Journal of Cybersecurity Education, Research and Practice

Volume 2021 | Number 1 Article 2

July 2021

An exploratory study of mode efficacy in cybersecurity training

Michael D. Workman
Texas A&M University, College Station, workmanfit@yahoo.com

An exploratory study of mode efficacy in cybersecurity training

Abstract

Cybersecurity capabilities in organizations and governmental agencies continue to lag behind the threats. Given the current environment, these entities have placed renewed emphasis on cybersecurity education. However, education appears to lack its full potential in most settings. Few empirical studies have systematically tested the efficacy of various training methods and modes, and those that have been conducted have yielded inconsistent findings. Recent literature on the use of gamified simulations have suggested that they may improve cybersecurity behaviors. Similarly, live activities such as hackathons and capture the flag events have been surmised to augment learning and capabilities. We conducted an exploratory study of these compared to a traditional classroom/laboratory approach to assess the applied behavioral contribution of each. We found that a combination of simulations with live activities in conjunction with classroom study produced the best outcomes.

Keywords

Pilot study, training, cybersecurity, simulations

INTRODUCTION

The state of the cybersecurity among democratic nations is grave, and there is little dispute regarding the need to significantly improve (Veksler, Buchler, Hoffman, Cassenti, & Sugrim, 2018). This need is present in many different verticals, but it is especially pressing within organizational and national critical infrastructure, where attackers are highly motivated and the consequences of failure may be catastrophic (Center for Strategic and International Studies, 2017).

Due to the importance of the threats, obtaining access to information on cybersecurity matters is not particularly difficult. Bookstores, universities, and the Internet are overflowing with good advice and best practices. However, countermeasures are often not put into practice until after a problem has been discovered. We suffer not from ignorance of knowing what to do, but from a seeming inability or unwillingness to put the knowledge into practice. In other words, there is a significant knowing-doing gap (Workman, Bommer & Straub, 2008). Consequently, cybersecurity training has become a focal point in both inculcation of new information as well as refreshing awareness.

However, the few empirical studies of the efficacy of various training methods and modes that have been conducted have yielded inconsistent findings (Arthur, Bennett, Edens, & Bell, 2003; Thatcher & Perrewé, 2002; Veksler, et al., 2018). Recent literature on the use of gamified simulations (e.g. Jalali, Siegel & Madnick, 2019; Jin, Tu, Kim, Heffron, & White, 2018) have suggested that highly targeted learn-practice simulations carefully crafted to address the needs of a particular audience may present an opportunity for improving cybersecurity behaviors (i.e. doing better), leading to tangible improvements in the cybersecurity stance (Arthur, et al., 2003; Rumeser & Emsley, 2018).

Beyond gamified simulations, there has been speculation that "live-fire" exercises such as hackathons and capture the flag events may further improve learner capabilities (Ernits et al., 2015). Moreover, a survey of the literature (e.g. Ernits et al., 2015; Hoffman, et al., 2005; Schepens, et al., 2002) shows both the need and the value of cybersecurity games and competitions that go beyond the typical cyber training exercises and simulations, yet there have been few if any systematic tests of these propositions to our knowledge. Such a study could prove informative to the cybersecurity training literature, as simulations and competitive games have been shown to be effective in other areas such as identifying exploitable flaws in cyber infrastructure (Pan, Teixeira, López & Palensky, 2017).

In addition, domain general studies on training effectiveness (e.g. Arthur, et al., 2003) have shown that learning occurs best when the training is targeted to a specific set of behaviors or skills, and are situated in context relevant to the learner, and are actionable. In other words, training and development that can be used immediately rather than merely instilling "head knowledge." Given these findings, best pedagogical practice uses the present-test-practice-assess (PTPA) approach to facilitate optimal learning-doing behaviors (See Figure 1). The PTPA model has been a commonly recognized best-practice pedagogy dating back to Dewey (1998) in which practice immediately follows topical instruction.

