Journal of Forensic and Investigative Accounting
Volume 11: Issue 1, January–June 2019

Mitigating Cyberattacks: An Active Learning Instructional Resource

David C. Hayes
Ann D. O'Brien
*Chelley M. Vician**

Introduction

Cybercrime now occupies the number two spot for United States (U.S.) companies in a 2016 global economic crime survey by PricewaterhouseCoopers (PwC) and may soon move to the largest reported kind of economic crime against organizations, overtaking "asset misappropriation." Data breaches and security incidents continue to cause reputation issues and financial consequences for corporations, healthcare organizations, and government agencies (PwC, 2018; Verizon Enterprise, 2018). The U.S. government enacted cybersecurity information sharing legislation in 2015, as part of the 2016 omnibus spending package (Risen, 2015) and preceded by Executive Order 13691 (National Archives, 2015; White House—Office of the Press Secretary, 2015). Accountants, in their role as trusted business advisors, are becoming more and more involved in helping organizations address cybersecurity concerns.

Accounting industry leaders stress the importance and relevance of understanding cybersecurity issues as well as understanding the connection with professional standards. In 2014, the American Institute of Certified Public Accountants' (AICPA) Center for Audit Quality (CAQ) issued an official alert to its members about the necessity of treating cybersecurity "as a broader business issue" and relevant to external auditors of companies (Tysiac, 2014).

Kastiel (2015) posted the full Weil alert "SEC Disclosure and Corporate Governance" highlighting the increasing societal and regulatory expectations regarding cybersecurity priorities for boards, executives, and auditors. Accountants' stake in cybersecurity is especially evident as they are called upon to attest to the safety of information in the "cloud" and outsourced services provided to clients. In 2011, the Auditing Standards Board AICPA implemented a new Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization, effectively replacing SAS 70. The Service Organization Control (SOC) reports "are internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service" (AICPA, 2016). SSAE 18 supersedes SSAE 16 and aims to clarify and enhance the usefulness and quality of SOC reports (Bantz, 2018). Most recently, the AICPA created an overarching "Cybersecurity Risk Security Management Reporting Framework," addressing key aspects of secure information (security, availability, processing integrity, confidentiality, and privacy) and communications about the extent and effectiveness of controls (AICPA, 2018). The AICPA renamed SOC reports to stand for "system and organization controls." Clearly cybersecurity issues are of increasing importance for the accounting profession.

Consequently, accounting educators must prepare students with knowledge of the fundamentals of cybersecurity. How can the complex topics and relevance of cybersecurity in our modern world of transformative technologies be taught to accounting students? Learning by doing and active learning, along with authentically situated problem-solving, are well-established models for education. Games and simulations have been highlighted by Carnegie Mellon's Software Engineering Institute as an effective learning tool for cybersecurity, noting:

> "…it is only with the game or simulation that cybersecurity professionals can truly put their skills to the test and prepare themselves for events in the real world, without risking real-world assets. (Herr and Allen, 2015, p. 8)."

This article presents an authentically situated active learning instructional resource developed around the Department of Defense (DoD) CyberProtect simulation (Carney News, 2010). The simulation addresses fundamental cybersecurity

*The authors are, respectively, professor at James Madison University, senior lecturer at University of Wisconsin—Madison, and associate professor at University of St. Thomas.

knowledge (e.g., common cyberattacks and mitigating security tools) and allows active experimentation with differing cybersecurity strategies in a simulated network environment based on limited resource budgets. By completing the cybersecurity instructional resource, students should acquire increased knowledge of cybersecurity attacks and mitigating controls to reduce the likelihood of exposure to these attacks.

The Assignment

This project is a fun introduction to system security concepts where, acting as a system administrator in the DoD CyberProtect video-game-type simulation, you protect your systems from attacks such as viruses, flooding, data theft, jamming, etc. You complete at least one round (four quarters) during which you experience multiple attacks to security measures implemented. Each of these attacks may be either successful (your controls failed to prevent the attack) or unsuccessful (the controls stopped the attack from doing damage). You note the attacks that were perpetrated on your system during each step of the simulation and note whether or not the controls you implemented were effective, noting failures in security in the previous quarter, and determining why the controls you had in place did not prevent the attack. You then attempt to improve your system for the subsequent quarter. The ultimate objective of the simulation as originally designed by the DoD is to produce a ninety percent readiness rating. If this is achieved, then you can print out a certificate that states that you have reached that level (for your resume perhaps). You are not required to reach a ninety percent readiness rating, just complete at least four quarters with a seventy-five percent or higher rating.

To start the simulation, open the DoD link: http://iatraining.disa.mil/eta/cyber-protect/launchpage.htm.

