-of-class learning approach could raise cybersecurity awareness among the students.

For example, in an introductory-level course of a cybersecurity program, the instructor could arrange the opportunities for the students to engage in face-to-face interactions with some cybersecurity professionals (e.g., arranging a project for the students to interview some cybersecurity professionals). Alternatively, the instructor could select some topics (e.g., cyberterrorism, medical identity theft) and require the students to conduct the research on these topics, search for, and watch some documentary videos about the topics. These arrangements would allow the students to examine and learn more about cybersecurity.

It is also crucial to coordinate the out-of-class learning activities with the in-class lessons to enable the students to justify what they have learned in their classrooms and motivate them to learn more. The instructor may want to align the out-of-class learning activities with the learning objectives of the course. For instance, when teaching principles of secure coding, the instructor may require the students to interact with some Web penetration testers. Through communicating with some Web penetration testers, the students could better understand how hackers exploit the vulnerabilities of Web applications. This understanding would then help the students to justify the defense mechanisms taught in the secure coding lessons.

Regarding research implications, future studies should be conducted using the methodology employed in this study to investigate the effectiveness of the two out-of-class learning activities (i.e., cybersecurity professional interview project and cybercrime research project) integrated into the introductory-level courses of the cybersecurity programs in other universities. Future studies may be conducted to investigate the effectiveness of the two out-of-class learning activities by comparing the results from the introductory-level courses with and without the out-of-class learning activities. Besides, some longitudinal studies tracking the retention rates of the students in the cybersecurity programs that adopt and that do not adopt the out-of-class learning activities would provide an interesting finding. Results of these future studies would help to verify and generalize the findings of this study.

Additionally, as different out-of-class learning activities may lead the students to attain different learning outcomes, future studies may be conducted to examine the effectiveness of other out-of-class learning activities; for example: job shadowing, attending cybersecurity conferences, internship, developing cybersecurity systems or tools for actual customers, working on cybersecurity research with faculty members.

Furthermore, this study was conducted in the introductory-level course (i.e., Introduction to Cybersecurity). The findings may not be generalized to other higher-level and more technical-oriented courses (e.g., Secure Coding, Penetration Testing, Vulnerability Testing). Thus, future studies may be conducted to examine which out-of-class learning activities would be effective for the higher-level and more technical-oriented courses.

Finally, cybersecurity education is a highly technical program. Thus, future research could build on our findings to investigate the effectiveness of the out-of-class learning approach in promoting other academic programs that are characterized by intensely complex and technical nature, similar to cybersecurity programs. For example: engineering program, bio-tech program, and computer science program. This type of programs require its students to put ample efforts in learning and apply high cognitive skills to understand its subject matter.

Limitations

This study was not without limitation. In this study, the data were collected from only a student-centered public university located in the Midwestern region of the United States. Therefore, the research findings may apply to the student-centered public universities with a mission of providing education that teaches real-life skills in favor of student's gainful employment. The findings of this study may reflect the attitude of the students participating in this study toward the cybersecurity program in this particular university. To verify and generalize the findings of this study, more studies replicating this study and conducted in other universities would be needed. Additionally, the sample size of this study was small (N=37) and this sample was from the students enrolling in two different class sessions in the same semester. Hence, researchers may need to be cautious when they refer to the research findings of this study; that is, these findings may be peculiar to the particular small sample in this study. Furthermore, as this study was conducted in the introductory-level course (i.e., Introduction to Cybersecurity), the findings may not be generalized to other higher-level and more technical-oriented courses (e.g., Secure Coding, Penetration Testing, Vulnerability Testing).

Conclusion

This study was conducted to investigate the effectiveness of the out-of-class learning approach on cybersecurity learning. Specifically, the researchers examined whether the out-of-class learning approach could produce any valuable learning outcomes for cybersecurity learning and could enhance the perceived value of cybersecurity education among the students. In conclusion, the findings of this study revealed that, for cybersecurity education, the out-of-class learning approach could help the students to attain several valuable learning outcomes. That is, for cybersecurity education, the analysis of this study found the following results.

- The two out-of-class learning activities examined in this study could help the students to realize their career goal and intellectual growth.
- The two out-of-class learning activities examined in this study could help the students to expand their knowledge base about the cybersecurity profession and produce justification of learning, especially for the students who interviewed cybersecurity professionals.

- The two out-of-class learning activities examined in this study could raise cybersecurity awareness among the students, especially for the students who conducted the research on cybercrime topics.
- However, the two out-of-class learning activities examined in this study could not alter or enhance the perceived value of cybersecurity learning among the students although the students obtained several valuable learning outcomes from participating in the activities.

