IADIS International Journal on Computer Science and Information Systems
Vol. 15, No. 2, pp. 91-106
ISSN: 1646-3692

MODELLING SERIOUS GAMES FOR ENHANCING END USER CYBER SECURITY AWARENESS

Mathew Nicho
College of Technology Innovation, Zayed University, Dubai, United Arab Emirates

ABSTRACT

The objective of this paper is to present a serious games model that assist organizations to substantially enhance computer user's cyber security awareness. Extensive research into academic literature revealed that a comprehensive model for designing serious games for training users to reduce user vulnerabilities in lacking. This paper thus focusses on strategically deploying serious games to educate, train and aware organizational users to detect, prevent, eliminate/mitigate and report instances of social engineering threats deployed by advanced persistent threat (APT) vectors, that predominantly target organisational user vulnerabilities. Training computer users on APT threat vectors which deploys simple social engineering yet complex technical methods to exploit internetworked computer user and subsequent vulnerabilities is a challenging task faced by organizations worldwide as is evident from publicly reported attacks. Serious games find immense applications in the domain of education, information systems and information security due to convenience of time, instant feedback, attractiveness and the ease of simulating novel and multiple attack scenarios. While serious games and models have been proposed by researchers in cyber security domain, attributes for building a serious gaming model for APT is wanting in both academic and practitioner domains. In this respect, we propose a serious game model GAM-APT by integrating the serious gaming model components namely the 'player', 'game' and 'knowledge' dimensions with Gagne's nine events.

KEYWORDS

Serious Games Model, Security Awareness, Advanced Persistent Threats, User Vulnerabilities

1. INTRODUCTION

Security education, training and awareness (SETA) programs has been an integral part of organizational countermeasures against cyber threats. Being an integral part of ISO 27K requirements, this has gained prominence among organizations to comply with relevant security standards. However, past and current efforts in this direction to improve information-security practices have not had the desired impact (Bada, Sasse, & Nurse, 2019). Thus, despite the implementation of SETA programs by organisations, hackers are still successful in penetrating organizational network using social engineering skills (Aldawood & Skinner, 2019) due to end user vulnerabilities.

End users have become an integral part where she/he has the knowledge to circumvent the systems, or the lack of knowledge that is needed to protect this information, as well as the well-being of the organization's network itself (Hight, 2005). Hence, the end user has been termed as the 'weakest link' in the security chain (Guo, Yuan, Archer, & Connelly, 2011; Paans & Herschberg, 1987). Furthermore, computer users represent one of the most persistent vulnerabilities in many computing systems wash (Wash & Cooper, 2018). Hence, cyber hackers find it easier to exploit humans rather than breaking into systems directly (Gupta, Arachchilage, & Psannis, 2018).

During the last two decades, APTs have emerged as a significant security challenge for a cyber- physical system due to their stealthy, dynamic and adaptive nature (Huang & Zhu, 2020). In this respect, an opportune mix of socio-technical factors have contributed to APT's success in exploiting organizational systems (Nicho & McDermott, 2019). Detection of APT vectors using conventional signature-based detection systems is a challenge since, APT use a combination of social engineering tactics along with zero-day exploits to exploit user vulnerabilities (Kamati, Jat, & Chamotra, 2021) at the workplace leading to organizational systems compromise. In this respect, focusing on user vulnerabilities and providing appropriate scenario based simulated training can considerably reduce these threats. Hence, we pose the research question: How can organizations built and deploy simulation to train organizational users to detect, prevent, mitigate/eliminate and report instances of cyberthreats targeting end users?

To answer this question the paper is structured as follows. Section II explores the concept of security awareness and training methods using simulation followed by section III that discusses the user perspectives in APT while section IV explores serious games from the perspective of history, objectives, research, user decisions and models. Section V presents the GAM-APT taxonomy of attributes, followed by conclusion (section V). The remainder of the paper uses the term 'user' or 'employee' to signify 'organizational internetworked computer user'. 'Threats' refer to advanced persistent threats using APT tools and vectors. 'Security' refers to information systems security in organizations.

2. USER AWARENESS THROUGH SETA

Security awareness programs in the information systems domain includes three major components namely security education, training and awareness commonly referred to as SETA. In this respect, user awareness of cyber threats requires the knowledge and the process required to detect, eliminate or mitigate, and report malicious intrusions using technical skills. Hence, the conventional method deployed in SETA programs has failed to stem the rise in cyber-attacks worldwide. While commercial and academic efforts in technical cyber security tools and models along with awareness and training has contributed to its abatement to some extent, the increase in successful attacks pose serious questions on the effectiveness of existing user awareness and training methods. SETA has been defined as a managerial program designed to improve the security of information assets by providing targeted knowledge, skills, and guidance or organizational employees (Whitman & Mattord, 2019). Since, the primary purpose of cyber security-awareness campaigns is to influence the adoption of secure behaviour online (Bada et al., 2019), serious games are advocated as promising technologies supporting training and increasing skills necessary to deal with new, complex and unexpected situations (Heldal, Wijkmark, & Pareto, 2016).

