



Activity Simulation for Experiential Learning in Cybersecurity Workforce Development

John Burris¹(✉), Wesley Deneke²(✉), and Brandon Maulding¹

¹ Southeastern Louisiana University, Hammond, LA 70402, USA
jburris@southeastern.edu

² Western Washington University, Bellingham, WA 98225, USA
Wesley.Deneke@wwu.edu

Abstract. A significant challenge to maintaining security within an organization is the training of a non-technical workforce to respond appropriately to cybersecurity threats. This work describes an online environment that utilizes experiential learning to give non-technical workers an increased exposure to issues in cybersecurity. We present a simulation-based approach that provides a better understanding of specific cybersecurity threats through experiential learning. The presented interface uses simulations of cybersecurity threats to provide concrete experiences rather than descriptions. While moving through the simulation, the user can attempt multiple actions and is provided with an “awareness” measure. For each, the system provides continuous feedback to allow active experimentation. After each threat has been exposed, the environment provides a narrative of the user’s actions with suggested improvements to allow for reflective observation. This work includes a user study of the interface, shows the results of usability testing, and evaluates the effectiveness of the training through simulation.

Keywords: Cybersecurity · Experiential learning · Workforce development
Simulation

1 Introduction

Cybersecurity has been described by the National Science Foundation as a defining issue of our time [1]. Entities such as the “Shadow Brokers” have highlighted cybersecurity as a significant weakness in the United States’ national security by obtaining classified documents through cyberattack [2]. Global businesses face an estimated cost of \$400 billion (US) each year due to cyberattacks [3]. Cybersecurity awareness has become a critical concern not only to organizations, but among individuals as well. Over eight million adults in the United States were victims of identity theft in 2005, with 56% of the victims not even knowing how their personal information was taken from them [4].

A popular response has been the introduction of frameworks that provide standards, guidelines, and best practices to help organizations understand and manage cybersecurity risks. These frameworks have led to national certifications such as CompTIA Security+, Certified Ethical Hacker (CEH), and Certified Information Systems Security

Professional (CISSP) that train and certify security professionals on the policies and responses. This has provided organizations with a means to bolster the cybersecurity awareness of their technical workforce. According to the National Institute of Standards and Technology (NIST), however, these efforts to improve cybersecurity are undermined by a lack of comparable training for the non-technical workforce [5]. Non-technical workers often lack knowledge of how to recognize and respond to cybersecurity threats. Consequently, they become the ‘weakest link’ in the security circle. Techniques such as shoulder surfing, phishing, dumpster diving, and impersonation are all established techniques that could be addressed with additional awareness and training, but national certifications for the non-technical workforce do not exist today [5].

The problem this work explores is how to expose the non-technical workforce to key cybersecurity threats so that they will have an increased awareness of these threats. Training content must be presented in a way that is natural to the intended trainee. Due to their lack of technical expertise, a trainee may be familiar with checking their email, but may not understand statements used to describe recognizing a potential threat, like “check the sender’s domain”. Similarly, a trainee may recognize a potential threat, but not be aware of the severity of the threat or how to respond appropriately. Existing solutions for workforce cybersecurity education largely target technical workers, such as security professionals, or lack hands-on training [6–9]. Hands-on training like [10–15] provide effective training through experiential learning, but as before target technical workers.

The focus of this work is the presentation of the training content. This paper introduces a simulation-based approach that emphasizes experiential learning to provide non-technical workers a better understanding of how to recognize and respond to cybersecurity threats. Learning has been the focus of significant research and debate. The theory of Experiential Learning was introduced as early as 1938, but has been increasing in popularity as it has been shown to increase retention and enrich the learning experience. Kolb give four “modes” of learning: (1) concrete experiences, (2) reflective observation, (3) abstract conceptualization, (4) active experimentation. The proposed certification process uses these modes to provide a better understanding of specific cybersecurity threats [16]. Users are presented with simulations of cybersecurity threats to provide concrete experiences. While moving through the simulation, the user can attempt multiple actions and is provided with an “awareness” measure. For each, the system provides continuous feedback to allow active experimentation. After each threat has been exposed, the environment provides a narrative of the user’s actions with suggested improvements to allow for reflective observation.