Presently, cybersecurity is facing a critical shortage of talent nationally and globally (Executive Office of the President, 2016; Zadelhoff, 2017). The Information Systems Audit and Control Association (ISACA), a non-profit information security group focusing on IT governance, predicted that the world would face a shortage of two-million cybersecurity specialists by 2019 (Kauflin, 2017). Additionally, the attrition rate of the students in cybersecurity programs would be high, similar to the high attrition rates of the students in information technology programs and in computer science programs. Thus, to ease the critical shortage of cybersecurity talent, it is essential to increase the retention rate of the students in cybersecurity programs.

As the results of this study showed that, for cybersecurity education, the out-of-class learning approach could help the students to attain several valuable learning outcomes, these results would suggest using the out-of-class learning approach in cybersecurity education, especially in the introductory-level courses of cybersecurity programs. The valuable learning outcomes the students attain could help to increase the retention rate of the students in cybersecurity programs. That is, by providing the opportunities for the students, especially those students in the introductory-level courses, to participate in the out-of-class learning activities related to cybersecurity, the students would attain several valuable learning outcomes and could develop their interest and purpose that would sustain them throughout their cybersecurity programs.

REFERENCES

Agar, M. H. (1980). *The professional stranger*. New York, NY: Academic Press.

Beaubouef, T., & Mason, J. (2005). Why the high attrition rate for computer science students: Some thoughts and observations. *SIGCES Bulletin*, *37*(2), 103-106. https://doi.org/10.1145/1083431.1083474

Brophy, J. (1999). Toward a model of the value aspects of motivation in education: Developing appreciation for particular learning domains and activities. *Educational Psychologist*, *34*(2), 75–85. https://doi.org/10.1207/s15326985ep3402_1

Conklin, W. A., Cline, R. E., & Roosa, T. (2014, January). Re-engineering cybersecurity education in the US: An analysis of the critical factors. In *Proceedings of the 47th Hawaii International Conference on System Sciences (HICSS),* Waikoloa, HI (pp. 2006-2014). Retrieved from https://www.computer.org/csdl/proceedings/hicss/2014/2504/00/2504c006.pdf

Cooper, D., & Schindler, P. (2000). *Business research methods* (7th ed.). New York, NY: McGraw-Hill.

Dark, M., & Mirkovic, J. (2015). Evaluation theory and practice applied to cybersecurity education. *IEEE Security & Privacy*, *13*(2), 75–80. https://doi.org/10.1109/MSP.2015.27

Davis, J., & Dark, M. (2003, June). Defining a curriculum framework in information assurance and security. In *Proceedings of the 2003 ASEE Annual Conference,* Nashville, TN (pp. 1-15). Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.8.4227&rep=rep1&type=pdf

Executive Office of the President. (2016, July 12). *Federal cybersecurity workforce strategy*. Retrieved from http://www.ncsl.org/documents/statefed/Federal_Cybersecurity_WorkforceStrategy.pdf

Goodman, K. (2007, November). The impact of out of classroom experiences on college student development. In *Proceedings of the Annual Meeting of the Association for the Study of Higher Education,* Louisville, KY. *15*, 2013.

Guo, S. (2011). Impact of an out-of-class activity on students' English Awareness, vocabulary, and autonomy. *Language Education in Asia*, *2*(2), 246–256. https://doi.org/10.5746/LEiA/11/V2/I2/A07/Guo

Hattie, J., Marsh, H. W., Neill, J. T., & Richards, G. E. (1997). Adventure education and Outward Bound: Out-of-class experiences that make a lasting difference. *Review of Educational Research*, *67*(1), 43–87. https://doi.org/10.3102/00346543067001043

Kauflin, J. (2017, March 16). The fast-growing job with a huge skills gap: Cyber security. *Forbes*. Retrieved from https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/

Keller, J. M. (1987). Strategies for stimulating the motivation to learn. *Performance Improvement*, *26*(8), 1–7.

Kessler, G. C., & Ramsay, J. D. (2014, January). A proposed curriculum in cybersecurity education targeting homeland security students. *Proceedings of the 47th Hawaii International Conference on System Sciences (HICSS),* Waikoloa, HI, (pp. 4932-4937). Retrieved from https://pdfs.semanticscholar.org/e637/61e32c4a4ca8c9d9b274cf69b1ffa10eb40c.pdf

Kuh, G. D. (1993). In their own words: What students learn outside the classroom. *American Educational Research Journal*, *30*(2), 277–304. https://doi.org/10.3102/00028312030002277

Kuh, G. D. (1995). The other curriculum: Out-of-class experiences associated with student learning and personal development. *Journal of Higher Education*, *66*(2), 123–155. https://doi.org/10.1080/00221546.1995.11774770

Lang, C., McKay, J., & Lewis, S. (2007, June). Seven factors that influence ICT student achievement. In *Proceedings of the 12th Annual SIGCSE Conference on Innovation and Technology in Computer Science Education ITiCES'07,* Dundee, Scotland, U.K., 221-225. https://doi.org/10.1145/1268784.1268849

Maasik, S., & Solomon, J. (2012). *Sign of life in the USA: Readings on popular culture for writers* (7th ed.). Boston, MA: Bedford/St. Martin's.

