DESIGN OF A GAME FOR CYBERSECURITY AWARENESS

A Paper
Submitted to the Graduate Faculty
of the
North Dakota State University
of Agriculture and Applied Science

By

Jagjot Bhardwaj

In Partial Fulfillment of the Requirements
for the Degree of
MASTER OF SCIENCE

Major Department:
Computer Science

February 2019

Fargo, North Dakota

North Dakota State University
Graduate School

Title

Design of a Game for Cybersecurity Awareness

By

Jagjot Bhardwaj

The Supervisory Committee certifies that this ***disquisition*** complies with North Dakota State University's regulations and meets the accepted standards for the degree of

MASTER OF SCIENCE

SUPERVISORY COMMITTEE:

Dr. Kendall E. Nygard
Chair

Dr. Simone Ludwig

Dr. Ronald Degges

Approved:

March 27, 2019
Date

Dr. Kendall. E. Nygard
Department Chair

ABSTRACT

The primary objective of this paper is to use the Bloom's Revised Taxonomy educational objectives in creating a game called Cyber Air-Strike for learning basic concepts of cybersecurity. Bloom's Revised Taxonomy is used to design the course material as it makes the learning process easy and effective. This taxonomy divides the course material into increasing levels of complexity starting from basic to advanced. A comprehensive literature was reviewed to understand the research domain and identify the gap in previous research.

Cyber Air-Strike aims to target amateur computer users. They will acquire knowledge about the basic concepts of cybersecurity, the most common cyber threats, and their countermeasures. Therefore, the research reported in this paper can help people identify and avoid the cyberattacks addressed in the game.

ACKNOWLEDGEMENTS

I express my sincere thanks to my advisor and graduate committee's chairperson Dr. Kendall. E. Nygard for believing in me and providing me the opportunity to pursue my degree at North Dakota State university. The encouragement and guidance throughout the research project and coursework was of paramount importance. I would like to thank my committee members, Dr. Simone Ludwig and Dr. Ronald Degges for their valuable guidance and helpful comments.

I sincerely express my gratitude to my parents for their unconditional encouragement and support. Lastly, I would like to thank my sister and friends, notably Jashandeep Kaur, Sapna Sharma, Swarda Radkar, Niyati Shah and Vikas Kulkarni for their continuous love and support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

1.1. Overview

The increasing use of information and communication technology (ICT) in all spheres of modern life makes the world a richer, more efficient, and interactive place. The internet has become an integral part of the lives of millions of people around the world. Governments, businesses, and individuals across the globe are dependent upon the capabilities and services that the internet provides. It has offered a great opportunity to connect everything. Some experts predict that by 2020 there will be 200 billion connected things (Cerrudo, 2017). Cars, planes, homes, cities, and even animals are being connected. But, with increased use of and reliance on technology, we are becoming more vulnerable to risks. With all our information available online, it is difficult to protect it from the cyber-attackers. Hence, cybersecurity has become the biggest challenge for companies, states, and individuals.

"Cybersecurity" is a very broad term which can be interpreted in a variety of different ways. It strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against cyber-attacks. Some of the cyber-attacks are malware, spam, phishing, denial of service, ransomware, and social engineering. There main purpose is to have either financial gain or social gain (Ng et al., 2009; Workman et al., 2008; Woon and Tan, 2005).

Over the past years we have seen a growing trend in the number of cyber-attacks (Kapersky, 2013). There severity and impact on organizations is indicated by the following statistics:

- According to Cybersecurity ventures, since 2013 there are 3,809,448 records stolen from breaches every day (Milkovich, 2018)
- Over 75% of health care industry has been infected with malware over last year.

- The U.S. Department of Homeland Security's (DHS) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reported nearly 300 incidents against U.S. industrial control systems in 2015 (Auffret et al., 2017)
- In 2016, the Identity Theft Resource Center saw a 40% increase in the total number of breaches (Cleveland & Cleveland, 2018).
- According to a report by the Center for Strategic and International Studies (CSIS) and McAfee in 2018, cybercrime costs the world almost $600 billion, or 0.8 percent of global GDP (McFee, 2018).
- In relation to the worldwide internet economy, the cost of cybercrime was $4.2 trillion in 2016 (McFee, 2018).
- As more business infrastructure gets connected, cybercrime will cost businesses over $2 trillion total in 2019 (Juniper Research, 2015)
- According to the University of Maryland, there is a hacker attack every 39 seconds (Cukier, 2007).

Most of the cyber-attacks result due to lack of awareness and knowledge. Attackers may use different technique to harm an organization in different ways. Awareness and implementation of policies is the best solution to face these cyber-attacks.

1.2. Background and Problem Statement

Cyberspace is a domain characterized by the use of electronic and electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures (Rouse, 2008). It has given capabilities to share information on a common platform. But this cyberspace is shared by the cybercriminals as well who are often more skilled, more motivated, and have better equipment than their victims. In addition to individual users, small and medium-sized organizations also experience various security related challenges. As

95% of cybersecurity breaches are due to human error (Milkovich, 2018), so it is important for everyone to be familiar with security risks and their preventive measures. They should know how to manage their personal cyber security in their everyday personal and professional lives.

Education can be used as a key resource in tackling cyber threats and in increasing its awareness. It is hard to be aware of security problems when you don't know what these could be. That's why well thought-through security awareness training is so important. Appropriate knowledge about the cybersecurity could reduce the vulnerability and make cyberspace a safer environment.

Cybersecurity can be a difficult thing to teach. Even though there is a lot of information available, still people are unable to understand its basics. Cybersecurity education is lacking in most computer science curricula at both lower and higher education levels. There are just a few dedicated programs that emphasize certifications and some basic essential skills.

The traditional classroom techniques have their own pros and cons. In the era of technology, it seems hard to learn through theoretical books. Although the recent smart-class rooms have provided students a better environment for learning, but it still fails to completely engage the students in the subjects. In order to train students practically, there needs to be a method other than classical course material. Also, the teaching method should have the potential to influence behavior of a wide audience, including average end-users such as amateur internet users.

1.3. Objectives

The problem statement clearly explained the issue of cybersecurity teaching methodology. It is difficult to learn the complex concepts without learning the basics of cybersecurity. There needs to be a teaching method which is better than the traditional classroom techniques and is able to teach the fundamental concepts of cybersecurity.

