

# Out-Of-Class Learning: A Pedagogical Approach of Promoting Information Security Education

*Completed Research Paper*

**Hwee-Joo Kam, D.Sc.**  
Ferris State University  
ismhweejoo@gmail.com

**Pairin Katerattanakul**  
Western Michigan University  
p.katerattanakul@wmich.edu

## Abstract

To promote information security education, this study integrates out-of-class learning approach into a traditional classroom setting. Mainly, this study assesses whether out-of-class learning projects would encourage the first-year students to espouse the information security education and augment the students' perceived values of the information security education. Our findings suggests that the five emerging learning outcomes from out-of-class learning, including knowledge acquisition of information security profession, career choice and development, intellectual growth, learning justification, and information security awareness, do not enhance student's perceived values of the information security education. Nevertheless, this study posits that out-of-class learning is a viable pedagogical approach to support information security education through (1) first-year student retention and (2) first-year student motivation in learning.

## Keywords

Out-of-Class Learning, College Impact Model, Information Security Education.

## Introduction

Information security education poses challenges for students (Saunders 2002) to learn the complex subject matters (Chin, Irvine, and Frincke 1997; Yurcik and Doss 2001). First-year students who are "testing the water" may shy away from the difficult information security courses given the challenges. Therefore, it is important for faculty to devise a mechanism for promoting information security education in support of persistence of the first-year students.

One mechanism suggested by this study was out-of-class learning approach. Out-of-class learning approach has been adopted to promote student development in the college settings (McKinney, Saxe and Cobb 1998; Goodman 2007) and enhance student learning in some disciplines such as Sociology (McKinney et al., 2004), Outdoor and Leadership (Hattie et al., 1997) and Language (Pickard 1996; Guo 2001). Drawing on the College Impact Model, 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 (Pascarella and Terenzini 1991; Kuh 1993).

However, there has been virtually no literature discussing out-of-class learning approach in the information security discipline. There is very little evidence that demonstrates if out-of-class learning approach is a viable mechanism for promoting information security education and enhancing student's perceived value for the overall information security education. Many prior studies related to information security education either highlight the implementation of information security education in higher education (Chin, Irvine, and Frincke 1997; Hentea, Dhillon, and Dhillon 2006) or present the in-class learning approach to facilitate student learning in an isolated laboratory environment (Hill et al., 2001; Hu, Meinel, and Schmitt 2004; O'Leary 2006).

Hence, this study fills in the gap. That is, the main objective of this study was to assess the effectiveness of out-of-class learning approach on information security education. Specifically, this study intended to examine whether out-of-class learning approach would (1) produce several valuable learning outcomes for information security education and (2) encourage the first-year students to espouse the information security education and augment their perceived values of the information security curriculum.

## **Theoretical Framework**

The College Impact Model emphasizes "less on the internal psychological processes associated with dimensions of change and more on the external environmental and sociological condition" (Kuh 1995, pg. 126). That is, the College Impact Model highlights the external environment (e.g., IT industry), sociological conditions (e.g., diversity workforce), and origins of change (e.g., innovation, paradigm shift) so as to document the interaction between students and the external environment as well as changes in the society (Kuh 1995). For instance, researchers can observe how students interact with the growing trend, such as cybercrimes.

The College Impact Model also posits that the learning outcomes of out-of-class learning approach encompass 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 (Pascarella and Terenzini 1991). These learning outcomes are the results of the out-of-class activities including "*volunteer work, internships, service learning, research with faculty, academic-based peer relationships, involvement in campus organizations, and other co- and extra-curricular activities*" (McKinney et al., 2004).

Learning well in the classroom does not necessarily translate into doing well outside the classroom (Resnick, 1987); that is, in-class learning itself may be insufficient to prepare students for the real-world challenges. Out-of-class learning encourages students to transcend the formal classroom, studio, and laboratory settings, etc. so students can participate in out-of-class activities related to their course work. Contrary to the 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).

