UNIVERSITY OF THE AEGEAN

SCHOOL OF ENGINEERING

DEPARTMENT OF INFORMATION AND COMMUNICATION SYSTEMS ENGINEERING

Raising Information Security Awareness: the role of Gamification

MASTER THESIS

by

Andreas Kourtis

Supervisor: Associate Professor Dr. Maria Karyda

Thesis Committee Members:

- Professor Dr. Evaggelia Mitrou
- Associate Professor Dr. Spyros Kokolakis
- Associate Professor Dr. Maria Karyda

Samos, February 2020

This page intentionally left blank

Table of Contents

Summary

Information is one of the most valuable assets of today's world, with the organizations, businesses, governments and even individuals to try and safeguard it from exposure. With the fast-paced evolution of Information and Communication Systems, the newly-introduced means of transmitting, storing or even deleting information have become a great benefit for everyone making use of them. Though, with the growth of Information and Communication Technologies, so the threats against them have increased, with breach and exposure incidents to occur in a daily basis and in an extensive scale. Whatever form the information may have or wherever is stored, it must properly secured. To that end, Information Security has become a field that has observed a significant growth over the years, offering specialization on many areas, from networks and databases to even digital forensics. A main target of Information Security specialists is the so called insider threats. By the term insider threat is defined any current or former employee, partner or contractor that has or used to have access to the organization's digital assets, and may intentionally or unintentionally abuse this access (ENISA, 2019: 69). The second category, the "negligent insider" is the type of threat that is the most difficult to mitigate due to human behavior being unpredictable.

Several ways have been introduced to mitigate with the threat of employees or members of the organizations not being aware of their actions causing severe security incidents. The first training programs that were used were containing mandatory lectures, videos and presentations. But all these methods were not effective as several audit reports were showing, because they were lacking an important element, with that to be the people engagement. Generally, people learn better when they "Do" rather than when they "See". For the purposes of engagement, a process, that was firstly used for marketing purposes, was introduced to Information Security Awareness training as well and that is the approach of Gamification.

The derived results of the literature review performed in terms of this study, have tried to provide an insight of the Gamification use as a Security Awareness Training approach. Several research papers included experiments on how gamification could be used as a training approach presenting positive results, with the participants to have adopted a more joyful attitude for the training and a much deeper knowledge of the subject they were trained about. It cannot be ignored though the fact that besides the positive feedback there was also a small amount of participants that was not willing to finish the experiment.

Concluding, information security awareness was and still is an important field of several studies and gamification, with the results of its use so far, has been introduced in the area of training as a very innovative and promising approach.

1. Introduction

In this section, an introduction for the purposes of literature review is provided. First, the problem is defined along with the question related to it and an attempt will be made to be fulfilled during the current literature review and, finally, a structure of the thesis is demonstrated.

1.1. Problem Definition

"Human Factor" is the so called number one cause of a variety of security breaches, data leaks, phishing and cyber-attack incidents that are revealed on several reports. Organizations and public sectors are using Information Technologies extensively, something that makes security one of the most important points of interest. For this reason, organizations set and deploy security measures and policies that specify how the employees or citizens should behave. Though, many of the individuals cannot comply with these measures and policies basically for two reasons, either they are not aware of the risks or they do not understand what a security-correct behavior is (Bada, Sasse and Nurse 2019: 2).

Security seems to be a hard thing to teach or adopt on everyday activities. Even employees in major organizations than are more security aware, present an apathy to take all the appropriate actions to mitigate with security problems that may arise. But who can blame them, since all the security awareness trainings are common for all organizational levels and statuses, providing the same information and skills to everyone irrespective of their role in the organization or even society. Some of these trainings are long videos and many hours of lectures or presentations which lack of motivation for the participants, retention of the offered knowledge and skills and thus a retention in the overall effectiveness of the security awareness training is observed.

A promising approach in the field of security awareness training is the application of gamification. It appears to be a training technique that can provide the desired flexibility and motivation that is required for an effective security-centric behavior adoption. Gamified training methods present a way of training that places the participants under pressure of solving a real-life problem into a virtual environment. Following a qualitive literature review, the main goal of this thesis is to present the importance of Information Security Awareness trainings and determine, through several researches that are conducted by specialists, whether gamification may be applied as the main training method and if it will provide a long-term effect.

1.2. Research Question

Each individual uses computers, hardware and software programs which have vulnerabilities and problems. Empowerment of security awareness is mandatory to mitigate these problems. The gamification approach has the potential to achieve this goal by providing a motivating, flexible and fun

environment which targets to equip participants will all the necessary knowledge to overcome any security issue they may encounter.