A learning or serious game using simulation methods can be defined as a system in which learners are placed in a 'problem-based environment', constrained by rules (Van Voorhis & Paris, 2019a). From a cyber security perspective, the 'problem-based environment' relates to cyber-attacks targeted at computer users which can be simulated where the players (computer users) play by pre-defined rules that motivates the user to elicit desired actions. Serious games which were initially created for military purposes, subsequently were extended to educational and business world including health care testing, emergency resolution, corporate training, virtual tour, education as well as creating behavioural change (Yang, 2018). Since cyber-attacks exploit human element of security, there is an urgent demand to educate and train users on how to protect themselves from cyber threats (VanSteenburg, 2017).

3. USER PERSPECTIVES IN APT

Advanced Persistent threats extensively use social engineering methods on internal users to enter organizational systems (Chen, Desmet, & Huygens, 2014). This user vulnerability is evident in the fact that by mistake they provide useful information to APT attackers (Alshamrani, Myneni, Chowdhary, & Huang, 2019). As the entry of APT is normally via the computer user interface, the APT perspective provides a socio-technical dimension to the APT problem. This socio vulnerability makes APT a predominantly a socio issue where reliance on cyber technological countermeasures is inadequate. Hence, training the computer user through the use of simulated attacks (multiple APT user interface attack scenarios) combined with defensive (detective, preventive, responsive) strategies (DS) by means of serious games can enhance user's capabilities for DS. APT attacks happen due to a combination of hacker skills and the inadvertent behaviour of computer users. Apt threats use apparently simple (social engineering) but complex (cyber technological) methods to gain privileged entry, escalate privileges and subsequently exfiltrate data via the opened backdoor. Advanced Persistent Threats (APTs) as the name implies use multiple social engineering techniques, while employing advanced cyber hacking techniques on cyber-physical systems; remains persistent till its successful and proceeds to deploy potent zero-day malware threat on the compromised cyber-physical asset. Since its emergence in the early half of the twenty first century, the potent nature of the threat as well as the frequency of attack targeted at critical organizations has not decreased, despite advances in network security and cyber defences. In this respect, analysis of multiple APT attacks has pointed out the unintentional mistakes of computers users in opening a vulnerability paving the way for asset compromise, privilege escalation and subsequent exfiltration. Hence, users play a vital role in securing the weakest link in the security chain to achieve behavioural transformation.

APTs have emerged as a significant security threat as well as challenge for a cyber-physical system due to their stealthy, dynamic, persistent and adaptive nature (Huang & Zhu, 2020). APT is a serious issue for current detection methods because the common defensive methods deployed by organizations, depend on known signatures of attacks, while APTs make heavy use of unknown security holes for attacks which makes detection difficult. Furthermore, errors and omissions, sabotage caused by employees, criminal agent, industrial or commercial espionage and malicious programs combined make this threat potent and successful (Rodríguez-Corzo, Rojas, & Mejía-Moncayo, 2018). Thus, organisations ought to take steps to ensure that their employees are aware of sensate information which should not be shared via the Internet in answer to unexpected requests (Furnell, 2013). Taking mitigation strategies into account, encouraging progress have been made in the utilization of games for preparing end-users. In this respect, serious games have emerged as a new approach that can complement instruction-led or

computer-based security training where players learn and practice cyber security concepts through the game (Hart, Margheri, Paci, & Sassone, 2020).

4. SERIOUS GAMES

Initially created for military purposes, it emerged as a promising approach to self-train computer users in changing their profile from a 'weakest link' to a 'strong link' in the network chain. Serious games are tutoring tools, usually computerized in nature, utilizing methods and approaches of the gaming sector for purposes other than amusement. Ever since researchers began designing simple games and simulations as part of their research in the early 1950s, games have evolved to become an effective mode of learning. However, it was 'Odyssey' by Magnavox, one of the world's first commercial home video game consoles (launched in the USA in 1972), that emphasized the device's potential as an educational tool, and thus might be considered one of the first serious video game (Laamarti, Eid, & El Saddik, 2014). Simultaneously, in 1970, Clark published the concepts of using serious games where he emphasized the use of games in education, occupational choice and training, including problem solving in government and industry (Clark, 1970). Serious or educational games immerse the participants into complex, realistic project situations, provides learners (players) with practical experience without exposing them to the risks or costs, and offers significant value to educators and trainers who otherwise find it challenging to prepare learners to cope with complex problems (Rumeser & Emsley, 2019). Serious games which are attractive to young computer users have become an effective method of simulation based learning and training in a dynamically changing world of complex cyber security issues (Furuichi & Aibara, 2019).