To further inform the body of cybersecurity literature, we conducted a systematic test of three modes of cybersecurity education (classroom training, simulations, live-fire exercises) compared to the traditional baseline instruction (traditional model), as well as examined the interactions on training efficacy using the PTPA approach. For this, we provided short topical instruction, followed by a short quiz on the topic. This was the baseline. The simulations replaced the midterm and final exams in the traditional class/lab instruction baseline with passing two simulation challenges presented by Codebashing® and Secure Code Warrior®. Our live fire activities included a University-wide hackathon against the OWASP® Mutillidae™ in a controlled environment, and a CTF365® activity. CTF365 is an online capture the flag environment commonly used for capture-the-flag instruction and competitions. Our primary interest was to determine the contribution of each mode of learning on cybersecurity response to factor into training evaluation and benefit analysis.

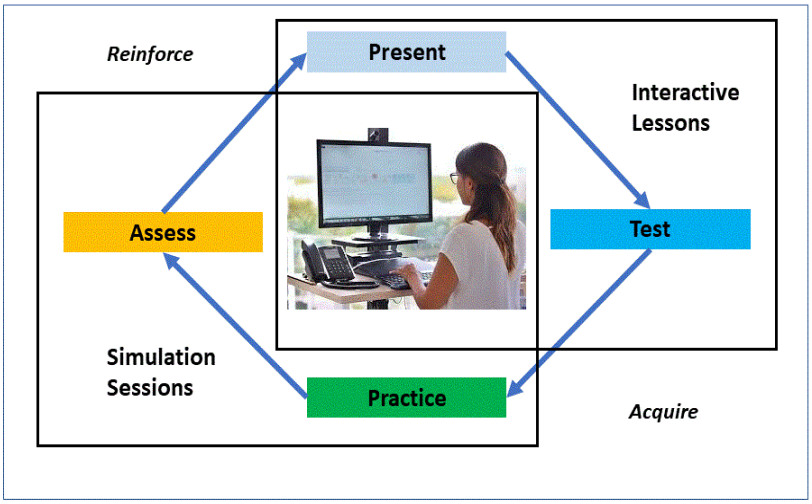

Figure 1: PTPA Training/Learning Approach

THEORY AND HYPOTHESES

Instructional Theory and Design

The contemporary model for cybersecurity instruction is based on a lecture and laboratory approach (TeachThought, 2019). To confirm, we surveyed the cybersecurity courses taught at fifty tier-1/R1 universities in the United States as listed in US News and World Report College Rankings, which indicated the wide use of a dialectical-contextual social constructivism method in which classroom lectures and team-based tasks are paired with laboratory exercises. All of the programs examined were in MIS, CIS, CS, or other IT program such as technology management. Students were all upper-class undergraduates with prerequisites in operating systems and networking. Laboratory exercises commonly used in these programs are Wireshark®, GNS3®, Cain/Abel®, Achilles®, IDS such as Zabbix® and Solar Winds® along with various cryptography labs such as PGP/GPG. By most accounts, this approach has been shown to be effective for rote knowledge (Arthur, et al., 2003). The ability to learn and practice has demonstrated knowledge acquisition benefits (Ferdig, 2006; TeachThought, 2019). Because this is the most common in-use best practice learning model, we assumed this

approach for our baseline comparative. This baseline course, used in all sections, was predicated on education to drive behavioral change by incorporating the following features (Arthur et al., 2003; Conetta, 2019; Hoke, Reuter, Romeas, Montariol, Schnell, & Faubert 2017; Sitzmann & Weinhardt, 2017):

Materials must be targeted with participant learning characteristics in mind. Participants should have materials presented to them in a way that it is clear why poor cybersecurity practices will adversely affect their missions, allowing for different learner characteristics and cognitive styles. By contextualizing the security training materials, cybersecurity can become an important means to helping participants achieve their educational goals as well as fostering effective learning outcomes.

Materials must be experientially in context for the learner. Learning materials are not sufficient to change habituated behaviors unless they are incorporated into an environment or ecosystem in which the learner will actually apply the knowledge. The materials must present commonly used technologies that the learner will likely encounter in the field. The goal is to present enough material to drive meaningful behavioral change, but not so much that it is overwhelming. Importantly, it must consider that rare anomalous activities are hard for humans to detect (c.f. Hogan & Bell, 2009); and likewise, too much stimuli tend to be ignored as noise (Banks, 2007). Moreover, the instruction must also consider the Anderson (2000), Baldwin and Ford (1988) and Burke (1997) foundational understanding of learning/knowledge decay through scaffolding and continuous reinforcement.