The rest of this paper is organized as follows: the approach for simulating cybersecurity threats is described in Sect. 2. Section 3 evaluates the results gathered from a system prototype. Finally, conclusions and next steps are summarized in Sect. 4.

2 Using Experiential Learning for Cybersecurity Workforce Development

2.1 Approach for Simulating Cybersecurity Threats

This work describes a prototype of a system that uses simulations of cybersecurity threats to provide concrete experiences rather than traditional descriptions such as videos or textual narratives. While moving through the simulation, the user is able to attempt multiple actions and provide an “awareness” measure. For each, the system provides continuous feedback to allow active experimentation. After each threat is exposed, the environment provides a narrative of the user’s actions with suggested improvements to allow for reflective observation.

As an example, the user could select “Phishing” as a cybersecurity threat. Phishing is the process of sending emails to manipulate recipients into providing personal information. To simulate such a scenario, the user would progress to a simulated email client. The user’s email address is shown as user@example.com. They receive an email from boss@example.com with an “important” attachment. Note the domain of the “boss” account is misspelled. This provides a concrete experience of a real-world phishing attempt. This simulation is conceptualized in Fig. 1. The simulation shown in Fig. 1 will progress the user through emails that are not at risk of being phishing attempts to judge the competency of the user both when a threat is present and when there are no threats. In addition, the simulation will repeat scenarios until the responses demonstrate a determined level of competency.


<p>To: user@example.com From: boss@example.com Subject: Urgent – Respond Immediately</p> <hr/> <p>Hey, Look, this form is way overdue and I need you to fill it out and return ASAP. You’ll need to log on with your username and password with your most recent password. Thanks!</p> <hr/> <p> EmployeeInfoForm.doc</p>	<p>What is your “threat level” at?</p> <table> <tr> <td>Response:</td> <td>Suggested:</td> </tr> <tr> <td>5- <input type="checkbox"/></td> <td>5- <input type="checkbox"/></td> </tr> <tr> <td>4- <input type="checkbox"/></td> <td>4- <input type="checkbox"/></td> </tr> <tr> <td>3- <input type="checkbox"/></td> <td>3- <input type="checkbox"/></td> </tr> <tr> <td>2- <input type="checkbox"/></td> <td>2- <input type="checkbox"/></td> </tr> <tr> <td>1- <input type="checkbox"/></td> <td>1- <input type="checkbox"/></td> </tr> </table> <p>What do you do?</p> <p><input type="button" value="Open Attachment"/></p> <p><input type="button" value="Contact Boss"/></p> <p><input type="button" value="Call IT department"/></p> <p><input type="button" value="Delete Email Immediately"/></p>	Response:	Suggested:	5- <input type="checkbox"/>	5- <input type="checkbox"/>	4- <input type="checkbox"/>	4- <input type="checkbox"/>	3- <input type="checkbox"/>	3- <input type="checkbox"/>	2- <input type="checkbox"/>	2- <input type="checkbox"/>	1- <input type="checkbox"/>	1- <input type="checkbox"/>
Response:	Suggested:												
5- <input type="checkbox"/>	5- <input type="checkbox"/>												
4- <input type="checkbox"/>	4- <input type="checkbox"/>												
3- <input type="checkbox"/>	3- <input type="checkbox"/>												
2- <input type="checkbox"/>	2- <input type="checkbox"/>												
1- <input type="checkbox"/>	1- <input type="checkbox"/>												

Fig. 1. A mockup of a simulated cybersecurity threat - phishing

The implementation of the prototype focused on increasing the amount of feedback during experimentation to maximize retention. Using previous guidelines for color selection and components, a traditional green/red color scheme was used for positive and negative feedback respectively [17]. The prototype design also considered the possible reasons for non-use [18]. The text of emails were chosen so that it would seem relevant to any industry or position to avoid issues such as disenfranchisement or disenchantment. The vocabulary and traditional design were chosen to prevent active resistance to the training. These issues were addressed to increase usage and engagement for the purpose of increased learning and retention. The initial prototype can be seen in Fig. 2. Figure 2 displays the beginning of a threat simulation. The colors are homogenous to draw attention first to the content being displayed to the user for evaluation and response. At this point, the instructional text has been minimized. Audio instructions provide additional details to the user.

