Cybersecurity Skills Training: An Attacker-Centric Gamified Approach

Mackenzie Adams and Maged Makramalla

> *It is said that if you know your enemies and know yourself, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle.*
>
> Sun Tzu (544 BC – 496 BC)
> Military general, strategist, and philosopher
> in *The Art of War*

Although cybersecurity awareness training for employees is important, it does not provide the necessary skills training required to better protect businesses against cyber-attacks. Businesses need to invest in building cybersecurity skills across all levels of the workforce and leadership. This investment can reduce the financial burden on businesses from cyber-attacks and help maintain consumer confidence in their brands. In this article, we discuss the use of gamification methods that enable all employees and organizational leaders to play the roles of various types of attackers in an effort to reduce the number of successful attacks due to human vulnerability exploits.

We combine two separate streams – gamification and entrepreneurial perspectives – for the purpose of building cybersecurity skills while emphasizing a third stream – attacker types (i.e., their resources, knowledge/skills, and motivation) – to create training scenarios. We also define the roles of attackers using various theoretical entrepreneurial perspectives. This article will be of interest to leaders who need to build cybersecurity skills into their workforce cost-effectively; researchers who wish to advance the principles and practices of gamification solutions; and suppliers of solutions to companies that wish to build cybersecurity skills in the workforce and leadership.

Introduction

Cybersecurity training is a crucial response to a growing number of intrusions and attacks (Nagarajan et al., 2012). Human vulnerabilities account for 80% of total vulnerabilities exploited by attackers (IBM, 2013) yet the focus of cybersecurity in information technology has been on systems tools and technology (Hershberger, 2014). Human vulnerabilities include, but are not limited to, employee negligence, leadership misinformation and limited cybersecurity skills training, malicious insiders, and third parties who have access to an organization's network. The need to build cybersecurity skills and increase knowledge in the workforce and leadership has become apparent to top corporate decision makers, governmental bodies, and academic researchers (Evans & Reeder, 2010). After the 2013 data breach of Target Corporation, an analysis of the attack concluded that the Target security systems detected the breach but the leadership and employees responsible for taking the steps to respond lacked the necessary skills and knowledge (Hershberger, 2014).

Limited knowledge and skills training in cybersecurity is not unique to Target and it is not an unusual occurrence. A recent study found that almost 70% of critical infrastructure providers across 13 countries suffered a data breach in 2013, and it was found that 54% of those breaches resulted from employee negligence; however, the most unexpected finding was that only 6% of these companies provided cybersecurity training for all employees (Unisys, 2014). Any employee in an organization can be a potential point of entry for attackers; therefore, knowledge and skills training in cybersecurity for all employees is essential in reducing human vulnerabilities. Companies that did not provide security training for new hires reported average annual losses in the amount of $683,000, whereas those who conducted new-hire training reported average annual losses at $162,000 (PwC, 2014).

In general, current cybersecurity skills training are limited to IT personnel while awareness campaigns and education are often offered to all employees. Cybersecurity training for all employees is inefficient in conveying the necessary knowledge and skills for employees and organization leaders to reduce the number of successful attacks. These training approaches can include: web-based classrooms, teleconferencing, instructor-led training, thematic cybersecurity events, newsletters, and awards/incentives programs (Annetta, 2010; Cone, 2007; Nagarajan et al., 2012). These approaches were found to be ineffective because the participants were not engaged in the learning process. The training sessions provided a large amount of information in a short period of time, which created a passive, overwhelming, and disconnected learning experience (Annetta, 2010; Cone, 2007). Classroom instruction and the dissemination of online advice are ineffectual ways to learn; a more immersive and interactive training is required.

In this article, we describe a gamification approach to building cybersecurity skills in all employees and leadership in an organization. Using gamified solutions in cybersecurity skills training promotes active learning and motivation while increasing retention of the learnt skills in comparison to traditional learning approaches such as instructor-led classes (Jordan et al., 2011).

The gamification approach uses entrepreneurial perspectives, which complement attacker types based on their motivation, knowledge, and resources. We use entrepreneurial perspectives, which refer to characteristics of seeking opportunities, taking risks, and having the focus to pursue an idea to fruition (Kuratko, 2013), to help view the challenge through the eyes of cyber-attackers. Some of the similarities drawn between hackers and entrepreneurs include their problem-solving capabilities, willingness to take advantage of opportunities, working hard, as well as taking risks (Blanchard, 2013; Kang, 2012; Warikoo, 2014).

