Issues in Information Systems
Volume 17, Issue III, pp. 59-69, 2016

PREPARING STUDENTS FOR SECURITY CERTIFICATION: AN EXPLORATORY EXPERIMENT

Thomas L. Ngo-Ye, Alabama State University, tngoye@alasu.edu
Jae Choi, Pittsburg State University, jchoi@pittstate.edu

ABSTRACT

Nowadays Cybersecurity becomes a paramount issue for companies and government. Individuals with practical security skill are in high demand on job market. Many IS educators agree to incorporate Security Certification objectives into academic curriculum, because Security Certification may be potentially useful to enhance students' resume and job prospect. In this descriptive study, we report the concrete actions we undertook to prepare students for Security Certification. First, we documented how we prepared and passed CompTIA Security+ Certification Exam. Next, we presented our exploratory experiment to teach students to be prepared for the exam. Due to the lack of financial resources, we had to resort to a labor-intensive approach to manually collect free online Security+ practice questions and transform them into Blackboard quizzes. This study will be helpful to instructors planning to teach students to pass Security+ under very low budget.

Keywords: Cybersecurity Curriculum, Security Certification, Pedagogy, CompTIA Security+ Certification Exam

INTRODUCTION

As organizations and society grow more dependent on technology and Internet, we become more vulnerable to cyber-attacks and cybersecurity seems to become worse (Garfinkel, 2012). Cybercriminal activities threat e-commerce operation and harm consumer confidence (Smith A. D., 2004). Information security breaches in the healthcare industry will not only have financial impact, but also risk exposing patients' sensitive health data and invade their privacy (Martin, Imboden, & Green, 2015). High-profile cybersecurity breach is reported in the news almost every month. As mobile computing and cloud computing fundamentally transform how organizations conduct business, cybersecurity becomes even more paramount to organizations. Moreover, in the era of big data, as huge amount of data stored and transmitted over Internet, it is mandated to put the best and most effective security practices in place (CompTIA, 2016).

Given the continuous rising cybersecurity threats on organizations, there is a clear need for more well-trained cybersecurity professionals, who can protect networks and digital assets. Security is one of the highest demand job categories (Clarke, 2014). The number of people working in the security field continues growing strongly and it was estimated to have about 4.2 million information security professionals worldwide in 2015 (Ayoub, 2011). According to U.S. Bureau of Labor Statistics (http://data.bls.gov/projections/occupationProj), from 2014 to 2024, the number of "Information security analysts" positions will increase 14,800 or 17.9%. Moreover, if considering both normal growth and replacement needs, there will be 25,500 new job openings between 2014 and 2024. Furthermore, typical entry-level education requirement for Information Security Analyst is Bachelor's degree and the median annual wage is $90,120 in 2015. Understanding the importance of filling labor gap for information security, in recent years, government has stepped up its support for academic programs in information security (Paullet, Davis, & Wang, 2013). For example, National Centers of Academic Excellence in Information Assurance (IA) Education (CAEIAE) was instituted by the National Security Agency (NSA) and the Department of Homeland Security (DHS) (Paullet, Davis, & Wang, 2013).

LITERATURE REVIEW

Cybersecurity Education

It is consensus among IS educators that cybersecurity curricula are essential in Higher Education (Smith, Koohang, & Behling, 2010). While some higher education institutions developed new degree programs devoted to teaching information security, for most computer programs there is at least one course dedicated to teaching information security (Paullet, Davis, & Wang, 2013). The IS 2010 model curriculum recommends to have "IT Security and Risk Management" as an elective course (Topi, et al., 2010). In some universities, where Information System program does not have a devoted Information Security course, network management courses are offered to cover the topics related to security (Panko & Panko, 2013). The challenges of cybersecurity curriculum was the focus of a panel discussion in SAIS 2012 (Koohang, Floyd, Smith, & Ashford, 2012).

Due to the dynamic nature of cybersecurity, IS curriculum should stay relevant and be valuable by being current and competitive (Floyd & Yerby, 2014). It is a challenge to revise IS curriculum to keep up with the industry demand (Al-Rawi & Lansari, 2008). Some higher education institutions have developed new digital forensics program with practical active hands-on learning opportunities in lab environment (Floyd & Yerby, 2014). To address the issue of the homogenization of standard-based information security education, the Survey of Strategic Global Cybersecurity course was developed as an example of differentiation (Smith & Randolph, 2015). It provides a higher-level view by emphasizing on critical thinking and a leadership worldview. It serves the long range interest of universities and helps to distinguish from other technical training programs (Smith & Randolph, 2015). Proprietary training programs usually concentrate on low-level technical skills tackling operational issues (Smith, Koohang, & Behling, 2010).

