https://doi.org/10.48009/1_iis_2019_100-107

ENHANCING ORGANIZATIONAL CYBERSECURITY: A HANDS-ON IMMERSIVE LEARNING PROJECT

Jensen J. Zhao, Ball State University, jzhao@bsu.edu
Dr. Allen D. Truell, Ball State University, atruell@bsu.edu
Dr. Edward J. Lazaros, Ball State University, ejlazaros@bsu.edu
Dr. Chris Davison, Ball State University, cbdavison@bsu.edu

ABSTRACT

The growing popularity of Internet-based e-commerce, e-banking, e-investment, e-payment, e-education, e-government, social media, and Internet of things around the world now is bringing increased privacy and security threats to people, businesses, and governments. The cyber attackers' primary purpose of cyberspace intrusion and attack was to steal customer data, defame celebrities, damage brands, and manipulate markets for illegal financial gains. The cybercrimes gave attackers 1,425% return on investment. This paper introduced a real-world immersive learning project for computer information systems students to develop hands-on skills of assessing the security and vulnerability of e-business, e-government, and social media sites by (1) reviewing the current cyber world to better understand what is going on with the cyber-world security and threats; (2) developing a cybersecurity auditing instrument; (3) identifying a company, a government agency, or an organization that needs assistance to measure the cybersecurity of its e-business, e-government, or web services; (4) working in team and using the auditing instrument to examine the cybersecurity strengths and vulnerabilities of the website systems; (5) applying their intelligences and developing proactive solutions to the problems related to cybersecurity; and (6) presenting a written proposal for solving the real-world web security problems. The pedagogical and practical implications of the project were also discussed.

Keywords: Cybersecurity, Cybercrime, Hacker, Intrusion, Prevention, Vulnerability.

INTRODUCTION

With the continuous technology advancement, the Internet-based e-commerce, e-banking, e-investment, e-payment, e-education, e-government, social media, and Internet of things (IoT) are growing more and more popular around the world. According to an Internet Retailer analysis of industry data and historical U.S. Commerce Department figures, the U.S. consumers spent $517.36 billion online in 2018, up 15% from $449.88 billion spent in 2017. Total retail sales, not including the sale of items not normally bought online like fuel, automobiles and food at restaurants, hit $3.628 trillion in 2018, up 3.9% over the previous year of $3.490 trillion. E-commerce represented 14.3% of total retail sales in 2018. Amazon accounted for 40% of U.S. online retail (Fareeha, 2019).

However, the growing popularity of Internet-based e-business, e-government, social media, and IoT has also resulted in privacy and security threats to people, businesses, and governments. As the *Symantec 2019 Internet Security Threat Report* indicates, Web attacks increased by 56% in 2018. Specifically, form jacking attacks skyrocketed with an average of 4,800 websites compromised each month. Ransomware shifted targets from consumers to enterprises, where infections rose 12%. More than 70 million records were stolen from poorly configured S3 buckets, a casualty of rapid cloud adoption. Supply chains remained a soft target with attacks ballooning by 78%. The IoT was a key entry point for targeted attacks; most IoT devices are vulnerable. Symantec's research findings were generated from 123 million sensors recording thousands of threat events every second from 157 countries and territories (Symantec, 2019).

Furthermore, as industrial Internet of things (IIoT) grows in prominence, so does its status as a target for malicious hackers. The latest and potentially most dangerous threat is called Triton, which targets the industrial safety system that monitors and secures valves, turbines, and the like and shuts them down if it determines they are about to fail and cause explosions or other consequences that could damage the facility or cause harm to people (Gold, 2019).

As research showed, the website attacks mainly targeted at networks' TCP/IP (Layer 4), SSL (Layer 5), HTTP and FTP (Layer 7) according to the Open Systems Interconnection Reference Model (McNurlin & Sprague, 2009). Overall, cyber attackers' primary purpose of cyberspace intrusion and attack was to steal customer data, defame celebrities, damage brands, and manipulate markets for illegal financial gains. The cybercrimes gave attackers 1,425% return on investment (e.g., Ashford, 2014; Symantec, 2019; Trustwave, 2015).