Manning, P., & Cullum-Swan, B. (1994). Narrative, content, and semiotic analysis. In N. K. Denzin, & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (pp. 463–477). Thousand Oaks, CA: Sage.

McKinney, K., Saxe, D., & Cobb, L. (1998). Are we really doing all we can for our undergraduates? Professional socialization via out-of-class experiences. *Teaching Sociology*, *26*(1), 1–13. https://doi.org/10.2307/1318675

Mirkovic, J., Tabor, A., Woo, S., & Pusey, P. (2015, August). Engaging novices in cybersecurity competitions: A vision and lessons learned at ACM Tapia 2015. In *Proceedings of the 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15),* Washington, DC, 1-8. Retrieved from https://www.usenix.org/system/files/conference/3gse15/3gse15-mirkovic.pdf

Much, N., & Mentkowski, M. (1982). *Student perspectives on liberal learning at Alverno College: Justifying learning as relevant to performance in personal and professional roles. Final report to the National Institute of Education: Research report number seven*. Retrieved from https://files.eric.ed.gov/fulltext/ED239563.pdf

Myers, M. D. (1997). Qualitative research in information systems. *MIS Quarterly*, *21*(2), 241–242. https://doi.org/10.2307/249422

Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012, May). Exploring game design for cybersecurity training. In *Proceedings of the 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems,* Bangkok, Thailand, (pp. 256-262). Retrieved from https://ieeexplore.ieee.org/document/6392562/

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST Special Publication 800-181).* National Institute of Standards and Technology. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

Pascarella, E. T., & Terenzini, P. T. (1991). *How college affects students*. San Francisco, CA: Jossey-Bass.

Pastor, V., Díaz, G., & Castro, M. (2010, June). State-of-the-art simulation systems for information security education, training and awareness. In *Proceedings of the 2010 IEEE Education Engineering Conference,* Madrid, Spain, (pp. 1907-1916). Retrieved from https://ieeexplore.ieee.org/document/5492435/

Pearson, N. (2004, September). The idiosyncrasies of out-of-class language learning: A study of mainland Chinese students studying English at tertiary level in New Zealand. In *Proceedings of the Independent Learning Association Conference,* Melbourne, Australia.

Pickard, N. (1996). Out-of-class language learning strategies. *ELT Journal*, *50*(2), 150–159. https://doi.org/10.1093/elt/50.2.150

Resnick, L. B. (1987). The 1987 presidential address learning in school and out. *Educational Researcher*, *16*(9), 13–54.

Saunders, J. H. (2002, June). Simulation approaches in information security education. In *Proceedings of the 6th National Colloquium for Information System Security Education,* Redmond, WA, 1–14. Retrieved from https://www.researchgate.net/publication/228612714_Simulation_approaches_in_information_security_education

Schmidt, R. (1994). Deconstructing consciousness in search of useful definitions for applied linguistics. *AILA Review*, *11*, 11-26.

Schneider, F. B. (2013). Cybersecurity education in universities. *IEEE Security & Privacy*, *11*(4), 3–4. https://doi.org/10.1109/MSP.2013.84

Soh, L., Samal, A., & Nugent, G. (2007). An integrated framework for improved computer science education: Strategies, implementation, and results. *Computer Science Education*, *17*(1), 59-83. https://doi.org/10.1080/08993400701203782

Tobey, D. H., Pusey, P., & Burley, D. L. (2014). Engaging learners in cybersecurity careers: Lessons from the launch of the national cyber league. *ACM Inroads*, *5*(1), 53–56. https://doi.org/10.1145/2568195.2568213

Weber, R. P. (1985). *Basic content analysis*. Beverly Hills, CA: Sage.

Yurcik, W., & Doss, D. (2001, November). Different approaches in the teaching of information systems security. In *Proceedings of the Information Systems Education Conference,* Cincinnati, OH, (pp. 32-33). Retrieved from https://www.researchgate.net/publication/2382007_Different_Approaches_in_the_Teaching_of_Information_Systems_Security

Zadelhoff, M. (2017, May 4). Cybersecurity has a serious talent shortage. Here's how to fix it. *Harvard Business Review*. Retrieved from https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it

BIOGRAPHIES

Dr. Hwee-Joo Kam is an Assistant Professor of Cybersecurity in University of Tampa, Tampa, Florida. She has taught various courses in Cybersecurity, including penetration testing, digital forensics, secure software design, principle of information security. Dr. Kam has published her research in some refereed journals, including Computers & Education, Journal of Information Privacy and Security, Journal of Information Systems Education.

Dr. Pairin Katerattanakul has published articles in several refereed journals, including European Journal of Information Systems, Communications of the ACM, and Communications of the AIS. Currently, Dr. Katerattanakul is a professor in Department of Business Information Systems, Western Michigan University. He received his Ph.D. from University of Nebraska–Lincoln.