The aim of this thesis is, through existing literature and researches, to provide a consolidated insight of the security awareness necessity and how it can be supported through the gamification approach and the serious games that are currently available or are still under development. In order to achieve this, the following research question should be answered:

How can gamification as a training approach be applied on Information Security Awareness and how its outcome is evaluated?

1.3. Thesis Structure

The remainder of this thesis is structured as follows:

- Section 2 provides an analysis of Information Security and its threats, the combination and the differences of Awareness with Training and Education and the need for measurement of the effectiveness of the aforementioned aspects
- Section 3 introduces the uses of games, the importance of rewards through games and how the games involved and eventually led to the birth of the term "Gamification" that is currently a trend in Security Awareness trainings
- Section 4 presents how the need for a more dynamic way of security awareness training introduced gamification to this field and what games are currently developed for that purpose. In addition, in the same section are presented any limitations or concerns that were raised or observed during the gamification of security awareness
- Finally, Section 5 provides an overall summary of what was analyzed during the thesis body and whether the research question was answered

2. Information Security Awareness Background

2.1. Information Security Definition

Information Security nowadays has become the center of every discussion, forum, lecture but the main question is, what is Information and why it must be safeguarded. Information is a valuable asset for every business, organization or even an individual, that like other important assets, must be protected with the most effective way possible.

Information can be stored, transmitted or destructed. There are many ways Information can be stored, from electronic form in data files, material form such as paper even with the form of knowledge or experience of the individuals. Information is transmitted with various means such as couriers, electronic communication through the Internet and last but not least verbal communication. Depending on the needs, Information may become redundant at some point and thus a need for destruction arises (ISO/IEC 27000, 2018: 12).

Whatever form the Information may take and no matter what action will be performed, it always needs the appropriate protection. Every means of storage, irrespectively of whether they have digital or material form must always be protected by taking into consideration all the possible threats that may expose this Information to non-eligible parties. The same applies to the transmission of the Information, as it must be reassured that it will reach only the rightful recipient. Finally, although it might seem less important, destruction is an important step of the lifecycle of the Information as in the wrong hands it can be harmful, even though it may be classified as redundant.

To that end, Information Security has become an important aspect of each organization's everyday activities to ensure that Information will always be secure and available only to eligible parties. Information security's primary focus is known as the CIA triad, which stands for Confidentiality, Integrity and Availability of the data, in an efficient way where it will not "sabotage" an organization's productivity. It typically involves preventing or at least reducing the probability of unauthorized access, use, disruption, deletion, destruction, corruption, modification or inspection, although it may also involve reducing the impacts of incidents (Coss and Samonas, 2014 by Wikipedia, *Information Security*).

Information Security is a broad topic covering all aspects of modern technology, though since the threats are becoming more focused on various sectors, several branches of the vast topic of Information Security have started to become more distinct, with Cisco (*What is Information Security?*, n.d.) defining them as:

- Application Security

Web and mobile applications are increasing with a significant speed, so as the vulnerabilities these applications and the respective Application Programming Interfaces (APIs) are exposed to. These vulnerabilities can be found in user authentication/authorization, in code integrity and configuration as well as to several policies and procedures established

- ❖ Cloud Security

Shared Environments, known as "Cloud", are becoming the trend of the future since several businesses and organization are recognizing the benefits of such technology. Though, building and hosting applications on cloud environments and consuming third-party cloud applications can be extremely risky when it comes to shared resources

- ❖ Cryptography

The need to protect the data has increased, so the need for powerful cryptographic algorithms and digital signatures to verify the authenticity of it. Cryptography and encryption have become important and they are even used to protect classified government information

- ❖ Infrastructure Security

This branch of Security aims for the protection of networks, labs, data centers, servers, desktops and mobile devices

- ❖ Incident Response

While all the above categories were aiming to what can be done to protect the information from malicious actions, this is a function that monitors for and investigates potential abnormal behavior. Each IT department should have prepared in advance an incident response plan for system restore in case of a threat becoming real. In addition, the capability of evidence preservation should be established as part of the upcoming forensics analysis

- ❖ Vulnerability Management

In an attempt to be proactive, vulnerability management is a process that scans an environment for weak points and prioritizes remediation based on the risk assessment performed

But how the "holy" triad of Information Security is achieved; a structured risk management process is essential that will involve:

- Identification of all the information and the assets involved along with the potential threats and vulnerabilities those come with
- Evaluation of the risks
- Fortification of the assets for the potential risks or acceptance of the risk
- Where risk mitigation is required, selection and implementation of the appropriate security control
- Monitoring the activities and applying upgrades if needed

As Blakley, McDermott and Geer (2001: 98) state, Information Security starts with policies. These policies describe 'who can do what' to sensitive information. Once the policy is defined, the next step is to enforce the policy. To that end, organizations apply a mix of processes and technical mechanisms that fall in five categories:

- Protection measures that aim to prevent undesired events from occurring

- Detection measures to alert the organization of an adverse event
- Response measures to deal with the consequences of adverse events and allow the organization to return to its previous state
- Assurance measures to evaluate the effectiveness of the above three measures
- Audit, where all the above are logged based on their effectiveness and evaluation

Many policies can be beyond the borders of an organization or business and become a part of a global standardization which are then driven by a variety of laws and regulations that affect how data is accessed, processed, stored, transferred and destroyed.