In this paper, we designed a serious interactive game (Cyber Air-Strike) to teach the fundamental concepts of cybersecurity by using Bloom's Revised Taxonomy. The Cyber Air-Strike was designed and developed in such a way that it satisfies the learning objectives by incorporating the 'Remember' and 'Understand' level of the Bloom's Revised Taxonomy. The main objectives of this game are to cover the following cybersecurity concepts:

- Importance of firewall
- Importance of having an antivirus
- How to avoid phishing emails
- Importance of strong passwords
- How to avoid attacks like adware and spyware

1.4. Structure of Paper

The chapters in the paper are organized as follows:

- Chapter 2 presents the Definition of Games and their Importance in Learning Cybersecurity
- Chapter 3 presents an overview of original Bloom's Taxonomy learning objectives and a detail introduction about the levels in Revised Bloom's Taxonomy.
- Chapter 4 illustrates how the Remember level, the first cognitive level, of the revised Bloom's taxonomy can be incorporated with tutorial learning material.
- Chapter 5 illustrates how the Understand level, the second cognitive level, of the revised Bloom's taxonomy can be incorporated with tutorial learning material.
- Chapter 6 presents a set of conclusions and the limitations related to the work. It also provides with a recommendation for future work.

2. IMPORTANCE OF GAMES IN LEARNING CYBERSECURITY

The existing methods of training include face-to-face exercise and workshops, paper-based posters and newsletters, and online videos and computer-based training (Abawajy, 2014). However, to make learning more effective, an engaging, entertaining and challenging activity is required. Games and simulations have become increasingly accepted as having enormous potential as powerful teaching tools that may result in an "instructional revolution"(Cone et al., 2007).

Before going forward, let's discuss what is game? A game is a voluntary interactive activity, in which one or more players follow rules that constrain their behavior, enacting an artificial conflict that ends in a quantifiable outcome (Zimmerman, 2004). There are eight genres of game defined by Adams, 2010, namely: action games, strategy games, role-playing games, sports games, vehicle simulation games, construction and management simulations, adventure games, and artificial life and puzzle games. Our research will focus on strategy games which are also known as serious games.

Serious Games can be defined as games with a purpose other than pure entertainment (Damien et al., 2011). These games have become an indispensable topic in the educational technology domain. The idea and concept of serious games in education is not new. Already in the sixties, video games were implemented in the United States of America for the military and medical schools, as well as in the general academic community (Bergeron, 2006). Recently a new and growing interest in video games designed for the use in educational settings has emerged (Annetta, 2010).

Teaching using games is based on the notion that not only can a computer game provide education (Raybourn and Waern, 2004), but also games potentially provide a better learning environment, because they motivate the user and keep attention by providing immediate

feedback (Amory and Seagram, 2004; Prensky, 2001). However, the school systems are set up in a way that values traditional teaching methods, and even though some innovative solutions are used, there is still reluctance in using games for teaching (Adams, 2009). Games are seen as play, as entertainment, and not as serious instruments that could be used for teaching.

The goal of gamification is to take content that is typically presented as a lecture or an e-learning course, add game-based elements (story, challenge, feedback, rewards, etc) and create a gamified learning opportunity either in the form of full-fledged educational game, in the form of game elements on top of normal tasks like running for exercise, or in the form of an engaging classroom experience wherein learners participate in a story-based challenge to master the content presented (Kapp, 2012). In games, the cause and effect can be more clearly identified. For example, cyber threats have bad effects such as monetary loss, personal identification theft, and many other types of losses. These are mostly caused by unawareness towards cybersecurity. A game can easily explain this impact as the player will have to make decisions based on his/her knowledge in cybersecurity that would have different effects in terms of success in that game.

In addition to above pros, games can enhance the social skills of students as well as improve their skills in understanding and solving problems (Kirikkaya et al., 2010). Thus, there is no doubt in the potential of games for the purpose of teaching cybersecurity and education using games should be promoted and implemented in the current education system.

3. USING A TAXONOMY FOR LEARNING

Interactive serious games can serve as an effective tool for teaching the importance of cybersecurity to the internet users. It is important to create a practice environment to teach the users on how to play safely in the world full of cyber attackers. The development of such games must use instructional design learning objectives to engage and encourage the users for learning different cyber-attacks and their countermeasures. Thus, the game design should incorporate a learning taxonomy to define the design and structure of that game.

For designing learning objectives of a course, one must think as to what type of work should the students do to demonstrate that they have achieved the desired outcomes of that course objective. Educational taxonomies are a useful tool in developing learning objectives and assessing student attainment. A taxonomy is a classification system that is ordered in some way.

A lot of research has been done on different types of taxonomies. There are many types of learning taxonomies used such as SOLO (Structure of Observed Learning Outcomes), Finks Taxonomy, and Bloom's Taxonomy. The most common and earliest used learning taxonomy is Bloom's Taxonomy proposed in 1956 by a group of educators directed by Benjamin Bloom (Krathwohl, 2002).

3.1. Bloom's Taxonomy

Bloom's Taxonomy was created in 1956 under the leadership of educational psychologist Dr Benjamin Bloom and his associates. It was intended to provide a classification of educational goals, especially to help teachers, administrators, professional specialists, and research workers to discuss curricular and evaluation problems with greater precision (Bloom, 1994).

The main purpose of this learning taxonomy was to promote analyzing and evaluating concepts, processes, and principles, rather than just remembering facts referred to as

rote learning. It is most often used when designing educational, training, and learning processes. Thus, it can be used to design the educational computer games.

The taxonomy is based on three domains of learning. The committee identified three domains of educational activities or learning (Bloom, Engelhart, Furst, Hill, and Krathwohl, 1956)

- **Cognitive:** mental skills (*knowledge*)
- **Affective:** growth in feelings or emotional areas (*attitude or self*)
- **Psychometer:** manual or physical skills *(skills)*

3.1.1. Cognitive Domain

The cognitive domain involves knowledge and the development of intellectual skills (Bloom et al., 1956). The cognitive domain is categorized in six major levels, starting from the simplest to most complex. The complete structure of cognitive domain is shown in the Table 1.

Table 1: The Original Taxonomy

Knowledge

1.10 Knowledge of specifics

1.11 Knowledge of Terminology

1.12 Knowledge of specific facts

1.20 Knowledge of ways and means of dealing with specifics

1.21 Knowledge of conventions

1.22 Knowledge of trends and sequences

1.23 Knowledge of classification and categories

1.24 Knowledge of criteria

1.25 Knowledge of methodology

1.30 Knowledge of universals and abstractions in a field

1.31 Knowledge of principles and generalizations

1.32 Knowledge of theories and structures

2.0 Comprehension

2.1 Translation

2.2 Interpretation

2.3 Extrapolation

3.0 Application

4.0 Analysis

4.1 Analysis of elements

4.2 Analysis of relationships

4.3 Analysis of organizational principles

5.0 Synthesis

5.1 Production of a unique communication

5.2 Production of a plan, or a proposed set of operations

5.3 Derivation of a set of abstract relations

6.0 Evaluation

6.1 Evaluation in terms of internal evidence

6.2 Judgements in terms of external criteria

All the levels except the application were broken into sub-categories. The levels are arranged from simplest to the most complex, and their definition (Anderson et al., 2001) are shown in Table 2.