In the remainder of the article, we examine the use of gamification to develop employee skills and identify various entrepreneurial perspectives that are relevant to this approach. Then, we discuss what is required to create a training approach that uses gamification to deliver immersive learning in cybersecurity. In the final section, we provide conclusions.

Using Gamification to Build Skills in Employees

Gamification is a process of enhancing a specific service by implementing game design elements in a non-game context to enhance the user’s overall value creation and experience (Huotari & Hamari, 2011; Deterding et al., 2011). Deterding and colleagues (2011) define gamification as “the use of design elements characteristic for games in non-game contexts”. Thus, gamification reflects the use of game thinking including progress mechanics (such as points systems), player control (such as avatar use), rewards, collaborative problem solving, stories, and competition in non-game situations (Deterding et al., 2011; Kapp, 2012). Underlying gamification is an understanding of motivation as significantly correlated with and predictive of desirable human outcomes such as achievement, success, and the attainment of distinction and rewards (Kapp, 2012). When designed and applied in an appropriate manner and setting, gamification provides an alignment between motivation and desire that leads to the anticipated purpose of its use. For instance, when used to increase employee engagement, gamification can improve teamwork and transform routine, often dull, tasks by motivating employees through "play" and competition within the same team and across teams (Korolov, 2012; Zichermann & Cunningham, 2011).

Although it is usually considered an effective user involvement tool, gamification can also be used to develop skills of participants and employees. Burke (2014) highlights the effectiveness of using gamification concepts in employee training while using the “Ignite Leadership Game” created by NTT Data as a relevant example. This specific gameful design is built on first assessing the employees’ knowledge to identify their strengths and weaknesses; the identification allows them to develop the required skill sets more efficiently. The main benefits of using gamification approaches to develop skills are creating an atmosphere that enables employee active involvement (Zichermann & Linder, 2013), improving the participants’ motivation to achieve better results (Burke, 2014), and enhancing the overall learning process due to the established collaborative environment (Burke, 2014).

Gamification elements
When designing games for training and educational purposes, training goals must be clearly defined (Nagarajan et al., 2012). Designing effective and relevant games requires the selection of the appropriate gamification elements that would best suit the training approach needed (Kapp, 2012). Four elements of gamification are highlighted below for cybersecurity skills training:

1. *Progress mechanics:* related to player motivation through the provision of progress tools such as points, leader boards, and badges.

2. *Player control:* the use of a character (a third-person perspective) to engage in the gamified training. This character is commonly known as an "avatar". Research has shown that the use of avatars, through the use of different roles, influences behaviour.

3. *Problem solving:* a crucial element in gamification when learning and retaining new information is the goal of the training. Collaboration and identification of a shared purpose are essential in developing strong problem-solving skills that can easily translate into practical knowledge outside of the training environment.

4. *Story:* A narrative that is present to create an attachment or a bond between the learner and their avatar, as well as a bond between the avatars participating in the gamified training. Stories also motivate the learner to keep on "playing" to find out the rest of the story

Existing gamification training solutions
Currently, a handful of cybersecurity training and awareness programs started to introduce gamification techniques in their own curricula. As shown in Table 1, six main, and most evolved, gamified approaches were identified and further elaborated. These "games" were compared according to the following four aspects:

Table 1. Existing gamified training solutions for employee cybersecurity skills

	Awareness	Defensive Strategies	Offensive Strategies	Attacker Centricity	References
CounterMeasure	• Basic knowledge	• *None*	• Authentication and password bypassing	Limited	Jordan et al. (2011)
CyberCiege	• Basic knowledge • General assessment	• Penetration prevention	• *None*	*None*	Cone et al. (2007)
CyberNexs	• *None*	• System assessment • Penetration prevention	• Capture the flag	*None*	Nagarajan et al. (2012)
CyberProtect	• Basic knowledge • General assessment	• *None*	• *None*	*None*	Labuschagne et al. (2011)
NetWars	• Skill assessment	• System assessment • Penetration prevention	• System penetration scenarios	Limited	SANS (2015)
Micro Games	• Basic knowledge • General assessment	• Penetration detection • Password management	• *None*	*None*	Wombat (2015)

1. *Awareness:* requires a minimal amount of knowledge for the participants. Awareness is mainly concerned with assessing the level of vulnerabilities in an entity, while providing participants with general knowledge in detecting and avoiding successful penetration attempts.

