NURTURING FUTURE CYBERSECURITY PROFESSIONALS: AN EXPERIENTIAL LEARNING PEDAGOGY

D.M. Konidala*, H.G. Tan, Y.T. Ng, H.J. Ong, S.C. Tan, Y.H. Liew, and M.S. Omar

Ngee Ann Polytechnic/School of InfoComm Technology, Singapore

*Divyan_KONIDALA@np.edu.sg

Abstract

This paper documents the journey undertaken by the Diploma in Information Security & Forensics in Ngee Ann Polytechnic in adopting experiential learning as the signature pedagogy throughout the course to nurture future cybersecurity professionals.

It was noted that training students in various and seemingly discrete security concepts, tools, and systems would neither serve the ever-growing demand for skilled, passionate and motivated cybersecurity professionals, nor help in alleviating the high turnover rate and demands faced by the cybersecurity industry currently. Students needed a more “practice-based” and innovative curriculum that will immerse students into the ecosystem of cybersecurity and also nurture them to be ready as cybersecurity professionals by inculcating the essential traits needed for this industry.

These requirements led to the adoption of Experiential Learning for this course. The experiential learning model (Kolb, 1984) is a process of learning through experience and reflection on doing. Experiential learning needs to be intrinsically woven into the course’s curriculum for its effectiveness. In the design of the curriculum, the experiential learning is being experienced both within a module and within a course where the different stages of experiential learning are being anchored in different modules using a variety of innovative teaching and learning approaches. These innovative teaching and learning approaches include state-of-the-art lab facilities, hands-on practical exercises, real-world case studies, open assignments; usage of industry recognized security tools, invited expert talks, industry visits, internships, study trips cum masterclasses, participation in competitions, and showcasing projects at external conferences.

The paper provides evidences of our students inherently applying Kolb’s experiential learning cycle to develop the essential traits of a cybersecurity professional while pursuing their diploma.

Keywords: Experiential learning, cybersecurity, Kolb’s learning model

Introduction

The School of InfoComm Technology (ICT) in Ngee Ann Polytechnic had offered a specialisation option in Information Security & Forensics under its Diploma in Information Technology where students studied cybersecurity related modules such as Information Security, Ethical Hacking, Malware Analysis & Antivirus Technologies, Digital Forensics, and Mobile Device Security & Forensics. However, due to increase demand in the industry for well-trained cybersecurity professionals, ICT started to offer a 3-year diploma course in Information Security & Forensics (ISF) where students are trained in a wider range of cybersecurity topics and more opportunities for students to develop the unique qualities of a cybersecurity professional.

Designing the Curriculum

To achieve this outcome, the teaching team had to determine the traits, competencies and professional attitudes of the “cybersecurity” professional to develop a programme that would meet the needs of the industry. The teaching team reviewed requirements of a cybersecurity professional with industry partners and also referenced the Skills Future Framework for Infocomm professional (SkillsFuture Framework, 2018), which is a list of professional competencies that is co-created by key stakeholders such as employers, industry associations, union and government for the Singapore workforce in a specific industry. The output was a list of traits that were identified for the cybersecurity professionals and that ISF graduates are required to have in addition to their competency in the subject knowledge. The traits are listed in Table 1.

Table 1: Traits desired in a Cyber Security Professional.

<table>
<thead>
<tr>
<th>Trait</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>T-shaped skills</td>
<td>Striving for accuracy</td>
</tr>
<tr>
<td>Problem solving skills</td>
<td>Integrity and responsibility</td>
</tr>
<tr>
<td>Critical thinking</td>
<td>Perseverance</td>
</tr>
<tr>
<td>Lateral thinking</td>
<td>Continuous learning</td>
</tr>
<tr>
<td>Analytical thinking</td>
<td>Communication skills</td>
</tr>
<tr>
<td>Self-directed learning</td>
<td>Community service</td>
</tr>
</tbody>
</table>
The list of traits gave the teaching team with a “direction” as to the type of learning experience and approaches that they will require in order to develop these traits in their students. The review of literature shows that Experiential Learning was most suitable for this course as the learning process will provide the opportunities for the development of “traits” of the profession.

Experiential Learning as ISF’s signature pedagogy

Experiential learning was initially proposed and discussed in the works of John Dewey (1938) followed by Kurt Lewin (1951) and Jean Piaget (1970, 1976). David A. Kolb was influenced by these works and developed the modern theory of experiential learning (1984). Experiential Learning Theory (ELT) defines learning as “the process whereby knowledge is created through the transformation of experience. Knowledge results from the combination of grasping and transforming experience” (Kolb, 1984, p. 41).