IS Certification and Security Certification

Industry certifications offer a valid assessment of competency, skills and abilities in specific areas and are often used as a screening tool for technical position (Al-Rawi & Lansari, 2008; White, 2006). Companies prefer to hire candidates with certification also because minimum on-the-job training is needed for certified candidates (Al-Rawi & Lansari, 2008). Firms are demanding certifications; job candidates with certifications are more competitive and able to differentiate (Al-Rawi & Lansari, 2008; White, 2006). Certification helps candidate to make a great first impression on HR and contributes to getting one's foot in the door (CompTIA, 2016). Moreover, earning IT certifications gives certified person a greater sense of confidence and area specific computer self-efficacy (Al-Rawi & Lansari, 2008).

IT professionals are pressed to continuously acquire new skills of emerging technologies and certification becomes an important venue to develop and demonstrate the IT skills portfolio (Anderson, Barrett, & Schwager, 2002). It is generally agreed upon among academics that certifications do improve students' marketability and teaching the objectives of industry certifications in curriculum will better meet industry needs (White, 2006).

As the initial gatekeepers in the IT professionals' hiring process, HR managers' perceptions on education, certification, and experience are consequential. An empirical study revealed that education, certification, and experience are imperfect substitutes for each other and they all have unique positive impact on HR managers' opinion formation of a job candidate (Anderson, Barrett, & Schwager, 2002). Moreover, HR managers seem to prefer a balanced candidate with both theoretical knowledge and technical and applied skills. The implication is that traditional theoretical-oriented IS curriculums will be strengthened by including industry certification programs and internship programs (Anderson, Barrett, & Schwager, 2002).

For people intending to work in the field of IT security, IT Security Certification has become an increasingly critical qualification (Tate, Lichtenstein, & Warren, 2007). In recent years, there are so many IT security certifications on the marketplace, which warrants a thorough evaluation (Lim, 2008; Tate, Lichtenstein, & Warren, 2007; Tate, Lichtenstein, & Warren, 2008). Among others, it was mentioned that Computing Technology Industry Association (CompTIA) has established Security+ as an Information Security Certification in 2002 (Lim, 2008).

The competitive job market puts pressure on higher education institutions to incorporate IT certification into academic curriculum (Al-Rawi & Lansari, 2008). Do IS students need to pass security certification? What role does academic curriculum play in preparing students passing security certification? These two questions were addressed in a SAIS 2012 panel discussion (Koohang, Floyd, Smith, & Ashford, 2012). While university IS programs usually include a security component as a part of curriculum, they normally do not take additional steps to prepare students with necessary knowledge and skills for taking and passing Information Security Certification exam (Smith, Koohang, & Behling, 2010). Smith, Koohang, & Behling (2010) argued that higher education should undertake the initiative to prepare students for cybersecurity skills and knowledge and enable them to become certified security professionals. Security certification programs offer better understandings about what industry professionals regard as important skills, knowledge, and issues, and therefore, enhancing university IS curriculum (Smith, Koohang, & Behling, 2010).

White (2006) proposed a four-course network infrastructure concentration based on industry certifications, aiming to meet industry needs and standards and prepare students for entry level technical positions. Upon completion of the network security course, students are supposed to be ready to take on CompTIA Security+ Certification, a vendor-neutral certification (White, 2006). CompTIA Security+ certification is considered to be a relevant credential expected for a general IT worker (White, 2006). Security+ certification exam objectives cover most of the basics of security and can be integrated into the first network security course (Al-Rawi & Lansari, 2008). In fact, after a systematic investigation Al-Rawi & Lansari (2008) concluded that CompTIA Security+ Certification is the only security certification which can be effectively integrated into a single IS course. Al-Rawi & Lansari (2008) proposed a Master level Network and Information Security course syllabus as a framework to integrate Security+ Certification exam objectives into IS curriculum.

Security+ and its Benefits

According to (CompTIA, 2016), "CompTIA Security+ is the certification globally trusted to validate foundational, vendor-neutral IT security knowledge and skills. As a benchmark for best practices in IT security, this certification covers the essential principles for network security and risk management – making it an important stepping stone of an IT security career." Obtaining the Security+ certification can demonstrate that the certified individual has the skills to secure a network and deter hackers and he/she is ready for the security job. It is approved by the U.S. Department of Defense (DoD) as one of the required certification options for Information Assurance Technical Level II and Management Level I job roles and fulfills Directive 8570.01-M requirements (Lachance & Clarke, 2014). Security+ also meets the ISO 17024 standard. Furthermore, Security+ is compliant with government regulations under the Federal Information Security Management Act (FISMA) (CompTIA, 2016).