2. *Defensive strategy:* requires the participants – in this case the defenders – to have substantial knowledge that will provide them with proper tools and strategies to fend off cyber-attacks efficiently.

3. *Offensive strategy:* focuses mainly on putting the participants in their rivals' shoes in order to properly understand their strategies and approaches.

4. *Attacker centricity:* uses known characteristics of cyber-attackers to train participants in anticipating an attacker's motivation and behaviour in carrying out certain attacks. This anticipation enhances the creation and application of both offensive and defensive strategies against cyber-attacks.

Note that only three of the six gamified training programs incorporate offensive strategies for their participants. This observation is in line with the current dominant practice in cybersecurity to react, largely, to attacks and not engage in anticipatory or offensive strategies. Moreover, two of the six games have limited attacker-centricity, mostly based on the skills of hacking a system but not specific attacker types. Once again, this reflects a current state in cybersecurity training where the characteristics of attackers are seldom incorporated in training employees to understand these attackers or anticipate their attacks.

Attacker Types and Their Characteristics

Based on an extensive search of existing literature, and to the best of our knowledge, there are no current applications of cyber-attacker characteristics being used in gamified cybersecurity skills training for employees. As a result, we reviewed literature on cyber-attackers based on a search that included the following keywords: "cyber criminals", "insiders", and "hackers". We expanded our keyword search to accommodate the terminology differences in existing literature when describing individuals or groups that commit cyber-attacks. We focused on cyber-attackers to identify attacker types and their motivations, resources, and knowledge/skills. Identifying attacker types is important in developing more accurate profiles when creating and implementing solutions intended to reduce cybercrimes (Rogers, 2011).

Based on the literature review, the following eight types of cyber-attackers were identified:

1. *Script kiddies:* attackers who depend on existing tools (e.g., exploit programs and scripts) and are unwilling to learn how these tools function (Hald & Pedersen, 2012). They are immature attackers whose primary motivation is to create mischief and get attention (Aggarwal et al., 2014; Rogers, 2011).

2. *Cyber-punks* (including virus writers): attackers who write viruses and exploit programs for the sake of causing trouble and gaining fame (Hald & Pedersen, 2012). Motivated by admiration and recognition, these attackers disrespect authority and social norms. They are only slightly more skilled than script kiddies (Rogers, 2011) and enter systems to cause damage (Dogaru, 2012).

3. *Insiders:* attackers who are imbedded within the organization they attack who cause intentional or unintentional harm because of their authorized access (Hald & Pedersen, 2012). Because access is not a challenge they face, most insider attackers have minimal technical skills (Williams, 2008). As such, they become easy targets for criminals who persuade them to perform an action that exposes the system (Crossler et al., 2013; Parmar, 2013).

4. *Petty thieves:* attackers who commit online fraud such as identity theft and system hijackings for ransom with no other motivation than money (Hald & Pedersen, 2012). Their activities are not sophisticated and they are not dependent on the gains from their crimes. They are attracted to criminal activities that include credit card and bank fraud (Rogers, 2011).

5. *Grey hats:* attackers who are a mix of black hats (i.e., malicious or illegal hackers) and white hats (i.e., hackers intending to improve security). They may attack systems to prove their abilities or to find flaws within a system, and may alert the target to the vulnerability (Aggarwal et al., 2014; Bodhani, 2013; Hald & Pedersen, 2012). Often highly skilled, they write scripts that cyber-punks and script kiddies typically employ (Rogers, 2011).

6. *Professional criminals:* attackers who are hired to infiltrate systems. They are also known as cyber-mercenaries (Hald & Pedersen, 2012). Sometimes these cyber-attackers act on behalf of institutions and enter competitors' systems for financial gain (Dogaru, 2012). They operate in the most secretive environment and are governed by strict rules of anonymity so they cannot be identified (Kowalski & Mwakalinga, 2011; Rogers, 2011).

7. *Hactivists:* attackers who are motivated by ideology. This type can include terrorist groups. Pushed into activism by strong psychological dispositions and beliefs, some hackers may become hacktivists and perceive their motives to be completely selfless (Hald & Pedersen, 2012; Papadimitriou, 2009).

8. *Nation states:* attackers who are assumed to be working on behalf of a governmental body. Every resource is targeted towards the disruption of the enemy's systems or the protection of the nation state's own systems. This group includes paramilitary organizations and freedom fighters, and their goals are not dissimilar to those of recognized governments (Dogaru, 2012; Hald & Pedersen, 2012; Rogers, 2011).

