An e-ADR (elaborated Action Design Research) Approach Towards Game-based Learning in Cybersecurity Incident Detection and Handling

Dixon Prem Daniel R
Indian Institute of Technology – Madras
dixdan2008@gmail.com

Sundarraj R P
Indian Institute of Technology – Madras
rpsundarraj@iitm.ac.in

Abstract

The growth of internet has significantly increased the cybersecurity threat instances. Therefore to equip people with skills to mitigate such attacks, this paper provides a Cybersecurity game-based learning artefact designed using the e-ADR approach. The artefact teaches the Incident Detection and Handling procedures that need to be undertaken in the event of a cybersecurity threat. As per NIST's guide to malware incident prevention and handling, an incident response process has four major phases: preparation, detection and analysis, containment/eradication/recovery, and post-incident activity. Our gaming artefact delves into the detection and containment phase to design a game that teaches users to detect and then perform containment actions on the cybersecurity threat.

1. Introduction

Research suggesting digital games could enable learning, Subrahmanyam and Greenfield, and De Freitas sparked focus on commercial games [1, 2]. Games have also enabled training and learning in an intrinsically motivating approach [3]. This then led to focus attention on Game-based Learning (GBL) [2], serious games which were games with educational goals and had purposes other than pure entertainment [4]. The earliest games were developed to provide training and learning [2]. The objective of our game is to train IT as well as non-IT professional in cybersecurity Incident Detection and Handling procedures. These Incident Handling procedures available in NIST [5] were employed to teach the procedures to be adopted in the event of a cybersecurity threat. As part of our research project we: (i) develop Game-based Learning (GBL) artefacts that train users in the concepts of cybersecurity; and (ii) embed industry experts to assess our artefacts and provide value. We develop our gaming artefact using the e-ADR approach [6].

Cybersecurity is the top five most important IT management concerns and also lists in the top five largest IT investments [7]. The losses caused by breach in network security has always been an issue. As a result of lapses in security by organizations, enormous budgets have been set aside to protect information systems [8]. Internet has become all pervasive at home and at workplace. Therefore online security is a high priority task for the management in organizations, computer users at home and also the society [9]. Security being a primary issue, leads to expanding expenditures with respect to firewalls, authentication systems and other techniques that are concerned with the systems.

But there is another aspect to security which is not concerned with systems – the user [10]. The sophisticated security systems lose their effectiveness if passwords are mismanaged by the users [11]. Carlton and Levy enumerate top platform independent skills for Non-IT Professionals to mitigate cybersecurity vulnerabilities [12]. Our artefact delves into two of the skills mentioned in the paper, prevention of malware related incidents and password management.

Takahashi and Kadobayashi provide a reference ontology for cybersecurity information and look at cybersecuirty threats from the standpoint of cybersecurity operations [13]. The security systems fail if the professionals responsible for the cybersecurity operations of organization do not respond effectively to the threats. The severity and frequency of malware attacks has increased and large number of malicious software programs are affecting organizations who find it difficult to deal with these programs in an efficient way [14]. Therefore training users to effectively handle cybersecurity operations in an organization should be a priority and this motivated us to develop our gaming artefact.

2. Literature

URI: https://hdl.handle.net/10125/64365
978-0-9981331-3-3

An increasing research interest on the ways games influence learning in education can be observed [15]. Use of games for teaching helps us discern the effects of games on motivation and cognitive development of individuals [15, 16]. Game-based Learning describes an environment in which knowledge and skill acquisition is augmented by game content and game play, and where the players feel a sense of achievement as a result of game activities that involve problem solving and challenges [15]. In recent years, gamification, which draws game design elements from games has dispersed itself into many areas. Similarly in the educational context which uses games for teaching and learning, GBL has established itself [17]. There are studies that develop video games for students to promote learning in an engaging manner.

CyberCIEGE [18], is one such that provides information assurance awareness using a construction and management resource simulation video game. PicoCTF [19], a computer security competition for high school students, designed to introduce computer security concepts to students at a younger age. Along the same lines there are other events such as CTF (Capture the Flag) that are computer security contests between teams [20]. CTFs can be considered as full-simulation cyber war-game. Such games are technically demanding, Gondree, Peterson and Denning target a small community of security-minded students and professionals [21]. Since the target group is niche, the focus of the game design stays on imparting the cybersecurity objectives and not on the nature of the interactive experience. Thus we design a game that merges the cybersecurity and gaming objectives. The gaming objectives focus on the interactive experience. Additionally the existing cybersercurity games address: (1) threats such as malware, Trojan horses, un-patched software flaws that expose limitations in security mechanisms [22]; (2) challenges to increase computer security awareness [23]; and so on. Despite all the measures taken to prevent such threats, residual risks inevitably persist and no solution is foolproof [5]. We therefore depart from these games by designing a game that addresses the scenarios in which the focus is on Incident Detection and Handling. This game would teach the steps that have to be taken as part of the standard operating procedures once we detect that an attack has occurred. We employ Design Science Research framework to develop our artefact.