4.1 Purpose of Serious Games

Serous games provide effective knowledge acquisition and behavioural change in game users. In contrast to entertainment games, serious games are games which have been intentionally designed to support learning (Boyle et al., 2014). Education and training are two emerging domains where there has been an ever-increasing application of simulations and serious games (Coovert, Winner, Bennett, & Howard, 2017), Winner, & Ben, 2017) that influence behavioural and academic change (De Freitas & Ketelhut, 2014). Serious games not only assists in assessing higher order thinking skills, which is a necessary step to improve them (Laamarti et al., 2014), but also improve skill of knowledge, rehabilitation, medical treatments, training and education (Furuichi & Aibara, 2019). This is mainly due to its ability to provide interactive environments that are complex and open for exploration that learners can use to demonstrate and expand their skills, and assessment (Van Voorhis & Paris, 2019b). Being a mental contest played with computer in accordance with specific rules that uses entertainment to further government or corporate training, education, or health (Yang, 2018), these games are designed to include cognitive activities to assure participants' engagement levels remain high (Salameh, 2019). Serious games has proved that effective learning is most 'effective' when it is active, experiential, situated, problem-based and when it provides immediate feedback (Connolly, Boyle, MacArthur, Hainey, & Boyle, 2012). Subsequently, serious games are advocated as promising technologies supporting training and increasing skills necessary to deal with new, complex and unexpected situations (Heldal et al., 2016).

4.2 Serious Games in Cybersecurity

SETA programs have a defined objective of ensuring behavioural change in the participant's use of computer systems. In this respect, serious games contains easy to understand objectives, continuous assessment and feedback, and narratives that provide the player with sense of identity (VanSteenburg, 2017). Hence, serious games are effective methods of simulation based learning and training in a dynamically changing world of cyber security issues (Furuichi & Aibara, 2019). However, since 'hacking' in cyber domain involves competing players where the 'hacker' tries to penetrate the 'victim's computer while the victim intentionally or unintentionally attempts to defend her/his IS assets, serious games in cyber security thus follows a competing pattern. Saunders (2001) has classified activity simulation in the information security domain into five categories namely 1) Packet Wars, 2) Sniffers + Network Design Tools, 3) Canned Attack/Defend Scenarios, 4) Management Flight Simulators, and 5) Role-playing (see table 1). Training and education in serious games in cyber security involve presenting multiple scenarios to the trainee. Since, in this paper we are targeting to train unsuspecting computer users with limited IT knowledge, serious games for training on social engineering attacks (related to APT) comes under the 'attack/defend scenario'. Furthermore, multiple scenarios have to be designed and populated into the game database.

Table 1. Types of activity simulation (adapted from Saunders, 2001)

Categories	Description	Purpose
Packet wars	Tactical network attack and defence scenarios.	These types of simulations exist for technical personnel primarily on the local network or at best enterprise level
Network design tools	Network modelling & simulation (NMS)	NMS Packages which are paired with sniffer data to provide real network visualization
Canned attack/ defence	These are typically standalone applications that can be utilized in a game like manner.	This facilitate learning to individuals who are trained in IT, but not yet conversant in finer points specific to information security.
Management flight simulators	Built using system dynamics or discrete event simulation tool	The purpose of this security model was to look at the overall impact of a computer fraud attack on the flow and reconstruction of organizational data
Role playing	They are face to face, actor-oriented without the use of computer simulation	Their purpose is to play out scenarios, to gain a better understanding of the roles of different organizations and personnel in defending large-scale attacks

4.3 Research on Serious Games in Cybersecurity

Research on serious games to train computer users in detecting the social engineering phase of APT attack is lacking in academic and practitioners' fora. With serious games gaining popularity to train computer users, a survey on serious games in cyber security training by (Tioh, Mina, & Jacobson, 2017) listed eighteen papers on innovative serious games for cyber security with thirteen serious games available for user training on the Internet. However, the emphasis on these games focus more on generic cyber security, phishing, and spear-phishing rather than

on APT. A search on google scholar for APT user training games using the term "serious games" and "advanced persistent threats" (from 2015 to 2020) turned up only seven papers (Feng, Xiong, Niyato, & Wang, 2019; Huang & Zhu, 2020; Katsantonis, Kotini, Fouliras, & Mavridis, 2019; Luh, Temper, Tjoa, Schrittwieser, & Janicke, 2020; Min, Xiao, Xie, Hajimirsadeghi, & Mandayam, 2018; Yang et al., 2018; Yasin, Liu, Li, Fatima, & Jianmin, 2018) focusing on serious game algorithm, and methodologies along with three papers focusing on cyber security in general among the 18000 results. However, a comprehensive model on developing serious games to train users to detect, prevent, eliminate/mitigate and report APT attacks is lacking in the research domain. Hence, serious games in cyber security involves two parties where a genuine computer user tries to outwit the simulated malicious adversary (hacker). In this respect, the success of the game depends on the player's decision-making skills (the knowledge of malicious as well as genuine IT processes and the ability to differentiate between these two).

A. Decision Making in Serious Games in Cybersecurity

Four types of decisions are encountered by interconnected computer/ smartphone users in a player-hacker attack scenario (Nicho & Khan, 2018). These are termed as true positive (where the user detected the threat prior to entering the system), true negative (where genuine IS process was identified and processed), false positive (where genuine IS process was identified as threat and thus stopped) and false negative (where malicious threat was identified as genuine IS process and allowed inside the network) in terms of decisions facing a user in a player-hacker attack scenario (see table 2). Here the orientation of the users namely 'True' represents correct judgement while 'False' denotes wrong judgement of the user when confronted with an IS process (the IS process can be genuine or malicious).