It is important to note a common theme found in hacker communities: willingness to share information and collaborate in problem solving with peers (Biros et al., 2008; Denning, 1996; Jordan & Taylor, 1998; Mookerjee et al., 2009). Sharing information helps build stronger bonds within the community while encouraging and challenging others to learn and engage more (Arief & Besnard, 2003).

Entrepreneurial Perspectives

Entrepreneurs are described as risk takers, innovators, and problem solvers who are confident, persistent, collaborative, able to recognize opportunities, skilled at gathering information and knowledge, have a need for achievement and reward, and seek change and profit (Blanchard, 2013; Kang, 2012; Kim, 2014). Although there are many definitions of the term "entrepreneur", the following definition is most apt for this article: entrepreneurs are "those who identify a need – *any* need – and fill it. It's a primordial urge, independent of product, service, industry, or market" (Nelson, 2012). Thus, it can be inferred that this primordial urge is driven by different motivations and capabilities, which may be better understood through entrepreneurial perspectives.

Entrepreneurial perspectives are examined in this article for two reasons: i) to consider the similarities between various entrepreneurial perspectives and cyber-attacker characteristics and ii) to remove the negative connotation connected to the term "attacker" in the training. Taking the perspective of someone about whom an individual has negative perceptions and attitudes may compromise the in-depth immersion into a cyber-attacker's motivation and approach, and reduce "buy-in" to the gamification approach to training. Thus, taking an entrepreneurial perspective helps trainees empathize with cyber-attackers so that they may better learn to protect their organizations against them.

From the literature, we identified the following six entrepreneurial perspectives:

1. *Bricolage:* a perspective where an entrepreneur uses whatever diverse resources happen to be at hand to start a new venture. The concept was originally used in artistic contexts and usually starts in an environment with limited resources (Baker & Nelson, 2005). This perspective requires creativity, and the resulting innovations may need several testing stages before then come to fruition.

2. *Effectuation:* a perspective where an entrepreneur takes "a set of means as given and focus[es] on selecting between possible effects that can be created with that set of means" (Saravathy, 2001). This perspective connotes that an entrepreneur is considered as highly knowledgeable in using their own resources. That is, they may not have access to a large amount of resources, but they are considered experts in utilizing their available resources in many innovative ways.

3. *Causation:* a perspective whereby an entrepreneur focuses on a specific goal that is highly desired and uses all the available resources to reach this certain goal. In this perspective, the setting itself is usually rich in resources which requires high knowledge in how to use these resources to achieve optimal results and achieve greater outcomes (Sarasvathy, 2001).

4. *Emancipation:* a perspective where a person, who is suffering from some kind of physical or emotional oppression, decides to break free to improve their situation. It can also apply to improving the situation in their area, community, or even country. Rindova and colleagues (2009) identified three core elements of emancipation: seeking autonomy, authoring, and making declarations.

5. *Hubris:* a perspective in which an entrepreneur's belief in the success of a new venture is based on socially constructed confidence (Hayward et al., 2006). An optimistic overconfidence propels the individual to start a venture regardless of the potential failure.

6. *Social:* a perspective where an entrepreneur's main motivations are social goals (social, political, environmental) and sharing part of their gained resources with community causes (Christopoulos & Vogl, 2015).

Proposed Gamification Approach to Build Cybersecurity Skills

Cybersecurity training is mislabelled in most organizations; it should be more appropriately referred to as cybersecurity information and awareness training that is provided to all employees. Cybersecurity skills training is mostly offered to highly technical IT administration and security professionals. All employees need foundational skills training with customizations to tailor scenarios based on functional roles and potential attack vectors with an emphasis on learning how to mitigate or cope with an attack (Council on Cybersecurity, 2014).

Based on our review of the literature, we propose a gamified approach to cybersecurity skills training. Using the elements of gamification, we outline four components required to create a comprehensive cybersecurity skills training: i) story, ii) player control, iii) problem solving, and iv) progress mechanics.

Story
The stories of the training games will be based on the eight identified cyber-attacker types and they will provide realistic, virtual recreations of the work environment and simulate the types of attacks that may occur. For this gamified cybersecurity training, there are three relevant components that help keep the trainees engaged and motivated:

1. *Feedback:* such as losing lives, triggering warning screens, receiving encouraging messages, or earning rewards. This feedback is based on the trainee's progress: as long as they are engaged in the game, the game is providing feedback, assessing skill levels, and creating obstacles to evaluate the various skillsets of the trainees and comparing those results to the target level of achievement.