Materials must be actionable. Corporate and governmental infrastructure such as transaction servers and power grids have both shared and unique characteristics. The approach must allow for the learning materials to drive learners toward simple but effective steps they can take immediately to improve the cybersecurity of all aspects of typical operations. These considerations include procedural knowledge as well as domain general and domain specific knowledge.

Simulation as Learning Augmentation

There is substantial anecdotal and some scientific evidence that simulations may augment procedural, declarative, and experiential cybersecurity knowledge and hence learning effectiveness (Jin, Tu, Kim, Heffron, & White, 2018; Veksler, et al., 2018). Popular simulations include Checkmarx® Codebashing, and Secure Code Warrior®. Unfortunately, few studies have systematically tested this proposition (Voskoboinicov &. Melnyk, 2018); however, there is strong theoretical justification to support it (e.g. Miranda, 2018). The few studies that have looked at various aspects of cybersecurity simulations on learning (e.g. Hendrix, Al-Sherbaz, & Bloom, 2016; Jalali, Siegel, & Madnick, 2019, Jin et al., 2018; Landers & Armstrong, 2017; Miranda, 2018; Voskoboiniov &. Melnyk, 2018) have provided partial insights into how simulations may be utilized to augment cybersecurity training. These studies, however, have not cut across learning modes to identify modal contributions to the learning outcomes.

Nevertheless, one way in which simulations are surmised to improve learning effectiveness is by motivating and engaging the learner, largely because they are animated with procedural challenges in a manner similar to a game -i.e. they are "gamified" (Reio & Wiswell, 2001). Beyond this, simulations facilitate learning

effectiveness through reinforced encoding specificity, in which learners incorporate the situational environment along with the educational tasks (Trafton & Trickett, 2001).

Next, simulations have the ability to facilitate the connection of mental representations to the real-world environment (Miranda, 2018), which should improve performance and promote positive behavioral change relative to cybersecurity hygiene (Goode, Levy, Hovav, & Smith 2018; Veksler, et al., 2018). Simulations also allow for experimentation in a controlled environment, so that students can learn experientially (Veksler, et al., 2018). Moreover, they are surmised to enhance cognitive cueing and improve metacognitive awareness by prompting learners to reflect on their learning progress and allowing them to repeat material at critical junctures if needed (Arthur, Bennett, Edens, & Bell, 2003; Conetta, 2019). Therefore,

> H1. Cybersecurity simulations will improve applied learning performance compared to conventional classroom/lab study alone.

Live Activity Event as Learning Augmentation

A live activity such as a "hackathon" (or sometimes, live-fire-activity) or "capture the flag event" goes beyond simulation by placing the learner in active real-world situation in which participants compete to try to compromise and defend/remediate systems (Leune & Petrilli, 2017; Sommestad & Hallberg, 2012). Where simulations allow for reinforcement and elaborative rehearsal, a live activity "puts knowledge to the test" (Hoke, Reuter, Romeas, Montariol, Schnell, & Faubert 2017; Sitzmann & Weinhardt, 2017). Participants learn the effectiveness of what they have learned by means of practical application and execution of what they know (Landers & Armstrong, 2017). In that sense, it is a reinforcing reciprocal learning process – it reinforces what works, and illuminates what does not work (Hoke, et al., 2017).

Finally, unlike simulations, which are sequential, live activities are non-sequential in nature (Kirschner & Paas, 2001; Retalis & Skordalakis, 2002) requiring acute situational awareness and optimal behavioral habituation to respond effectively "on the fly" (Torkzadeh & Van Dyke, 2002). This mode of learning is surmised link information to the activity, which augments knowledge scaffolding opportunities (Hoke, et al., 2017) and enhances the student's ability to gather, organize, and integrate information in order to apply it (Landers & Armstrong, 2017). As a result:

> H2. Live activities will improve applied learning performance compared to conventional classroom/lab study alone.