Table 2. User decision models in a simulation game

User Perception		**Outcome**	**User assessment**	**Outcome**
True	Positive (TP)	User detected the threat	Correct user judgement. Threat prevented	Desirable
	Negative (TN)	No attack has taken place. User identified genuine IT processes	Correct user judgement. Correctly identified genuine IS process	Desirable
False	Positive (FP)	False alarm. Genuine IS process detected as threat and stopped	Wrong user judgement	Moderate/ Tolerable decision
	Negative (FN)	APT entered the system masquerading as genuine IS process/ user vulnerability	Wrong judgement	Critical/ Unacceptable

Out of the four decision scenarios, FN (represented by 'y') is critical as it is a function of SETA (represented as 'x') where $y = f(x)$ and $y \propto 1/x$. In a traditional SETA program, 'x' must be increased substantially to decrease the incidence of 'y'. However, in a cyber security serious game, a moderate increase of 'x' can result in a substantial decrease of 'y' saving the organization not only from attacks, but also savings in terms of cost and effort. Hence, consider these four decision scenarios while designing serious games for APT ensures 'effectiveness' and 'efficiency'.

B. Serious Games Models

A review of literature had provided three framework/models for serious games developers. The process of playing a serious game relies on representations of the following sub-systems

namely the knowledge model (learning objectives), the game model (the game mechanics, challenges and content), the player model (characteristics and mental states of the player during the process of play) which all come together in the frame of operation and effectiveness (Westera, 2017), . Laamarti et al. (2014) proposed a taxonomy of serious games that provides a holistic view of APT serious game attributes that considers the application, activity, modality, interaction and the environment. Furthermore, success in serious games focus on nine events of instruction by Gagne, namely gain attention (GA), inform learners of the objective (LO), stimulate recall of prior learning PL), present stimulus material (SM), provide learning guidance (LG), elicit performance (EP), provide feedback (PF), assess performance (AP), and enhance retention and transfer (RT) (Hricko, 2008). Integrating these three models provide a holistic perspective of serious game for cyber security (table 3).

Table 3. Serious game attributes based on taxonomy (domains and methods), events and components

Domains	Methods	Gagne' Nine events	Component Focus
(Laamarti et al., 2014)		(Hricko, 2008)	(Westera, 2017)
Application area	Training & Education	PL/ LO	Player/ Knowledge
Activity (type of activity performed by the player as required by the game)	Mental	GA/ SM/ LG/ EP/ PF/ AP/ RT	Game/ player
Modality (information communication channel from computer to the player)	Visual	GA/ LO/ PL/ SM/ LG/ EP/ PF/ AP	Game/ knowledge
Interaction style (interface)	Keyboard/ mouse	EP	Game
Environment (player environment)	2D/ 3D	RT	Game

Integrating the Gagne's nine events and the domains of Laamarti into the three constructs of Westera provides detailed attributes of how a serious game can be developed.

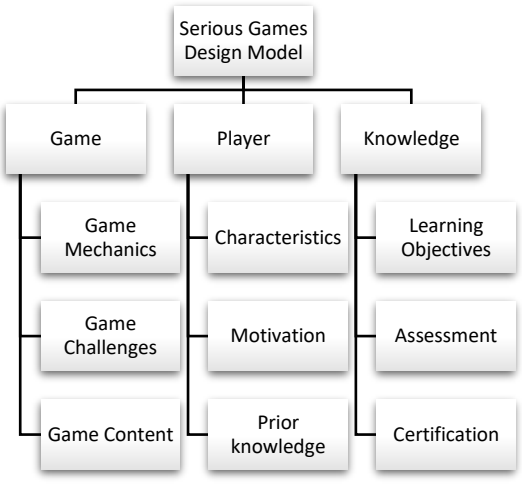

Figure 1. Serious gaming components (Adapted from Westera (2017)

The serious game components of Westera, Gagne's nine events, and Laamarti's domains integrate to provide a rich attribute for game developers. However, since exchange of knowledge ensures when player interacts with the game, integrating Westera's gaming components (figure 1) into APT provides rich guidelines for game designers.

5. SERIOUS GAME DESIGN MODEL for APT (GAM-APT)

The serous game design model for APT (GAM-APT in figure 2) provides information regarding the dimensions and attributes of a serious game focussing on training interconnected computer users in detecting, preventing, mitigating and reporting APT attacks. The game dimension focus on increasing the attractiveness and reducing the complexity through the deployment of APT game characteristics. This includes the assortment of APT scenarios, objectives of each game, including rules, the levels of challenge corresponding to user skills and knowledge populated with a immersive content of rich scenarios representing APT threats. The objective of the player component being identifying APT user vulnerability via motivation and attractiveness, it gets incorporated into the game attributes. Improving users' skills in detecting, preventing, mitigating and reporting APT threats being the objective of the knowledge component, this is done through assessment and a continuous improvement feedback loop. The model, which is explained in detail in table 4, 5 and 6 provides high levels as well as detailed guidelines for serious game developers to develop serous games that target not only user vulnerabilities related to APT but also for generic SETA programs.

Through this model we are proposing a serious interactive game that incorporates the following functionalities to prevent user targeted attacks with respect to APT threats.