Table 2: The Original Bloom's Taxonomy

Level	Description
Knowledge	To remember or retrieve material that has be learnt before
Comprehension	To be able to grasp or construct meaning from material
Application	To be able to utilize learnt material, or to apply material in new and concrete settings
Analysis	To be able to classify or distinguish the components of material into its parts whereby its structure of organization to aid the understanding of the material
Synthesis	To be able to put components together for building up a coherent or unique new whole
Evaluation	To be able to judge, check, and even critique the material value for a given objective

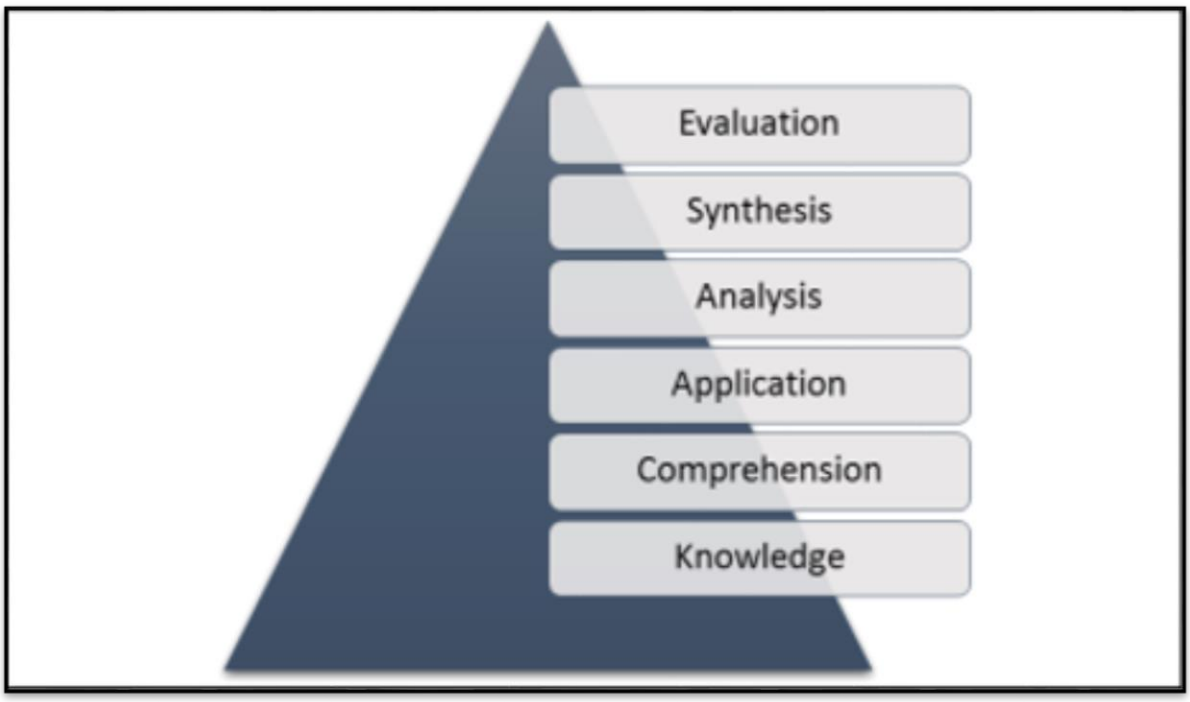

Figure 1: The Original Bloom's Taxonomy

The Bloom's Taxonomy is unidimensional in nature and is presented graphically in Figure 1. Although, the original taxonomy is widely used by teachers, researchers, curriculum designers, and assessment writers, but there was a major need for revision because of the criticism. The taxonomy was designed according to the classroom practice and educational environment based on 1950. The Bloom's Taxonomy was discovered to have several weaknesses (Krathwohl, 2002). A notable weakness is the assumption that cognitive processes are ordered on a single dimension of simple to complex behavior (Furst, 1994). Another reason was to include the recent developments in the educational and psychological literature. The original taxonomy focused mainly on the school curriculum and instruction. To address all these weaknesses, Bloom's Original Taxonomy was revised.

3.2. Revised Bloom's Taxonomy

In 1990 a former student of Bloom's, Lorin Anderson and David R. Krathwohl along with a group of psychologists, revised the Original Bloom's taxonomy and referred it as Revised Bloom's Taxonomy (Krathwohl, 2002). The revised taxonomy includes many changes in terms of assumption, structure, and terminology.

3.2.1. Changes in Terminology

The Bloom's Original Taxonomy underwent a lot of terminological changes when revised. Four major changes in terms of terminology change that occurred are:

- The names of six categories of the cognitive processes were changed from noun to verb form.
- The sub-categories of the six major categories were replaced by verbs. (e.g. interpreting, exemplifying, inferring, etc.)
- The knowledge dimension was considered inappropriate in terms of thinking. The sub-categories of knowledge domain were reframed categorizing knowledge domain in four parts: Factual, conceptual, procedural, and metacognitive knowledge.
- Comprehension was retitled to understanding and synthesis was renamed to creating.