Therefore, we contend that out-of-class learning entails any educational activities enabling students to interface with and learn about the real-life application (Pearson 2004). Drawing on the College Impact Model, this study refers out-of-class learning to the interaction between students and institution's environment (e.g. cybercrimes investigation in the real world). For information security discipline, out-of-class learning activities may include research projects about the real-life incidents of hacking, interactions with the external agents such as FBI Infragard representatives and banking compliance officers, and assignments that require solving real-world problems related to intelligence analysis, etc.

## **Research Methodology, Data Analysis, and Results**

### ***Participants and Data Collection***

This study was conducted at a student-centered, public university in the Midwest region of the United States. We integrated out-of-class learning projects into the regular classroom setting. Data were collected from two sessions (i.e., Session A and Session B) teaching Introduction to Information Security. Session A

had 21 students and session B had 16 students. Both sessions were taught by the same instructor and the syllabi, lectures, lab assignments, exams, and delivery methods were identical.

All of the students were first-year students so this was their first introductory-level course in the information security discipline. In each session, only one student was in criminal justice major and the rest of the students were in information security major. Furthermore, there were two female students in each session. The average age of students was 25 years old in session A and 21 years old in session B.

Students in Session A were required to work in the project that involved interviewing information security professional. Each group in Session A was assigned to interview a different information security expert. On the other hand, students in Session B worked on a group project to conduct research about cybercrimes. Each class session had six groups in which each group had two to four group members. The following Table 1 provides the details of group assignments for each session.

In Session A, prior to the interview, each group had to conduct research to gain an understanding of the interviewee's background and expertise. The students were required to prepare semi-structured questions for the interviews. All of the interviews were recorded after receiving the interviewees' written permissions. Upon completing the interviews, the students had to transcribe the interviews they recorded and then shared the interview transcripts among the group members. Next, group members used the transcript to prepare for their group reports.

On the other hand, students in Session B were required to collaborate in groups for conducting research about cybercrimes. Each group was assigned a specific cybercrime topic (see Table 1). Generally, every group had to prepare a report including an overview of the assigned cybercrime topic, citing at least two real-life incidents of the cybercrime, presenting the timelines and details of the two cybercrime incidents, suggesting how to prevent the cybercrime, and finally examining the negative impact of the cybercrime on the society.

The following Table 1 presents out-of-class group projects students conducted in this study.

Group	Session A	Session B
	Information Security Professional Interview Project	Cybercrime Research Project
Group 1	<i>Interviewee:</i> Head of Information Security at a Fortune 500 company <i>Expertise:</i> Application security, security policies and procedures, leadership	Cyberstalking
Group 2	<i>Interviewee:</i> IT Security Professional at a local company <i>Expertise:</i> Mobile devices security , SSL creation and management, and single sign-on	Medical Identity Theft
Group 3	<i>Interviewee:</i> Network Security Engineer at the large architectural firm <i>Expertise:</i> Disaster Recovery, Risk Management, and Vulnerability Analysis	Online Banking Fraud
Group 4	<i>Interviewee:</i> Digital Forensic Consultant <i>Expertise:</i> Digital recovery, digital forensic, and Xbox Hacking	Phishing /Crimes Committed over Social Network
Group 5	<i>Interviewee:</i> Senior Fellow for Homeland Security and Defense Issues at Washington, D. C. <i>Expertise:</i> cyberterrorism, cybersecurity, and homeland security.	Illegal Hacking
Group 6	<i>Interviewee:</i> Director Information Systems at a local county <i>Expertise:</i> Business Continuity Planning, Policies Compliance, and information security management	Denial of Service attack

**Table 1. Group Projects for Out-of-Class Learning**

Upon completing the out-of-class group projects, every student had to provide written feedback regarding his or her learning experience. Particularly, the students from both sessions were asked to share their views about how their out-of-class group projects benefited them. In addition, the students were encouraged to share any comments or suggestions they might have regarding their out-of-class group projects. Furthermore, the students were required to share whether the out-of-class group projects engendered higher perceived value for their information security education. This study collected more than 70 pages of written feedbacks from the 21 students enrolled in Session A and more than 50 pages of written feedbacks from the 16 students enrolled in Session B.