At the core of Information Security is the measure of Information Assurance, in order to maintain the Confidentiality, Integrity and Availability of Information, ensuring that no Information is compromised when critical issues occur. This measure does not apply only to digital world, since there are still paper-based procedures in several organizations or businesses, requiring their own set of Information Security practices (Coss and Samonas, 2014 by Wikipedia, *Information Security*).

Like all the measures, they cannot be effective if they are not properly managed. As such, a management system that will use a framework of resources to achieve an organization's objectives is always essential. Management involves activities to direct, control and improve the organization. Activities that are included in the Management could be to act, handle, direct, supervise and control the resources. These management structure can extend from one person up to many individuals. A management system allows an organization to (ISO/IEC 27000, 2018: 13):

- Satisfy the information security requirements of customers and other interested parties
- Improve an organization's plans and activities in order to increase productivity without risk
- Meet the organization's Information Security objectives
- Comply with regulations, legislation and industry mandates
- Manage Information assets in an organized way that facilitates continual improvement to current organizational goals

Nevertheless, all the measures and management procedures will not have a meaning since Information Security is, in a major level, dependent to how security aware the employees or the members of an organization are. Information Security culture is the ideas, the customs and the social behaviors that can affect the organization in both positive and negative ways. The way individuals think and feel about security and the actions they take can have a big impact on Information Security in organizations, as it will be observed in the sections to follow.

2.2. Threats to Information Security

Technology is evolving rapidly, infiltrating to almost every aspect of people's lives, from their working environment to the time they spend for their own. The same rate of evolvement do follow the software risks and attacks. Most people have experienced software attacks of some sort, from viruses, worms, phishing attacks and Trojan Horses to more serious compromises. But Information Security threats are not limited to the aforementioned ones. Some of the most common threats that can affect from an

individual to a large business or organization today, are software attacks and theft of intellectual property as described before, identity theft, theft of equipment or information, sabotage, information extortion and last but not least the forces of nature. Identity theft is described as an attempt to act like someone else in order to obtain a person's personal information or to take advantage of their access to vital information through social engineering. Since that most devices today are mobile, theft of equipment is becoming more prevalent, as such devices can more prone to theft and they are an easy way to immediate access to a variety of personal data. Sabotage was and is an attack that targets assets of an organization or even worse the confidence on the part of the customers. Information extortion on the other side, consists of theft of organization's property or information as an attempt to receive payment exchange in order to return the information back to its rightful owner.

Malicious hackers or crackers are those who break into a system without authorization or exceed the level of authorization granted to them. Although this category and the problems it causes get the largest amount of press coverage and movies, it only counts for a small percentage of the total picture. On the other side, dishonest or not security aware employees can cause a great deal of damage to an organization or even to individuals.

Several ways can be followed to protect someone's property and privacy, but the most effective and crucial precaution is to conduct periodical user awareness, especially if we are referring to large organizations with numerous employees. The number one threat to any organization are users or anyone that is granted access to the organization's property and they are also known as insider threats. From governments to military and private businesses own a great deal of confidential information about their employees, customers, products, researches and financial statuses. If such information fall into the wrong hands, such as a competitor, a hacker or a rival company the consequences will be devastating for the financial status and reputation of the organization. The difference between and organization and an individual though is the impact a security breach may have; from a business perspective, information security must be balanced between risk and cost. From the individual perspective, information security has a significant effect on privacy which is viewed differently per person (Wikipedia, *Information Security*). As Michael Whitman (2004: 50) stated in Figure 1, fifteen (15) years ago employees were one of the most serious threat to Information Security, holding the 2nd and 3rd place:

Threats	Ranking
Natural disasters	1
Accidental entry bad data by employees	2
Accidental destruction data by employees	3
Weak/ineffective controls	4
Entry of computer viruses	5
Access to system by hackers	6
Inadequate control over media	7
Unauthorized access by employees	8
Poor control of I/O	9
Intentional destruction data by employees	10
Intentional entry bad data by employee	11
Access to system by competitor	12
Other threats	13