The purpose of this paper was to introduce a real-world immersive learning project for computer information systems students to develop hands-on skills of assessing the security and vulnerability of e-business, e-government, and social media sites by examining the following issues:

a. The privacy and security policies and implementations
b. The information availability of the website systems
c. The computer network security of the sites

DESIGN AND PROCEDURES OF IMMERSIVE LEARNING PROJECT

Research indicated that traditional approaches to learning have often focused upon knowledge transfer strategies that have centered on text-based engagements with students and dialogic methods of interaction with instructors. Rather than the knowledge transfer from instructors and texts to students, the real-world hands-on immersive learning allows students to engage in more complex social interactions and to identify real-world problems (Freitas, Rebolledo-mendez, Liarokapis, Magoulas, & Poulovassilis, 2010). However, integrating hands-on immersive learning projects of real-world problems into curriculum is often an overlooked element of designing curriculum and courses (Mills, Hauser, & Pratt, 2008). Hands-on immersive learning projects of real-world problems enables students to identify specific areas where changes or improvements can be implemented in the workplace or real-world situations (Foxon, 1987).

Research also reported that immersive learning projects enable instructors to direct students to immerse into the society, communicate with people of varied age groups and occupations in different industries and communities, and identify real-world problems that disturb people who need solutions. In addition, learning through immersive projects, students would be able to apply critical and creative thinking and problem-solving skills along the seven-stage procedure of chaos-finding, data-finding, problem-finding, idea-finding, solution-finding, acceptance-finding, and proposal writing and presentation. Thinking critically and creatively of the disturbing problems and the market demand for solving the problems would inspire students to generate innovative solutions. Such innovative solutions will attract potential investment from innovation-driven companies and venture capitalists (Zhao, Alexander, & Truell, 2014).

The immersive learning project was designed as a form of hands-on learning in which learners are physically placed themselves in the current business world to accomplish the following six tasks: (1) to review the current cyber world to better understand what is going on with the cyber-world security and threats; (2) to develop a cybersecurity auditing instrument; (3) to identify a company, a government agency, or an organization that needs assistance to measure the cybersecurity of its e-business, e-government, or web services; (4) to work in team and use the auditing instrument to examine the cybersecurity strengths and vulnerabilities of the website systems; (5) to apply their intelligences and develop proactive prevention solutions to the problems related to cybersecurity; and (6) to present a written proposal for solving the real-world cybersecurity problems.

INSTRUMENT DEVELOPMENT

Based on the review of the current cyber-world security and threats, a cybersecurity auditing instrument was developed by the participating students under the instructor's guidance. The cybersecurity auditing instrument helps examine websites in terms of (a) privacy and security policies and their implementation, (b) network information availability of the websites, and (c) computer network system vulnerability to cyber intrusions and attacks. This immersive learning project guided students to develop the instrument by using three methods for data collection and analysis: Web content analytics, network system information auditing, and computer network vulnerability mapping.

Privacy and Security Policies

The web content analytics is commonly used in assessing organizations' web contents, deliveries, and strategies (e.g., Boggs & Walters, 2006; Campbell & Beck, 2004; Wilkinson & Cappel, 2005; Zhao & Zhao, 2010; Zhao & Zhao, 2015). This method is used for systematically and objectively identifying and recording the privacy and security policies available at the websites and then analyzing what privacy and security measures were stated as in implementation. This method generated the following content categories for analysis: (a) existence of privacy, security, child-protection, proper-use, and no-liability policies; (b) anti-hacking notice; (c) data transmission encryption; (d) intrusion detection; (e) investigation of improper web activities; (f) login authentication and duo security; and (g) web traffic monitoring.

Network Information Availability

To find out what network information of the websites is publicly available on the Internet and how vulnerable the sites are to cyber intrusion and attack, student teams are required to conduct Google search for related websites and auditing tools. For example, three websites, *ZoneEdit.com*, *arin.net*, and *insecure.org*, offer the auditing tools. The *ZoneEdit.com* site is a leading website in DNS (Domain Name System) and domain management solutions. It provides a free DNS lookup utility tool, which enables any online user to enter a website domain name (e.g., yahoo.com) for searching its IP (Internet Protocol, e.g., 216.115.108.245) address (see at http://www.zoneedit.com/lookup.html).