- Simulate the multiple entry points of cyber threats (where human intervention on the part of the users can cause a breach) through multiple scenarios;
- Allow the players (users) decide on the corresponding reaction to these threats, (alternatively suggest prescriptive reactions) using a scoring method.
- Game progression can be measured by providing objective feedback in the form of points. They are usually awarded for accomplishing certain tasks where the specific range and number of points can be allocated to different levels of employees. The rewards for obtaining points are usually increasing due to experience curve of players playing the game repeatedly over time;
- Create a user log to document the gradual progression of the user's learning process including motor skills and behavioural change;
- Map the behaviour of users to relevant IS security and data privacy regulations/standards to inform compliance/non-compliance, and
- Create different visual dashboards of the employees' IS security awareness level at different points in time.

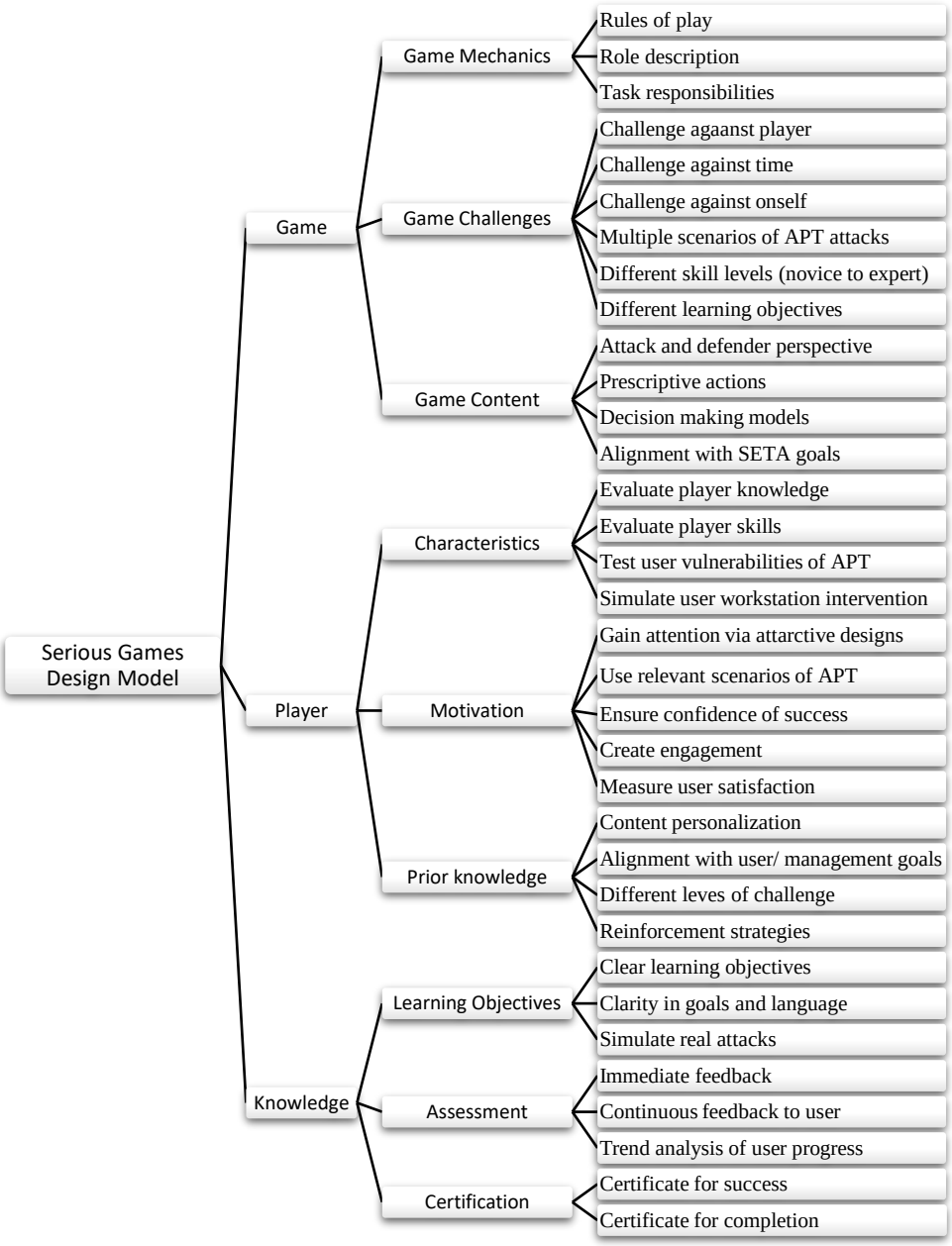

Figure 2. The GAM-APT: A Serious Game Model for Designing Cyber Security Games

Table 4. The attributes of game component of GAM-APT

Dimensions	Serious Game Attributes	APT Simulation Attributes/variables
Game	**Game mechanics**: Defined "as methods invoked by agents, designed for interaction with the game state" which encompasses those rules that are applied when the player interacts with the game, as well as low-level descriptions of game rules or clusters of game rules (Sicart, 2008).	Rules of play should be well explained. (Silva, Maneira, & Villachan-Lyra, 2018). Game design should have complete role descriptions including task responsibilities for each role (Rosenthal & Strecker, 2018). This ensures the APT game player to play the game as per multiple simulated attack patterns based on defence objectives of selected APT threats.
	Game challenges: This is ensured when learners are challenged slightly beyond the boundaries of their abilities, while avoiding both frustration and boredom (Westera, 2017).	The game becomes a challenge against time, a challenge against other players and against oneself, where the only thing which counts is to show to the web the level of technical finesse (Soriani, Ilardo, & Falconi, 2018) of the user in DS. Multiple scenarios (APT scenarios) can be created which allows for players of various skill levels and backgrounds to learn about information security (VanSteenburg, 2017). Serious games should have various levels of learning objectives and for many types of persons in general (Furuichi & Aibara, 2019).
	Game content: The objective of gamification is to take content that is typically presented to the audience, add game-based elements and create a gamified learning opportunity either in the form of full-fledged educational game, in the form of game elements wherein learners participate in a story-based challenge to master the content presented (Kapp, 2012).	For each cyber security scenario, there should be two scenarios, one for the intruder's perspective and the other from the defender's perspective (Lu, 2018) correlating with APT scenario (attack) and a defender mode/prescriptive actions. The four types of user decision models (table 1) in an APT scenario ensures reduction of APT attacks, including SETA cost and effort.

Table 5. The attributes of player component of GAM-APT

Dimensions	Serious Game Attributes	APT Simulation Attributes/variables