Design Science Research is a problem-solving paradigm. It enables creation and evaluation of IT artefacts that help solve organizational problems [24]. Design Science follows a sequencing approach which separates building from evaluating. With the growing need for research method that explicitly recognizes artefacts as emerging from interaction with the organization the authors in [25] proposed ADR. It is a research method for generating prescriptive design knowledge [25]. The original process mode of ADR was extended to give us the e-ADR [6] and we use the e-ADR to develop our gaming artefact. This paper is an extension of our work in [26].

3. Research Approach & Discussion

Our development of the gaming artefacts follows the design theory proposed in the e-ADR approach. The elaborated ADR approach puts together the principles of Design Science [24], Action Research [27] and is an extension of the ADR approach. The ADR methodology consists of four stages which enable generating prescriptive design knowledge [25]. This ADR method was elaborated by [6] to give rise to the e-ADR approach.

The e-ADR [6] is an extension of the work by Sein et al. [25]. It consists of the following four stages: (a) Diagnosis; (b) Design; (c) Implementation; (d) Evolution. Each stage has an intervention cycle which consists of five activities: (a) Problem Formulation (P); (b) Artefact Creation (A); (c) Evaluation (E); (d) Reflection (R); and (e) Learning (L). The e-ADR approach enables entry at any stage. We initiated our research project with the design stage (Figure 1). The game artefact went through two iterations of the design phase and we are now in the third iteration of the design phase. We developed five gaming artefacts four of which handle scenarios pertaining to Incident Detection and Handling and one scenario pertains to Password Management. These scenarios were taken from NIST [28]. The scenario objectives are provided in Table 1.

Table 1. Game scenario objectives

Scenarios	Objectives
Network Spike [Artefact 1]	To detect the threat and learn the sequence of steps that minimize the threat caused by Network Spike
Malicious Popups [Artefact 2]	To detect the threat and learn the sequence of steps that minimize the threat caused by Malicious Popups
Password Management [Artefact 3]	To determine the best possible resource to store the password in.
Unfamiliar Programs [Artefact 4]	To detect the threat and learn the sequence of steps that minimize the threat caused by Unfamiliar Programs
Mysterious Computer	To detect the threat and learn the sequence of steps that minimize the

Behaviour [Artefact 5]	threat caused by Mysterious Computer Behaviour

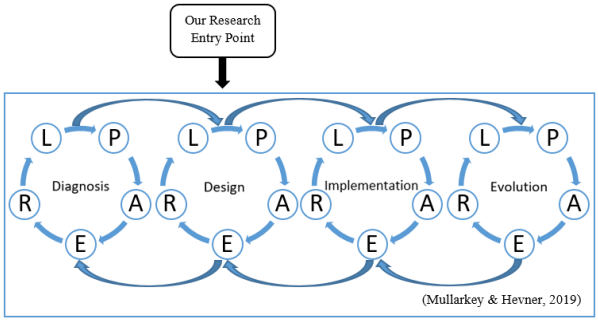


Figure 1. The elaborated ADR approach

3.1. Iteration 1

The first iteration provided us insights into the type of objectives required to design the artefacts. These objectives could be divided into cybersecurity and gaming objectives. We discuss the details of these objectives in section 4.1.

The first iteration focused on the cybersecurity objectives. The cybersecurity objective is to follow the right sequence of procedures to be adopted as part of Incident Detection and Handling in organizations. The NIST's guide to Incident Handling provides ways to handle malware threats which manifest themselves in various ways. We therefore adopted the manifestations of these threats from the NIST's guide into various scenarios (Table 1) and used the techniques provided in it to design the gameplay. In the first iteration we developed three gaming artefacts. The first and the second artefacts were developed to teach malware Incident Detection and Handling techniques. The third artefact was developed to teach password management. Therefore our Problem Formulation (P) activity was to design a game that enables users to learn the concepts of Incident Detection and Handling and the second problem was to design a game that enables users to manage passwords in an effective manner.

3.1.1 Artefact 1 and Artefact 2. The first and second artefacts were designed to train the users to take effective steps when they come across potential cybersecurity threat scenarios. The first artefact addresses a scenario in which an organization might face a spike in network traffic. The second scenario addresses the issue of malicious popups. In the game the player receives information about these issues through notifications via an email or a phone call (Figure 2.d). Based on the information received, the player has to perform the required steps (Figure 2.e) to mitigate the cybersecurity risks.

3.1.2. Artefact 3. The objective of the game is to look for resources to store the password in the most effective way possible. The game environment (Figure 3.a) consists of resources (Figure 3.b) (tables, chairs, shelves, laptops, printers, etc.) that are part of an office. The player views the objective (Figure 3.c) which requires the player to store the given password in the most secure way possible. The player provides his answer in a screen (Figure 3.d) that opens up at the end of the game.

This artefact was improved with a different game design approach. In this enhanced artefact the player could interact with the game resources as shown in Figure 4.d, Figure 4.e and Figure 4.f.