### ***Content Analysis and Crosstabulation***

In this study, we used two approaches to analyze data collected from students' written feedback related to their out-of-class learning experiences. In the first approach, we adopted content analysis under the semiotics approach. Semiotics approach pertains to the meaning of signs and symbols in language wherein words and signs can be categorized into main conceptual categories in support of theory testing (Myers 1997). In the context of semiotics approach, researchers could employ content analysis to discover structures and patterned regularities in the text so that they could later draw inferences based on these regularities (Myers 1997).

We adopted content analysis to identify different types of learning outcomes that the students participating in this study experienced from their out-of-class learning projects. Specifically, we started off by reading students' written feedback and searched for repeated patterns in relation to student learning outcomes. A pattern that appeared regularly would be identified as an emerging learning outcome. For instance, as part of the data showed that students benefited from intellectual growth, we would focus on this indication and keep track of its reoccurrences. If its reoccurrences were relatively high (i.e., appearing consistently among 7 or more students), we would then identify this indication as an emerging learning outcome from the out-of-class learning projects.

The second approach involved monitoring students' responses for a structured question. As mentioned in the preceding section, students were required to state whether their out-of-class learning experiences enhanced their perceived values for information security education. Reading students' responses with respect to perceived value, we classified their responses into two categories: students with enhanced perceived value and students without enhanced perceived value. We then kept track of the frequencies (i.e., the number of students) for each category.

To avoid biases, the researchers worked side by side to identify the emerging learning outcomes and to keep track of the frequencies for each category of the perceived value for information security education. We dissolved any disagreements by finding a common ground. Next, we ran crosstabulation analysis using Chi-Square tests to detect the significant differences in the student feedbacks between the two sessions. Content analysis and crosstabulation analysis enabled this study to yield meaningful findings.

### ***Analysis Results***

Out of the 21 students in Session A, 16 students (76.2%) claimed that the interview of information security professionals helped them to realize their career goals. Hence, career choice and development emerged as a student learning outcome. 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 information security. Now after the interview, I'm very interested in both; more so toward the government aspect. I am keenly interested in developing well developed cyber security 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 information security that I hadn’t been aware of and made me refine some of my original information security 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, 9 out of the 16 students in Session B (56.3%) mentioned that their out-of-class projects for cybercrime research made them realize their career goals, choice, and development. 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 [information security].”*

*“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 health care security is something I can look into for my future career.”*

From the 21 students in Session A, 17 students (81.0%) claimed that their interview projects shed light on the real-life information security profession. That is, students realized the learning outcome related to knowledge acquisition of information security profession. Some of these students mentioned that:

*“Classes and books about information security are informative, but it is very interesting to get a peek into the day-to-day world of a security professional...[The interviewee] spends 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 cyber security 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 information security 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, we found that none of the students in Session B suggested that their cybercrime research projects provided any insights of the information security profession.

Furthermore, results of the content analysis discovered that intellectual growth was another learning outcome. In the context of intellectual growth, students from both sessions showed that their out-of-class projects had increased their intellectual growth and curiosity related to information security subjects. From the 21 students in Session A, 14 students (66.7%) suggested that the interview of information security professionals helped increase their intellectual curiosity. Some of these students stated that:

*“This interview project did raise my interest and curiosity in information security. Penetration testing is something I’m very interested in. Every operating system has a 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 their cybercrime research projects raised their intellectual curiosity about information security subjects.

*“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 information security 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 information security. 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.”*

In addition to the three aforementioned learning outcomes, the collected students’ feedback also suggested another emerging learning outcome related to student’s justification of his/her learning. Seven of the students in Session A, but none of the students in session B, claimed this learning outcome. Some revealed that a peek into the information security profession made them realize that the in-class lectures taught them the sought-after skills.

*“The work that we do here at [the class] directly corresponds to tasks that an information security 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 information security.”*

*“[The interviewee] confirmed that the majority of what we are currently learning, [the interviewee] utilizes in his current work place, or has utilized, seeing as he’s pretty much ‘top-dog’.”*

*“[The interviewee] also said that he has 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 justification came from students’ beliefs that they would face many job opportunities upon graduation.

