


Chapter 28

Effectiveness of Increasing Realism Into Cybersecurity Training

Robert Beveridge

 <https://orcid.org/0000-0001-8884-4387>

Robert Morris University, Moon, USA

ABSTRACT

This article describes how cybersecurity is a field that is growing at an exponential rate. In light of many highly publicized incidences of cyber-attacks against organizations, the need to hire experienced cybersecurity professionals is increasing. The lack of available workforce to fill open positions is alarming and organizations are finding that potential candidates with academic degrees and certifications alone are not as valuable as those with experience. Gaining rapid experience requires immersion into realistic virtual environments that mimic real-world environments. Currently, cybersecurity competitions leverage many technologies that immerse participants into virtual environments that mimic real-world systems to improve experiential learning. These systems are expensive to build and maintain, and to continuously improve realism is difficult. However, the training value of cyber competitions in which the participants cannot distinguish from real-world systems will ultimately develop highly experience cybersecurity professionals.

INTRODUCTION

Cybercrime is becoming more prevalent today than ever. Data breaches resulting in millions of records stolen are causing organizations to increase their cybersecurity posture and creating new organizational units and jobs for security professionals. Current statistics show a global workforce shortage of approximately 3 million information security professionals (ISC2, 2018). Private training companies have emerged offering cybersecurity certifications and universities are developing cybersecurity degree programs. However, employers have difficulty filling these positions due to the lack of qualified and

DOI: 10.4018/978-1-6684-3554-0.ch028

experienced cybersecurity professionals (Harris, Patten, & Patten, 2015). Part of the problem is that traditional academic settings and certification training often focus on teaching foundational skills through didactic classroom environments that lack the experience building opportunities for cybersecurity students (Anderson, 2017). The need to rapidly train cyber professionals as well as enable them to gain valuable experience will help meet the demand of the current workforce shortage across all industries (Manson & Pike, 2014). To build the experience that is needed in the workforce, experiential learning needs to be incorporated in the curriculum by building cybersecurity training ranges that allow immersion into mimicked real-world environments.

Cyber training ranges are being constructed and utilized to allow immersion into hands-on training environments that build valuable experience (Cankaya, 2015). These environments allow students into a virtual world that allows them to safely learn and experiment without the risk of damaging production systems. These active learning environments are created with varying degrees of realism to replicate real-world operational systems to increase learning. Military pilots train in simulators in order to gain valuable experience before allowing to fly aircraft where mistakes can be costly to equipment and lives. Training in simulated environments that bring as much realism as possible increases experiences needed for real-world employment. Without realism, training value and the ability to build valuable experiences decreases. According to Walcott (2017), training value decreases as realism decreases within these environments. However, increasing realism in cybersecurity training ranges also increases complexity and cost. Research into the effectiveness of injecting realism into cybersecurity training will be done. The purpose of this paper is to develop the understanding that increasing realism in these training environments also increases learning.

CYBERCRIME

Over the last decade, cybercrime has a detrimental impact on all facets of technology used in homes and businesses and continues to increase exponentially. The global economic impact of cybercrime in 2014 cost an estimated 345 million to 445 million dollars, or .62% of global Gross Domestic Product (GDP) (Lewis, 2018). As of 2017, the impact to global GDP increased to .87% or an estimated 608 billion dollars (Lewis, 2018). This cost, which includes loss of reputation, intellectual property, online fraud costs, and other financial impact, continues to grow. A successful cyberattack on an organization within the United States that results in a data breach is estimated to cost an average of 5.4 million dollars per incident (Reed, 2019).

Hidden within the Internet are illicit online marketplaces that specialize in buying and selling stolen information as well as other illegal products and services. These sites reside online in an area commonly referred to as the “Dark Web” and are only accessible by using specialized software that anonymizes the user and the owners of these sites to limit or negate attribution (Kim, Han, Ha, Kim, & Han, 2018). Novice users can pay anywhere between \$1,000 - \$5,000 to purchase custom malware from cybercriminals which gives them the ability to perform illegal actions such as disabling corporate websites and stealing personal information such as bank accounts and credit card numbers (Sharma, 2007). Due to the lack of attribution, cybercriminals are not the only ones using the dark web for nefarious purposes. According to Gabriel Weimann (2016), the Federal Bureau of Investigation (FBI) announced in 2015 that Islamic terrorists were using the dark web to recruit new members, publish book and guides on bomb-making and the effective use of them, and as a propaganda platform to encourage members to perform terrorist

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/effectiveness-of-increasing-realism-into-cybersecurity-training/292131

Related Content

Assessment for Learning Regarding the Strategy of Rhetorical Competence Development in Initial Teacher Training

Rata Iulian, Birnaz Ninaand Elena Aurel Railean (2020). *Assessment, Testing, and Measurement Strategies in Global Higher Education* (pp. 193-213).

www.irma-international.org/chapter/assessment-for-learning-regarding-the-strategy-of-rhetorical-competence-development-in-initial-teacher-training/248982

The Effect of Psychological Safety on the Performance of Students in Graduate-Level Online Courses

George Hanshawand Jacob Hanshaw (2023). *International Journal of Innovative Teaching and Learning in Higher Education* (pp. 1-21).

www.irma-international.org/article/the-effect-of-psychological-safety-on-the-performance-of-students-in-graduate-level-online-courses/333864

Integrating Service-Learning Pedagogy Into Community College Coursework: A Phenomenological Study

Timothy Leonardand Patrick J. Flink (2020). *International Journal of Innovative Teaching and Learning in Higher Education* (pp. 25-36).

www.irma-international.org/article/integrating-service-learning-pedagogy-into-community-college-coursework/245771

Preparing Principals in Educational Leadership Programs: Exploring Problems of Practice With Self-Directed Learning Projects

Sarah L. Craryand Elizabeth A. Gilblom (2022). *Self-Directed Learning and the Academic Evolution From Pedagogy to Andragogy* (pp. 173-192).

www.irma-international.org/chapter/preparing-principals-in-educational-leadership-programs/294370

A Qualitative Study of Student Expectations of Online Faculty Engagement

Christopher W. Berg, Melanie Shaw, Anthony L. Contentoand Scott W. M. Burrus (2019). *Fostering Multiple Levels of Engagement in Higher Education Environments* (pp. 1-17).

www.irma-international.org/chapter/a-qualitative-study-of-student-expectations-of-online-faculty-engagement/220573