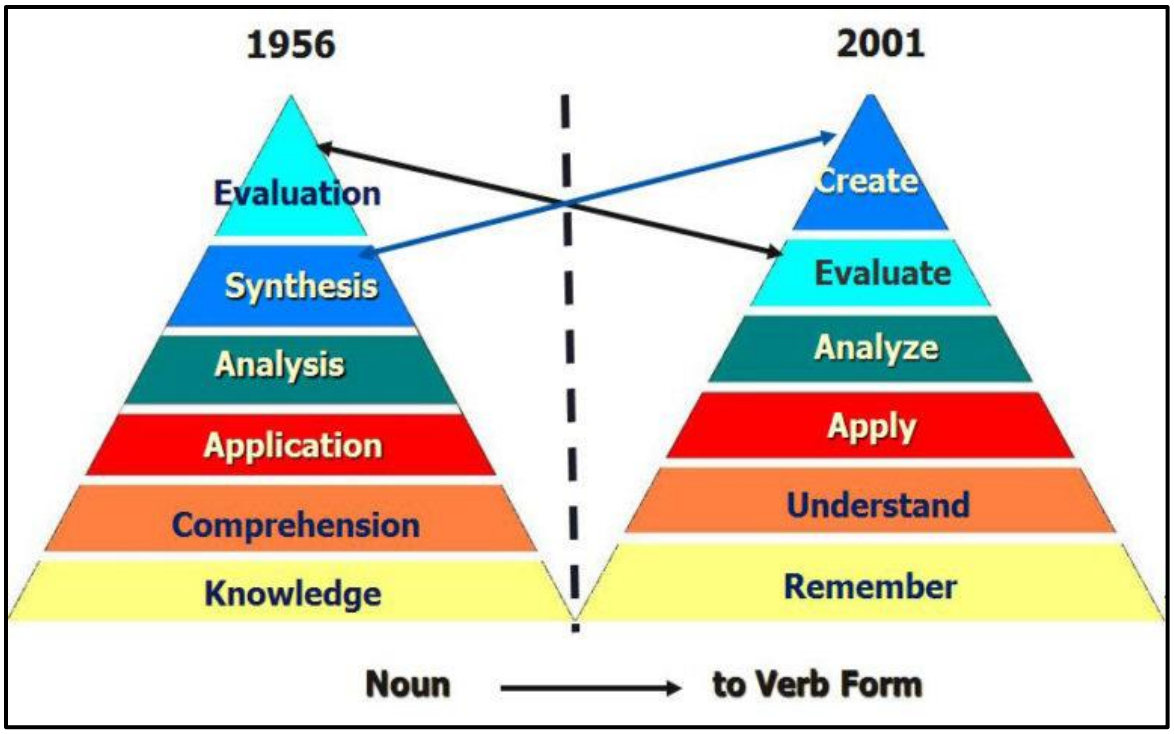

Figure 2: Comparison between Original and Revised Bloom's Taxonomy

3.2.2. Changes in Structure

The most notable change in the revised taxonomy is the change in structure. The original taxonomy was a unidimensional form. In the original taxonomy, the knowledge category embodied both noun and verb aspects (Krathwohl, 2002). The definition of *knowledge* was described in verb aspect and the sub-categories represented the noun aspect. Due to this, the unidimensional framework had an anomaly as the knowledge domain was dual in nature.

The revised taxonomy was turned into a two-dimensional table. This anomaly was eliminated in the revised taxonomy by allowing these two aspects, the noun and verb, to form separate dimensions, the noun providing the basis for the knowledge dimension and the verb forming the basis for the cognitive process dimension (Krathwohl, 2002).

Table 3: Two-Dimensional Structure of Revised Bloom's Taxonomy

Knowledge Dimension	**Cognitive Process Dimension**					
	Remember	*Understand*	*Apply*	*Analyze*	*Evaluate*	*Create*
Factual Knowledge						
Conceptual Knowledge						
Procedural Knowledge						
Meta-Cognitive Knowledge						

As shown in the table above, the knowledge domain is a separate dimension which forms the vertical axis of the table with its four levels and the cognitive process dimension formed the horizontal axis of this table with six levels.

3.2.2.1. The Cognitive Dimension

The cognitive dimension has six levels and are further subdivided into seven sub-categories as shown in the Table below. It depicts all the terminological changes that we mentioned in the above section.

Table 4: Structure of Cognitive Process

Dimension of the Revised Taxonomy
1.0 ***Remember*** – Retrieving relevant knowledge from long-term memory
1.1 Recognizing
1.2 Recalling
2.0 ***Understand***- Determining meaning of instructional message, including oral, written and graphical information
2.1 Interpreting
2.2 Exemplifying
2.3 Classifying
2.4 Summarizing
2.5 Inferring
2.6 Comparing
2.7 Explaining
3.0 ***Apply***- Carrying out or using a procedure in a given situation
3.1 Executing
3.2 Implementing
4.0 ***Analyze***- Breaking material into its constituent parts and detecting how the parts relate to one another and to an overall structure and purpose
4.1 Differentiating
4.2 Organizing
4.3 Attributing
5.0 ***Evaluate***- Making judgements based on criteria and standards.
5.1 Checking
5.2 Critiquing
6.0 ***Create***- Putting elements together to form a novel, coherent whole or make a original product.
6.1 Generating
6.2 Planning
6.3 Producing

3.2.2.2. The Knowledge Dimension

The knowledge dimension was categorized in four major categories which were further sub-divided. The structure is shown in Table 5.

Table 5: Structure of the Knowledge Dimension of the Revised Taxonomy

Structure of the Knowledge Dimension Level	
Categories	**Definition and Subcategories**
Factual Knowledge	The basic elements that learners must know in order to be acquainted with a discipline or solve problems in it. ***Knowledge of terminology.*** ***Knowledge of specific details and elements.***
Conceptual Knowledge	The interrelationships among the basic elements within a larger structure that enable them to function together. ***Knowledge of classification and categories.*** ***Knowledge of principles and generalizations.*** ***Knowledge of theories, models, and structures.***
Procedural Knowledge	The interrelationships among the basic elements within a larger structure that enable them to function together. ***Knowledge of subject specific skill and algorithm.*** ***Knowledge of subject specific techniques and methods.*** ***Knowledge of criteria for determining when to use appropriate procedures.***
Metacognitive Knowledge	Knowledge of cognition in general as well as awareness and knowledge of one's own cognition. ***Strategic knowledge.*** ***Knowledge about cognitive tasks, including appropriate contextual and conditional knowledge.*** ***Self-Knowledge.***

3.2.3. Emphasis Change

Bloom's Taxonomy was used by unexpectedly countless groups. However, bloom designed this taxonomy to address a smaller group of educators. The revised taxonomy addressed that issue by keeping broader audience in mind. Emphasis is placed upon the use of the revised taxonomy as a tool for curriculum development, instructional design, and preparing assessment plans (Forehand, 2010).

4. INCORPORATING THE REMEMBER LEVEL THROUGH GAME

The Bloom's Revised Taxonomy has the 'Remember' level as the first or we can say the lowest level in the cognitive distribution of techniques. This dimension has been subdivided into two categories: ***Recognizing*** and ***Recalling***. 'Recognizing' refers to identifying or locating knowledge in a long-term memory which is consistent with the presented memory and 'Recalling' refers to as retrieving relevant knowledge from a long-term memory.

The learning outcome of this level is that learner should be able to locate knowledge consistent to the present material in long-term memory and retrieve relevant information from long-term memory (Mayer, 2002). The technologies used in order to achieve this level in the course design are: book marking, flash cards, rote learning based on repetition, and reading.

In order to incorporate the 'Remember' level in the work presented in this paper, we tried to cover both the factual and conceptual knowledge in corresponds to the 'Remember' level. Table 6 shows the taxonomy matrix for the 'Remember' level.

Table 6: Taxonomy Table for Remember Level

Knowledge Dimension	**Cognitive Process Dimension**					
	Remember	*Understand*	*Apply*	*Analyze*	*Evaluate*	*Create*
Factual Knowledge	***X***					
Conceptual Knowledge	***X***					
Procedural Knowledge						
Meta-Cognitive Knowledge						

Factual knowledge is defined by the basic elements that the learners must be acquainted with the course. In order to achieve this, the game designed has a starting menu page which has an info icon. The info icon directs to a document which has information about all the icons used in the game. Different icons are used to represent different enemies and allies in the game. So, the information document has all the definitions and icons which provide the learners with the required information to achieve the 'Remember' level in factual knowledge domain. The in the game is designed in a way that requires some knowledge of the icons that the player sees. Every time the player hits the wrong icon, the player will be kicked out of the game which makes the player to grab the basic knowledge of these icons. Learners learn about the icons and use them in the game again and again and they use their memory to remember these icons.