Jobs that use Security+ include: Security Specialist/Administrator, Security Consultant, Security or Systems Administrator, and Network Administrator (CompTIA, 2016). CompTIA Security+ is frequently used in many organizations such Apple, Dell, Fuji Xerox, Hitachi Systems, HP, IBM, Intel, and various major U.S. government contractors (CompTIA, 2016; Gibson, 2015). Security+ is recommended as the first step in launching professional career as a Network Security Administrator or Systems Security Administrator (Gibson, 2015). Security+ certification demonstrates certified individuals possess security knowledge and skill to solve technical and business problems. The value of Security+ certification is well documented (Barrett, Weiss, & Hausman, 2015).

Security+ certification exam covers "network security, compliance and operation security, threats and vulnerabilities as well as application, data and host security. Also included are access control, identity management, and cryptography (CompTIA, 2016)." The current version of Security+ Certification Exam was launched on May 1, 2014. The industry version Exam Code is SY0-401. JK0-022 is the academic version, although it has the exactly identical content as SY0-401. The length of test is 90 minutes and it has a maximum of 90 questions. Type of questions includes multiple choice and performance-based. The exam score is on a scale of 100-900 and 750 is the passing score. Although CompTIA recommends that an individual to pass CompTIA Network+ Certification Exam first and has at least two years of previous experience in IT administration with a security focus, Network+ Certification and IT work experience are not actually required.

While it is generally agreed among IS educators that Security Certifications are beneficial to students, to the best of our knowledge, we are not aware of any published study documenting detailed implementation of how to help students pass Security Certifications. To that end, we take an initial step to report the concrete actions we undertook to prepare students to pass Security+ Certification exam.

HOW INSTRUCTORS PREPARED AND PASSED SECURITY+ CERTIFICATION EXAM

In this section, we report how we prepared and passed Security+ Certification exam in our first attempt. In additional to sharing the actual resources adopted, we offer our unique exam preparation strategy. IS instructors interested in passing Security+ may consider replicating our tested practice. Moreover, we present our first-hand experience of taking the exam and hope our insight may help others setup what to expect in the real exam.
To get students prepared for Security+ Certification exam, instructors need to first personally pass the exact same exam. Then the lessons learned and tips accumulated can be shared with students attempting the same goal. In this approach, instructors can also serve as a real-life role model for students. It is critical to stress that passing exam itself is not the real goal for instructors. The ultimate objective is to help students pass exam with the first-hand experience. Because of the dual goals – passing exam as a short-term goal and helping students pass exam as a final goal – we took extra steps of recording personal study notes when encountering all the relevant resources deemed useful for passing the exam.

We subscribed to the guiding principle of certification exam preparation – triangulation. Instead of relying on just a single medium such as books, we adopted multiple channels simultaneously to the maximum extent, only limited by time and financial resource available for this endeavor. Primary resources include YouTube Security+ training videos, Security+ books (Barrett, Weiss, & Hausman, 2015; Gibson, 2015) and mock test questions from a variety of sources.

YouTube Security+ Training Videos

A popular free online Security+ training course is adopted (http://www.professormesser.com/security-plus/sy0-401/sy0-401-course-index/). It covers all the exam objectives in detail. For each sub-topic, a short free video clip with PowerPoint presentation is provided. Video's transcript text is also available on its website. The same videos are also posted on YouTube, organized in the following two playlists.

https://www.youtube.com/watch?v=dv7I0SkF6P8&list=PLG49S3nxzAnkcKd71N4OjSv4cUXNhoPlQ
https://www.youtube.com/watch?v=CdAekWEN4wA&list=PLG49S3nxzAnlhMM1KV5ST1qi3kI87hMpY

We watched all 257 video clips. They offer several advantages not found in other adopted resources. Being compared to the content of Security+ books (Barrett, Weiss, & Hausman, 2015; Gibson, 2015), the video clips provide vivid images of the objects and concepts discussed in PowerPoints, dynamic animations, as well as narrative audio. The multimedia-rich approach is useful to keep audience's attention and may deepen one's understanding. Another advantage is that we can play the video clips in the background and just listen to them while multitasking (Books demand more visual attention). This is especially useful when playing the video for the second time, when less attention is needed.