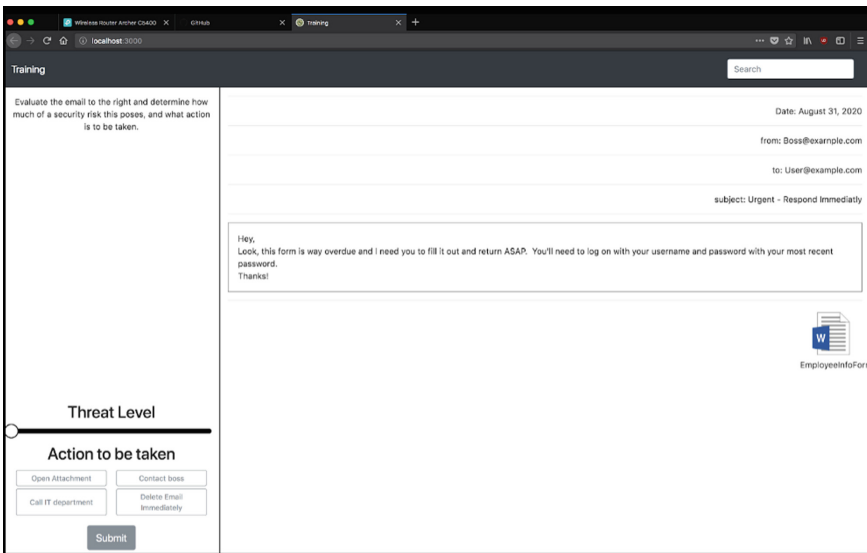


Fig. 2. Prototype of cybersecurity training simulation as initially displayed to user. (Color figure online)

Figure 3 shows the prototype providing active feedback to the user. Since there are multiple points of interaction, the consistent use of colors is key to preventing user confusion. The points of interaction are all concentrated on the bottom left section of the interface. The three provided points of interaction are: a slider used to determine the level of threat, a multiple choice selection for action to be taken, and a submit button that prevents submission without an acceptable input.

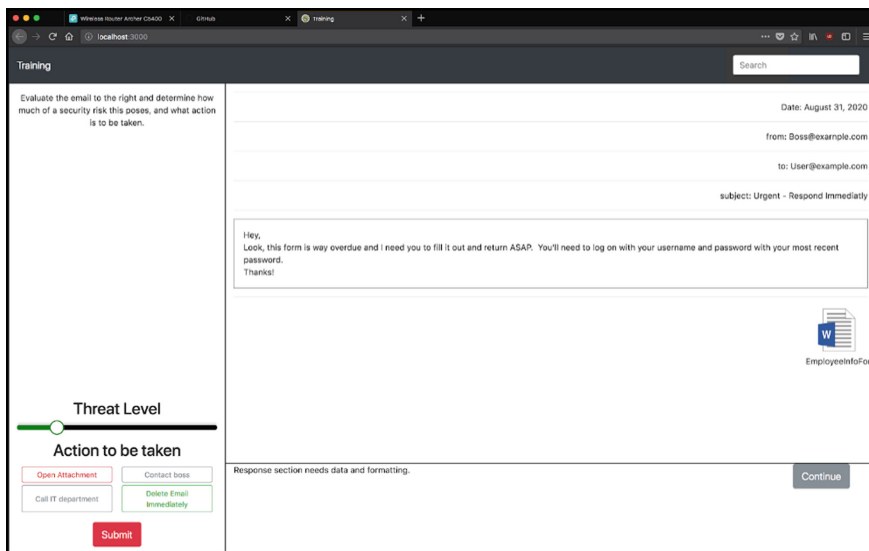


Fig. 3. Prototype of cybersecurity training simulation with active feedback displayed. (Color figure online)