> H3. Live activities will improve applied learning performance compared to conventional classroom/lab study combined with simulations.

METHOD

Participants

Two-hundred and nine undergraduate students at a top tier university in the United States in a computer science program participated in this study. These students have an interdisciplinary background including in business, human factors, operating systems, and networks. This population was selected because they have sufficient experience with these topics to understand cybersecurity. The students were randomly assigned to one of

four sections of the cybersecurity course (described in more detail under Instrumentation). Section 1 (lecture/lab) had 46 students, ages ranged from 20 to 23, 7 were females. Section 2 (lecture/lab + simulation) had 53 students, ages ranged from 19 to 23, 8 were females. Section 3 (lecture/lab + live activity) had 61 students, ages ranged from 20 to 25, 11 were females, and Section 4 (lecture/lab + simulation + live activity) had 49 students, ages ranged from 21 to 23, 9 were females. A knowledge pre-test was given to all participants prior to commencement. The distribution was even across all four sections, and there was no statistical difference in pre-test scores across the sections; hence there was no need to adjust for pre-test scores in the analysis. Nevertheless, there was some variance, hence we used the pre-test scores as a covariate.

Instrumentation

To address instruction variability, the same instructor taught all four sections over three semesters, and the same textbook was used (Workman et al., 2013) and core instruction was used in all four sections and employed educational best practices (as described earlier). The course assignments and exams were identical, and presentation materials were the same, except where noted below. The course content covered threats and countermeasures to be applied to a variety of non-specific cybersecurity threats to systems and applications. The materials also specifically covered the OWASP top 10 vulnerabilities for Web applications.

At crucial learning points during the presentations of the materials, students were prompted to respond to questions or suggest remediations to programming code, firewalls, open ports, and so forth. There were several group projects, and one group presentation. Laboratory exercises included working with IDS (host and network), threat modeling tools, network analyzers, infrastructure monitors, log analyzers, port scanners, penetration testers and vulnerability scanners, writing a cryptographic program and then running static and dynamic code analyzers against their code.

The baseline instruction (Section 1) consisted solely of the classroom and laboratory work, along with quizzes from the textbook, a mid-term and a final examination. Section 2 replaced the textbook quizzes and with simulation challenges. The simulation had two parts, the first presented a series of scenarios; for example, it rendered a Webpage with a login, then had the participants follow instructions to enter various kinds of information, such as to determine whether the page was vulnerable to a SQL Injection. The participants would then try to identify the vulnerable code and correct remediation. The second part was a guided game in which participants would assume a role as attacker or defender (ultimately both) in which they would try to exploit or select a solution to remediate the vulnerabilities. Section 3 replaced the textbook quizzes with two live competitive activities. In the first, the environment incorporated the OWASP Mutillidae with modifications, and the second was an activity with CTF365. Participants would take active roles in trying to compromise systems, while simultaneously striving to find and fix vulnerabilities. Section 4 replaced the quizzes, midterm and final with first the simulation challenges, followed by the live activities.

Figure 2: Sample Fixtures and Panes for Integrated Simulation

At the end of the course for all four sections, students underwent an assessment. The assessment tested analytical and procedural skills, in other words, how well students identified vulnerabilities and took appropriate actions. This was done by two means. This first part were timed case studies of attacks, countermeasures, and remediation. The case studies were based on real incidents, and presented all the facts but did not specify the flaw(s). The participant had to correctly identify the main vulnerability, and any additional issues. One case study, for instance, presented a problem in which open-source Web Application Firewall (WAF) was misconfigured to allow too many permissions, violating the least-privilege principle. This was followed by a Server-Side Request Forgery (SSRF) attack, and subsequent failures by humans-in-the-loop to notice the alarms from the monitors that signaled unusually large downloads from Amazon Web Services (AWS) S3 buckets. Case studies had clear and definable vulnerabilities and remediation solutions.