Additional 26 free video clips for Security+ training were selected and watched in the following two playlists.

https://www.youtube.com/user/777stevej777/videos
https://www.youtube.com/watch?v=aGlm87dP0MA&list=PLO2DDwYR8wZA8LZttE2OKtv7PxkL5gOVE

Due to the limit of our time devoted to Security+ project and diminishing marginal return, it was decided not to explore more videos beyond the above three resources.

Read Security+ Books and Practice Assessment Questions in Books

Reading books is a conventional and essential way of learning. In additional to watching videos, two Security+ preparation books (Barrett, Weiss, & Hausman, 2015; Gibson, 2015) were adopted and reviewed. Gibson (2015)'s book was selected as a primary resource based on the sales rank and popularity on Amazon.com. When encountering challenging and unfamiliar topics, we recorded notes for further review. We also practiced all 420 assessment questions of the Gibson's book at least twice. These practice questions gave us a sense of what the real exam questions may look like. These mock tests not only helped us strengthen our grasp of the Security+ subject knowledge, but also enhanced our confidence in passing Security+. The auxiliary text (Barrett, Weiss, & Hausman, 2015) was reviewed to cover "Exam Alerts" and assessment questions (at least twice).

Port Number Summary

Port numbers and protocol IDs mentioned in Security+ videos and books were summarized. Organizing these information in tables may faciliate memorization and review.

TCP Port Number	Application	TCP Port Number	Application	UDP Port Number	Application
15	Netstat	389	LDAP	53	DNS name services lookups
20	FTP actual data transfer	443	HTTPS	69	TFTP
21	FTP control	445	SMB	88	Kerberos
22	Secure shell (SSH), SCP, SFTP	465	SMTP with SSL/TLS	123	Network Time Protocal (NTP)
23	Telnet	636	LDAP with SSL/TLS	137	NetBIOS
25	SMTP	989	FTPS	138	NetBIOS
49	TACACS+	990	FTPS	161	SNMP
53	DNS zone transfers	993	IMAP4 with SSL/TLS	162	SNMP sends traps
80	HTTP	995	POP3 with SSL/TLS	389	LDAP
88	Kerberos	1433	Microsoft SQL Server	500	IPsec uses Internet Key Exchange (IKE) for VPN tunnel
110	POP3	1723	VPN using PPTP	1701	IPsec L2TP
119	NNTP	3389	Remote Desktop Protocol (RDP)	1812	RADIUS
139	NetBIOS	8443	Remote manage web server	3389	Remote Desktop Protocol (RDP)
143	IMAP4 with SSL/TLS				

Table 1. TCP/UDP Port Number and Application

Instructors Taking Security+ Certification Exam

Because the institution where the first author is associated with is a member of the CompTIA academic program, the first author was eligible to purchase a CompTIA Academic Voucher for taking JK0-022 version of Security+ exam. CompTIA Academic Voucher is priced at $195 for a single attempt (much cheaper than the $311 retail price of regular Security+ Certification Exam Voucher sold at CompTIA Marketplace stores

(http://www.comptiastore.com/)). The Exam Voucher expires in one year from the date of purchase. As we were preparing for the exam, we scheduled the exam date, time, and location with the exam test provider – Pearsonvue (http://www.pearsonvue.com/comptia/). We had about one month time to prepare Security+ exam, including about two weeks of dedicated time in winter break. On the day of exam, we reviewed our note as well as port number tables before the exam. We arrived at the exam site about half hour early. The staff checked our two forms of government issued identification including a photo ID and took photocopies of them. The staff also took digital photo of our head shot to be printed on exam report later. We were asked to turn in all books, notes, cell phones, or watches before entering into exam room. We were given a pen and erasable board to use for the purpose of calculation or anything needed to be written down during the exam. The exam was administered on computer. The only application running on the PC was the exam. Internet, web browsers, and search engines were not available during the exam. There is CCTV camera in the exam room and the staff remotely monitors the exam in a different room. We were told to speak to the CCTV camera if we have any questions and/or finish the exam. After the exam started, we noticed a count-down timer. The exam question was presented one at a time on screen. We can mark a question for future revisit and move back and forth and change answers. The first few questions are performance-based questions. We were asked to drag and drop items to categorize them or match items by drawing links. For a firewall rules question, we were asked to type in port numbers in textbox, which was the only data entry we had during the exam. After tackling the initial few performance-based questions, we were presented with many multiple choice questions. While some questions directed us to pick only one answer (with indicator term such as best), other questions explicitly told us more than one answer was expected. In our exam, we encountered a total of 69 questions including both performance-based and multiple choice questions. We were able to answer all 69 questions and reviewed all but two questions marked earlier. One question was about sub-netting and involved complicated calculation. We realized the shortcoming of manual calculation without calculator or Excel spreadsheet. After 90 minutes exam time runs out, we were presented with a survey with questions such as our demographic information, how we prepared Security+ exam, and future goals. After completing the survey the computer revealed our final scores, indicating that our first goal of passing the exam in the first attempt was achieved. Then we signaled to the CCTV camera to get the staff coming to exam room. We received a printout report with our exam score, detailed analysis of our performance in each sub area, as well as our headshot photo in color. The official CompTIA Security+ Certifications were mailed to us a few weeks later, concluding the phase of instructors passing Security+ exam.