Conceptual knowledge is defined as the interrelationship among the basic elements in the larger structure. The game is designed in order to target this domain. The player will learn about the icons used in the game through the information page. The concepts learned will be checked

as the icons will be introduced in the real world where they would affect the player's ability to play. Through this activity, the player will be able to achieve the conceptual knowledge in the 'Remember' level. The player's ability to succeed in this game depends upon the knowledge of icons used in this game. In order to gain knowledge about these icons, the player will have to read the information about the icons by referring the Info icon and then memorize the information while playing the game. Hence, the game design has the ability to make the player reach the Remember Level of the cognitive domain.

5. INCORPORATING THE UNDERSTAND LEVEL THROUGH GAME

The Bloom's Revised Taxonomy has the 'Understand' level as the second level in the cognitive distribution of techniques. The purpose of this level is to construct meaning from the instructional messages, including oral, written, and graphics. The activities included in this level are interpreting, exemplifying, summarizing, inferring or explaining, etc.

This game is incorporating this level with respect to the 'Factual' and 'Conceptual' level of the knowledge domain according to the two-dimensional Bloom's model which is shown in the following table:

Table 7: Taxonomy Table for Understand Level

Knowledge Dimension	**Cognitive Process Dimension**					
	Remember	*Understand*	*Apply*	*Analyze*	*Evaluate*	*Create*
Factual Knowledge		***X***				
Conceptual Knowledge		***X***				
Procedural Knowledge						
Meta-Cognitive Knowledge						

Understand + Factual means summarizing the features of the game that were told in the 'Remember' level whereas the **Understand + Conceptual** means classifying the nature of characters in the game which is the main purpose of designing this game. The information presented in the info icon is relevant with the game scenarios. The 'Understand' level involves providing the basic and relevant information to the player with the help of graphics, images, text.

The player can easily construct meaning out of that information and apply that to the real-world scenarios. By referring the Info icon, the player can easily make decisions in the game. Hence, the game design can successfully incorporate the ‘Understand’ level.

6. THE GAME DESIGN

This chapter consists of the details about the design of **Cyber Air-Strike** game in detail and the tool used to design this game.

Cyber Air-Strike covers a broad range of cybersecurity concepts focusing mainly on the fundamental ones. The aim of this game is to teach cybersecurity in an interactive manner by incorporating the Bloom's Revised Taxonomy. It targets a wide range of users.

The game plot is based on different types of cyberattacks. The attacks include malware attacks, phishing attacks, password hacking, virus, and unauthorized data. Cyber Air-Strike depicts a scene where the player is controlling a fighter plane which is in a war arena. The cyber attackers or hackers are attacking the player with malicious content. The game menu has an info icon which introduces the player with the different types of attacks as enemies and the countermeasures to these as the allies of the player.

The player controls the plane and his/her main objective is to save the plane from cyberattacks either by using the allies or by simply ignoring them. This is an endless game which means there are no explicit goals or levels defined. The success is measured in the terms of distance travelled by the plane.

6.1. The Game Navigation

Figure 3 below shows the menu editor of Cyber Air-Strike. This diagram represents all the screens in this game and all the possible navigations available.

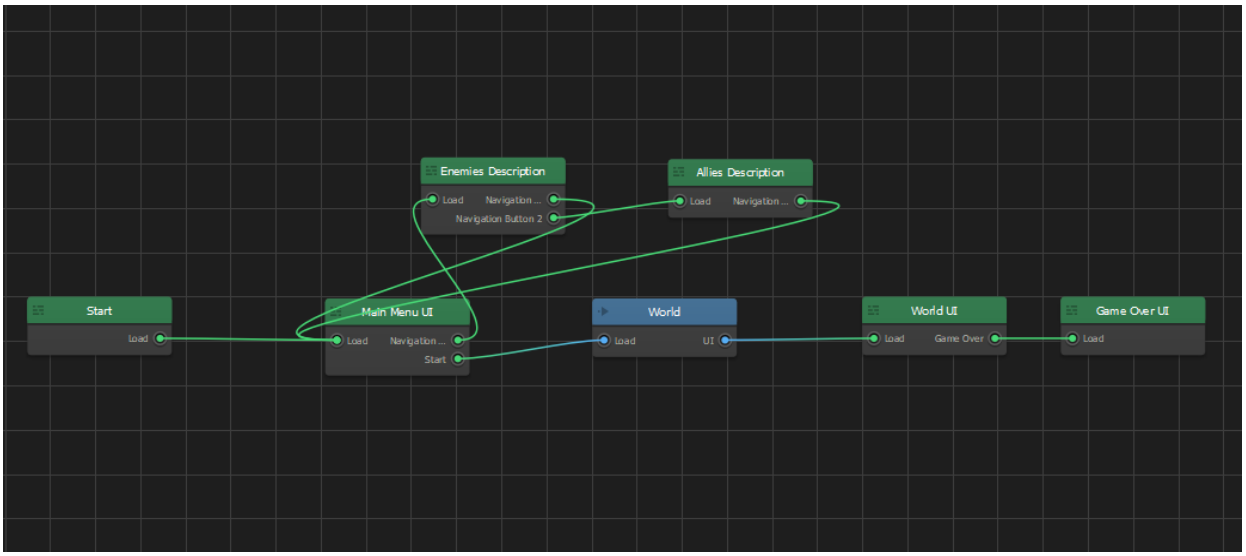

Figure 3: Menu Editor Screen

6.2. The Success Scenarios of Cyber Air-Strike

- Once the game is launched, the system shows player a menu screen. The menu screen provides the player with two options. Either the player can click the "Start" button to begin playing the game or can press the "Info" icon. Figure 4 below represents the menu:

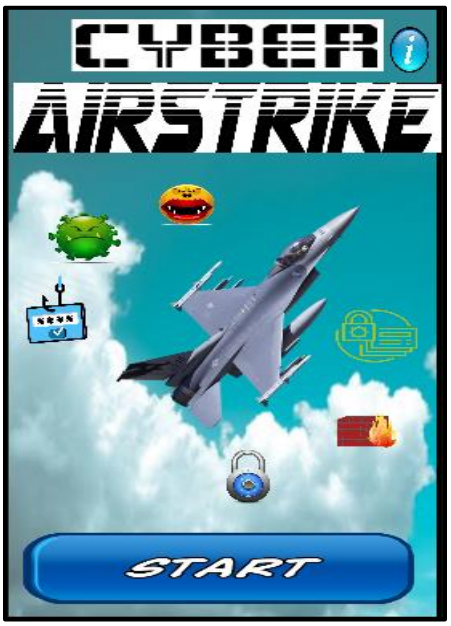

Figure 4. Cyber Air-Strike Menu Screen

- If the player clicks the “Info” icon, the game navigates the player to the info screens which makes the player familiar with the icons being used in the game along with their description. This “Info” screen is further divided into two parts to represent the Cyber-attack icons on one screen and its countermeasures on the other screen as illustrated by Figure 5 and 6 below:

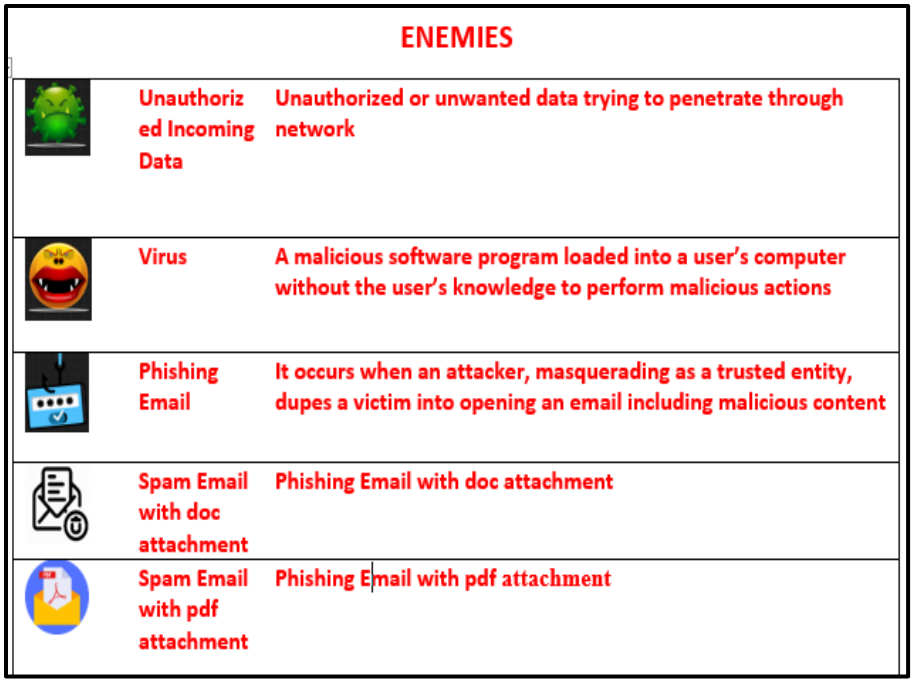

Figure 5: Cyber Air-Strike Info Screen 1

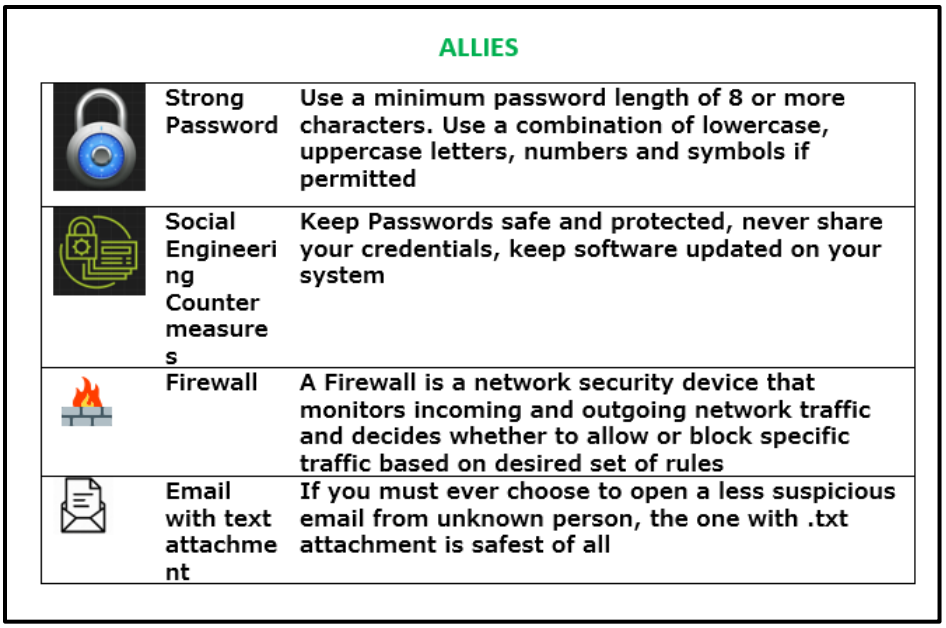

Figure 6: Cyber Air-Strike Info Screen 2

- If "Start" button is pressed, the system navigates the player to the "Start" screen as shown in Figure 7 below:

Figure 7: Cyber Air-Strike Start Screen

- As the player fails, the game ends and the system navigate the player to “Game Over” screen as represented by the Figure 8 below:

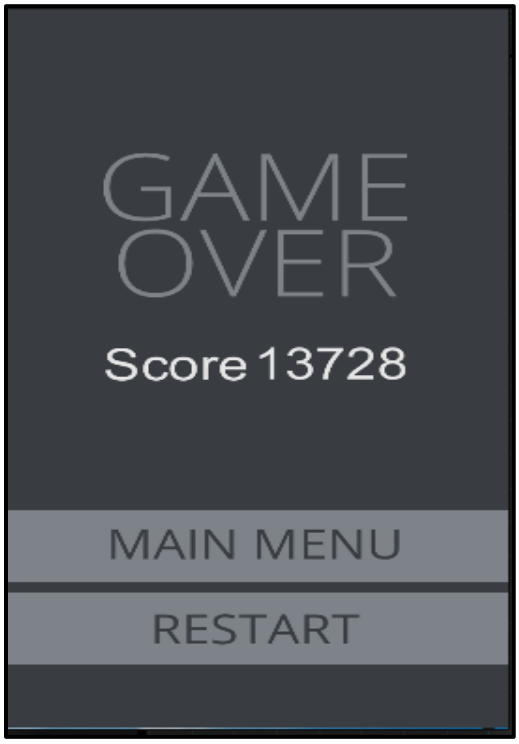

Figure 8: Cyber Air-Strike Game Over Screen

6.3. Alternate Scenarios of Cyber Air-Strike

In this section, some of the alternate scenarios and explanation of few scenes used in the game are discussed. Game is divided and designed in different scenes. The player encounters different scenarios that are randomized in order to make this game more interesting.