Player	**Player characteristics**: Players' characteristics include players' learning preferences (e.g., background knowledge, interests), the gaming skills, the goals set by the players and the players' motivation (Katsantonis et al., 2019).	APT vulnerabilities of users include employee mistakes, lack of awareness of APT, not reading communications, unethical behaviour, low awareness of security among non-IT staff, low motivation, accessibility vs security, issues with training, not reading security policies and consumer preference (Nicho & McDermott, 2019). Hence, intervention is required at the dimension where the user interacts with the workstation in order to assist the user to make a correct decision when confronted with a genuine or malicious APT vector (Nicho & Khan, 2018).
	Motivation: According to the ARCS Model, four conditions are necessary for increasing the motivational appeal of an instructional material, namely **A**ttention, **R**elevance, **C**onfidence and **S**atisfaction (Salameh, 2019).	Serious games can boost motivation (Lu, 2018). In SETA programs, engagement is an important factor for activating attention and creating interest in changing behaviour (Salameh, 2019); the APT game has to be tailored to ensure relevance to participating professionals (Gasiba, Lechner, Rezabek, & Pinto-Albuquerque, 2020); APT games can be created where, "users became more confident about their judgments after the game or the tutorial conditions" (Sheng et al., 2007); "when designing tools to educate people, it is highly recommended to measure users' satisfaction" (Micallef & Arachchilage, 2017) which translates to feedback.
	Prior knowledge: Refers to the learners' knowledge states where a deficit results in increased challenge (Westera, 2017).	Adaptation of APT games could be through the personalization of content to the user's knowledge and goals (Streicher & Smeddinck, 2016) with different levels of game difficulty. "Splitting content into levels, scenarios, or modules allows for players to come back later to reinforce previous lessons or learn new material that they have not played before" (VanSteenburg, 2017).

Table 6. The attributes of knowledge component of GAM-APT

Dimensions	Serious Game Attributes	APT Simulation Attributes/variables
Knowledge	**Learning objectives:** A serious game will have learning objective for players in terms of knowledge, skills and competencies to be achieved (Westera, 2017)	Clear and worthwhile objectives in game scenarios are necessary to create an effective serious game for cybersecurity training and awareness. Furthermore, serious games should contain easy to understand unambiguous objectives, synchronize learning and gameplay objectives (VanSteenburg, 2017). Thus, "a game would consistently fulfil cyber security strategies' objectives in terms of education and awareness" (Le Compte, Elizondo, & Watson, 2015). Since APT uses multiple methods, defined specific objectives for each scenario provides focus on the learning objective.
	Assessment: Game assessment imply that the game matches technical and pedagogic expectations, while maximising players' engagement and enjoyment (Le Compte et al., 2015)	Serious games should provide continuous assessment immediate feedback regarding the progress toward those objectives (VanSteenburg, 2017). Gamification elements, including clear goals, points, achievements, feedback and leader boards, increase motivation (Alqahtani & Kavakli-Thorne, 2020). Provision of assessment and feedback regarding success or failure during each APT gaming scenario enhances player knowledge.
	Certification: This refers to positive reinforcement in which rewards were given after a fixed number of correct responses (Nagle, Wolf, Riener, & Novak, 2014)	Motivation for the games is either recognition (financial or other incentives like prizes for first, second and third places in the competition) or certification to enhance your professional career. (Nagarajan, Allbeck, Sood, & Janssen, 2012). Continuous improvement can be gained through tangible awards after the success of any game scenario.