*“Before the interview, I am not sure that there are many information security 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...”*

Furthermore, 9 students in Session B and 2 students in Session A claimed that, upon completing their out-of-class learning projects, they learned about the danger of cybercrime including how to protect their personal data. That is, another emerging learning outcome was information security awareness.

*“..Illegal hacking...is a topic that I now believe everyone should be aware of because it can effect 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 changes 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.”*

Analysis results of the collected data (i.e., the students’ written feedback) showed that many students attained at least one of the five emerging learning outcomes. That is, from both Session A and B and across

all the five emerging learning outcomes, 46.1% of the overall students' feedback claimed that out-of-class projects helped them achieve any one of the five emerging learning outcomes (see Table 1).

Learning Outcomes	Session A Interview Project (n = 21)	Session B Research Project (n = 16)
Career choice and development	16 (76.2%)	9 (56.3%)
Knowledge acquisition of information security profession	17 (81.0%)	0 (0%)
Intellectual growth	14 (66.7%)	13 (81.3%)
Learning Justification	7 (33.3%)	0 (0%)
Information Security Awareness	2 (9.5%)	9 (56.3%)
<i>Overall average: 46.1%</i>		

**Table 2. Learning Outcomes between Session A and Session B**

To test whether the two out-of-class learning projects provided any different effectiveness, we conducted crosstabulation analysis using chi-square tests to check the significant differences in the students' feedback between the two sessions for each of the five emerging learning outcomes. Results of the chi-square tests in Table 3 suggest that the learning outcomes from the students in Session A and in Session B were significantly different (at p-value < 0.05) in the learning outcome related to "Knowledge Acquisition of Information Security Profession", "Learning Justification", and "Information Security Awareness".

		Session		Total
		A	B	
Career choice and development:	No	5	7	12
	Yes	16	9	25
	Total	21	16	37
<i>Significant level of Chi-square score: 0.199</i>				
Knowledge Acquisition:	No	4	16	20
	Yes	17	0	17
	Total	21	16	37
<i>Significant level of Chi-square score: &lt; 0.001</i>				
Intellectual Growth:	No	7	3	10
	Yes	14	13	27
	Total	21	16	37
<i>Significant level of Chi-square score: 0.322</i>				
Learning Justification:	No	14	16	30
	Yes	7	0	7
	Total	21	16	37
<i>Significant level of Chi-square score: 0.010</i>				
Information Security Awareness:	No	19	7	26
	Yes	2	9	11
	Total	21	16	37
<i>Significant level of Chi-square score: 0.002</i>				

**Table 3. Crosstabulation and Chi-Square Test**

Finally, a majority of the students from both sessions expressed that their out-of-class learning experiences did not change their perception for the information security program. Specifically, 19 out of

the 21 students (90.5%) in Session A claimed that their perceived values were not altered but they appreciated their out-of-class learning experiences.

*“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 information security 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 information security 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 their out-of-class learning experiences did not affect their perception of the information security program. Nonetheless, their out-of-class learning experiences increased their knowledge about the current information security program.

*“No it didn’t. I only learned a different aspect of [information security] program. It was a very informative project.”*

*“No I knew it was good I just had no idea how good it really was but now I know”*

Students also claimed that they had already formed a preconceived notion about the 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.

*“This interview project did not change my perspective of the information security and intelligence program. 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 learn about all aspects relating to the field.”*

In the following Table 4, results of the crosstabulation and chi-square test for the “perceived value” learning outcome show that there is no significant difference (at p-value < 0.05) in the “perceived value” learning outcome between students’ feedback from the two sessions.