HOW TO PREPARE STUDENTS TO PASS SECURITY+ CERTIFICATION EXAM

After succeeding in passing the Security+ Certificate exam as instructors, we embarked on the challenging journey of helping students pass Security+. We recognize the huge gap between instructors and students in preparing for the Security+ Certificate exam. We cannot expect students simply replicate our practice due to the constraints of students' previous knowledge, motivation level, amount of dedicated study time, as well as available financial resources.

Knowledge Gap

First, there is a huge knowledge gap between instructors and students about security. Even before preparing Security+ exam, we, as instructors, have taught Network Fundamentals multiple times. We had solid knowledge foundation about basic network concepts and applications. We also had extensive general knowledge about security, organizational policies, and business-related topics such as disaster recovery and risk management from teaching other relevant courses. On the other hand, most students have very minimum exposure to network and security knowledge, and even less work experience involving network. To address the knowledge gap, we plan to conduct effective knowledge transfer through interactive lecture (to be discussed in detail in the later section). Moreover, we provide as much relevant resources as possible to students. Network and Security are infamous for so many Acronyms. In addition to the resources we described before, we expanded our personal study notes to include many relevant terminologies and jargons encountered in preparing security+. Our rationale is that it can save students' precious time and effort doing their own research. Our notes (a text file) serve as the first go-to place, whenever students face unfamiliar terminologies. Furthermore, we provided students with three additional Security+ Glossary and Acronyms documents based on the following sources:

http://www.examcompass.com/malware-glossary/
http://www.examcompass.com/comptia-security-plus-certification-exam-glossary/
http://getcertifiedgetahead.com/index.php/security/security-acronyms/

Motivational Issue

While instructors have very strong motivation to study and pass Security+, students may not share the same level of motivation and thus unlikely to devote needed amount of time to study. We gave students an informal introduction to Security+ Certification and tried to convey the message that Security+ Certification will enhance their résumé and be beneficial to starting their professional career in IT. We stressed that Security+ Certification is an achievable goal with instructors' help and students' dedication to study. We reasoned with students that Security+ is usually considered as the first step in starting career in security and it is much easier compared to other more advanced Security Certifications. After our repeated attempts to convince students the value of Security+, several students showed interest in undertaking the journey to pass Security+.

Resources Issue

Another critical barrier for students to pass Security+ is resources issue. First, most students do not have the luxury of enough time to sit down and study for Security+. In the real-world, students are taking multiple courses, not just Security or Network Fundamental course. Besides the burden of full-load of classes, many students work part-time to make ends meet, as well as taking care of family members. Practically, it is unimaginable that students can set aside huge blocks of quality time to study Security+. Second, many students do not have financial resources to purchase Security+ preparation books or pay exam fee. Cost of security certification exam was identified as a key barrier to security certification. One suggested strategy to mitigate cost concern is to find a sponsor such as employers who can pay certification fee (Tate, Lichtenstein, & Warren, 2008). Severely constrained by very limited study time and minimum to none financial resources, instructors have to work within the parameter to maximize the available resources. Given that students may not have time to watch Security+ training videos, we were forced to focus on transferring our Security+ knowledge in face-to-face meetings.