Figure 1: Threats Ranking (Adopted from Michael Whitman 2004: 50)

Although technology has evolved and new training techniques were introduced, according to ENISA Threat Landscape Reports of 2015 and 2018 (ENISA, 2016: 7 & ENISA 2019: 9), insider threats are still in the top 10 of the Threat Ranking, as depicted in Figures 2 and 3 below:

Top Threats 2014	Assessed Trends 2014	Top Threats 2015	Assessed Trends 2015	Change in ranking
1. Malicious code: Worms/Trojans	↑	1. Malware	↑	→
2. Web-based attacks	↑	2. Web based attacks	↑	→
3. Web application /Injection attacks	↑	3. Web application attacks	↑	→
4. Botnets	↓	4. Botnets	↓	→
5. Denial of service	↑	5. Denial of service	↑	→
6. Spam	↓	6. Physical damage/theft/loss	⊃	↑
7. Phishing	↑	7. Insider threat (malicious, accidental)	↑	↑
8. Exploit kits	↓	8. Phishing	⊃	↓
9. Data breaches	↑	9. Spam	↓	↓
10. Physical damage/theft /loss	↑	10. Exploit kits	↑	↓
11. Insider threat	⊃	11. Data breaches	⊃	↓
12. Information leakage	↑	12. Identity theft	⊃	↑
13. Identity theft/fraud	↑	13. Information leakage	↑	↓
14. Cyber espionage	↑	14. Ransomware	↑	↑
15. Ransomware/ Rogueware/Scareware	↓	15. Cyber espionage	↑	↓

Legend: Trends: ↓ Declining, ⊃ Stable, ↑ Increasing
Ranking: ↑Going up, → Same, ↓ Going down

Figure 2: ENISA Threats Ranking (Adopted from ENISA 2016: 7)

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	⊃	1. Malware	⊃	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	⊃	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	⊃	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	⊃	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	⊃	10. Physical manipulation/ damage/ theft/loss	⊃	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Legend: Trends: ↓ Declining, ⊃ Stable, ↑ Increasing
Ranking: ↑Going up, → Same, ↓ Going down

Figure 3: ENISA Threats Ranking (Adopted from ENISA 2019: 9)

But the main question is what can lead users to errors and negligence. Some of the underlying reasons behind user errors are the lack of experience in utilizing security tools, the complexity of the security tools and job stress due to time pressure and workload. On the other hand, although several reasons can justify this negligence, another important factor would be considered the lack of awareness and motivation for the use of the aforementioned tools and the adoption of security culture.

2.3. Information Security Awareness

Many individuals think Information Security in terms of technical controls, not realizing that they as individuals are targets and their behavior can increase risks or on the other hand provide countermeasures to risks and threats. But Information Security, especially for large organizations, is not a matter of an individual rather of everyone. As threats have matured and information has increased in value, attackers have increased their capabilities, developed more attack methods and targeted and successfully exploited individual's human behavior to breach into corporate networks and infrastructure. Targeted individuals who are unaware of information and threats may unknowingly ignore traditional security controls and processes and enable a breach in the organization. In response, Information Security Awareness is evolving. The goal of it is to make everyone aware that they are susceptible to the opportunities and challenges in today's threat landscape, change human behavior and create or enhance a secure organizational culture.

To that end comes Information Security Awareness which is one of several key principles of Information Security. Information Security Awareness can be defined as the need to equip the members of an organization with the required consciousness, knowledge and attitude to respond effectively to potential risks and threats which target human behavior. It seeks to understand and enhance human risk behaviors, beliefs and perceptions about Information and Information Security while also to understand and enhance organizational culture as a countermeasure to rapidly evolving threats (Wikipedia, *Information security awareness*). Being security aware means, that you have the ability to understand the necessity to support the assets of an organization from, deliberately or not, steal, destroy or misuse the data stored in the organizations' systems. An alternative definition of Awareness is provided by NIST Special Publication 800-50 stating that '*Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly'.* NIST also provides a differentiation between training and awareness as *'in awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance…The most significant difference between training and awareness is that training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus an individual's attention on an issue or set of issues*' (Mark Wilson and Joan Hash, 2003: 8).