The *arin.net* (American Registry of Internet Numbers) site provides a free database search service at *ws.arin.net*. The search service allows any online user to find a website's registration information for resources registered with ARIN. The ARIN database contains IP addresses, autonomous system numbers, network name, type, and range, organizations or customers that are associated with these resources, and related points of contact. By entering a site's

IP address into the search tool, any person can get all the registered information of the site's network systems (see at http://www.arin.net/whois/).

Network Security Mapping

The computer network security mapping is a major method of using software tools for assessing the vulnerability of an entire computer network system without intrusion and identifying areas of potential security threats (e.g., Garcia, 2004; Winkler, 2004). To assess the vulnerability of the computer network systems of websites, a popular, free network mapping utility tool, *Nmap*, provided by the *insecure.org* can be selected. *Nmap* is a port scanning and network mapping software. It uses raw Internet protocol (IP) packets to determine what hosts are available on the network; what ports are open, filtered, firewalled, or closed; what services and servers those hosts are offering; what operating systems they are running; as well as many other characteristics (see at http://insecure.org/).

To ensure that using *Nmap* for this project is legal and ethical, the related literature was reviewed and found in a Georgia District Court case of "Moulton v. VC3," where the judge declared a port scan in the case legal because it did not impair the integrity nor availability of the network. The judge found that since the activity performed no damage to the target, it could not be illegal (Jamieson, 2002). The implication of this case is that a port scan is not an attack and usually causes no damage to a target network; the legality and ethics of a port scan depend on whether the intent of a port scan is to cause damage or to improve security. As the purpose of this project was to provide websites' administrators with the findings that they need for continuous improvement of their site security, using *Nmap* for the immersive learning projects is justified.

Table 1 presents the details of the cybersecurity auditing instrument developed by students for their hands-on immersive learning project—Enhancing Organizational Cybersecurity.

Table 1. Cybersecurity Auditing Instrument

Company/Organization Name: ______________________ URL: ________________________________

Auditing Date: ____/____/____ Auditor Name: ________________________________

Directions: Please read each of the following questions carefully and audit the site meticulously. You must save each of your search results digitally, print out a hard copy, and attach it to its audit instrument for double-checking.

PART I. Privacy and Security Policy Status

1. Is there a Privacy Policy statement or disclaimer on the company/organization's homepage?
   __Yes
   __No

2. Is there a Security Policy statement or disclaimer on the company/organization's homepage?
   __Yes
   __No (please skip Question 3 and continue on Question 4).

3. Which of the following security measures were stated in use? (Please check all that apply.)
   __a. Monitoring: using software programs to monitor traffic
   __b. Auditing: identifying unauthorized attempts to upload or change information or otherwise cause damage
   __c. Investigation: investigating improper activities to identify individual persons
   __d. Authentication: using username and password to protect for account privacy and security
   __e. Encryption: using secure socket layer (SSL) encryption to protect data transmissions
   __f. Other (Please specify: ____.)

4. Does the security/privacy statement provide a no-liability note similar to the following?
   "The information contained in this policy should not be construed in any way as giving business, legal, or other advice, or warranting as fail proof, the security of information provided via this website."
   __Yes
   __No

5. Is there a Proper Use or Anti-Hacking statement on the homepage?
   __Yes
   __No

PART II. Web Portal System Security Status

6. Does the DNS utility—ZoneEdit.com (http://www.zoneedit.com/lookup.html)—find out the IP address of the site?
   __Yes (Please record the IP address here: ________________________________.)
   __No

7. Which of the following network information are revealed from the ARIN.database at http://ws.arin.net? Please check all that apply:

   __a. OrgName: ______________________________
   __b. OrgID: ______________________________

__c. Address: ______________________________
__d. City: ______________________________
__e. State/Prov: ______________________________
__f. Country: ______________________________
__g. NetRange: ______________________________
__h. CIDR: ______________________________
__i. NetName: ______________________________
__j. NetHandle: ______________________________
__k. Parent: ______________________________
__l. NetType: ______________________________
__m. NameServer: ______________________________
__n. NameServer: ______________________________
__o. Comment: ______________________________
__p. RegDate: ______________________________
__q. Updated: ______________________________
__r. RTechHandle: ______________________________
__s. RTechName: ______________________________
__t. RTechPhone: ______________________________
__u. RTechEmail: ______________________________
__v. Other (Specify: ____.)