Choice of Face-to-face Teaching Sessions

An empirical study investigating the effectiveness of information security training found that while the computer-based trainees had a higher level of knowledge retention within the 60 days' time frame, instructor-based trainees had higher levels of knowledge transfer (Kim & Homan, 2012). We conducted several experimental face-to-face teaching sessions to train students for Security+. First, we organized Security+ preparation session outside regular class meeting time when no other class meetings are scheduled. We observed that the attendance fluctuated greatly. The initial session has a record of 10 students attending, and then drops to about 5 students, finally only 2 students. Among the students came to the sessions, some came late and some left early. More importantly, no single student attend all security+ sessions. We informally asked students why they cannot attend the sessions. Students cited reasons such as conflict with their work schedule. Overall, the attempt to hold study sessions outside regular class meeting time were shown unsuccessful. Next, we moved the Security+ study sessions into our regular Security class meeting time. We condensed the class meeting time spent on regular security teaching and used the freed time to teach Security+. This tactic seems to work, at least the attendance is much better and stable.

Interactive Lecture and 100 Free Assessment Questions from Gibson (2015)'s Book

To engage a diverse body of students, a research has designed and used several interactive hands-on activities for teaching information security course (Heinrichs, 2015). Recognizing the importance of lecturing as an essential and fundamental element of learning and teaching, mobile technology was adopted to facilitate interactive lectures in higher education (Balakrishnan & Gan, 2015). We also tried our best to adapt our lecture to be more interactive. While most students did not have Gibson (2015)'s book, a copy of sample kindle book is freely available on Amazon.com. This free sample copy does not include the whole 11 chapters, end-of-chapter assessment questions, and 100 post-study assessment questions. Those contents are available only after one purchases the book. However,

the free sample book does include the 100 questions of Pre-Study Assessment Exam and answers with the detailed explanations for the first 65 questions. In our first several Security+ sessions in regular class meeting time, we presented these 65 questions from Amazon.com website on big screen and discussed both the questions and answers in class. We also elaborated on the underlying concepts by switching to our study notes to explain new terminologies and Acronyms. Towards the later part of the 65 questions, several students can correctly answer them in class. Informal discussions with several students seemed to indicate this way of teaching/learning is effective. The free sample Kindle version of Gibson (2015)'s book can be found in the following link:

http://www.amazon.com/CompTIA-Security-Certified-Ahead-SY0-401-ebook/dp/B00NNWKN3G

Collecting Free Online Security+ Practice Questions and Converting to Blackboard Quizzes

Recognizing the reality that many students do not have financial resources to purchase Security+ preparation books, we undertook a massive project of manually collecting free online CompTIA Security+ practice questions and answers to transform them into Blackboard quizzes. We did an extensive online search and located the following websites containing free Security+ practice questions and answers.

https://certification.comptia.org/training/sample-questions/
http://www.examcompass.com/comptia/security-plus-certification/free-security-plus-practice-tests/
https://crucialexams.com/exams/comptia/security+/sy0-401/
https://www.concise-courses.com/test-yourself/securityplus/
http://blogs.getcertifiedgetahead.com/free-security-practice-test-questions-2/
http://blogs.getcertifiedgetahead.com/free-security-practice-test-questions-1-4/
http://www.gocertify.com/quizzes/comptia/security-plus-sy0301.html
http://www.gocertify.com/quizzes/comptia/Page-3.html
http://www.proprofs.com/mwiki/index.php/Comptia_Security%2B_Certification_Exam
http://www.certiology.com/comptia-certification/comptia-securityplus/free-security-plus-practice-tests.html
https://www.4tests.com/exam/security-plus-sy0-401/0/29494403
https://quizlet.com/tbovard2
https://quizlet.com/34103289/security-plus-sy0-301-set-3-flash-cards/

We manually copied the questions and answers one by one from the websites and pasted them in a text document in Notepad++. Then we manually edited the text to ensure that each question entry/answer entry only occupy one single line and the correct answer(s) is (are) marked with * in front of it. Between two questions, we manually inserted a blank line. The following six lines serves as an example.

7. What is the primary function of a DNS server?
A. Resolve 32-bit addresses in IPv4
B. Find other DNS servers
*C. Resolve Fully Qualified Domain Names to IP addresses
D. Find MAC, 48-bit hardware addresses
E. Find MAC address for an IP address