According to OECD (2002:10 & 2015: 9 - 11) and also referenced by ENISA, the participants to an Information Security culture should follow the below nine principles:

- Awareness

Participants should be aware of the need for security of information systems and networks and what they can do to enhance security. They should understand that security failures may significantly harm systems and networks under their control and also be aware of the potential harm to others arising from interconnectivity and interdependency. Participants should be aware of the good practices they can implement or follow to enhance security

- Responsibility

All participants are responsible for the security of information systems and networks. They should be accountable in a manner appropriate to their individual roles. Participants should review the policies and practices and assess whether these are appropriate to their environment

- Response

Recognizing the interconnectivity of information systems and networks and the potential for rapid and widespread damage, participants should act in a timely and co-operative manner to address security incidents

- Ethics

Participants should respect the legitimate interests of others. Given the pervasiveness of information systems and networks in our societies, participants need to recognize that their action or inaction may harm others. Ethical conduct is therefore crucial, and participants should strive to adopt best practices and to promote conduct that recognizes security needs and respects the legitimate interests of others

- Democracy

The security of information systems and networks should be compatible with essential values of a democratic society. Security should be implemented in a manner consistent with the values recognized be democratic including freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency

- Co-operation

All stakeholders should co-operate, including across borders. Since technology and organizations' activities have gone global so the need for co-operation on digital security risk management did. It should take place within governments, public and private organizations and individuals and also at regional and international levels

- Risk Assessment

Participants should conduct risk assessments. Risk assessment identifies threats and vulnerabilities and should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications. Because of the growing interconnectivity of information systems, risk assessment should include consideration of the potential harm that may originate from others or be caused to others

- Security Design & Implementation

Participants should incorporate security as an essential element of information systems and networks. Systems, networks and policies need to be properly designed, implemented and coordinated to optimize security

- Security management

Participants should adopt a comprehensive approach to security management. Security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations

- Reassessment & Innovation

Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures. New and changing threats and vulnerabilities are continuously discovered. Participants should continually review, reassess and modify all aspects of security to deal with these evolving risks

Although the above principles may not seem to target the non-technical users, this can be explained as Security Awareness should be focused on the organization's entire user population. Management should set the example for proper IT security behavior within the organization. Successful Information Security Awareness culture should begin with an effort that can be deployed and implemented in various ways and is aimed at all levels of the organization including senior and executive managers. Paulsen and Coulson (by Roer and Petric, 2017: 32) also define Information Security Awareness as a tool that will lead all the members of an organization to adopt a security culture by actively practicing good security habits and making security-minded decisions.

Roer and Petric (2017: 33 - 34) identify seven core dimensions of Information Security culture that can be adopted through Awareness in organizations:

- Attitudes - Employees' feelings and thoughts about taking care of sensitive information
- Responsibilities - Employees' understanding of the roles and responsibilities they have as a critical factor in sustaining or endangering the security of information, and thereby the organization
- Communication – Awareness of communication channels for incident reporting and security issues support
- Compliance – Awareness and adherence to organizational security policies and the ability to recall the substance of such policies
- Knowledge – Employees' awareness and knowledge regarding policies, practices and activities related to Information Security
- Norms – Perception of security related practices from employees and their peers and the influence they may have to each other
- Behaviors – Deliberate of unintentional actions employees may take and the direct or indirect impact those may have on Information Security

As already mentioned, Information Security Awareness is one of the key principles of Information Security, though a program focusing on Awareness aims to direct attention to Information Security material with the purpose to ensure that every employee or individual will understand his/her role and responsibility in protecting the organization's information or his/her own sensitive information. Sometimes, though it is essential not only to be aware of the risks and threats but also how to use the appropriate tools to fortify the systems and yourself from them. And here is where Information Security Training and Education are coming to the foreground to enhance the effectiveness of Awareness.

2.4. Information Security Training

The first step to a more secure Information Ecosystem is to direct the attention of the employees of an organization or the individuals in general, to Information material targeting that each one will understand his/her role towards the protection of the organization's information or assets. If the personnel does not understand how to maintain confidentiality of information, or how to secure it appropriately, not only there is the risk the most valuable business assets mishandled, inappropriately used, or obtained by unauthorized persons, but there is also the risk being in non-compliance of a growing number of laws and regulations that require certain types of information security awareness and training activities. Employees and individuals in general, can only be held accountable if they have been equipped with the necessary Information Security Training skills. However, the focus of such a training should be based on employees' roles and responsibilities and acquire the appropriate information security skills and information security knowledge based on those roles and responsibilities by using practical instructional methods such as seminars and workshops (Amankwa, Loock and Kritzinger, 2014: 249 - 250).

Training is defined in NIST Special Publication 800-16 and referenced also in 800-50 as follows: '*Training strives to produce relevant and needed security skills and competencies by practitioners of functional specialties other than IT security*'. While awareness seeks to focus an individual's attention on an issue or set of issues, training seeks to teach skills, which allow a person to perform a specific function. Although a formal degree is not necessary through that training, the whole process should be built upon the awareness foundation and security basics and sometimes, if necessary, to contain much of the same material of courses found in colleges or universities.