Select "Launch New CyberProtect." At the Login screen, select "Enter CyberProtect" and then type in your first and last name and select "accept." Select "OK" if you are warned about cookies being stored on your computer. Once you are at the main menu, watch the five-minute tutorial that explains the basic steps in a round.

Next, select "Navigation Overview" in the main menu for a quick guide on navigation. Next, select "Mark's Notes" to become familiar with potential mitigating tool descriptions, attack handling, and strategies. Once you are familiar with "Mark's Notes," you are ready to begin the game by purchasing resources and placing them in the system to defend your network. Select "Play" from the main menu and then "Tool Requisition" to begin. You can watch the tutorial again if needed for a refresher on how to play.

The following Table 1 shows all of the possible attacks in the CyberProtect simulation. You should become familiar with each attack, be able to describe the possible problems the attack could cause, and also be able to explain the control (or controls) that should be used to prevent the attack from being successful.

Deliverables: To confirm that you have completed one simulation, capture the end results of the simulation and submit an electronic copy of that document (note: it is probably easiest to just do a screen capture—control alt print screen—and paste it into your MS Word document if you experience a problem electronically printing the network configuration to your desktop). Also, include a screen capture of the network configuration at the beginning of the fourth quarter.

Table 1: Information Security Attacks

Attack	Description
Data Modification	Change or destroy information on a system
Data Theft	Steal sensitive information without owner knowing about it
Flooding	Bombards system with more messages or information than it can handle
Imitation or Spoofing	Pretends to be a valid user by using a stolen User ID/password or by "hijacking" a valid session
Jamming	Electronically disrupt transmission signals
Mole	A trusted person of an organization gives information to an outsider
Packet Sniffer	Tools collect information from network such as User ID, passwords, contents of E-mail messages, credit card numbers
Social Engineering	Information obtained by talking with people, obtaining their trust, and tricking them to give out information, like passwords
Virus	Malicious program that reproduces by attaching itself to a computer program

Case Efficacy

To test the efficacy of the simulation's ability to increase students' awareness of cybersecurity attacks and mitigating tools, thirty-eight students in an undergraduate accounting information systems course at a public university located in the Eastern U.S. played the simulation for two rounds. In the first round the students were instructed to only watch the tutorial and play the game. In the second round the students were instructed to read Mark's notes on strategies of tools that can be used to reduce the likelihood of cyberattacks. After playing two rounds of the simulation, students were asked their perception of the game and its effect (Likert scale where one represents strongly disagree, four represents neither agree nor disagree, and seven represents strongly agree).

The results of the students' perceptions in Table 2 reflect that the students indicated positive student experiences when using the learning resource. They felt that the simulation helped them learn more about cyberattack and mitigating tools to reduce the likelihood of attacks. They also agreed that they would benefit from more assignments like this one where they could apply the knowledge learned, and that they enjoyed the assignment.

Table 2: Student Self-Assessment of CyberProtect Simulation

Survey Statements (N = 38)	Mean* (Std Dev)	# (%) of 5, 6, 7, responses	t-stat / p-value (h_o=4)
I learned additional knowledge about computer Cyberattacks by completing this assignment.	5.5 (1.4)	29 (76%)	6.5 <.001
Mark's Notes were helpful in determining which Mitigating Controls (Tools) to purchase.	6.1 (1.0)	35 (92%)	12.9 <.001
I learned additional knowledge about Mitigating Controls (Tools) by completing this assignment.	5.5 (1.4)	31 (82%)	6.6 <.001
I would benefit from having more assignments like this one where I can apply knowledge that I have learned.	5.5 (1.4)	30 (79%)	6.8 <.001
I enjoyed this assignment.	5.5 (1.1)	31 (82%)	7.9 <.001

*Scale: 1=Strongly Disagree, 2=Disagree, 3=Somewhat Disagree, 4=Neither Agree nor Disagree, 5=Somewhat Agree, 6=Agree, 7=Strongly Agree

In addition to the students' perception, a pre/post-test of the operational readiness rating was analyzed to see if the students did reduce the likelihood of future cyberattacks. The pre/post-test mean (standard deviation) final "Operational Readiness Rating" increased from 79.4% (11.1%) to 83.9% (8.3%). This 4.5% mean increase is significant (t-stat=2.0, p-value = .023) and provides evidence that the students did learn and apply knowledge of tools to mitigate the likelihood of cyberattacks.