2. *Increased challenges:* the complexity of the story will dictate the amount of challenges the trainee will have to overcome in order to progress.

3. *Opportunities for mastery:* providing opportunities to develop and excel.

Player control
The six entrepreneurial perspectives are used to create resource- and motivation-based attacker roles for the training solution. The entrepreneurial perspectives are matched to the attacker types as shown in Table 2. This step enables avatars to be created for the game without any preconceived notions on how the avatar should act, thereby allowing for exploratory learning in the scenarios.

Problem solving
Problem solving is an important element in gamification that allows trainees to learn and retain new information. As trainees collaborate to find answers, they create a community of shared information and purpose. Such activities are particularly helpful during attacker-centric cybersecurity skills training due to the collaborative nature of the cyber-attacker community and its ability to find common goals.

Progress mechanics
For all employees and organization leaders participating in the gamified training, the progress mechanics will vary based on the avatar's characteristics and areas of learning and achievements. For example, if an employee's avatar is “the architect” as listed in Table 2, a quick review of their in-game resources would show that the avatar has many resources available for them to complete a task so the challenge in gaining more resources or points may be linked more to problem solving skills or collaboration efforts.

Gamified Training Scenario

To understand how the training would be used and what the expected learning outcomes are, consider the following scenario. A graphic designer in the marketing department must complete his cybersecurity skills training. At the beginning of the training, he is given a short knowledge-assessment questionnaire. Based on his answers, he is assessed as having “average” cybersecurity knowledge, which would then determine his entry level in the training game. He is then given the option to choose an avatar with very little descriptive information about the avatar such as its strengths, weaknesses, and resources to progress along in the game. He selects “The advocate” as his avatar and, based on his assessment, he begins at level 2 of the training. The story he will work through is based on “The hacktivist” attacker type and an attack type of en-

Table 2. Gamification element: player control (avatars and their characteristics)

Avatars (Attacker Roles)	**Avatar Characteristics (Attacker Types)**
Bricolage: "The rookie"	• Script kiddies • Cyber-punks • Petty thieves
Effectuation: "The adroit"	• Insiders
Causation: "The architect"	• Nation states • Professional criminals
Emancipation: "The liberator"	• Insiders • Hacktivists
Hubris: "The optimist"	• Grey hats
Social: "The advocate"	• Hactivists

tering a secure area by following an employee who entered using their own access key to plant malware in one of the computers in a certain department. As he progresses through the game, he may need to collaborate with other trainees or other avatars in the game to complete a mission or a step. As he progresses along, there is information provided such as warnings, hints, and other learning opportunities to successfully complete the level. There are different rewards and incentives provided to keep him engaged and motivated.

By the end of this training, the employee is able to plant the malware after a few failed attempts. During the training, the employee learns the desired skills, progressing from prevention to anticipation to reaction to response, as described below:

1. *Prevention:* the importance of securing access against unauthorized individuals when entering secure areas.

2. *Anticipation:* a method used by some attackers to gain access to the system.

3. *Reaction:* the importance of communication with others in the organization.

4. *Response:* the proper procedure to follow when confronted with a similar situation. The impact of a successful attack.

In comparison, instructor-led classroom training would have provided the information to the trainee without any practical, hands-on activities to show the steps involved or to visually witness the impact of the security breach. It would also be difficult for the trainee to retain the procedural information to deal with this type of issue. Most importantly, it is difficult to keep the attention of the employee on the training material without the interactive and immersive game element.

The gamified cybersecurity skills training approach promotes:

1. The prevention > anticipation > reaction > response sequence

2. Skills training for all employees in an organization, from entry-level staff to C-level executives

3. Hands-on, immersive, and interactive training that moves away from classroom-based, instructor-led training

4. A distinction between cybersecurity awareness only training and cybersecurity skills training

Conclusion

The main objective of this article was to provide an innovative approach to train all employees and organization leaders to develop cybersecurity skills and better defend against and react to data breaches. The gamified training approach was developed by reviewing the following literature streams: gamification, cyber-attackers and their characteristics, and entrepreneurial perspectives.