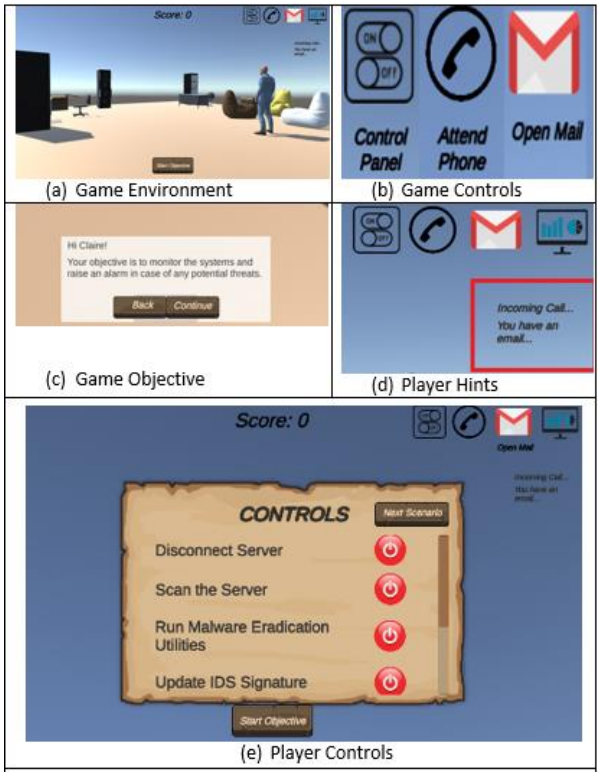


Figure 2. Iteration 1: Artefact 1 and Artefact 2

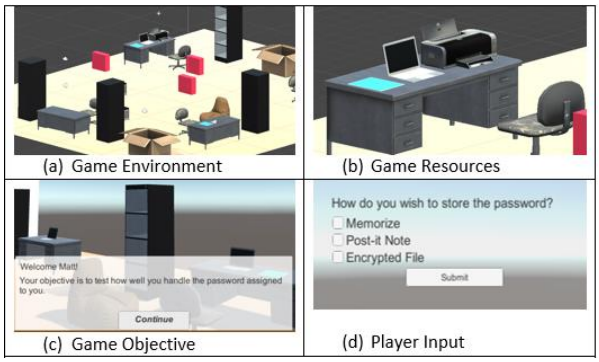


Figure 3. Iteration 1: Artefact 3

The game environment (Figure 4.a), game resources (Figure 4.b) and the game objectives (Figure 4.c) are same as in the previous version of the game. But here the player gets to explore the environment and as the player moves about, the interaction between the player and the game resources is made possible. This interaction takes place in the form of hints (Figures 4.d, 4.e) prompting the player the option of storing the password in a given resource. The player then stores the password (Figure 4.f).

3.1.3. Feedback and Learning. The feedback that our gaming artefacts received from the Embedded Expert and the ADR team is provided below:

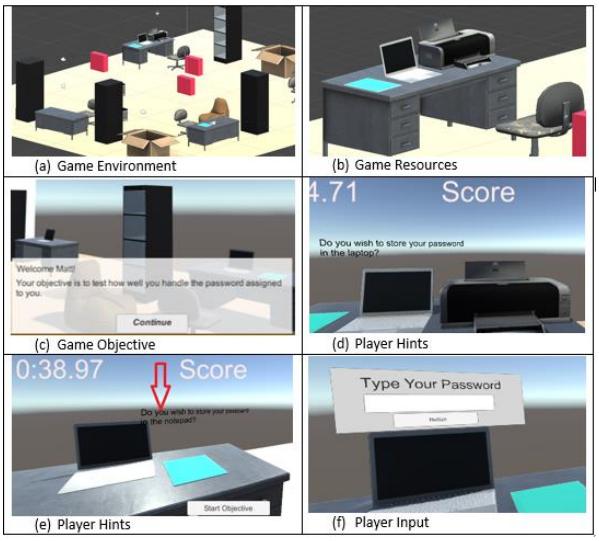


Figure 4. Iteration 1: Enhanced Artefact 3

Table 2. Iteration 1: ADR Team Feedback

Feedback from the Embedded Expert	The objective of the game is to teach the users, concepts in cybersecurity. Therefore the game requires a teaching component.
Feedback from rest of the ADR Team	The feedback from the ADR team was primarily on the aesthetics of the game. We mention few of those below: 1. The game background could be made more realistic. 2. The positioning of the game objective panels could be improved. 3. The gaming controls could be presented as buttons. 4. The game hints could be hidden once they are used.

The focus in the first iteration was to determine the objectives that the game had to meet. Since the artefact focused on developing a game that teaches concepts in cybersecurity, there were two aspects to be looked into. The gaming and the teaching aspect. To address the needs of the gaming aspect we had to develop gaming objectives and to address the needs of the teaching cybersecurity concepts we had to develop teaching or cybersecurity objectives. This leads us to the first guideline:

Guideline 1: A serious game artefact development requires two types of objectives that ought to be met: (a) Gaming objective and; (b) Teaching objective.

3.2. Iteration 2

3.2.1. Kernel Theories. Our artefacts in the second iteration were designed on the basis of concepts in user engagement**.** Educational games require an engaging environment to enable learning. Using games proves to be a promising strategy to increase user engagement [29, 30]. A concept used to understand engagement with an activity is flow [31, 32]. Games attempt to focus player's attention using a main character or avatar, Lin and Wang which enables achieving flow [33]. Our gaming artefact uses an avatar that the players can control. This helps us achieve engagement and the storyline is designed in a way that enables teaching the intended cybersecurity concepts.