According to Herold (2005: 59), many training attendees have declared that the most common reasons employees tend to not comply with security requirements are:

1. Pressure to be productive since the impression of meeting the deadlines seems more critical to their job success and job preservation than complying with security requirements that may negatively impact their productivity.
2. Having to obey to superiors who may tell them to do something against security requirements, e.g. to share their password with a colleague for faster results

One of the most important goals of an Information Security Training program should be to cultivate in personnel's minds that information security is not an obstacle to their everyday tasks rather an integrated aspect with job performance and appraisal process. In other words, except from providing to employees the required knowledge to safeguard Information, a motivation should be provided that will make them

to include Information Security to their everyday tasks without feeling pressed. As Rebecca Herold (2005: 63 - 64) suggests, there are at least five ways in which personnel can be motivated to participate in Information Security training activities as well as to comply with policies and procedures:

1. Include security as specific objectives in job descriptions. Job descriptions should include specific security assignments to avoid endangerment of assets, to adhere to policy and to protect and make employees accountable for the organization's information assets
2. Periodically personnel to be required to sign security agreement that supports the organization's policies and standards. This way, personnel will be required to review the policies in an annual basis
3. Security to be established as specific objectives within the scheduled periodic performance appraisals. Annual job appraisals should include specific evaluations and discussions of the employee's support and practice of security
4. The review of security compliance of managers should also be allowed by executive management. It is vital that all levels of personnel are aware that everyone within their organization, no matter at what level, is responsible and accountable for following security requirements
5. Security program rewards and penalties to be established based on the principles inherited by the training programs. Rewards should be established to motivate employees who follow the principles that were communicated to them through the training programs

Information Security training strives to ensure that employees or individuals handling Information will be fully capable to protect it against most of the risks possible. One level above, targeting more security-oriented people, comes Information Security Education to produce specialists on the field.

2.5. Information Security Education

In contrast with Information Security Awareness and Information Security Training, Education is targeting people that are about to become specialists on the field and not just aware of the potential risks. It is more in-depth and is targeted by professionals and those whose jobs require expertise in security.

Education is defined in NIST Special Publication 800-16 and referenced also in 800-50 as follows: '*The Education's level integrates all of security skills and competencies of the various functional specialties into a common body of knowledge, adds a multidisciplinary study of concepts, issues and principles (technological and social), and strives to produce IT security specialists and professionals capable of vision and pro-active response*'. An example of education is a degree program at a college or university. Some people take courses to develop or enhance their skills in a particular discipline. This is training as opposed to education. Many colleges and universities offer certificate programs, wherein a student may take two, six, or eight classes, for example, in a related discipline, and is awarded a certificate upon completion. Often, these certificate programs are conducted as a joint effort between schools and software or hardware vendors. These programs are more characteristic of training than education. Those responsible for security training need to assess both types of programs and decide which one better addresses identified needs.

Cooper et al (2009: 110) define Information Security Education as a set of technical and managerial controls designed to ensure confidentiality, possession of control, integrity, authenticity, availability and utility of information and information systems. Finally, Amankwa, Loock and Kritzinger (2014: 249) state that a working definition of Information Security Education should include focus, purpose and method, thus they define Information Security Education as an endeavor to provide insight into and an understanding of Information Security documents in order to ensure that every employee is equipped with the necessary information security skills and information security knowledge to protect organizational information by using academic instructional methods.

For all of the Information Security Awareness, Training and Education programs there are some success indicators that can ensure or at least assist on such programs to thrive. According to Wilson and Hash (NIST) (2003: 39), '*CIOs, program officials and IT security program managers should be the primary advocates for continuous improvement and for supporting an agency's security awareness, training and education program. It is critical that everyone be capable and willing to carry out their assigned security roles in the organization. In security, the phrase, Only as strong as the weakest link, is true. Securing an organization's information and infrastructure is a team effort*'. Some key indicators are also mentioned in the same publication, as following:

- Security strategy to be supported from the respective sufficient funding
- The appropriate employees should be placed to the correct position in order to secure the efficient implementation of the strategy
- There should be a sufficient distribution of awareness items
- Seniors should alert employees with messages regarding security
- Metrics should be used concerning number of incidents related to security awareness etc.
- Equality upon security controls between employees and upper management
- Level of attendance at mandatory security briefings
- Recognition of security contributions with awards
- Motivation demonstrated by those playing key roles in managing/coordinating the security program