The second part of the assessment involved an applied lab in which participants had to scan systems, log files, routers, firewalls, and so forth, to find ten major vulnerabilities in a Web application and correctly remediate them. Thus, this assessment part of our study added an active detection element, and consisted of a platform with a simulated network, and attack modules that would carry out various kinds of attacks. Participants utilized tools they had worked with such as intrusion detection systems, monitors and so forth to identify the attack and take corrective actions. The attack/detection/remediation activity consisted of several components. At a macro-scale, these included a simulation engine with selectable infrastructure templates; attack modules that executed a particular attack; an API set that would allow custom applications and attack modules; a database to store state and other information, a student

monitoring system to track student accuracy and point allocations for competitions; and a set of open source monitoring tools that the student would use to identify the attack.

Five hundred points were allotted to this assessment, for which students received T-Shirts and mugs, but were not included in the students' grades. The case studies were worth 1/2 of the points with 1/2 allocated to the lab. These were used as the dependent variable performance scores in the analysis.

Figure 3: Sample Attack/Detection/Remediation Fixtures and Panes

RESULTS

After data screening and pretests, we were sufficiently confident in our analyses. The Muachly's test of sphericity was not significant ($\chi 2 = 3.22$, $p = .59$), which indicates that the correlation matrix was not significantly different from the identity matrix in the correlations among variables (Myers, Well & Lorch, 2010). This combined with a relatively large sample size, we were confident that the assumption of sphericity had not been violated. In support of continuing with the remaining analyses, the test for homogenity of variances was validated because the scatter was relatively equal (Myers, et. al., 2010). Finally, given the correlations among pretest scores, we tested the group means using t-tests with Bonferroni, none of which were significant, therefore we determined that the groups were not statistically different from each other prior to training.

Table 1. Pretest Means and Pearson Correlations Among Groups Prior to Training

	Study Condition	μ	σ	1	2	3	4
1	Classroom/Labs	114.17	1.11	--			
2	Simulations	109.83	1.26	-.64**	--		
3	Live Activity	116.19	1.57	.68**	.62**	--	
4	Simulations + Activity	112.32	1.34	-.60**	.69**	-.63**	--

N = 209. *p < .05, **p < .01, ***p < .001

Assured of the integrity of our data, we tested our hypotheses using multivariate analysis of covariance (MANCOVA). There was some variance, hence we used the pre-test scores as the covariate. We wanted to determine whether there were significant differences among the modes of training delivery on the applied performance outcome. The overall MANCOVA was significant ($F = 1.33$, $p < .000$, $r^2adj = .76$) indicating that there were differences in the overall model. Since we posited that there would be applied performance differences based on training mode, hypotheses must be based on univariate results and not on the overall multivariate test, thus we conducted individual ANCOVA for the hypotheses.

Hypothesis 1 proposed that cybersecurity simulations (μ=301.11, $\sigma = 0.26$) would improve applied learning performance compared to conventional classroom/lab study alone (μ= 233.19, $\sigma = 0.34$). This hypothesis was supported ($F = 7.88$, $p < 0.00$, $\eta^2 = 0.29$). Hypothesis 2 stated that live activities (μ= 256.19, $\sigma = 0.20$) would improve applied learning performance compared to conventional classroom/lab study alone (μ= 233.19, $\sigma = 0.84$). This hypothesis was not supported ($F = 1.88$, $p = 0.19$, $\eta^2 = 0.14$).

Table 2. Posttest Means, F-Scores and Eta Squared for Hypotheses

	Study Condition	μ	σ	F	η^2
	Classroom/Labs	233.19	0.34	--	--
H1	Simulations	301.11	0.26	7.88***	0.29
H2	Live Activity	256.19	0.84	1.88	0.14
H3	Simulations + Activity	388.88	0.40	11.29***	0.31

N = 209. *p < .05, **p < .01, ***p < .001

Finally, hypothesis 3 indicated that live activities combined with simulations and conventional classroom/lab study (μ=388.88, $\sigma = 0.40$) would improve applied performance compared to conventional classroom/lab study alone (μ= 233.19, $\sigma = 0.34$). This hypothesis was supported ($F = 11.29$, $p < 0.00$, $\eta^2 = 0.31$). In summary, cybersecurity simulations improved applied performance over classroom and lab instruction. As seen by the differences in applied performance means in pretest scores, as well as the results, adding activities such as capture the flag and hackathons alone to the lecture/lab baseline appeared to add little benefit to the applied learning outcomes, yet when combined with simulations, that combination yielded the greatest gains in applied learning performance.