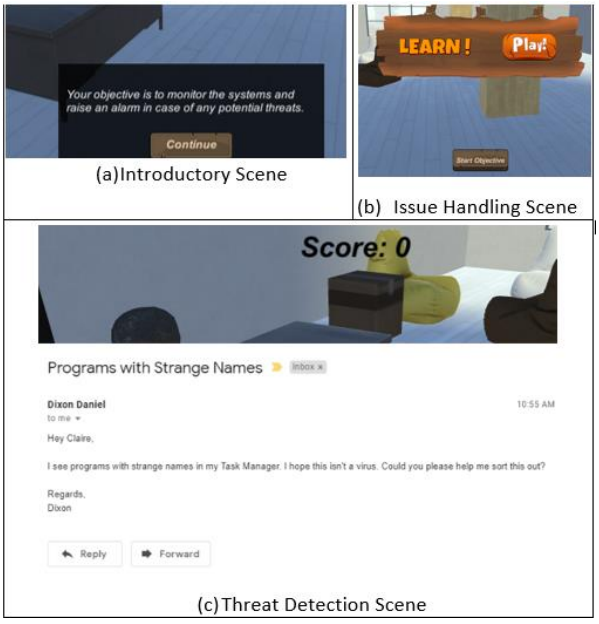
3.2.2. Artefacts. The feedback provided by the embedded experts in iteration 1 was incorporated and brought about design changes in the game. Primary feedback was to introduce a teaching component to the game and this led us to develop the teaching sublevels (Figure 6). The feedback from embedded experts helped us focus on the teaching component in the game. Therefore the Problem Formulation (P) activity was to enhance the gaming artefact by introducing a teaching component to each of the artefact developed in the previous iteration. In this iteration we developed two new artefacts for cybersecurity Incident Detection and Handling. These artefacts modeled the unfamiliar programs (Table 1: Artefact 4) and mysterious computer behavior (Table 1: Artefact 5) scenarios.

The iteration 2 also brings in gaming objectives in addition to the cybersecurity objectives which were developed in iteration 1. The artefacts were now integrated into one holistic game that provided the player a range of scenarios that could be presented at random. The following scenarios now became part of this game: (a) Network Spike; (b) Malicious Popups; (c) Unfamiliar Programs; (d) Mysterious Computer Behavior. The objectives of these scenarios are as

mentioned in the Table 1. The integrated game consists of two levels: (a) Main Level; (b) Sub-levels.

The player starts with the main level followed by the sublevels. The main level introduces the player to the game providing the objectives. The player starts off by familiarizing himself/herself with the environment. When the player enters the main level. The "Start Objective" button gets activated. The player would have to go through the steps mentioned in the button to be able to grasp the game objectives (Figure 5.a). The game objective involves waiting for call or emails from employees facing issues in the organization. Once the player goes through the objective of the game, two new controls get activated.

These are the "Receive Call" and "Open Email" controls. When the player receives any phone call or email, the respective notification pops up which enables the player to attend the call or open the email reporting the issue (Figure 5.b). The reported issue can be analyzed to determine the type of issue at hand and then the player can proceed with the game by choosing to either learn the game or proceed playing the game that simulates the issue at hand (Figure 5.c).



(a)Introductory Scene

(b) Issue Handling Scene

(c) Threat Detection Scene

Figure 5. Iteration 2: Main Level

The sublevels are split into Teaching (Figure 6) and Gaming (Figure 7) levels. The teaching sublevel teaches the player, the sequence of steps required to mitigate different cyber security threat scenarios. It consists of number of controls for the player to choose from. In the case of "Network Spike" scenario (Figure 6.a) the player is provided with the following controls in the game; (a) Firewall Check; (b) Network Scan; (c) Disconnect Server; (d) Scan Affected Server; (e) Update IDS Signatures; (f) Disconnect Network; (g) Run Malware Utilities (h) Scan Network.

The objective of this sublevel in the case of the Network Spike scenario (Figure 6.a) is to teach the player, the sequence of steps required to mitigate cybersecurity threat that manifests itself as a spike in the network traffic. The player learns the sequence by clicking on the controls available. When the player clicks a particular control, the system provides a feedback about the control and the order in which that control needs to be clicked. The sequencing of controls is designed in such a way that the player working on the controls minimizes the impact of the threat detection and containment on the business activities in the organization. This level provides feedback based on the sequence of controls chosen while learning the game. It serves to teach the player the containment procedures.

(a) Incident Detection and Handling Teaching Sublevel

(b) Password Management Teaching Sublevel

Figure 6. Iteration 2: Teaching Sublevel

In the gaming sublevels, the players apply the concepts learnt in the teaching sublevel. The gaming sublevel is an entirely gaming scenario with a plot that involves picking up the right controls in the right sequence within a given time period. This serves to provide the player with an engaging experience of the game.