- Once the game is “Over”, the user can choose between restarting the game by pressing the “Restart” button or choose to navigate back to the main menu to read the information about the icons again by pressing the “Main Menu” icon.
- The scene represented in the Figure 9 below shows three types of icons. The green icon represents the unauthorized data which an attacker is trying to penetrate in user’s

computer. The player can either hit this enemy by missile or can choose firewall icon to kill the enemy.

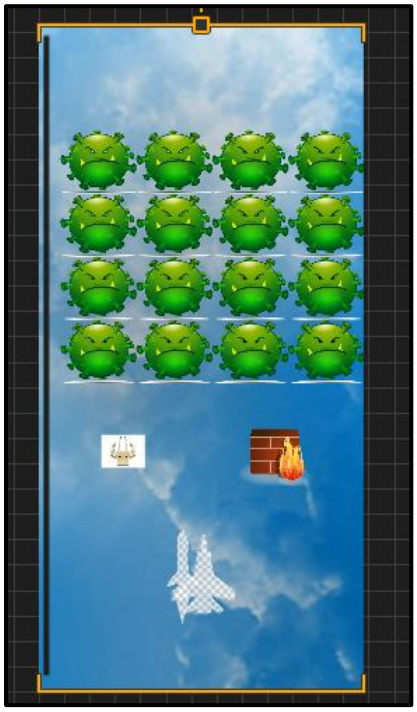

Figure 9: Unauthorized Data and Firewall Icons Screen

- The Figure 10 below illustrates another scene where the player encounters the virus attacks. In this scenario the player has two options. Either he/she can dodge the attack or can use their ally which is antivirus icon. This antivirus will make the player invincible against this virus attack.

Figure 10: Virus Attack Scene

- Shown below in Figure 11 below illustrates another scene where the player is facing a spyware and a phishing email attack. In order to gain success in this scenario, the player has to use the social engineering countermeasures icon which will kill all the enemies represented in this particular scenario.

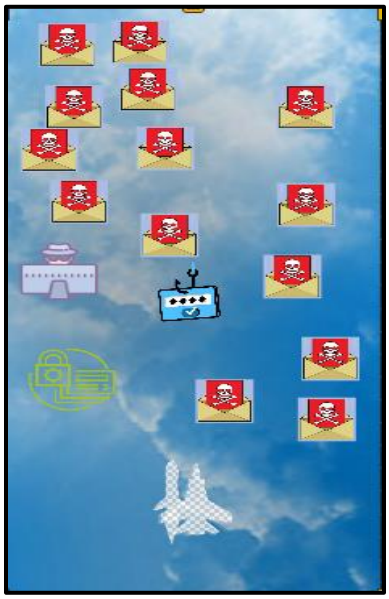

Figure 11: Scene Representing Phishing Attack

- The player encounters a phishing email attack. In this attack, the player received three types of emails with three types of attachments. There is an email with docx attachment, another with pdf attachment and one with txt attachment. If the player chooses the one with txt attachment, it will be a safe option. Choosing the other two options would kill the player.

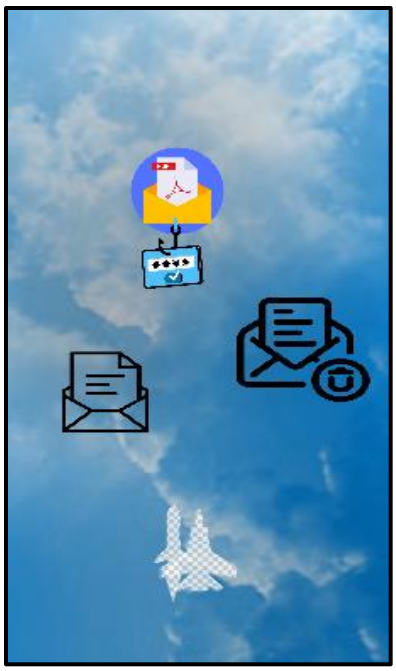

Figure 12: Phishing Email Attachment Attack

6.4. Outcome of the Game

The main aim of this game is to prove itself as a better teaching methodology. The player playing this game recognizes the icons and gets familiar with them by playing the game. The familiarity with icons as to which are attacks and what countermeasures can we use to encounter them makes the player learn about the cybersecurity.

The player understands and encounters the challenges in this game. The more the player is familiar with the cybersecurity concepts, it will be easy to play the game and score more which is the eventual goal of this game. The concepts are best learnt when tested. This game is testing

player's learning capability in each step. Hence, this game as teaching methodology can prove itself as easy and effective. The success in this game is based on the cybersecurity knowledge one has. Hence, the goal of learning and providing feedback to player is achieved.

6.5. Tool Used to Develop the Game

Buildbox was used to design and develop this game. Buildbox is drag-and-drop game building software and focused on game creation without programming, coding or scripting (Mooney, 2014). The core audience for the software are entrepreneurs, designers, and other gaming enthusiast without prior game development or coding knowledge (Valentaten, 2015). Buildbox was founded by Trey Smith in August 2014. It is a cross platform development tool that can be run on both Windows Operating System and OSX (Klosowski, 2015). Since, its public release in January 2015, Buildbox has created more than 150 hit games that have been featured by Apple, broken the top charts of the app store and picked up by major publishers.

The main features of Buildbox are the image drop wheel, asset bar, option bar, collision editor, scene editor, monetization options, and sliders that change the physics within the game (Game Headquarters, 2016)

The deployment of game developed through Buildbox is very easy. It can be easily exported as a gaming app in Windows Store, Android Store, iOS Steam or as a Windows exe.

7. CONCLUSION

Learning by doing is a popular approach used in cybersecurity education. Unawareness about cyber security is a serious issue as we face an increasing number of crimes in this area. To address this issue, we need to familiarize people with the possible cyber-threats and concepts of cybersecurity right from the lower level of education. Numerous efforts have been done to teach this topic, but these traditional methods seem to be failing in reaching out to mass and in making the cybersecurity learning more interesting.

For this paper, our goal was to make the users aware about cybersecurity by using the 'Remember' and 'Understand' levels of the Bloom's Revised Taxonomy. To do so, we developed a game with an aim to teach the malware attacks and their associated preventive measures. We incorporated the 'Remember' level of the cognitive domain of the Bloom's Revised Taxonomy by providing detailed information about the icons used in the game. A player achieves the remember level by memorizing the fundamental concepts of cybersecurity provided in the game. Also, the game is able to incorporate the 'Understand' level by remembering the information and applying that while playing the game. In order to target the amateur users, we made this game very simple. We used games instead of traditional teaching methods as the former are more effective, interesting, engaging, and entertaining in nature.

8. LIMITATIONS AND FUTURE WORK

The game is designed and developed but not tested by the actual users. Evidence is required to evaluate the understanding of concepts by the users. Since, the game is a web-based application, it is restricted to users having internet access. Also, the concepts are taught by game which will not be able to reach out the population which is not interested in gaming.