The ELT model portrays two dialectically related modes of grasping experience: concrete experience (CE) and abstract conceptualization (AC) and two dialectically related modes of transforming experience: reflective observation (RO) and active experimentation (AE). According to the four-stage learning cycle depicted in Figure 1, immediate or concrete experiences are the basis for observations and reflections. These reflections are assimilated and distilled into abstract concepts from which new implications for action can be drawn. These implications are actively tested and serve as guides in creating new experiences (Kolb, Boyatzis, and Mainemelis, 2001).

Experiential Learning at the Module Level

Ethical Hacking (EH) is a core module taken by the students of the Diploma in ISF during their first semester in Year 3. This module offers foundational ethical hacking and penetration testing knowledge and skills. Students learn the techniques and tools malicious hackers use, but in a lawful and legitimate manner, with a goal to assess the potential impact and risk of an actual cyberattack, and to deploy necessary countermeasures. In addition to the content knowledge that students acquire during the experience learning process, students are also able to develop professional traits that are essential for the cybersecurity professionals in the EH module. Table 2 summarizes the implementation of experiential learning stages in the EH module, along with the professional traits honed by the students at each stage.

Table 2: Implementation of Experiential Learning Stages in the EH Module

<table>
<thead>
<tr>
<th>Experiential Learning Stages</th>
<th>Supporting T&amp;L Approaches Implemented in the EH Module</th>
<th>Professional Traits Honed by the Students</th>
</tr>
</thead>
<tbody>
<tr>
<td>CE</td>
<td>Hands-on lab exercises</td>
<td>Problem solving</td>
</tr>
<tr>
<td>RO</td>
<td>Document observations, and reflections while doing the lab exercises</td>
<td>Critical thinking Analytical thinking</td>
</tr>
<tr>
<td>AC</td>
<td>Open-assignment on real-world cyber-attacks</td>
<td>Self-directed learning Continuous learning Communication skills</td>
</tr>
<tr>
<td>AE</td>
<td>Pen-testing assignment on a testbed that simulates an IT infrastructure for a small and medium enterprise</td>
<td>Lateral thinking Analytical thinking Integrity &amp; responsibility Perseverance Striving for accuracy</td>
</tr>
</tbody>
</table>

Stages 1 & 2: Concrete Experiences & Reflective Observations.

In the EH module, students gain concrete experiences and carry out reflective observations through hands-on lab exercises. Students are provided lab worksheets to learn and practice the basic hacking tools and skills using industry recognized pen-testing tools such as Kali Linux and Metasploit. During the reflective observation process, students think through how their own experience has impacted their understanding of “Hacking”. These observations made during the hands-on lab exercises also allow students understand the modus operandi of hackers, which will enable them to better protect networks, systems, and applications.
Stage 3: Abstract Conceptualizations.

Students experience this stage of “abstract conceptualizations” through an open-assignment on real-world cyberattacks. This process gives students the opportunity to draw on their understanding from their hands-on experience and reflective observations done previously as a reference in their research and further study into the topic.

This open-assignment is a self-directed learning exercise whereby every student gets a chance to choose a latest system hack to research on, construct a demo and a worksheet to teach others in a step by step manner. Students need to present their findings and perform a live demo in front of their peers. They are also given a chance to better their grade by creating a demo video.

Stage 4: Active Experimentations.

In this stage, students are given access to a testbed that simulates an IT infrastructure for a small and medium enterprise. Students apply skills acquired in previous stages and carry out active experimentations via a pen-testing assignment on this testbed. This is a group assignment consisting of two to three students per team. Students brief the tutors on their findings and action plan.

Although students are provided with a brief about the project and have support from their tutors, the teams are very much left on their own to develop the proposal by themselves. This is the opportunity for students to showcase the knowledge and skills that they have acquired over the course of the module, and to demonstrate the traits that they have developed as a result of their experiential learning journey.

Effectiveness of Experiential Learning in a Module

Feedback from students have been positive, with many recognising that the process not only allowed them to have a better understanding of the topic, it also provided them with the opportunity to develop key traits such as team work, perseverance, problem solving etc. The quotes below are extracts from students’ feedback on their learning experience.

“I think that the experiential learning in penetration testing assignment has been a very meaningful learning experience as teams were highly motivated to research on the various vulnerabilities and exploits on their own accord instead of waiting for instructions from the lecturers.”

“This module had taught me the attributes of a penester, and one of them is being able to succeed even when you are stuck at one point, especially during my Assignment 2, where most of my exploitations did not work initially. With the help of my friends and tutor, I was able to work another way around and finally managed to exploit into the machine. It made me learn not to give up even when things go south.”