In this article, eight attacker types were selected using their motivation, knowledge/skills, and resources as attacker characteristics. Furthermore, six entrepreneurial perspectives were used highlighting their motivation, knowledge/skills, and resources. The attacker types and their characteristics were combined with the entrepreneurial perspectives to create avatars for the game. By creating the avatars, the type of attacker and the characteristics of the attacker are now used in creating the story used during the training. This approach allows the trainees to experience an attack through the eyes of a cyber-attacker and therefore from entrepreneurial perspectives.

Cybersecurity Skills Training: An Attacker-Centric Gamified Approach

Mackenzie Adams and Maged Makramalla

Our article is limited by the lack of practical, tested evidence that the approach would produce the expected outcomes and improve employees' abilities in preventing or reacting to data breaches. Some of the research has pointed to the importance of identifying attacker characteristics to better defend against cyber-attacks (Colwill, 2009; Cremonini & Nizovtsev, 2006; Gold, 2011; Liu & Cheng, 2009), and further research linking the attacker characteristics to the attack type may advance knowledge in cybersecurity prevention and training. We would also recommend a more comprehensive project that examines the similarities and differences between entrepreneurs and attackers.

About the Authors

Mackenzie Adams is a serial entrepreneur, a Senior Technical Communicator, and a graduate student in the Technology Innovation Management (TIM) program at Carleton University in Ottawa, Canada. She is also a VP/Creative Director at SOMANDA, a consulting company. Over the past 15 years, Mackenzie has worked in a variety of fields ranging from social work to accounting and has used those experiences to develop strong strategic and analytical skills. She is interested in the fields of artificial intelligence and quantum computing, and how they relate to cybersecurity.

Maged Makramalla is a current graduate student in the Technology Innovation Management (TIM) program at Carleton University in Ottawa, Canada. He holds a Bachelor of Science degree in Mechatronics Engineering from the German University in Cairo, Egypt. For three years, he has been working as Manager of the Sales and Marketing Department of TREND, a trading and engineering company based in Cairo. His primary research interest lies in the improvement of educational techniques by introducing experiential learning into the regular curriculum while promoting gamification of educational methods.

References

Aggarwal, P., Arora, P., & Ghai, R. 2014. Review on Cyber Crime and Security. *International Journal of Research in Engineering and Applied Sciences,* 2(1): 48–51.

Annetta, L. A. 2010. The "I's" Have It: A Framework for Serious Educational Game Design. *Review of General Psychology,* 14(2): 105–112.
http://dx.doi.org/10.1037/a0018985

Arief, B., & Besnard, D. 2003. *Technical and Human Issues in Computer-Based Systems Security.* Technical Report Series: University of Newcastle upon Tyne Computing Science. Newcastle, UK: Newcastle University.

Baker, T., & Nelson, R. E. 2005. Creating Something from Nothing: Resource Construction through Entrepreneurial Bricolage. *Administrative Science Quarterly,* 50(3): 329–366.
http://dx.doi.org/10.2189/asqu.2005.50.3.329

Biros, D. P., Weiser, M., Burkman, J., & Nichols, J. 2008. Information Sharing: Hackers vs Law Enforcement. In *Proceedings of the 9th Australian Information Warfare and Security Conference.* Perth, Australia: Edith Cowan University.

Blanchard, K. 2013. Entrepreneurial Characteristics in SMEs: A Rural, Remote Rural, and Urban Perspective of Lincolnshire Businesses. *Strategic Change,* 22(3/4): 191–201.
http://dx.doi.org/10.1002/jsc.1932

Bodhani, A. 2013. Bad... In a Good Way. Engineering & Technology, 8(12): 64–68.
http://dx.doi.org/10.1049/et.2012.1217

Burke, B. 2014. *Gamify: How Gamification Motivates People to Do Extraordinary Things.* Brookline, MA: Bibliomotion, Inc.

Chiang, O. 2010. Wombat Security Makes Online Games That Teach Cybersecurity Awareness, Nabs $750,000 US Airforce Contract. *Forbes Magazine.* Accessed January 10, 2015:
http://www.forbes.com/sites/oliverchiang/2010/10/08/wombat-security-makes-videogames-that-teach-cybersecurity-awareness-nabs-750000-us-airforce-contract/

Christopoulos, D., & Vogl, S. 2015. The Motivation of Social Entrepreneurs: The Roles, Agendas and Relations of Altruistic Economic Actors. *Journal of Social Entrepreneurship,* 6(1): 1–30.
http://dx.doi.org/10.1080/19420676.2014.954254