In the case of the Incident Detection and Handling (Figure 7.a) the objective of the game is to control a character in the game. The player receives hints about the ways to move the character before the game starts. The game environment consists of treasure chests

which have controls within them. The location of these controls are available in a map in the game environment. The player can use this map to trace the locations of the controls. These controls need to be picked up in the right sequence before the allotted time runs out.

In the case of the password management (Fig 7.b) the objective of the player is to pick up the right resources in the game. The game environment spawns obstacles as well as resources such as printers, notepads and laptops which the player could use to store the password. The spawning rate of the obstacles increases with time and this increases the game difficultly. The player earns points by picking up resources and loses health when he crashes against obstacles.

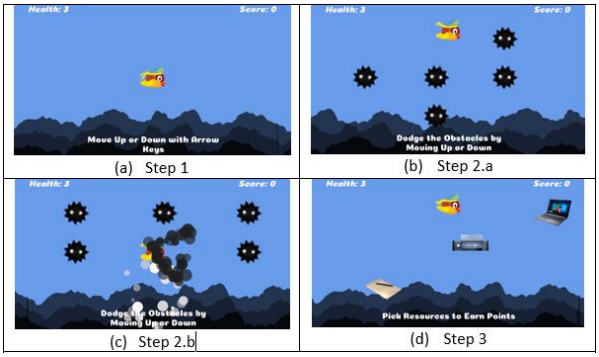
The training phase is the initial part of the game that the player comes across when he starts the game. In this very brief phase the player in taught the techniques to adopt to play the game. The training happens as part of the game. Step 1 (Figure 8.a), teaches the player to move up or down with arrow keys.

(a) Incident Detection and Handling Gaming Sublevel

(b) Password Management Gaming Sublevel

Figure 7. Iteration 2 – Gaming Sublevel

Steps 2.a and 2.b (Figure 8.b-c), shows the player the obstacles that need to be avoided by using the arrow keys because crashing into these obstacles in the game, reduces the player's health. The player doesn't lose any health when he crashes into an obstacle during the training phase. Step 3 (Figure 8.d), teaches the player to pick game resources such as laptops, printers or notepads which the player could choose to store their passwords in. Picking these resources helps the player earn points. The player doesn't score any point just as he doesn't lose any health in the training phase.



(a) Step 1 (b) Step 2.a

(c) Step 2.b (d) Step 3

Figure 8. Iteration 2: Artefact 3 – Training Phase

In the gaming phase (Figure 9) once the player learns the 3 steps the game starts. In the gaming phase, crashing into the obstacles would deduct health whereas picking up resources would increase score. When the player's health reaches zero, the game ends displaying the 'Score' and the 'High Score'. The game can be restarted by hitting 'R' on the keyboard.

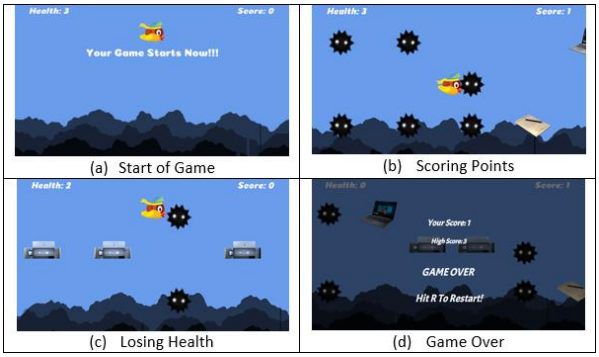
3.2.3. Feedback and Learnings. The feedback that our gaming artefacts received from the Embedded Expert and the ADR team is provided below:

Table 3. Iteration 2: ADR Team Feedback

Feedback from the Embedded Expert	The players are required to perform unproductive moments before they get to carry out the required steps in the game. This uses up time that could actually be used to focus on the objective at hand.
Feedback from rest of the ADR Team	We provide few of the points made by the team: 1. The control icons in the teaching sublevel could be more representative of the actions they perform. 2. The control icons could be made interactive to make it more engaging. 3. The game background could be decluttered by removing unnecessary controls and presenting the controls to the players as and when needed.

The second iteration improved upon the teaching aspects of the artefacts. Therefore we introduced gaming artefacts that provided feedback based on player actions. The feedback systems enabled the

players to learn the sequence of steps. Once learnt, these steps could be executed in a gaming environment.



(a) Start of Game (b) Scoring Points (c) Losing Health (d) Game Over

Figure 9. Iteration 2: Artefact 3 – Gaming Phase

The gaming environment introduced an avatar that the player could assume to play the game. Since the primary objective of the artefact is to teach the concepts in cybersecurity, a trade-off between the gaming and the teaching objectives is needed. Inputs from the embedded experts suggested that the presence of unproductive movements affected the teaching objectives in the game. This leads us to the second and third guidelines:

Guideline 2: A study of the trade-off required between the Gaming and the Teaching objectives enables development of the gaming artefact that meets the needs of the stakeholders.