“The self-directed learning in open assignment has made profound impact on my learning as it has nurtured me to become more self-directed in my learning.

Although we started of not knowing anything about ethical hacking, this assignment has allowed us to understand the various vulnerabilities that exist and the numerous ways in which we could exploit these vulnerabilities…”

Experiential Learning at the Course Level

The curriculum for Diploma in ISF requires each student to complete 21 core, 3 disciplinary elective modules and an internship. In addition, students are also required to complete 8 interdisciplinary modules. Figure 2 depicts the core and elective modules, and their dominant association with one of the four stages of experiential learning.

It can be seen in Figure 2 that the year 1.1 (year 1 semester 1) modules emphasize more on providing concrete experiences to the students. Year 1.2 modules are best at creating opportunities for students to carryout reflective observations. Year 2.1 modules support students to derive abstract conceptualizations. Finally, year 2.2 to 3.2 modules allow students to carryout active experimentations.

Table 3 shows how the experiential learning process is anchored in the different modules within a course and the teaching and learning (T&L) approaches used in these modules to hone the traits of a cybersecurity professionals.

Table 3: Implementation of Experiential Learning Stages at the Course Level

<table>
<thead>
<tr>
<th>EL Stages</th>
<th>Modules</th>
<th>Supporting T&amp;L Approaches Implemented in the Modules</th>
<th>Professional Traits Honed by the Students</th>
</tr>
</thead>
<tbody>
<tr>
<td>CE</td>
<td>Cryptography</td>
<td>Hands-on exercises, Simulation tools</td>
<td>Problem solving, Analytical thinking</td>
</tr>
<tr>
<td>RO</td>
<td>Vulnerabilities 101</td>
<td>Invited expert talks, Real-world case study</td>
<td>Lateral thinking, Communication skills</td>
</tr>
<tr>
<td>AC</td>
<td>Information Security</td>
<td>Open assignment</td>
<td>Self-directed learning, Critical thinking</td>
</tr>
<tr>
<td>AE</td>
<td>Digital Forensics</td>
<td>Use of Industry recognized tools</td>
<td>Integrity &amp; responsibility</td>
</tr>
<tr>
<td></td>
<td>Governance &amp; Data Protection</td>
<td></td>
<td>Striving for accuracy</td>
</tr>
<tr>
<td>Internship</td>
<td>6-months Internship</td>
<td></td>
<td>T-shaped skills, Continuous learning</td>
</tr>
</tbody>
</table>
One such sequence of modules supporting each stage of the experiential learning at the course level is presented below.

**Stage 1: Concrete Experiences.**

Cryptography (CTG) is a core module in ISF that is taken by students in their first year, first semester. This module covers the essential concepts of cryptography, including public key infrastructure, digital certificates, digital signatures, and encryption/decryption algorithms. The fundamental concepts of cybersecurity originated from cryptography. Therefore, to grasp rest of the modules in ISF, it is essential for students to have a very good understanding of cryptography.

In this module, students gain concrete experiences by building their own cipher tools using cardboard and papers, as shown in Figure 3. A handmade cipher tool “scytale”, provides students with a good introduction into the concepts of encryption, decryption, secret key, plain text, cipher text, and the transposition method of ciphering. In another exercise, students create a cipher wheel, which helps them to easily understand the concepts of symmetric encryption and shift cipher.

Another way that students are able to have a concrete experience is to leverage on technology by using simulation tools to depict the operations of some of the modern and more complex cipher and hash algorithms.

**Stage 2: Reflective Observations.**

Vulnerabilities 101 (V101) is a core module offered to the students during their first year, second semester. This module provides a broad overview of the various security vulnerabilities, threats and attacks in different domains (end-user, physical, data, network, software, system). This module engages cybersecurity professionals from the industry to give lectures pertaining to real world attacks and security problems in different domains. Students are expected to reflect on the talks by the experts in the light of their own experiences in the previous module on cryptography.

In V101 module, students, based on their concrete experiences in the CTG module, get to choose a case study of a real-world cyber-attack to research into, construct an article to share with all concerned. The articles must be in the multimedia format using the Microsoft (MS) tool called the “Sway” and are posted in MS Office 365 for sharing and learning with their peers. Students are also required to present and defend their findings. This approach allows students to derive reflective observations from their peers’ work.

Study Tour cum Masterclasses. The bigger security industries and research institutes are largely based in USA, Japan and Europe. There are so many areas that the students could observe and reflect from these industries and institutions. The various security industries in USA include Palo Alto, Cisco Systems, Fortinet and NXP Semiconductors.