2.6. The Need for Measurement

One of the greatest challenges associated with Security Awareness, Training or Education is to quantify the success as this is related to the learning that has taken place. Such formal evaluation and feedback mechanisms are crucial to any organization as it can determine the success of the programs of awareness, training and education or contribute to the continuous improvement by providing a sense of how the existing program is working. Teams that are responsible to operate such programs confront two major challenges, What to measure and How to measure. In their effort to explain how important the measurement of the effectiveness of Information Security Awareness is, Kruger and Kearney (2006: 295) state that '*Having implemented an information security awareness program does not automatically guarantee that all employees understand their role in ensuring the security and safeguarding of information and information assets. In order for security awareness programs to add value to an*

organisation and at the same time make a contribution to the field of information security it is necessary to follow a structured approach to study and measure its effect'. Though, no such program can thrive without management's support and an appropriate program funding, marketing and management.

Cooper et al (2009: 122) state that the assessment of Information Awareness programs is usually conducted through a combination of processes. Some of these take place before the start of the program such as validation and some after the program becomes operational such as accreditation. In addition, some of these processes are internal such as periodic program review and some are external such as the US accreditation of academic programs containing Information Awareness content. Internal subject review can be consisted or include student/employee feedback, employer input as well as external input from third parties associated with the organization. On the other side, accreditation refers to higher education programs providing a degree of knowledge and most of the times is not referring to an organization's target for the Information Security Awareness program.

Another categorization for the evaluation of an Information Security Awareness program is provided by Rantos et al. (2012: 4) where an evaluation can be based on qualitative or quantitative techniques or a combination of the two.

- Qualitative techniques are targeting employees' behavior and attitude regarding awareness and whether they truly exercise security awareness. The results of such techniques do not contain any numeric metrics and sometimes they may lead to speculations and conjectures, their significance should not be underestimated. Commonly deployed qualitative techniques include users' feedback, independent observations and silent monitoring of employees' reactions during awareness cases.
- Quantitative techniques attempt to present the evaluation results in a more solid and numeric-centric way providing benchmarks. Methods that can be deployed are metrics, also known as key performance indications (KPI), which can provide a better view of the effectiveness of an Information Security Awareness program. According to ENISA (2010: 91), '*organizations appear to find it very difficult to put effective quantitative metrics in place. However, there is little consensus on the most effective measures. Ideally, organizations would like to be able to measure actual changes in staff behavior resulting from the awareness activities*'.

Rantos et al. (2012: 7 – 14) and Wilson and Hash (NIST) (2003: 36 – 38) propose some ways to measure the effectiveness of Information Security Awareness discreetly and without overwhelming the user in order to avoid negative implications. Some of these methods are presented below (also schematically by NIST):

1. Surveys

Such questionnaire-based surveys should be conducted on a regular basis (usually annual) including a number of topics, being different per category of employees, having unambiguous and unbiased questions, asking for employees' feedback and asking for suggestions and recommendations where major weaknesses may be revealed

2. Awareness/Security Days

Security days offer a unique opportunity for the awareness team to directly communicate with the employees and get their feedback. Though, such initiatives should not be compulsory rather target to have a clearer view by measuring the level of attendance

3. Independent Observations

Independent observations on the security behavior of employees should be carried out silently by awareness team members or representatives that have been assigned to this task. There is no need to alert people and, for example, clean desk policy, which is one of the targets of independent observations, can be performed outside working hours so that it will go unnoticed

4. Audit Department Reports

The metrics that will be provided by the Audit Department concerning security awareness related incidents can be used to measure the effectiveness of such a program. In addition, such an observation on the metrics can also provide valuable information regarding areas on which awareness team should focus or to bring issues to the surface that were not dealt and need to be included in the program

5. Risk Department Reports

The input from Risk Department can be used to identify whether risks that were confronted on the previous awareness session were eliminated during the current report

6. Security Incidents

Security incidents can be a valid point of reference for the program evaluation, where their volume and nature can indicate whether employees exercise security-aware working behavior and on the other side if they remain vigilant during their everyday work

7. E-learning

Statistics can provide useful information regarding the number of employees visiting, registering and completing the e-learning program

8. Selective Interviews

Such a process is more personalized than a group and may encourage participants to be more forthcoming in their critique of the program

9. Security Program Benchmarking (External View)

Many organizations incorporate Security Program Benchmarking as part of their continuous improvement. The external focused form of the security benchmarking compares an organization's performance against a number of other organizations and provides a report back to the agency on where they fall based on observed baselines across all organizations with data currently available

Figure 4: Evaluation and Feedback Techniques (Adopted from NIST 2003: 37)