6. CONCLUSION

Moving away from the traditional security awareness training that focus on a one way (trainer imparting training) or a two way (trainer led interactive workshop) method to impart the 'DOs' and 'DON'T's', we propose an innovative, comprehensive multiple cyber threat scenario gaming model that encompass all existing/current threat vectors (where employees/users pay a role – especially the initial stages of Advanced Persistent Threats) to provide a scalable, interactive and engaging performance based gaming environment to the trainee. The increase in APT attacks using dynamic, novel and sophisticated methods targeting organizational networks via inadvertent user mistakes has prompted organizations to focus aggressively on SETA training. Serious games come with the added advantage of encompassing the entire organizational users in a short time with increased effectiveness, less cost, time and effort. In this respect, our GAM-APT model provides the methodology for serious game developers to develop games that target internetworked computer users in organisations as well as work from home users. While research and industry has targeted interconnected computer users with simulated games on different aspects of cyber security, this is the first such model that demonstrates the essential attributes of a serious gaming model for APT scenarios, where the user/trainee holds the key to open a vulnerability or demonstrate the ability to detect, prevent, mitigate and/or report the simulated malicious actor.

Limitations of this research focus on three areas for which subsequent research is required. First, researchers need to ascertain the cause and effect of the variables in the taxonomy to ascertain the precursor events. Identifying the pre cursor events for game attractiveness and success can enhance game effectiveness. Second, this taxonomy needs to be validated with experts in the cybersecurity field to bring out its strength and weakness. Third, the taxonomy needs to be translated into a prototype and tested on an experimental group to evaluate its effectiveness. We hope that this model will serve as a baseline for serious game developers in creating training simulations.

REFERENCES

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet, 11*(3), 73.

Alqahtani, H., & Kavakli-Thorne, M. (2020). Design and Evaluation of an Augmented Reality Game for Cybersecurity Awareness (CybAR). *Information, 11*(2), 121.

Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. *IEEE Communications Surveys & Tutorials*.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.

Boyle, E. A., MacArthur, E. W., Connolly, T. M., Hainey, T., Manea, M., Kärki, A., & Van Rosmalen, P. (2014). A narrative literature review of games, animations and simulations to teach research methods and statistics. *Computers & Education, 74*, 1-14.

Chen, P., Desmet, L., & Huygens, C. (2014). *A study on advanced persistent threats.* Paper presented at the IFIP International Conference on Communications and Multimedia Security.

Clark, C. A. (1970). Serious games. *Nueva York: Viking*.

Connolly, T. M., Boyle, E. A., MacArthur, E., Hainey, T., & Boyle, J. M. (2012). A systematic literature review of empirical evidence on computer games and serious games. *Computers & Education, 59*(2), 661-686.

Coovert, M. D., Winner, J., Bennett, W., & Howard, D. J. (2017). Serious games are a serious tool for team research. *Int. J. Serious Games, 4*(1), 41-55.

De Freitas, S., & Ketelhut, D. J. (2014). Preface: Introduction for the Journal of Information Sciences special issue on serious games. *Information Sciences—Informatics and Computer Science, Intelligent Systems, Applications: An International Journal, 264*, 1-3.

Feng, S., Xiong, Z., Niyato, D., & Wang, P. (2019). Dynamic resource management to defend against advanced persistent threats in fog computing: A game theoretic approach. *IEEE Transactions on Cloud Computing*.

Furnell, S. (2013). Still on the hook: the persistent problem of phishing. *Computer Fraud & Security, 2013*(10), 7-12.

Furuichi, M., & Aibara, M. (2019). *A Challenge of Developing Serious Games to Raise the Awareness of Cybersecurity Issues.* Paper presented at the DiGRA Conference.

Gasiba, T., Lechner, U., Rezabek, F., & Pinto-Albuquerque, M. (2020). *Cybersecurity Games for Secure Programming Education in the Industry: Gameplay Analysis.* Paper presented at the First International Computer Programming Education Conference (ICPEC 2020).

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems, 28*(2), 203-236.

Gupta, B., Arachchilage, N. A., & Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems, 67*(2), 247-267.

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers & Security*, 101827.

Heldal, I., Wijkmark, C. H., & Pareto, L. (2016). *Simulation and serious games for firefighter training: Challenges for effective use.* Paper presented at the Norsk konferanse for organisasjoners bruk at IT.

Hight, S. D. (2005). The importance of a security, education, training and awareness program, November 2005. *Security, 27601*, 1-5.

Hricko, M. (2008). Gagne's Nine Events of Instruction *Encyclopedia of Information Technology Curriculum Integration* (pp. 353-356): IGI Global.

Huang, L., & Zhu, Q. (2020). A dynamic games approach to proactive defense strategies against advanced persistent threats in cyber-physical systems. *Computers & Security, 89*, 101660.

Kamati, T. H., Jat, D. S., & Chamotra, S. (2021). *Design and Development of System for Post-infection Attack Behavioral Analysis.* Paper presented at the Proceedings of Fifth International Congress on Information and Communication Technology.

Kapp, K. M. (2012). *The gamification of learning and instruction: game-based methods and strategies for training and education*: John Wiley & Sons.

Katsantonis, N. M., Kotini, I., Fouliras, P., & Mavridis, I. (2019). *Conceptual framework for developing cyber security serious games.* Paper presented at the 2019 IEEE Global Engineering Education Conference (EDUCON).

Laamarti, F., Eid, M., & El Saddik, A. (2014). An overview of serious games. *International Journal of Computer Games Technology, 2014*.