DISCUSSION AND CONCLUSIONS

A significant amount of work by the cybersecurity community has gone into providing the rationale for using gamified simulations and live activities such as hackathons and capture the flag competitions in cybersecurity education, but there have been few, if any, studies that have systematically compared these modes. Given that we conducted this at one educational institution, we classify this research as exploratory. However, we do provide strong evidence that modes of education and activities are significant in learning outcomes in cybersecurity, and that none of these modes are optimal in isolation. Furthermore, we have reviewed and summarized cybersecurity educational best practices, which should help to inform cybersecurity pedagogy.

Within the cybersecurity space, industry-accepted certification schemes, such as the CISSP and associated programs (e.g., Dulaney, 2009; Tipton & Henry, 2007) already provide interested parties with a wealth of information related to information security. As an example, the "Official (ISC)2 Guide to the CISSP CBK" contains nearly 1000 pages of study material. Despite this wealth of information, in practice, organizations typically suffer penetrations and compromises due to poor user behavior or incorrectly managed systems. It is often the case that the system fails not because of ignorance on the part of the defender, but because basic but well-known steps were not taken (Workman, et al., 2008). There remains a significant knowing-doing gap, as evidenced by rampant cybersecurity breaches that have recently taken place.

In our study, one of our core goals was, therefore, to suggest how to change the behavior of participants, moving them toward actions that enhance cybersecurity. In the cybersecurity space, improving awareness of the principles of information assurance and moderating behaviors is often more important than presenting an overwhelming amount of information that is not put in to practice. Beyond that, getting practitioners to habituate affirmative behaviors using best practice methods is clearly beneficial. Furthermore, as actual preventative steps change quickly, care must be taken to produce learning materials that are actionable, but that have a reasonable period of applicability before obsolescence.

Consequently, we sought to understand the actual state of the art in cybersecurity education and gain insight into neglected areas, and the approximate level of awareness and technical understanding of the issues. We wished to ensure that our curriculum was both complete and focused, aimed at changing core behaviors that would immediately bolster the stability of cyber infrastructure. In essence, we derived from our research that our educational philosophical approach should be: (1) to stimulate change in a reasonable number of behaviors, rather than to educate broadly that create no lasting benefits, and (2) imbue and reinforce learning through "live-fire" practice with realistic simulations.

Next, our goal from the research was to determine ways for "doing better". Motivated students who understand the importance and applicability of the materials presented to them learn better. To this end, we suggest to change the traditional learning approach from the present-memorize-test model to a show-test-practice-assess model. Moreover, we introduced how incremental chunks of knowledge situated in real-world contexts, that is, gamified, may instill a sense of emotional and cognitive investment in the scenarios by the learner. With regard to commercial, civil, and governmental

organizations, regardless of the size or sophistication of the entity, a program that clearly but concisely communicates and experientially situates real threats posed to cyber infrastructure will help engage participants and aid knowledge retention and implementation. Most importantly, we argue that this approach will produce responsive actors who will apply their knowledge when it most counts.

Limitations and lessons learned from our study include the notions that the quantity of cybersecurity information available in books or articles, or online from researchers, companies, user groups, and blogs provide a virtual "firehose" of warnings and advice related to cybersecurity. Indeed, perhaps the largest problem is the overwhelming and untargeted raft of information available. Cybersecurity risks surround us, but there is little understanding on the part of users, technologists and managers that links a particular behavior to an undesirable outcome. For example, users who infect their machines often have no idea of the source of infection, or the choices that led to it; they simply know something has gone wrong. This low-quality feedback mechanism has jaded users at all levels, and led to a laissez-faire approach to cybersecurity. Users know better, but threats are abstract, distant, and omnipresent, all at the same time, and this accounts for why people may know better but don't do better (Workman, et al., 2008). We aimed to carefully articulate a pedagogical approach with material that can be been personalized or will allow customization that can be optimized for the learner using mixed-modes.