Colwill, C. 2009. Human Factors in Information Security: The Insider Threat – Who Can You Trust These Days? *Information security Technical Report,* 14(4): 186–196.
http://dx.doi.org/10.1016/j.istr.2010.04.004

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. 2007. A Video Game for Cyber Security Training and Awareness. *Computers & Security,* 26(1): 63–72.
http://dx.doi.org/10.1016/j.cose.2006.10.005

Council on CyberSecurity. 2014. *The Critical Security Controls for Effective Cyber Defense.* Version 5.1. Council on CyberSecurity. Accessed January 10, 2015:
http://www.counciloncybersecurity.org/

Cremonini, M., & Nizovtsev, D. 2006. *Understanding and Influencing Attackers' Decisions: Implications for Security Investment Strategies.* Presented at The Fifth Workshop on the Economics of Information Security (WEIS), 26–28 June 2006. Cambridge, UK: The University of Cambridge.
http://weis2006.econinfosec.org/docs/3.pdf

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. 2013. Future Directions for Behavioral Information Security Research. *Computers & Security,* 32, 90–101.
http://dx.doi.org/10.1016/j.cose.2012.09.010

Denning, D. E. 1996. Concerning Hackers Who Break into Computer Systems. In P. Ludlow (Ed.), *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace:* 137–164. Cambridge, MA: MIT Press

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. 2011. From Game Design Elements to Gamefulness: Defining Gamification. In *Proceedings of the 15th International Academic MindTrek Conference:* 9–15. New York, NY: Association for Computing Machinery.
http://dx.doi.org/10.1145/2181037.2181040

Dogaru, P. D. S. O. 2012. Criminological Characteristics of Computer Crime. *Journal of Criminal Investigation,* 5(1): 92-98.

Gold, S. 2011. Understanding the Hacker Psyche. *Network Security,* 2011(12): 15–17.
http://dx.doi.org/10.1016/S1353-4858(11)70130-1

Hald, S. L., & Pedersen, J. M. 2012. An Updated Taxonomy for Characterizing Hackers According to Their Threat Properties. In *Proceedings of the 14th IEEE International Conference on Advanced Communication Technology (ICACT):* 81–86. Pyeongchang, South Korea: IEEE.

Hershberger, P. 2014. *Security Skills Assessment and Training: The "Make or Break" Critical Security Control.* SANS Institute InfoSec Reading Room. Accessed January 10, 2015:
http://www.sans.org/reading-room/whitepapers/leadership/security-skills-assessment-training-critical-security-control-break-o-35637

Huotari, K., & Hamari, J. 2012. Defining Gamification: A Service Marketing Perspective. In *Proceedings of the 16th International Academic MindTrek Conference:* 17–22. New York, NY: Association for Computing Machinery.
http://dx.doi.org/10.1145/2393132.2393137

Hayward, M. L., Shepherd, D. A., & Griffin, D. 2006. A Hubris Theory of Entrepreneurship. *Management Science,* 52(2): 160–172.
http://dx.doi.org/10.1287/mnsc.1050.0483

Jordan, C., Knapp, M., Mitchell, D., Claypool, M., & Fisler, K. 2011. CounterMeasures: A Game for Teaching Computer Security. In *Proceedings of the 10th Annual Workshop on Network and Systems Support for Games:* Article 7. Piscataway, NJ: IEEE Press.

Jordan, T., & Taylor, P. 1998. A Sociology of Hackers. *The Sociological Review,* 46(4): 757–780.
http://dx.doi.org/10.1111/1467-954X.00139

Kang, H. 2012. The Entrepreneur as a Hacker. *Epicenter: National Center for Engineering Pathways to Innovation.* Accessed January 10, 2015.
http://epicenter.stanford.edu/story/hongwen-henry-kang-carnegie-mellon-university

Kapp, K. M. 2012. *The Gamification of Learning and Instruction: Game-Based Methods and Strategies for Training and Education.* San Francisco, CA: Pfeiffer (Wiley).

Kim, P. H. 2014. Action and Process, Vision and Values. In T. Baker & F. Welter (Eds.), *The Routledge Companion to Entrepreneurship,* 59–74. New York, NY: Routledge.

Korolov, M. 2012. Gamification of the Enterprise. *Network World.* Accessed January 10, 2015:
http://www.networkworld.com/article/2160336/software/gamification-of-the-enterprise.html

Kuratko, D. 2013. *Entrepreneurship: Theory, Process, and Practice.* Melbourne, Australia: Cengage Learning.