We collected a total of more than 1000 questions. We randomly picked 50 of them and assembled them to a quiz text file, with question number reordered to 1 to 50 in each quiz. We created 19 quiz text files. Then we used a free online Blackboard Test Generator (http://www2.byui.edu/ATS/testgen.htm) to convert these 19 quiz text files into Blackboard quiz format files one by one. Next, we uploaded these 19 quizzes into Blackboard class website. We performed additional editing in Blackboard to randomly order answers in each question and randomly order 50 questions in each quiz. Moreover, we controlled the quiz presentation in a way that only one question is shown on the screen at a time, while allowing students to move back and forth among quiz questions. It is extremely labor intensive to collet questions, transform into Blackboard quiz format, load into Blackboard, and further edit presentation of quizzes. However, it placed minimum burden on students. All students need to do are actively participating interactive lectures and practicing Security+ quizzes in Blackboard, a familiar environment. We essentially adapted Blackboard to a simulated Security+ test environment, providing almost identical experience as

the real Security+ exam. Given the limited available class meeting time for Security+, we were able to discuss only one out of 19 quizzes in class. We assigned all 19 quizzes to students as homework with unlimited number of attempts allowed. We also gave out three in-class tests, with 50 randomly selected questions for each test.

Performance-based Questions

We acknowledged that the question type of 19 quizzes we put together is multiple choice only. We did not have financial resources to purchase commercial Security+ simulation software and practice test-banks. Therefore, we could not provide students with hands-on practice experiences for the performance-based questions. At this stage, all we could do about performance-based questions were to play a few relevant YouTube videos and present several diagrams and images of sample performance-based questions (see the following web resources).

http://gcgapremium.com/performance-based-question-demo/
https://www.youtube.com/watch?v=JSNn4w1aBho
https://www.youtube.com/watch?v=t4q8EAsGhP8
https://www.youtube.com/watch?v=b_1s9njlWLU

SUMMARY

In this paper, we documented our endeavor to prepare students for Security+ Certification, a credential generally regarded as beneficial to students about to enter job market. This study makes the following potential contributions. First, based on existing literature, we argued that preparing students for Security+ is a useful and meaningful tool to train students about practical security knowledge and skills. Furthermore, we proposed that IS educators should take more active role in preparing students for Security Certification. Second, interested instructors may replicate our proven practice to prepare and pass Security Certification. Third, in a time when higher education institutions face the constraints of financial resources and student motivation, our exploratory experiment in preparing students for Security Certification may serve as a useful and practical reference. With all the implementation details and relevant web resources presented in the paper, IS educators can easily duplicate and adapt our experiment. Due to the demanding high passing score (750/900 or about 84%,), passing CompTIA Security+ Certification exam will be a challenge for many students even though they can pass the security course which integrates the Security+ objectives (Al-Rawi & Lansari, 2008). As for the outcome of our initial experiment, we also expect that only a few students may pass Security+ in the first year. We acknowledge that this ongoing project is still in its early stage and we pay close attention to the progress. We will continuously use students' feedback to improve teaching and report back new lessons learned in a future study. Moreover, we intend to develop a more formal assessment survey of the effectiveness of the proposed teaching approach.

REFERENCES

Al-Rawi, A., & Lansari, A. (2008). *Integrating the Security+ exam objectives into information technology curricula.* American Society for Engineering Education. Retrieved May 13, 2016, from https://peer.asee.org/integrating-the-security-exam-objectives-into-information-technology-curricula.pdf

Anderson, J., Barrett, K., & Schwager, P. (2002). Information systems certification: The perspective of the human resource manager. *Proceedings of the Eighth Americas Conference on Information Systems (AMCIS 2002)* (pp. 2134-2142). Dallas, TX, U.S.A.: Association for Information Systems. Retrieved May 13, 2016, from http://aisel.aisnet.org/amcis2002/291

Ayoub, R. (2011). *The 2011 (ISC)2 global information security workforce study.* Frost & Sullivan. Retrieved May 13, 2016, from https://www.isc2.org/uploadedfiles/landing_pages/no_form/2011gisws.pdf

Balakrishnan, V., & Gan, C. L. (2015). Mobile technology and interactive lectures: The key adoption factors. In *Mobile Learning Design* (pp. 111-126). doi:10.1007/978-981-10-0027-0_7

Barrett, D., Weiss, M., & Hausman, K. (2015). *CompTIA Security+ SY0-401 Exam Cram* (4th ed.). Pearson IT Certification.

Clarke, G. E. (2014). *CompTIA Security+ Certification Study Guide* (2nd ed.). McGraw-Hill Education.