3 Evaluation

A small-scale user study with twenty-nine participants was performed to determine the performance of this approach when compared to a traditional approach for introducing non-technical workers to cybersecurity threats. All twenty-nine participants were given a pretest to determine their awareness of the threat and knowledge of appropriate actions. As a control, fourteen participants were given an email about phishing as sent from a company IT department. Fifteen participants used the prototype for experiential learning as an introduction to phishing. All participants were then given the same questions from the pretest as a posttest.

The test included multiple choice and true/false questions about phishing scams. Six questions were on the types of phishing attacks that were included in the simulation. Four questions were on phishing techniques that were not included in the simulation. The study was designed this way so that the control would maintain the benefit of having the capacity for more information and not having to have the detail required for simulation.

The user study does not include a second posttest to measure the retention for users after an extended period of time. The pretest, training, and posttest were all done in a lab at a single sitting. The process lasted no more than 20 min to complete.

Highlighted increases in scores for each method are shown in Table 1. The results are shown as the total increase in scoring for the key points of interest in the study: the overall increase in performance, the increase in performance for attacks included in the simulation and the increase in performance for attacks not included in the simulation.

Table 1. Results of user study.

Measure	Training type	Change in score (rounded)
Total test score	Narrative email	34%
	Experiential learning	39%
		(+5%)
Phishing attacks shown in prototype	Narrative email	30%
	Experiential learning	54%
		(+24%)
Phishing attacks not shown in prototype	Narrative email	39%
	Experiential learning	15%
		(-24%)

Although the user study was limited, the results are promising. The participants that used the simulated cybersecurity threat did have an increased level of awareness and knowledge about those threats. However, the increase was drastically reduced when the tested scenario was not included in the simulated attack. The total test score improvement showed an advantage over the narrative email, but the number of questions were weighted to phishing attacks that were included in the simulation.

The narrative email resulted in an increased the level of awareness and knowledge on all variations of phishing. The improvements were consistent for both question types and the total test score.

The most significant result is the improvement shown by the questions on phishing attacks that were included in the prototype. A 54% improvement compared to the 30% improvement shown by the control shows that the approach does improve learning. The inverse improvements shown by the approach for questions on phishing attacks not included in the simulation are not as significant since it is more important to show that the improvements are a result of the simulation.

4 Conclusion

4.1 Summary of Results

This work presents an approach for non-technical, cybersecurity workforce development that uses experiential learning to increase the effectiveness of training. A prototype as developed that focused on a single cyber attack. The goal of prototype was to be an interface for education that provided the user with an approachable lesson with potential for experimentation and personal reflection. A user study was conducted to determine the increased awareness and knowledge resulting from the presented approach when compared to a traditional method for preventing cybersecurity attacks.

While significant challenges remain in the development of a comprehensive cybersecurity workforce development system, the initial results show that for non-technical workers, the increase in awareness can be substantial. Possible reasons for these results are the increased level of engagement and decreased disenfranchisement.

4.2 Future Work

Cybersecurity threats continue to evolve and diversify, which makes providing a wide variety of simulation-based training scenarios more desirable. However, training content is currently created manually, which is a time-consuming process that limits the diversity of the content. Future work should explore providing tools that support the rapid development of diverse simulation-based training content for experiential learning. An authoring tool like [19–22] can present authors with an intuitive, visual-based domain-specific language to specify desired simulation content in a declarative manner. The technical specifications of simulation design can be abstracted behind buttons, checkboxes, sliders, and other user interactions of a visual dashboard, such as depicted in Fig. 4. The benefit is that it removes the need to have a human user design content.