What our research also tells us is that electronic infrastructure is critical to the smooth and safe operation of all aspects of everyday operations. Attackers are well motivated, and do not approach problems the way most people typically expect, and smooth running is critical to businesses and individuals. Education should tie cybersecurity threats back to the system, using real examples, and illustrate how defenders should not "stovepipe" threats. Finally, it is important to realize that seemingly small behavioral changes by users, and how attackers can leverage small errors in operations, compromises many kinds and areas of systems that form the threat matrix and vectors to be considered in cybersecurity education.

In summary, in contrast to the materials that focus exclusively on managing cybersecurity or the more technical aspects of cybersecurity within an ecosystem, training materials at this level are challenging due to the massive range of environments we must consider – ranging from small companies to large corporations, and government infrastructure. It is tempting to provide a simple list of technical topics in a checklist, but doing so is actually a prime example of the wrong approach. Although topics such as secure remote access, patch management, change management, and the intersection of physical and cybersecurity are suitable for checklists, they simply fail to ignite behavioral change that is so needed in cybersecurity responsiveness. Immersion in an environment via simulations and live activities appear to us to be critical to applied learning performance.

REFERENCES

Anderson, J.R. (2000). *Learning and memory*, NY: John Wiley & Sons.

Arthur, W., Bennett, W., Edens, P.S., & Bell, S.T. (2003). Effectiveness of training in organizations: A meta-analysis of design and evaluation features. *Journal of Applied Psychology, 88 (2)*, 234-245.

Baldwin, T.T., & Ford, J.K. (1988). Transfer of training: a review and directions for future research. *Personnel Psychology, 41*, 63 105.

Banks, B. (2007). Using behavior analysis algorithms to anticipate security threats before they impact mission critical operations. *IEEE Conference on Signal Detection and Behavior, AVSS'07, Sept 5-7*, 307-312.

Burke, L.A. (1997). Improving positive transfer: A test of relapse prevention training on transfer outcomes. *Human Resource Development Quarterly, 8 (1)*, 115-126.

Center for Strategic and International Studies (2017). *Securing Cyberspace for the 45th Presidency*. https://www.csis.org/analysis/2017-global-forecast.

Conetta, C. (2019). Individual differences in cyber security. *McNair Research Journal*, 15 (4), 2-20.

Dewey, J. (1998). *The Essential Dewey: Pragmatism, education, democracy*. In, The Essential Dewey (L. Hickman & T. Alexander, Eds). Bloomington: Indiana University Press.

Dunaney, E. (2009). *CompTIA Security +*. Indianapolis, ID: Sybex.

Ernits, M., Tammekänd, J., Maennel, O. (2015). *A fully automated cyber defense competition for students*. In: Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication, SIGCOMM, New York, 113–114.

Ferdig, R.E. (2006). Assessing technologies for teaching and learning: understanding the importance of technological pedagogical content knowledge. *British Journal of Educational Technology, 37 (5)*, 749-760.

Goode, J., Levy, Y., Hovav, A., & Smith, J. (2018). Expert assessment of organizational cybersecurity programs and development of vignettes to measure cybersecurity countermeasures awareness. *Online Journal of Applied Knowledge Management, 6 (1)*, 67-80.

Hendrix, M., Al-Sherbaz, A., & Bloom, V. (2016). Game based cyber security training: Are serious games suitable for cyber security training? *International Journal of Serious Games, 3 (1)*, 53-61.

Hogan, L. C., & Bell, M. (2009). A preliminary investigation of the reinforcement function of signal detections in simulated baggage screening: Further support for the vigilance reinforcement hypothesis. *Journal of Organizational Behavior Management, 29*, 6-18.

Hoffman, L.J., Rosenberg, T., Dodge, R., Ragsdale, D. (2005). Exploring a national cybersecurity exercise for universities. *IEEE Security & Privacy, 3(5)*, 27–33.

Hoke, J., Reuter, C., Romeas, T., Montariol, M., Schnell, T., Faubert, J. (2017). Perceptual-cognitive & physiological assessment of training effectiveness. *Proceedings from the Interservice/Industry Training, Simulation and Education Conference (I/ITSEC), Orlando, FL. 1-12*.