A 2-week Information Security Study Tour to USA is targeted at Year 2 students. The Masterclass sessions are focused on the network security. The students are introduced to the NextGen firewall that performs deep inspection of traffic and blocking of attacks. Students had the opportunities to learn, observe and reflect on how to configure the NextGen firewall.
This study tour cum masterclass enabled students to observe and reflect on the academic, enterprise, culture, environment and economic aspect of US. The students visited reputable universities and prominent information security and technology companies.

**Stage 3: Abstract Conceptualization.**

Information Security (INS) is a core module offered to the students during their first semester in Year 2. This module provides an overview of the various domains of Information security. It aims to provide an appreciation of information security from an end-to-end perspective. This module covers security in 7 domains: data, physical, system, network, software, end-user and organization. Students will understand the various aspects of Information security and this will lead them to the more advanced modules such as Malware Analysis Tools & Techniques, Ethical Hacking and Digital Forensics.

As with the use of “Open Assignment” in Ethical Hacking, the assignment here gives students the opportunity to draw on their prior experience and new knowledge to develop new insights into the topic of their interest. The open assignment component is incorporated in to the INS module to encourage independent learning, and peer-learning. It fosters abstract conceptualization on latest issues in information security; and to let students experience learning in the “real” world. This assignment provides the students a chance to research into the problem, establish root cause and brain storm for solutions, produce a prototype for a chosen solution, carrying out testing and validation with stakeholders. A seminar cum competition is held at the end of the module for sharing and learning purpose. The deliverables of this assignment also include a poster and a report.

**Stage 4: Active Experimentation.**

The School of ICT has setup state-of-the-art lab facilities (one of which is depicted in Figure 4) to facilitate active experimentations for the modules in ISF. Digital Forensics (DF) is a core module taken by the students during their second semester in Year 2. This module gives an insight to the process of forensics investigation. It covers the various types of computer-related crimes, techniques of gathering electronic evidence, and recovering of deleted, damaged or encrypted data.

In this DF module students make use of the “system domain” specific abstract conceptualizations derived in the INS module to carryout active experimentations. Students use industry recognized forensic tool called the EnCase Forensic Software to perform forensic investigation. Besides the tools & techniques of investigation, students are encouraged to take on the role of forensic investigators to solve a real-world case study. They are given a simulated crime with evidence files to investigate. Through this active experimentation students understand the forensic investigation methodology and the proper handling of evidence.

Similarly, in another module “Governance & Data Protection (GDP)”, students make use of the “organization domain” specific abstract conceptualizations derived in the INS module to carryout active experimentations. Students use industry recognized, Governance, Risk, and Compliance (GRC) tool, called the RSA Archer, to carryout active experimentations and be trained in how risk and compliance are properly managed in organizations.

**Effectiveness of Experiential Learning at the Course Level**

There are encouraging signs to show that the students in ISF are developing attitudes and traits that are valued by the industry e.g. community service, integrity and responsibility and communication skills.

As part of the Active Experimentation process, students in ISF organised an awareness programme on End-User Security at a Community Centre. For one week, during the evenings, selected students and their posters were displayed at the community centre together with demo sessions at specific time slots. Students have to be ensure that their posters are able to convey the message to the residents in a manner that would be relevant to them. Residents would view the students’ posters and the students would be on stand-by to explain the concepts as depicted by the posters and suggest possible measures to be undertaken to protect the end-user from potential threats. Students have to take on the role of the “expert” to the community and they have to be responsible for the message and knowledge that they are sharing.

Students are also encouraged to showcase their projects at conferences and take part in cybersecurity competitions as shown in Figure 5.

Events like these not only allow students to hone their knowledge and skills on cybersecurity but also allow them to develop their competence in communicating with the community and to develop integrity and responsibility for the message that they are sharing.
Conclusion

The School of ICT has embarked on integrating experiential learning into the curriculum for Diploma in ISF both at the individual module level and at the course level. It is constantly reviewing this signature pedagogy and improving its T&L approaches to ensure that their graduates are prepared with the types of skills and knowledge that is required of their profession.

Experiential learning is not only able to allow students to acquire the necessary knowledge and skills that a competent cybersecurity professional requires but also the “traits” that are valued in the industry. Through the different stages of the Experiential learning cycle, students are constantly interacting with theory, and translating them into practice, modifying their understanding to suit issues in different context and actively proposing new ideas to meet real-world needs.

While this curriculum is still in its infancy, feedback from both students and industry partners have been positive, and the teaching team would continue to review the experiential learning process to ensure that their graduates would have the required skills of a cybersecurity professional.

References