CompTIA. (2016, May 13). *CompTIA Security+*. Retrieved from CompTIA: https://certification.comptia.org/certifications/security

Floyd, K., & Yerby, J. (2014). Development of a digital forensics lab to support active learning. *Proceedings of the Southern Association for Information Systems Conference (SAIS 2014)* (pp. 1-6). Macon, GA, U.S.A.: Association for Information Systems. Retrieved May 13, 2016, from http://aisel.aisnet.org/sais2014/7

Garfinkel, S. L. (2012, June). The cybersecurity risk. *Communications of the ACM, 55*(6), 29-32. doi:10.1145/2184319.2184330

Gibson, D. (2015). *CompTIA Security+: Get Certified Get Ahead: SY0-401 Study Guide* (3rd ed.). YCDA, LLC. Retrieved May 13, 2016, from http://www.amazon.com/CompTIA-Security-Certified-Ahead-SY0-401-ebook/dp/B00NNWKN3G

Heinrichs, L. (2015). Engaging a diverse student audience in an information security course. *Issues in Information Systems, 16*(3), 164-171.

Kim, P., & Homan, J. V. (2012). Measuring the effectiveness of information security training: A comparative analysis of computer-based training and instructor-based training. *Issues in Information Systems, 13*(1), 215-224.

Koohang, A., Floyd, K., Smith, T., & Ashford, T. (2012). Panel: The challenges of cybersecurity curriculum. *Proceedings of the Southern Association for Information Systems Conference (SAIS 2012)* (pp. 166-168). Atlanta, GA, U.S.A.: Association for Information Systems. Retrieved May 13, 2016, from http://aisel.aisnet.org/sais2012/28

Lachance, D., & Clarke, G. E. (2014). *CompTIA Security+ Certification Practice Exams* (2nd ed.). McGraw-Hill Education.

Lim, N. (2008, November). Escaping the computer-forensics certification maze: A survey of professional certifications. *Communications of the Association for Information Systems, 23*(1), 547-574. Retrieved May 13, 2016, from http://aisel.aisnet.org/cais/vol23/iss1/30

Martin, N. L., Imboden, T., & Green, D. T. (2015). HIPAA security rule compliance in small healthcare facilities: A theoretical framework. *Issues in Information Systems, 16*(1), 180-188.

Panko, R. R., & Panko, J. L. (2013). *Business Data Networks & Security* (9th ed.). Upper Saddle River, New Jersey, U.S.A.: Pearson Education.

Paullet, K., Davis, G. A., & Wang, W. (2013). Cyber forensics and information security: A new and innovative bachelor's degree program. *Issues in Information Systems, 14*(1), 244-250.

Smith, A. D. (2004). Cybercriminal impacts on online business and consumer confidence. *Online Information Review, 28*(3), 224-234. doi:10.1108/14684520410543670

Smith, J., & Randolph, A. B. (2015). The homogenization of standards based information security education: An example of differentiation. *Proceedings of the Southern Association for Information Systems Conference (SAIS 2015)* (pp. 1-6). Hilton Head Island, SC, U.S.A.: Association for Information Systems. Retrieved May 13, 2016, from http://aisel.aisnet.org/sais2015/33

Smith, T., Koohang, A., & Behling, R. (2010). Formulating an effective cybersecurity curriculum. *Issues in Information Systems, 11*(1), 410-416.

Tate, N. J., Lichtenstein, S., & Warren, M. J. (2007). Supporting user evaluation of IT security certification schemes. *Proceedings of the 18th Australasian Conference on Information Systems (ACIS 2007)* (pp. 70-81). Toowoomba, Queensland, Australia: Association for Information Systems. Retrieved May 13, 2016, from http://aisel.aisnet.org/acis2007/2

Tate, N. J., Lichtenstein, S., & Warren, M. J. (2008). IT security certifications: Stakeholder evaluation and selection. *Proceedings of the 19th Australasian Conference on Information Systems (ACIS 2008)* (pp. 991-1001). Christchurch, New Zealand: Association for Information Systems. Retrieved May 13, 2016, from http://aisel.aisnet.org/acis2008/60

Topi, H., Valacich, J. S., Wright, R. T., Kaiser, K., Nunamaker, J. F., Sipior, J. C., & Vreede, G.-J. d. (2010, April). IS 2010: Curriculum guidelines for undergraduate degree programs in information systems. *Communications of the Association for Information Systems, 26*, 359-428. Retrieved May 13, 2016, from http://aisel.aisnet.org/cais/vol26/iss1/18

White, G. L. (2006, August 4). Vendor/industry certifications and a college degree: A proposed concentration for network infrastructure. *Information Systems Education Journal, 4*(48), 1-7. Retrieved May 13, 2016, from http://isedj.org/4/48/ISEDJ.4(48).White.pdf