		Session		Total
		A	B	
Enhancing perception toward information security program:	No	19	14	33
	Yes	2	2	4
	Total	21	16	37
<i>Significant level of Chi-square score: 0.773</i>				

**Table 4. Crosstabulation and Chi-Square Test for Perceived Value**

## Discussion

The overall analysis results exhibited that, for information security education, out-of-class learning approach:

- brought about the realization of career choices and intellectual growth among students; and intellectual growth provoked student’s curiosity, propelling them to learn more
- expanded the knowledge base about information security profession among students who engaged in the out-of-class interview projects



- produced another interesting learning outcome, that is, justification of learning
- raised information security awareness among students
- did not alter or enhance students' perceived value of information security program despite its several valuable learning outcomes

Students from both sessions admitted that their out-of-class learning experiences made them realize their career goals and stimulate their intellectual growth. The Chi-Square test showed no significant differences in these two learning outcomes between both sessions, suggesting that out-of-class interview project and out-of-class cybercrime research project were equally effective in enabling students to recognize their career goals and facilitate their intellectual growth. In particular, intellectual growth provokes student's curiosity to seek for more knowledge, motivating students to take more information security classes and explore subject matters that sparked their interests.

On the other hand, the out-of-class interview project demonstrated significantly bigger effects on the knowledge acquisition of information security profession and the learning justification than those of the out-of-class cybercrime research project. This result could stem from the interactive contact embedded in the interview project. Mainly, the interview project incorporates more effective professional socialization that exposes students to the industry's ethic, standard, and expectation (McKinney et al., 1998). That is, students directly socialize and engage in face-to-face interactions with the interviewees who play the mentoring role to impart knowledge and provide guidance. Such experience is authentic (McKinney et al., 1998), thus enabling students to gain first-hand knowledge about the information security profession.

Additionally, based on the analysis results, such professional socialization justifies student learning. We assert that once students learn from the interviewees that students receive knowledge relevant to the information security profession and that the job market is promising, students establish a career-centered rationale (Much and Mentkowski 1982) for their information security education. That is, with a good job market, students conceive that they can practice their skills gained from the classroom in their career after college. This helps students to justify their time, efforts, and monetary investment they spend for learning, thereby engendering learning justification (Much and Mentkowski 1982).

Analysis results also exhibited that the out-of-class cybercrime project proved to have significantly larger effect on the learning outcome concerning information security awareness than that of the out-of-class interview project. We maintain that conscious learning (Schmidt, 1994) in relation to cybercrimes fosters students' security awareness in the subject matters that they are focusing on. Overall, conscious learning refers to learner's intention to learn, maintain high awareness for learning, and manage their learning processes (Schmidt, 1994). In this respect, student's intention of delving into the real-life cybercrime incidents produces higher information security awareness within the perimeter of their research topic. For example, students who had never heard of medical identity theft came to grasp its devastating effects and learned how to safeguard their medical data.

In spite of all these learning outcomes, the analysis results also showed that out-of-class learning approach did not enhance students' perceived value of information security education. That is, a high average percentage of students (89.2%) from both sessions showed that their out-of-class learning experiences did not reshape their perceived value of information security program. Additionally, there was no significant difference in the perceived value of information security education between the students from both sessions. We discovered that students had already formed their preconceived notions about the current information security program prior to enrollment. Despite the fact that out-of-class learning approach did not enhance students' perceived value of information security program, this approach brought about student's appreciation of and increased student's knowledge about the information security program. Overall, out-of-class learning experiences encourage students to look at the current information security program in a positive light.

## Conclusion and Research Implication

The findings of this study reveal that out-of-class learning approach enables students to attain the learning outcomes suggested by some prior studies (Pascarella and Terenzini, 1991; Kuh, 1993; Kuh, 1995). That is, in information security context, the out-of-class learning approach connects students to real-life scenario related to information security profession, guides students to their career choice and development, and stimulates student's intellectual growth.

Additionally, we contend that out-of-class learning approach helps to justify students' learning. Working in the out-of-class interview projects, students could recognize that their in-class lectures teach them the sought-after skills that they could practice in their future career supported by a good job market. This thus makes their learning worthwhile. As students acknowledge that their learning is worthwhile, they could then justify their learning and find a motivation to learn (Brophy, 1999).

Furthermore, out-of-class learning approach raises students' awareness about information security. Information security awareness is the outcome of researching, learning, and investigating real-life cybercrime incidents. Thus, after working on the cybercrime research projects, students become more aware of the threats of information systems. This awareness enables students to realize the criticality of information systems and helps making students believe that information security education delivers relevant knowledge.