Labuschagne, W. A., Veerasamy, N., Burke, I., & Eloff, M. M. 2011. Design of Cyber Security Awareness Game Utilizing a Social Media Gramework. In *Information Security South Africa,* 1–9. Johannesburg, SA: IEEE.
http://dx.doi.org/10.1109/ISSA.2011.6027538

Liu, S., & Cheng, B. 2009. Cyberattacks: Why, What, Who, and How. *IT Professional, 11*(3): 14–21. http://dx.doi.org/10.1109/MITP.2009.46

Mwakalinga, G. J., & Kowalski, S. 2011. *Modelling the Enemies of an IT Security System-A Socio-Technical System Security Model.* Presented at The 12th International Symposium on Models and Modeling Methodologies in Science and Engineering. March 27–30, 2011: Orlando, FL.

Mookerjee, V., Mookerjee, R., Bensoussan, A., & Yue, W. T. 2011. When Hackers Talk: Managing Information Security Under Variable Attack Rates and Knowledge Dissemination. *Information Systems Research,* 22(3): 606–623.
http://dx.doi.org/10.1287/isre.1100.0341

Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. 2012. Exploring Game Design for Cybersecurity Training. In *Proceedings of the 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER): 256–262.* May 27–31, 2012, Bangkok, Thailand.
http://dx.doi.org/10.1109/CYBER.2012.6392562

Nelson, B. 2012. The Real Definition of Entrepreneur – And Why It Matters. *Forbes.* Accessed January 10, 2015:
http://www.forbes.com/sites/brettnelson/2012/06/05/the-real-definition-of-entrepreneur-and-why-it-matters/

Parmar, B. 2013. Employee Negligence: The Most Overlooked Vulnerability. *Computer Fraud & Security,* 2013(3): 18–20.
http://dx.doi.org/10.1016/S1361-3723(13)70030-7

PwC. 2014. *US Cybercrime: Rising Risks, Reduced Readiness – Key Findings from the 2014 US State of Cybercrime Survey.* PricewaterhouseCoopers, CERT Division of the Software Engineering Institute, CSO Magazine, & United States Secret Service.

Rindova, V., Barry, D., & Ketchen, D. J. 2009. Entrepreneuring as Emancipation. *Academy of Management Review,* 34(3): 477–491.
http://dx.doi.org/10.5465/AMR.2009.40632647

Rogers, M. K. 2011. The Psyche of Cybercriminals: A Psycho-Social Perspective. In S. Ghosh & E. Turrini (Eds.), *Cybercrimes: A Multidisciplinary Analysis:* 217–235. New York, NY: Springer.
http://dx.doi.org/10.1007/978-3-642-13547-7_14

SANS. 2015. NetWars. *SANS Institute.* Accessed January 10, 2015:
http://sans.org/netwars

Sarasvathy, S. D. 2001. Causation and Effectuation: Toward a Theoretical Shift from Economic Inevitability to Entrepreneurial Contingency. *Academy of Management Review,* 26(2): 243–263. http://dx.doi.org/10.5465/AMR.2001.4378020

Unisys. 2014. Critical Infrastructure: Security Preparedness and Maturity. *Unisys.* Accessed January 10, 2015: http://www.unisys.com/insights/critical-infrastructure-security

Warikoo, A. 2014. Proposed Methodology for Cyber Criminal Profiling. *Information Security Journal: A Global Perspective,* 23(4-6): 172–178. http://dx.doi.org/10.1080/19393555.2014.931491

Williams, P. A. H. 2008. In a 'Trusting' Environment, Everyone Is Responsible for Information Security. *Information Security Technical Report,* 13(4): 207–215. http://dx.doi.org/10.1016/j.istr.2008.10.009

Wombat. 2015. Security Education Platform. *Wombat Security Technologies.* Accessed January 10, 2015: http://wombatsecurity.com/security-education

Zichermann, G., & Cunningham, C. 2011. *Gamification by Design: Implementing Game Mechanics in Web and Mobile Apps.* Sebastopol, CA: O'Reilly Media.

Citation: Adams, M., & Makramalla, M. 2015. Cybersecurity Skills Training: An Attacker-Centric Gamified Approach. *Technology Innovation Management Review*, 5(1): 5–14. http://timreview.ca/article/861

Keywords: cybersecurity, cyber attackers, gamification, entrepreneur, training