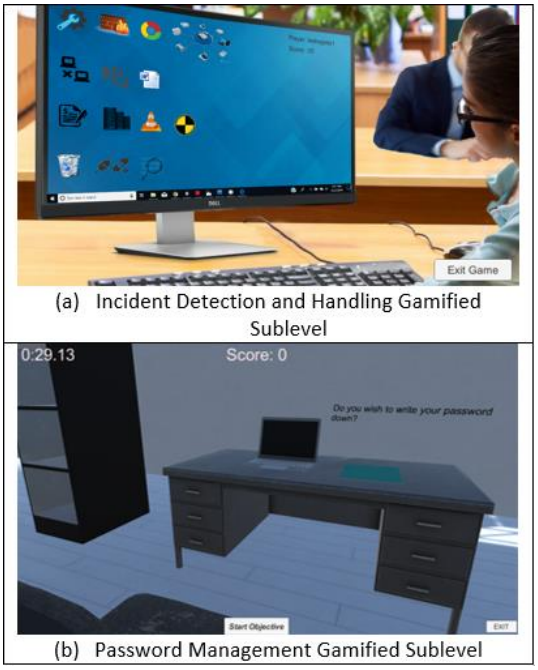
Guideline 3: Review the trade-off achieved in the game design with embedded experts because overemphasis on the gaming aspects hinder the attainment of teaching objectives of the artefact.

3.3. Iteration 3

3.3.1. Kernel Theories. We introduced a gamification based design artefact to the game in iteration 3. This artefact studies the player engagement when the game is designed with a gamification approach. We wanted to test and compare the levels of engagement achieved using game-based learning artefacts and gamification based artefacts. Previous works have shown that games, Moreno and Coller [34, 35] and gamification, Inbar et al. and Li et al. [36, 37] can improve one's learning outcomes, skills and diligence. The popularity of gamification, Hamari, Koivisto and Sarsa is clearly visible and we wanted to test if it is an effective technique in learning [38].

3.3.2. Artefact Description. In order to study the effectiveness of learning using gamification in Cybersecurity Incident Detection and Handling and Password Management, we design gamification based artefacts and integrate these artefacts to the gaming sublevel. The gamified sublevel simulates a real-time office scenario. It scores the player based on the actions taken in the scenarios. The player has controls available on his desktop (Figure 10.a). These controls include those that were available in the learning scenario as well as additional controls which might not be relevant to the issue at hand. The player is awarded points if he chooses the controls in the right sequence and loses points if he chooses the wrong controls. Once the player completes the game he could go back to the main level.

In the case of the password management (Figure 10.b) scenario the player can move around the environment.



(a) Incident Detection and Handling Gamified Sublevel

(b) Password Management Gamified Sublevel

Figure 10. Iteration 3: Gamified Sublevel

This environment consists of office assets such as tables, laptops, printers and notepads. The objective of the player in this environment is to choose the right resource which could be a laptop, printer or a notepad. The player can then click on the chosen resource and store the password. When the player selects a resource he receives feedback and information pertaining to the safety level of the selected resource. The player is awarded points based on the resource chosen to store the password.

In this iteration we worked on enhancing the gaming artefacts developed in the previous iteration. The avatar in the game spent time in unproductive

movements. The time ill spent in those movements could have been used to teach the player additional concepts in Incident Detection and Handling.

Table 4. Activity description of artefacts 1, 2 and 3 in iteration 1

Design Activity	Activity Description
Problem Formulation (P)	1. Design a game that enables users to learn Incident Detection and Handling Techniques. 2. Design a game that enables users to learn the best way to manage passwords.
Artefact Creation (A)	Developed a gaming artefact for the Network Spike [Artefact 1], Malicious Ads [Artefact 2] and Password Management [Artefact 3] scenarios.
Evaluation (E)	1. Evaluation by the ADR team. 2. Feedback: Inclusion of a teaching component to the game.
Reflection (R)	1. Game artefact development requires two objectives that ought to be met: (a) Gaming objective and; (b) Cybersecurity objective. 2. Inclusion of teaching component, gaming objectives were recognized. 3. Improvement in game UI elements was required.
Learning (L)	Infusion of gaming objectives into the artefact is required to make the game engaging.

Table 5. Activity description of artefacts 1, 2, 3, 4 and 5 in iteration 2

Design Activity	Activity Description
Problem Formulation (P)	1. Design a game that teaches users the Incident Detection and Handling techniques. 2. Design a game that teaches users to learn the best way to manage passwords.
Artefact Creation (A)	1. Enhanced the gaming artefact developed for the Network Spike [Artefact 1], Malicious Ads [Artefact 2] and Password Management [Artefact 3] scenarios. 2. Developed new Incident Detection and Handling scenarios: Unfamiliar Programs [Artefact 4], Mysterious Computer Behaviour [Artefact 5]. 3. Inclusion of the Teaching and Gaming sublevels to the existing artefact and integration of these sublevels to a Main Level.
Evaluation (E)	1. Evaluation by the ADR team. 2. Feedback: More emphasis required on the teaching component in the gaming artefact.
Reflection (R)	1. Unproductive player movements reduce the effectiveness of the teaching component in the gaming artefacts. 2. Study gamification based artefacts to understand user engagement and learning outcomes in comparison to game-based artefacts.
Learning (L)	Teaching component needs to blend with the gaming objectives

Table 6. Activity description of artefacts 1, 2, 3, 4 and 5 in iteration 3

Design Activity	Activity Description
Problem Formulation (P)	1. Enhance the existing gaming artefacts by reducing player movements on tasks unrelated to teaching cybersecurity concepts. 2. Design engaging gamified artefacts for Incident Detection and Handling and Password Management scenarios with emphasis on the teaching component.
Artefact Creation (A)	Our gaming artefacts are being enhanced to blend the teaching component with the gaming objectives and to meet the requirements of the formulated problems.