Although all these learning outcomes may not augment the students' perceived value of the current information security program, we argue that the learning outcomes, at the very least, shed a positive light on the existing information security program, thereby encouraging students to actively engage more in the information security education. These learning outcomes could help fostering student engagement in the information security discipline, especially for the first-year students, and would subsequently lead to good student retention rate.

In sum, the out-of-class learning approach is a viable pedagogical mechanism to promote information security education and curriculum by increasing (1) student retention rate and (2) learning motivation that is stemmed from learning justification and information security awareness, especially among the first-year students. In this respect, this study suggests three practical implications. First, instructors should incorporate out-of-class learning approach into some introductory-level courses in information security program to expose the first-year students to the job market potential, the nature of information security profession, and the opportunities for future success. For instance, in an introductory-level course related to intelligence analysis, instructors could mandate students to interact with intelligence analysts working in the industry. As an alternative, instructors could select a topic such as cyberterrorism and require students to watch some documentary videos relevant to the topic. This would allow students to learn and examine the external environment in relation to geopolitics and threats for cybersecurity. Additionally, to encourage student engagement, instructors could collaborate with the FBI Infragard or Homeland Security personnel to bring in guest speakers.

Second, it is important to coordinate out-of-class learning with in-class learning so as to enable students to justify what they have already learned in class and motivate them to learn more. Instructors may want to align out-of-class learning projects with the initial learning objectives. For instance, instructors could require students to interact with professional Web penetration testers when teaching the principles of secure coding. Through communicating with Web penetration testers, students would realize how hackers exploit the vulnerabilities of a Web application. This will then justify the defense mechanism they learned in secure coding lessons. As an example, when students understand the ubiquitous attacks of cross-site scripting (XSS), students would justify their learning in writing secure coding for input validation.

Third, the out-of-class learning projects with professional socialization are more effective in attaining the outcome for learning justification. When an out-of-class project offers opportunities for students to meet face-to-face with the information security professionals, it fosters professional socialization that exposes students to the real world, resulting in learning justification. Hence, we suggest that instructors could arrange face-to-face meeting with information security professionals when teaching a course. For instance, instructors could coordinate job shadowing as part of the class project.

On the other hand, out-of-class cybercrime project fares better in raising student's information security awareness. Promoting information security awareness would require instructors to prepare an out-of-class project that would immerse students into a highly focused topic related to the consequences of security breaches. For example, to make students understand the danger of medical identity theft, instructors could mandate students to watch YouTube videos that presented the loss suffered by medical identity theft victims.

Furthermore, we contend that our findings are generalizable to the highly technical programs. The future research could build on our findings to devise an out-of-class learning approach for promoting academic programs characterized with intensely complex, technical nature; for example, Engineering program, Bio-Tech program, Computer Science program etc. This type of programs requires students to put ample efforts in learning and apply high cognitive skills to understand a subject matter.

Finally, this study is not without limitation. The study only collected data from a student-centered, public university locate at the Midwestern region in the United States. Therefore, the research findings may be mostly applicable to the student-centered universities with a mission of providing education that teaches real-life skills in favor of student's gainful employment. Additionally, our sample size was small (N= 37) and our sample was made of students enrolling into two different sessions under the same semester. Hence, researchers may need to be cautious when referencing these research findings.