Le Compte, A., Elizondo, D., & Watson, T. (2015). *A renewed approach to serious games for cyber security.* Paper presented at the 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace.

Lu, Y. (2018). *CyberCraft, a security serious game.* (PhD), Politecnico di Torino. Retrieved from https://webthesis.biblio.polito.it/9474/

Luh, R., Temper, M., Tjoa, S., Schrittwieser, S., & Janicke, H. (2020). PenQuest: a gamified attacker/defender meta model for cyber security assessment and education. *Journal of Computer Virology and Hacking Techniques, 16*(1), 19-61.

Micallef, N., & Arachchilage, N. A. G. (2017). Involving users in the design of a serious game for security questions education. *arXiv preprint arXiv:1710.03888*.

Min, M., Xiao, L., Xie, C., Hajimirsadeghi, M., & Mandayam, N. B. (2018). Defense against advanced persistent threats in dynamic cloud storage: A colonel blotto game approach. *IEEE Internet of Things Journal, 5*(6), 4250-4261.

Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012). *Exploring game design for cybersecurity training.* Paper presented at the 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER).

Nagle, A., Wolf, P., Riener, R., & Novak, D. (2014). The use of player-centered positive reinforcement to schedule in-game rewards inreases enjoyment and performance in a serious game. *International Journal of Serious Games, 1*(4), 35-47.

Nicho, M., & Khan, S. N. (2018). *A decision matrix model to identify and evaluate APT vulnerabilities at the user plane.* Paper presented at the 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).

Nicho, M., & McDermott, C. D. (2019). *Dimensions of 'Socio'Vulnerabilities of Advanced Persistent Threats.* Paper presented at the 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM).

Paans, I. R., & Herschberg, I. S. (1987). Computer Security: The Long Road Ahead. *Computers & Security, 6*(5), 403-416.

Rodríguez-Corzo, J. A., Rojas, A. E., & Mejía-Moncayo, C. (2018). *Methodological model based on Gophish to face phishing vulnerabilities in SME.* Paper presented at the 2018 ICAI Workshops (ICAIW).

Rosenthal, K., & Strecker, S. (2018). *Business Process Modelling as Serious Game: Findings From a Field Study.* Paper presented at the ECIS 2018, Portsmouth, UK.

Rumeser, D., & Emsley, M. (2019). Can serious games improve project management decision making under complexity? *Project Management Journal, 50*(1), 23-39.

Salameh, R. (2019). *The Relationship between Engagement Levels and Players' Intended Behaviors in Game-Based Training for Cybersecurity.* Southern Illinois University at Carbondale.

Saunders, J. H. (2001). *The case for modeling and simulation of information security.* Paper presented at the Computer Security Institute Conference, http://www. johnsaunders. com/papers/securitysimulation. htm.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). *Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish.* Paper presented at the Proceedings of the 3rd symposium on Usable privacy and security.

Sicart, M. (2008). Defining Game Mechanics. *The International Journal of Computer Game Research, 8*(2).

Silva, M. C. A. P., Maneira, A., & Villachan-Lyra, P. (2018). Digital Educational Games: Inclusive Design Principles for Children with ADHD. *Proceedings of Play2Learn 2018*, 30.

Soriani, A., Ilardo, M., & Falconi, A. (2018). Videogames, Violence and Aggressive Behavior: an Educational Proposal. *Proceedings of Play2Learn 2018*, 11.

Streicher, A., & Smeddinck, J. D. (2016). Personalized and adaptive serious games *Entertainment Computing and Serious Games* (pp. 332-377): Springer.

Tioh, J.-N., Mina, M., & Jacobson, D. W. (2017). *Cyber security training a survey of serious games in cyber security.* Paper presented at the 2017 IEEE Frontiers in Education Conference (FIE).

Van Voorhis, V., & Paris, B. (2019a). Simulations and Serious Games: Higher Order Thinking Skills Assessment. *Journal of Applied Testing Technology, 20*.

Van Voorhis, V., & Paris, B. (2019b). Simulations and Serious Games: Higher Order Thinking Skills Assessment. *Journal of Applied Testing Technology, 20*(S1), 35-42.

VanSteenburg, M. (2017). *Applications of Serious Gaming to Cybersecurity Training and Awareness.* Utica College.

Wash, R., & Cooper, M. M. (2018). Who Provides Phishing Training? Facts, Stories, and People Like Me.

Westera, W. (2017). How people learn while playing serious games: A computational modelling approach. *Journal of Computational Science, 18*, 32-45.

Whitman, M. E., & Mattord, H. J. (2019). *Management of Information Systems*. Boston, USA: Cengage.

Yang, L.-X., Li, P., Zhang, Y., Yang, X., Xiang, Y., & Zhou, W. (2018). Effective repair strategy against advanced persistent threat: A differential game approach. *IEEE Transactions on Information Forensics and Security, 14*(7), 1713-1728.

Yang, L. (2018). *CyberCraft, a security serious game.* Politechnico di Torino, Torino.

Yasin, A., Liu, L., Li, T., Fatima, R., & Jianmin, W. (2018). Improving software security awareness using a serious game. *IET Software, 13*(2), 159-169.