8. Which of the following system-vulnerability information are revealed by using NMAP (http://insecure.org/)? Please check all that apply:

__a. Number of ports scanned: ___. (E.g., the 1662 ports scanned but not shown below are in state: closed)

__b. Number of ports not shown below are in state: __1) closed __2) filtered

__c. Number of ports shown below: ________

PORT	STATE	SERVICE	VERSION
__1) 22/tcp	open	ssh	______________________________
__2) 53/tcp	open	domain	______________________________
__3) 80/tcp	open	http	______________________________
__4) 135/tcp	open	msrpc	______________________________
__5) 443/tcp	open	ssl	______________________________
__6) 445/tcp	open	microsoft-ds	______________________________
__7) 2301/tcp	open	http	______________________________
__8) 3389/tcp	open	microsoft-rdp	______________________________
__9) 13722/tcp	open	netbackup	______________________________
__10) 13782/tcp	open	Veritas	______________________________
__11) 13783/tcp	open	arcserve	______________________________
__12) 49400/tcp	open	http	______________________________

__13) Other (Specify: ____.)

__d. Device type info: general purpose
__e. OS info:
__1) Running: Microsoft Windows
__2) Running (JUST GUESSING):

__f. OS details:
__1) details: ____
__2) Aggressive OS guesses: ____

__g. Service Info:

__1) Host: 1; OS: Windows
__2) No exact OS matches for host (test conditions non-ideal)

__h. Uptime: ________days
__i. Other (Specify: ____.)

PART III. Customer/User Account Security Status on the Website

9. Does My Account link use https:// (SSL) encryption?
__Yes
__No

10. To prevent from ID and password guessing, does the account login system limit three attempts for accessing the account?
__Yes
__No

11. To strengthening the login security, doe the login system require a duo-security for accessing the account? (E.g., asking the user to answer a pre-set security question or sending a security code to the user's cell phone or email and s/he has to enter the code within 10 minutes for accessing the account.)
__Yes
__No

12. Does the website's Search tool reveal sensitive information of customers or employees?
__Yes.
__No
- If yes, please specify: ____.)

-End-

ENHANCING AN ORGAINATION'S CYBERSECURITY

With the cybersecurity auditing instrument ready in hand, students formed small teams, contacted and identified a local company, a local government agency, or a nonprofit organization that needs assistance to audit the cybersecurity of its e-business, e-government, or web services. Each team used the auditing instrument to examine and log the cybersecurity strengths and vulnerabilities of the website systems. Upon completion of the audit, students applied their intelligences and developed proactive solutions to overcome the website vulnerabilities and strengthen the cybersecurity of the company or organization. Last, each student team wrote and presented a proposal for the company, or the local government agency, or the nonprofit organization to enhance its cybersecurity.

PEDAGOGICAL AND PRACTICAL IMPLICATIONS

Incorporating an immersive learning project into the design and delivery of real-world hands-on assignments has the following pedagogical and practical implications.

First, the immersive learning project would enable instructors (a) to guide students to develop a cybersecurity auditing instrument based on their classroom learning and review of related literature and the current cyber world; (b) to direct students to immerse into the society, communicate and find local companies, banks, government agencies, or nonprofit organizations that need assistance to identify their website vulnerability and to enhance their cybersecurity; and (c) to work with their clients and report the auditing results with detailed evidences and to recommend solutions to overcome the website vulnerabilities and to strengthen the cybersecurity of the organization.

Second, learning through the immersive project, students would be able to apply their IT skill set, business communication, and critical and creative thinking in solving the real-world problems. The demand for hiring college graduates with critical and creative thinking, innovative problem solving, and effective communication skills is growing among U.S. companies, government agencies, and nonprofit organizations for maintaining the global competitiveness.