Jalali, M.S., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *Journal of Strategic Information Systems, 28*, 66-82.

Jin, G., Tu, M., Kim, T. Heffron, J. & White, J. (2018). Game based cybersecurity training for high school students. *Proceedings of the ACM, SIGCSE'18, February 21-24*. Baltimore, MD., 68-73.

Kirschner, P. A., & Paas, F. (2001). Web-enhanced higher education: a tower of Babel. *Computers in Human Behavior, 17*, 347–353.

Landers, R.N., Armstrong, M.B. (2017). Enhancing instructional outcomes with gamification: An empirical test of the technology-enhanced training effectiveness model. *Computers in Human Behavior, 71*, 499-507.

Leune, K., & Petrilli, S. J. (2017). Using capture-the-flag to enhance the effectiveness of cybersecurity education. *Proceedings of the ACM, SIGITE'17, October 4–7*. Rochester, NY, 47-52.

Miranda, M.J.A. (2018). Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. *International Management Review, 14 (2)*, 5-10.

Myers, J. L., Well, A. D., & Lorch, R. F. (2010). *Research design and statistical analysis*. NY: Rourtledge.

Pan, K., Teixeira, A., López C.D., & Palensky, P. (2017). *Co-simulation for cyber security analysis: Data attacks against energy management system*. Proceedings from the IEEE International Conference on Smart Grid Communications (SmartGridComm), Dresden, Germany, 253-258.

Reio, T. G., & Wiswell, A. (2001). Field investigation of the relationship among adult curiosity, workplace learning, and job performance. *Human Resource Development Quarterly, 11 (1)*, 5-30.

Retalis, S., & Skordalakis, E. (2001). CADMOS: an approach to developing web-based instructional systems. *Computers in Human Behavior, 17*, 393–407.

Rumeser D. & Emsley, M. (2018). A systematic review of project management serious games: Identifying gaps, trends, and directions for future research. *The Journal of Modern Project Management, 6 (1)*, 33-44.

Schepens, W.J., Ragsdale, D.J., Surdu, J.R., Schafer, J., New Port, R. (2002) The cyber defense exercise: an evaluation of the effectiveness of information assurance education. *Journal of Information Security, 1(2)*, 118-127.

Sommestad, T., & Hallberg, J. (2012). *Cyber security exercises and competitions as a platform for cyber security experiments*. In A. Jøsang and B. Carlsson (Eds.): NordSec 2012, LNCS 7617, pp. 47–60, Springer-Verlag Berlin Heidelberg.

Sitzmann, T., & Weinhardt, J. M. (2019). Approaching evaluation from a multilevel perspective: A comprehensive analysis of the indicators of training effectiveness, *Human Resource Management Review, 29 (2)*, 253-269.

TeachThought (2019). Modern trends in education: 50 different approaches to learning. https://www.teachthought.com/pedagogy/modern-trends-education-50-different-approaches-learning/.

Thatcher, J. B., & Perrewé, P. L. (2002). An empirical examination of individual traits as antecedents to computer anxiety and computer self-efficacy. *MIS Quarterly, 26 (4)*, 381–396.

Tipton, H. F. & Henry, K. (2007). *Official (ISC)2 Guide to the CISSP CBK*. NY: Auerbach.

Torkzadeh, G., & Van Dyke, T. P. (2002). Effects of training on internet self-efficacy and computer attitudes. *Computers in Human Behavior, 18*, 479–494.

Trafton, G. J., & Trickett, S. B. (2001). Note-taking for self-explanation and problem solving. Human–Computer Interaction, 16, 1–38.

Veksler, V.D., Buchler, N., Hoffman, B.E., Cassenti, D.N., & Sugrim, S. (2018). Simulations in cyber-security: A review of cognitive modeling of network attackers, defenders, and users. *Frontiers In Psychology, 9*, 1-12.

Voskoboinicov, S. &. Melnyk, S. (2018). Cyber security in the modern sociation and improvement of preparation of future factors in the field of competent approach, *Social Work and Education, 5 (1)*, 103-112.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: An empirical test of the threat control model, *Computers in Human Behavior, 24,* 2799–2816.