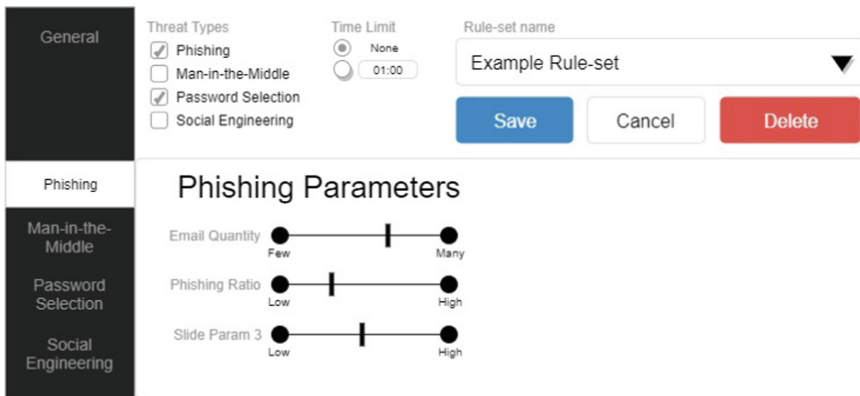


Fig. 4. A mockup of a visual authoring tool

While authoring tools can provide a high-level approach to create and modify training content, a human user must still design and validate the content produced. Another area of future work then is a simulation generator that can dynamically create diverse simulations. Specifications from the authoring tool can feed into an engine that employs procedural generation and AI planning to dynamically produce diverse simulations. Such a solution could provide variation in training content, without the need for manual, human design.

In addition to the authoring and generation tools, future work will include an element of gamification to encourage the completion of the workforce development process. This encouragement to gain exposure to multiple threats and improved response will lead to a more comprehensive understanding of cybersecurity in the non-technical workforce. Gamification is the addition of elements of traditional gameplay to areas outside of gaming. These elements can include scoring, awards, and competition. It is primarily used to increase user engagement in a process [23]. The proposed process for workforce development will use an award system similar to the

system used in the internationally recognized award system for the Olympic Games. While not indicative of performance in relation to any other user, it is indicative of the demonstrated level of competency for a particular cybersecurity scenario. An initial component for gamification is shown in Fig. 5.

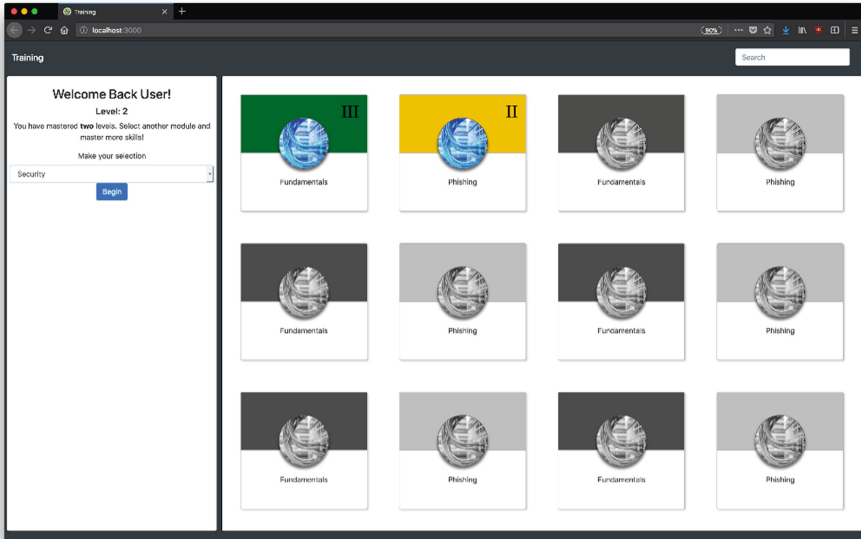


Fig. 5. Initial prototype of cybersecurity training scenarios with gamification aspect included.