Finally, the project would enable computer information systems students to establish a good relationship with their clients and work on more IT-related projects as an intern or employee.

REFERENCES

Ashford, W. (2014, October 3). Google could face $100 million lawsuit over nude celebrity pictures. *Computer Weekly*. Retrieved from http://www.computerweekly.com/news/ 2240232039/Google-could-face-100m-lawsuit-over-nude-celebrity-pics

Ashford, W. (2014, December 10). Social media threats to business on the rise. *Computer Weekly*. Retrieved from http://www.computerweekly.com/news/2240236398/Social-media-threats-to-business-on-the-rise-says-report

Boggs, R. A., & Walters, D. (2006). A longitudinal look at e-government in practice. *Issues in Information Systems, 7*(2), 161-164.

Campbell, D. & Beck, A. C. (2004). Answering Allegations: The Use of the Corporate Website for Restorative Ethical and Social Disclosure, *Business Ethics,13*(2), 100.

Fareeha, A. (2019, Feb. 28). U.S. e-commerce sales grow 15% in 2018. Digitalcommerce360.com. Retrieved from https://www.digitalcommerce360.com/article/us-ecommerce-sales/

Foxon, M. (1987). Transfer of training: A practical application. *Journal of European Industrial Training, 11*(3), 17-20.

Freitas, S. D., Rebolledo-mendez, G., Liarokapis, F., Magoulas, G., & Poulovassilis, A. (2010). Learning as immersive experiences: Using the four-dimensional framweork for designing and evaluating immersive learning experiences in a virtual world. *British Journal of Educational Technology, 41*(1), 69-85.

Garcia, R. C. (2004). Network security: Mapping intrusion and anomaly detection to very-high-degree polynomials. *Signals, Systems, and Computers, 2*(7), 1449−1452.

Gold, J. (2019, March 22). Triton and the new wave of IIoT security threats. *Network World*. Retrieved from https://www.networkworld.com/article/3375206/triton-and-the-new-wave-of-iiot-security-threats.html

Isaksen, S. & Treffinger, D. (1985). *Creative Problem Solving: The Basic Course*. Buffalo, NY: Bearly Limited.

Jamieson, S. (2002). The ethics and legality of port scanning. SANS Institute. Retrieved from http://www.sans.org/reading_room/whitepapers/legal/the_ethics_and_legality_of_port_scanning_71?show=71.php&cat=legal

McNurlin, B. C., & Sprague, R. H. Jr. (2009). *Information systems management in Practice* (8th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.

Mills, R. J., Hauser, K., & Pratt, J. A. (2008). A comprehensive two-level framework for information systems curriculum design, assessment and improvement. *Journal of Computer Information Systems, 48*(4), 1-14.

Symantec. (2019). Symantec 2019 Internet Security Threat Report. *Symantec Enterprise Security, Vol. 24. Symantec.* Retrieved from https://img03.en25.com/Web/Symantec/%7B1a7cfc98-319b-4b97-88a7-1306a3539445%7D_ISTR_24_2019_en.pdf

Trustwave, (2015). The 2015 Trustwave Global Security Report. Retrieved from https://www2.trustwave.com/rs/815-RFM-693/images/ 2015_TrustwaveGlobalSecurityReport.pdf

Winkler, I. (2004, July 19), What is a security audit? Tech Target. Retrieved from http://searchcio.techtarget.com/sDefinition/0,,sid182_gci955099,00.html

Zhao, J. J., Alexander, M. W., & Truell, A. D., (2014). Immersive learning of real-world problems and solutions: An innovative approach to attracting students to computer information systems programs. *Issues in Information Systems, 15*(1), 98-105.

Zhao, J. J. & Zhao, S. Y. (2010). The impact of IQ+EQ+CQ integration on student productivity in Web design and development. *Journal of Information Systems Education, 21*(1), 43-53.

Zhao, J. J. & Zhao, S. Y. (2015). Security and vulnerability assessment of social media sites: An exploratory study. *Journal of Education for Business, 90*(8), 458-466.