4. Conclusion and Future Directions

We used the elaborate ADR framework to design our gaming artefact. The artefact was developed over two Design Stage iterations. This artefact enables teaching cybersecurity Incident Detection and Handling procedures in an engaging manner.

We plan to equip the existing gaming artefact with modes that would enable dynamic increase of the game difficulty level based on player's performance. The game complexity can be increased in terms of: (a) Time provided to complete a task; (b) Game control availability in the gaming environment; (c) Terrain difficulty in the gaming environment. This complexity can be affected by the player's position in the leaderboard. We also envision increasing the granularity of the tasks to be performed in each level and extend the tasks to other stages of the Incident Response Life Cycle [5].

The study is an ongoing research to develop a gaming artefact that trains users in cybersecurity forensics. It focuses on "containment, eradication and recovery" phase of the NIST incident response life cycle. The artefacts developed in this study are aimed at containment and eradication of a cybersecurity breach. We plan to extend it to recovery and then to other phases of the entire incident response life cycle which would provide a holistic learning experience for the users.

The true success of the game can only be determined when its efficacy is tested with the end users. So we develop an evaluation plan that would assist us in testing the effectiveness of the game among end users when the artefact enters the implementation phase of the e-ADR cycle. This plan is based on Guskey's evaluation plan [39] which uses five critical levels of evaluation to achieve improved student learning outcomes in professional development programs. The critical levels of evaluation enable the assessment of various activities to see if they achieve their purposes. The game that we develop in this paper would also be part of professional development programs in organizations. Such programs impart cybersecurity knowledge to employees. Therefore we adopt this evaluation plan for our gaming artefact with modifications pertaining to our area of study. Our evaluation for the end users is presented in Table 5.

We sincerely acknowledge the financial support by Ministry of Human Resource Development and DRDO (Defence Research and Development Organization), Government of India. This project is carried out as part of IMPRINT (Impacting Research Innovation and Technology) an initiative of Ministry of Human Resource Development, Government of India.

Table 7. End-user evaluation plan

Education Level	What questions are addressed	How will information be gathered	What is measured or assessed	How will information be used
User's Reaction	Did they like it? Was their time well spent? Did the game make sense? Will it be useful?	Questionnaires administered at the end of the game	Initial satisfaction with experience	To improve game mechanics or the design
User's Learning	Did users acquire the intended knowledge and skills?	In-game evaluation in terms of points achieved, time taken to achieve objectives. Post-game Q&A evaluation	New knowledge and skills of participants	To improve the teaching objectives of the game
Users' Use of New Knowledge and Skills	Did users effectively apply new knowledge and skills?	In-game data generated from the user's performance in the gaming environment	Degree and Quality of Implementation	To improve the storyline/gaming objectives/gaming environment
User Learning Outcomes	What was the impact on users? Did it affect user performance or achievement?	Questionnaires, Structured Interviews	Cognitive (Motivation, Engagement, Performance) Psychomotor (Skills)	To focus and improve all aspects of the game. To demonstrate the overall impact of the game.

5. References

[1] K. Subrahmanyam and P. M. Greenfield, "Effect of video game practice on spatial skills in girls and boys," Journal of Applied Developmental Psychology, vol. 15, pp. 13-32, 1994.

[2] S. De Freitas, "Learning in immersive worlds," London: Joint Information Systems Committee, pp. 3-71, 2006.

[3] M. Prensky, "Digital game-based learning," Computers in Entertainment (CIE), vol. 1, no. 1, pp. 21-21, 2003.

[4] D. Liu, X. Li and R. Santhanam, "Digital games and beyond: What happens when players compete?," *MIS Quarterly*, pp. 111-124, 2013.

[5] M. Souppaya and K. Scarfone, "Guide to malware incident prevention and handling for desktops and laptops," in NIST Special Publication 800, 2013.

[6] M. T. Mullarkey and A. R. Hevner, "An elaborated action design research process model," European Journal of Information Systems, vol. 28, no. 1, pp. 6-20, 2019.

[7] L. Kappelman, V. Johnson, R. Torres, C. Maurer and E. McLean, "A study of information systems issues, practices, and leadership in Europe," European Journal of Information Systems, vol. 28, no. 1, pp. 26-42, 2019.