Concluding Remarks

Cybersecurity is, and will continue to be, a topic of critical importance for accountants in an era of expanding information systems and security issues. The cybersecurity instructional resource provides an active, authentically situated, and easy to implement learning approach to the topic of cybersecurity. The DoD developed and controls the simulation, limiting a user's ability to address evolving technology, or adapting materials to new cyberattacks. Enhancements and updating are in their hands. As currently configured, the DoD CyberProtect simulation provides students the opportunity to become more familiar with and solve the problem of potential cyberattacks, using mitigating tools and strategies for deploying resources within a fun learning environment.

The quantitative student feedback implies that student use of the resource can increase student knowledge of cyberattacks and mitigating tools. The results also suggest that most, if not all, students have enjoyable experiences using the cybersecurity resource.

The resource can be enhanced with additional activities and approaches depending on one's learning goals or course focus (e.g., cybersecurity, IT audit, information systems, forensics, etc.).[1] Work could be done individually, in teams, in or outside of class, and with a variety of supplemental materials. For example, students could research and discuss cybersecurity material available from the AICPA (e.g., SOC reporting, Trust services), ISACA (e.g., COBIT), National Institute of Standards and Technology Framework (NIST), accounting firms, and other professional resources. Another extension could be to map each cyberattack to a forensic analysis, having students further consider not only how to prevent, but also how to detect and correct the intrusion. Students could possibly discuss why the attacks listed are the most pertinent, the relative value of various mitigation approaches, and innovative alternative strategies. For deeper explorations of additional learning options, users could peruse the U.S. Department of Defense Information Assurance Support Environment catalogue and discover a plethora of cybersecurity resources that merit further consideration (DISA, 2018).

Cybersecurity is a quickly evolving critical topic for accounting professionals, with ever-expanding resources, emerging mitigation strategies, and possibilities for learning. The resource presented in this article offers access to foundational knowledge for building information security, integrity, and privacy expertise, hopefully inspiring further interest and competency in the arena of cybersecurity.

[1] The teaching materials are available upon request from the contact author.

References

AICPA (2016). Service Organization Control (SOC) Reports. http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/SORHome.aspx (accessed 07/07/2016).

AICPA (2018). SOC for Cybersecurity. https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative.html (accessed 06/13/2018).

Bantz, Josh. (2018). Introduction to SSAE 18 and Service Organization Controls (SOC) Examinations. https://www.macpas.com/introduction-to-ssae-18-and-service-organization-controls-soc-examinations/ (accessed 06/13/2018).

Carney "News" (2010). CyberProtect selected as finalist in 2010 Serious Games Showcase and Challenge. http://www.teamcarney.com/news/cyberprotect-selected-as-finalist-in-2010-serious-games-showcase-challenge/ (accessed 08/01/2016).

Herr, C. and Allen, D.M. (2015). Video games as a training tool to prepare the next generation of cyber warriors. Carnegie Mellon University: Software Engineering Institute—Cyber Workforce Development (CWD), https://resources.sei.cmu.edu/asset_files/Presentation/2015_017_001_442344.pdf (accessed 07/06/2016).

Kastiel, K. (2015, February 18). What's New in 2015: Cybersecurity, Financial Reporting, and Disclosure Challenges. Harvard Law School Forum on Corporate Governance and Financial Regulation, https://corpgov.law.harvard.edu/2015/02/18/whats-new-in-2015-cybersecurity-financial-reporting-and-disclosure-challenges/ (accessed 07/07/2016).

National Archives (2015). 2015 Executive Orders Disposition Tables: Barack Obama—2015. https://www.archives.gov/federal-register/executive-orders/2015.html (accessed 07/07/2016).

PricewaterhouseCoopers (2018). Pulling Fraud out of the shadows: Global Economic Crime and Fraud Survey 2018, https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf (accessed 11/30/2018).

Risen, T. (2015, December 18). Obama signs cybersecurity law in spending package. U.S. News and World Report. http://www.usnews.com/news/articles/2015-12-18/obama-signs-cybersecurity-law-in-spending-package (accessed 07/07/2016).

Tysiac, K. (2014, March 24). Auditors have important role in cybersecurity. *Journal of Accountancy*. http://www.journalofaccountancy.com/news/2014/mar/20149835.html (accessed 07/06/2016).

United States Defense Information Systems Agency (DISA) (2016). Information Assurance Support Environment—Online Training Catalog. http://iase.disa.mil/eta/Pages/online-catalog.aspx (accessed 06/13/2018).

Verizon Enterprise (2018). Data breach investigations report, https://enterprise.verizon.com/resources/reports/dbir/ (accessed 11/30/2018)

White House—Office of the Press Secretary (2015, February 13). Executive Order—Promoting Private Sector Cybersecurity Information Sharing. https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari (accessed 07/07/2016).