## REFERENCES

- Chin, S. K., Irvine, C. E., and Frincke, D. (1997). *An Information Security Education Initiative for Engineering and Computer Science*, Naval Postgraduate School, Monterey, CA.
- Brophy, J. (1999). "Toward a Model of the Value Aspects of Motivation in Education: Developing Appreciation for Particular Learning Domains and Activities," *Education Psychologist* (34:2), pp. 75-85.
- Donahue, L. (2004). "Connections and Reflections: Creating a Positive Learning Environment for First-Year Students," *Journal of the First-Year Experience & Students in Transition* (16:1), pp. 77-100
- Goodman, K. (2007). "The impact of Out of Classroom Experiences on College Student Development," *In the Annual Meeting of the Association for the Study of Higher Education*, Louisville, KY.
- Guo, S. C. (2011). "Impact of an Out-of-Class Activity on Students' English Awareness, Vocabulary, and Autonomy," *Language Education in Asia* (2:2), pp. 246-256
- Hattie, J., Marsh, H. W., Neill, J. T. and Richards G. E. (1997). "Adventure Education and Outward Bound: Out-of-Class Experiences That Make a Lasting Difference," *Review of Educational Research* (67:1), pp. 43-87.
- Hentea, M., Dhillon, H. S. and Dhillon, M. (2006). "Towards Changes in Information Security Education," *Journal of Information Technology Education* (5), pp. 221-233.
- Hill, J., Carver, C., Humphries, J., and Pooch, U. (2001). "Using an Isolated Laboratory to Teach Advanced Networks And Security", *In Proceedings of 32nd Technical Symposium on Computer Science Education (SIGCSE Bulletin)*, pp. 36-40, Charlotte, North Carolina.
- Hu, J., Meinel, C., and Schmitt, M. (2004). "Tele-Lab IT Security: An Architecture for Interactive Lessons for Security Education," *In the Proceedings of Proceedings of the 35th SIGCSE Technical Symposium on Computer Science Education*, Norfolk, VA.
- Kuh, G.D. (1993). "In their Own Words: What Students Learn outside The Classroom," *American Educational Research Journal* (30:2), pp. 277-304.
- Kuh, G. D. (1995). "The Other Curriculum: Out-of-class Experiences associated with Student Learning and Personal Development," *Journal of Higher Education* (66:2), pp. 123-155.
- Kuh, G.D., Cruce, T.M, Shoup, R., Kinzie, J., and Gonyea, R.M. (2008). "Unmasking the Effects of Student Engagement on First-Year College Grades and Persistence." *Journal of Higher Education* (79:5), pp. 540-563.
- McKinney, K., Saxe, D., and Cobb, L. (1998). "Are We Really Doing All We Can for Our Undergraduates? Professional Socialization via Out-of-Class Experiences," *Teaching Sociology* (26:1), pp. 1-13.
- McKinney, K., Medvedeva, M. A., Vacca, K., and Malak, J. (2004). "Beyond the Classroom: An Exploratory Study of Out-Of-Class Learning in Sociology," *Teaching Sociology* (32:1), pp. 43-60.

- Much, N., and 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 No. 7. Alverno Productions, Milwaukee, WI.
- O'Leary, M. (2006). "A Laboratory Based Capstone Course in Computer Security for Undergraduates," *SIGCSE Bulletin* (38:1), pp. 2-6.
- Pascarella, E.T. and Terenzini, P.T. (1991) *How College Affects Students: Findings and Insights from Twenty Years of Research*, Jossey-Bass, San Francisco, CA.
- Terenzini, P. T., Pascarella, E. T., & Blimling, G. S. (1996). "Students' Out-of-Class Experiences and Their Influence on Learning and Cognitive Development: A Literature Review," *Journal of College Student Development* (37), pp. 149-162.
- Pearson, N. (2004). "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 2003 Independent Learning Conference, Melbourne, Australia*.
- Pickard, N. (1996). "Out-of-class Language Learning Strategies," *English Language Teaching (ELT) Journal* (50:2), 150-159.
- Resnick, L.B. (1987). "The 1987 Presidential Address: Learning in School and Out," *Educational Researcher* (16:9), pp. 13-20.
- Saunders, J. H. (2002). "Simulation Approaches in Information Security Education," *In Proceedings of 6th National Colloquium for Information System Security Education, Redmond, WA*.
- Schmidt, R. (1994). *Deconstructing Consciousness in Search of Useful Definitions for Applied Linguistics*. World Congress of the International Association of Applied Linguistics (AILA) Review.
- Yurcik, W. and Doss D. (2001). "Different Approaches in the Teaching of Information Systems Security," *In the Proceedings of the Information Systems Education Conference (ISECON), Cincinnati OH*.