References

1. National Science Foundation: Cybersecurity: tech, tools, and training to safeguard the future (2017). https://www.nsf.gov/news/special_reports/cybersecurity/index.jsp. Accessed Nov 2017
2. Aftergood, S.: Cybersecurity: the cold war online. *Nature* **547**, 30 (2017)
3. Okenyi, P.O., Owens, T.J.: On the anatomy of human hacking. *Inf. Syst. Secur.* **16**(6), 302–314 (2007)
4. Federal Trade Commission: About Identity Theft (2006). <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html>. Accessed Nov 2017
5. NIST: NIST Impacts: Cybersecurity (2017). <https://www.nist.gov/industry-impacts/cybersecurity>. Accessed Nov 2017
6. Newhouse, W.: NICE cybersecurity workforce framework: national initiative for cybersecurity education. Special Publication (NIST SP)-800-181 (2017)
7. Paulsen, C., McDuffie, E., Newhouse, W., Toth, P.: NICE: creating a cybersecurity workforce and aware public. *IEEE Secur. Priv.* **10**(3), 76–79 (2012)
8. Conklin, W., Cline, R., Roosa, T.: Re-engineering cybersecurity education in the US: an analysis of the critical factors. In: *IEEE 47th Hawaii International Conference on System Sciences (HICSS)* (2014)

9. Sensato Education & Simulation: Sensato Cybersecurity Solutions. <http://www.sensato.co/sensato-education-simulation>. Accessed Dec 2017
10. Cheung, R., Cohen, J., Lo, H., Elia, F.: Challenge based learning in cybersecurity education. In: Proceedings of the 2011 International Conference on Security and Management (2011)
11. Assante, M., Tobey, D.: Enhancing the cybersecurity workforce. *IT Prof.* **13**(1), 12–15 (2011)
12. Abraham, S., Shih, L.: Instructional perspective: towards an integrative learning approach in cybersecurity education. *Inf. Secur. Educ. J.* **2**(2), 84–90 (2015)
13. Irvine, C., Thompson, M., Allen, K.: Active learning with the CyberCIEGE video game. In: Federal Information Systems Security Educators' Association Conference (2005)
14. Benjamin, C., Irvine, C., Thompson, M.: A video game for cyber security training and awareness. *Comput. Secur.* **26**(1), 63–72 (2007)
15. Fite, B.: Simulating cyber operations: a cyber security training framework (2014). <https://www.sans.org/reading-room/whitepapers/bestprac/simulating-cyber-operations-cyber-security-training-framework-34510>. Accessed Dec 2017
16. Kolb, D.A.: Experiential learning: experience as the source of learning and development. Prentice-Hall, Englewood Cliffs (1984)
17. Wright, P., Mosser-Wooley, D., Wooley, B.: Techniques & tools for using color in computer interface design. *Crossroads* **3**(3), 3–6 (1997)
18. Satchell, C., Dourish, P.: Beyond the user: use and non-use in HCI. In: Proceedings of the 21st Annual Conference of the Australian Computer-Human Interaction Special Interest Group: Design: Open 24/7 (OZCHI 2009), pp. 9–16. ACM, New York (2009)
19. Learning Management System. <https://www.agylia.com>. Accessed Dec 2017
20. Cyber Security eLearning. <https://www.delta-net.com/compliance/cyber-security>. Accessed Dec 2017
21. Benjamin, P., Patki, M., Mayer, R.: Using ontologies for simulation modeling. In: IEEE Winter Simulation Conference (WSC 2006) (2006)
22. Miller, J.A., Baramidze, G., Sheth, A., Silver, G., Fishwick, P.: Ontologies for modeling and simulation: an initial framework. In: Computer Science Department, University of Georgia, Athens, GA (2004)
23. Deterding, S., Sicart, M., Nacke, L., O'Hara, K., Dixon, D.: Gamification: using game-design elements in non-gaming contexts. In: CHI 2011 Extended Abstracts on Human Factors in Computing Systems (CHI EA 2011), pp. 2425–2428. ACM, New York (2011)