[8] M. Bishop, "Password management," Compcon Spring, 1991.
[9] R. Anderson and T. Moore, "The economics of information security," Science, vol. 314, no. 5799, pp. 610-613, 2006.
[10] L. Tam, M. Glassman and M. Vandenwauver, "The psychology of password management: a tradeoff between security and convenience," Behaviour & Information Technolog, vol. 29, no. 3, pp. 233-244, 2010.
[11] S. M. Furnell, A. Jusoh and D. Katsabas, "The challenges of understanding and using security: A survey of end-users," Computers & Security, vol. 25, no. 1, pp. 27-35, 2006.
[12] M. Carlton and Y. Levy, "Expert assessment of the top platform independent cybersecurity skills for non-IT professionals," in SoutheastCon, 2015.
[13] T. Takahashi and Y. Kadobayashi, "Reference ontology for cybersecurity operational information," The Computer Journal, vol. 58, no. 10, pp. 2297-2312, 2015.
[14] M. Maasberg, M. Ko and N. L. Beebe, "Exploring a systematic approach to malware threat assessment," in 49th Hawaii International Conference on System Sciences (HICSS), 2016.
[15] M. Qian and K. R. Clark, "Game-based Learning and 21st century skills: A review of recent research.," Computers in Human Behavior, vol. 63, pp. 50-58, 2016.
[16] S. de Freitas and M. Levene, "An investigation of the use of simulations and video gaming for supporting," in Proceedings of the IADIS Cognition and Exploratory Learning in the Digital Age Conference, Lisbon, 2004.
[17] J. Hamari and T. Nousiainen, "Why Do Teachers Use Game-Based Learning Technologies," in 48th Annual Hawaii International Conference on System Sciences (HICSS), Hawaii, 2015.
[18] B. D. Cone, C. E. Irvine, M. F. Thompson and T. D. Nguyen, "A video game for cyber security training and awareness," computers & security, vol. 26, no. 1, pp. 63-72, 2007.
[19] P. Chapman, o. Burket and D. Brumley, "PicoCTF: A Game-Based Computer Security Competition for High School Students," 3GSE, 2014.
[20] A. Davis, T. Leek, M. Zhivich, K. Gwinnup and W. Leonard, "The Fun and Future of {CTF}," in 2014 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 14), 2014.
[21] M. Gondree, Z. N. Peterson and T. Denning, "Security through play," IEEE Security & Privacy, vol. 11, no. 3, pp. 64-67, 2013.
[22] M. Thompson and C. Irvine, "Active learning with the CyberCIEGE video game," in CSET, 2011.
[23] T. Denning, A. Lerner, A. Shostack and T. Kohno, "Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education," in roceedings of the 2013 ACM SIGSAC conference on Computer & communications security, 2013.
[24] A. Hevner, S. March, J. Park and S. Ram, "Design science in information systems," MIS Q, vol. 28, pp. 75-105, 2004.
[25] M. Sein, O. Henfridsson, S. Purao, M. Rossi and R. Lindgren, "Action Design Research," Management Information Systems Quarterly, vol. 35, no. 1, pp. 37-56, 2011.
[26] D. P. D. Rajendran and R. P. Sundarraj, "An Elaborated Action Design Research Approach Towards Game-based Learning in Cybersecurity," in DESRIST, Worcester, 2019.
[27] R. Baskerville and A. T. Wood-Harper, "Diversity in information systems action research methods," European Journal of information systems, vol. 7, no. 2, pp. 90-107, 1998.
[28] P. Mell, K. Kent and J. Nusbaum, Guide to malware incident prevention and handling, Gaithersburg: US Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2005.
[29] C. Steinkuehler, S. Kurt and B. Sasha, Games, learning, and society: Learning and meaning in the digital age, Cambridge University Press, 2012.
[30] J. Hamari, D. J. Shernoff, E. Rowe, B. Coller, J. Asbell-Clarke and T. Edwards, "Challenging games help students learn: An empirical study on engagement, flow and immersion in game-based learning," Computers in human behavior, vol. 54, pp. 170-179, 2016.
[31] M. Csikszentmihalyi, Flow: The psychology of optimal experience, New York: Harper and Row, 1990.
[32] A. R. B. Soutter and M. Hitchen, "The relationship between character identification and flow state within video games," Computers in Human Behavior, vol. 55, pp. 1030-1038, 2016.
[33] H. Lin and H. Wang, "Avatar creation in virtual worlds: Behaviors and motivations," Computers in Human Behavior, vol. 34, pp. 213-218, 2014.
[34] J. Moreno, "Digital competition game to improve programming skills," Journal of Educational Technology & Society, vol. 15, no. 3, pp. 288-297, 2012.
[35] B. D. J. S. Coller, "Video game-based education in mechanical engineering: A look at student engagement," International Journal of Engineering Education, vol. 25, no. 2, p. 308, 2009.
[36] O. Inbar, N. Tractinsky, O. Tsimhoni and T. Seder, "Driving the scoreboard: Motivating eco-driving through in-car gaming," in Proceedings of the CHI 2011 Workshop Gamification: Using Game Design Elements in Non-Game Contexts, 2011.
[37] W. Li, T. Grossman and G. Fitzmaurice, "GamiCAD: a gamified tutorial system for first time autocad users," in Proceedings of the 25th annual ACM symposium on User interface software and technology, 2012.
[38] J. Hamari, J. Koivisto and H. Sarsa, "Does Gamification Work?-A Literature Review of Empirical Studies on Gamification," in HICSS, 2014.
[39] T. R. Guskey, "Does it make a difference? Evaluating professional development," Educational leadership, vol. 59, no. 6, p. 45, 2002.