The game includes 12 icons which target 5 types of cyberattacks and their counter-measures. However, this game can be extended to include more icons to teach more complex concepts of cybersecurity. Also, research can be extended by increasing capabilities of the game by incorporating all the higher order levels of Bloom's Revised Taxonomy.

REFERENCES

Abawajy, J. 2014. User preference of cyber security awareness delivery methods. *Behaviour and Information Technology*, 33, 3, 237-248.

Adams, E. 2009. *Fundamentals of Game Design (2nd ed.)*. Pearson Education, London, U.K.

Amory, A. and Seagram, R. 2004. *Educational game models: conceptualization and evaluation.* South African Journal of Higher Education 17, 2, 206 - 217.

Anderson, L. W., Krathwohl, D. R., Airasian, P. W., Cruikshank, K. A., Mayer, R. E., R.Pintrich, P., and Wittrock, M. C. 2001. *A taxonomy for learning, teaching and assessing. Longman New York*. Addison Wesley Longman, Boston, M.A.

Annetta, L. A. 2010. *The "I's" Have It: A Framework for Serious Educational Game Design.* Review of General Psychology, 14, 2, 105-112.

Auffret, J.P., Snowdon, J. L., Stavrou, A., Katz, J. S., Kelley, D., Rahman, R. S. and Warweg, P. 2017. Cybersecurity Leadership: Competencies, Governance, and Technologies for Industrial Control Systems. *Journal of Interconnection Networks* 17, 1, 1740001. https://doi.org/10.1142/S0219265917400011

Bergeron, B. P. 2006. *Developing Serious Games*. Charles River Media, Boston.

Bloom, B. S., Engelhart, M. D., Furst, E. J., Hill, W. H., and Krathwohl, D. R. 1956. *Taxonomy of Educational Objectives: The Classification of Educational Goals: Handbook I Cognitive Domain*. David McKay Company, Michigan.

Bloom, B. 1994. Reflections on the Development and Use of the Taxonomy. In *Bloom's Taxonomy: A Forty-Year Retrospective*, L. Anderson, and L. A. Sozniak, Eds., The National Society or the Study of Education, Chicago, 1-8.

Cerrudo, C. 2017. Why cybersecurity should be the biggest concern of 2017. Forbes. https://www.forbes.com/sites/forbestechcouncil/2017/01/17/why-cybersecurity-should-be-the-biggest-concern-of-2017/#2f1472475218.

Cone, B. D., Irvine, C. E., Thompson, M. F., and Nguyen, T. D. 2007. *A video game for cyber security training and awareness.* Computers and Security, 26, 1, 63-72.https://doi.org/10.1016/j.cose.2006.10.005

Cleveland, S. and Cleveland, M. 2018. Toward Cybersecurity Leadership Framework. In *Proceedings of the Thirteenth Midwest Association for Information Systems Conference, MWAIS 2018,* Saint Louis, Missouri.

Cukier, M. 2007. Hackers Attack Every 39 Seconds. University of Maryland.

Damien, D., Alvarez, J., Jessel, J.P. 2011. Classifying Serious Games: the G/P/S model. In *Handbook of Research on Improving Learning and Motivation through Educational Games: Multidisciplinary Approaches,* P. Felicia, Ed., Information Science Reference, Hershey PA.

Forehand, M. 2010. Bloom's Taxonomy: Original and revised. In *Emerging Perspectives on Learning, Teaching and Technology,* M. Orey, Ed., University of Georgia, 41-47.

Furst, E. 1994. Bloom’s Taxonomy: Philosophical and Educational Issues. In *Bloom’s Taxonomy: A Forty-Year Retrospective,* L. Anderson, Ed., The National Society for the Study of Education, Chicago, 28-40.

Juniper Research. 2015. Cybercrime will cost businesses over $2 trillion by 2019. https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

Kapersky Lab. 2013. Financial Cyberthreats in 2013. https://securelist.com/financial-cyber-threats-in-2013-part-2-malware/59414/

Kapp, K. 2012. *The Gamification of Learning and Instruction*. Pfeiffer & Company, San Franscisco, CA.

Kirikkaya, E. B., Iseri, S., and Vurkaya, G. 2010. A board game about space and solar system for primary school students. *Turkish Online Journal of Educational Technology*, 1-13.

Klosowski, T. 2015. Lifehacker. https://lifehacker.com/the-best-free-tools-for-making-your-own-video-games-1689905461

Krathwohl, D. R. 2002. A Revision of Bloom's Taxonomy: An Overview. In *Theory into Practice*, D. R. Krathwohl, Ed., Routledge, New York, 212-218.

Mayer, R. E. 2002. Rote Versus Meaningful Learning. In *Theory into Practice*, D. R. Krathwohl, Ed., Routledge, New York, 226-232.

McFee. 2018. The Economic Impact of Cybercrime-No Slowing Down. https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf

Milkovich, D. 2018. Cybint News. 13 Alarming Cyber Security Facts and Stats. https://www.cybintsolutions.com/cyber-security-facts-stats/

Mooney, P. 2014. VentureBeat. https://venturebeat.com/community/2014/08/20/buildbox-the-nearly-3k-drag-and-drop-app-game-making-software-launches-to-big-fanfare/

Ng, B. Y., Kankanhalli, A., and Xu, Y. 2009. Studying users computer security behavior: A health belief perspective. *Decision Support Systems*, 49, 815-825. https://doi.org/10.1016/j.dss.2008.11.010

Prensky, M. 2001. *The Digital Game-Based Learning Revolution*. McGraw-Hill, New York.

Raybourn, E. M. and Waern, A. 2004. Social learning through gaming. In *Extended abstracts of the 2004 conference on Human factors and computing systems - CHI '04*, Vienna, Austria.

Rouse, M. 2008. TechTarget. Cyberspace. https://whatis.techtarget.com/definition/cyberspace

Valentaten, D. 2015. Segment Next. Testing Buildbox- A drag and drop game creation tool. https://segmentnext.com/2015/01/15/testing-buildbox-drag-drop-game-creation-tool/

Woon, I. and Tan, G. 2005. A protection motivation theory approach to home wireless security. *ICIS 2005 Proceedings*. 31. https://aisel.aisnet.org/icis2005/31

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

Zimmerman, E. 2004. Narrative, Interactivity, Play, and Games: Four naughty concepts in need of discipline. In *First Person: New Media as Story, Performance, and Game*, N. Wardrip-Fruin and P. Harrigan, Eds., The MIT Press, Cambridge, MA, 154-164. https://doi.org/10.1002/mar

Game Headquarters. 2016. Buildbox 30 days challenge. https://articles.gamerheadquarters.com/softwarereview1buildbox.html