3. Gamification

3.1. Games and Rewards

Games were and are an important part of people's lives providing entertainment. Later the games started to encourage competition by providing rewards. Rewards were always a part of human's culture and were used as a means of behavior change and motivation enablement such as on children and pets as well as soldiers through ranks and badges for personal outstanding achievements which the same applies on students using grades. However, rewarding someone every time he/she unlocks an achievement could be non-profitable for some parties, such as casinos, and this is the point where "conditions" and "luck" where introduced so the rewards to be provided only to the "lucky" or "competent" few. However, if rewards are gone, this will eventually lead to loss of interest to a game and consequently loss of profit for the interested third parties. And this is where the term *Operant Conditioning* is coming to foreground that can keep the interest of people in games by cultivating the mindset that 'perhaps this time, I will get a reward' (Reiners and Wood, 2015: 56). And on this mindset are counting those designing slot machines and lottery tickets to keep people on playing a game without constant rewards.

According to Nicholson's work as edited by Reiners and Woods (2015: 60 – 72) there are six elements of games design that have inspired the term "Gamification" that will be introduced in the following paragraphs. These six elements can be defined as:

- Play

It is the idea of having the freedom to explore by in the meantime having boundaries, bumping up against them and occasionally crossing them. When players agree to play a game, they consequently accept to

follow certain rules and constraints. Though, if the constraints are too tight there will be no more fun and players will abandon it. Thus, players should be able to change it and make it more fun. And last but least, an important aspect of play is that it should be optional. Individuals should choose to engage with and not be obliged to

- Exposition

Each game design element is always consisted of a narrative layer. Exposition is the process of presenting this narrative layer to the player and it is analyzed to two parts: the development of a meaningful narrative element and the presentation of that narrative element to the player. The main use of exposition is to provide the players additional ways to be connected with the real-world setting. The most challenging part when designing the narrative layer of the game is to be careful the story not to have unwanted implications on the real world

- Choice

The element of Choice is introduced to let the player be in control of how he or she engages with the system. In combination with Play, such a system can offer more fun and positive attitude for the player if he/she can choose what he/she wants to engage with. The most commonly used way to offer the element of Choice is to give the players the opportunity to choose which activities they want to undertake. In order to avoid players being overwhelmed with choices, the best approach is to let players choose the goal and then provide the right guidance for accomplishing that goal

- Information

The concept of providing Information is based upon the idea of providing the player with the "why" and the "how" behind the game instead of just "what was done" and "how many points is it worth". If the player sees only rewards for specific behavior, he/she will learn only what behaviors have value for the game designers. The principle of Information in a game is that, while participants will still earn rewards, they will learn why those actions are being rewarded. There are three ways to provide Information to the player within the game. The first is by using the graphical user interface, displaying all the required information so the player to make the connection with the real world. The second way is the use of non-player characters that their only purpose will be to provide the participants all the required information, guidance and assistance. The third way is tied with the Exposition and this is to embed a narrative to provide the player with information about the story through elements in the game world that can be parallel to the real world

- Engagement

Most of the games are designed as single player where the player engages in his or her own journey. Engagement can be introduced by creating group of people within the same game as people have a more positive well-being when they interact with peers from the real world. Another definition of the Engagement is referring to the increase of the difficulty of the challenges that should match with the player's level of skills. Engagement opportunities can be offered also through competition or cooperation. The former, although it might discourage people of putting effort on it, it can be applied on a competitive real-world environment where competition can be enhanced by providing more tools to those who need to engage in the competition. The latter can serve a great purpose in the real-world by creating very powerful mentoring-based relationships as more experienced people can assist the new ones

- Reflection

The element of Reflection is creating opportunities for the players to step back and think about their game-based experiences and how these might connect to his/her own life. There are three basic components of Reflection. The first one is description, where the participant thinks and shares what he/she actually did as they engaged with the activity. The second one is analysis where the participants analyze what they did and think about how their actions connect to their own lives. The third one is application, where the participants are then urged to take action based upon what they have explored. Another way to enable Reflection is by creating a timeline of snapshots of the player's activity throughout the game. This can be done as the player engages with the activity or can be done later by capturing some key element of an accomplishment and asking the player to later reflect upon that

And by analyzing the benefits of the games and their reflection to the real world the term Gamification appeared, where most of the systems that have adopted this term focus on providing levels, leaderboards, badges and other human motivating elements to increase in popularity. Next, the term is further elaborated, providing a more detailed analysis.

3.2. The term "Gamification"

As already mentioned, games, at first, were used to provide entertainment. Then rewards started to be the purpose of the game in order to make the participants more engaged or not to lose their attention from it. From this new purpose of games, a new term has risen, the term "Gamification". According to Deterding et al. (2011: 1) '*Gamification is the use of game design elements in non-game contexts*', a definition that is often cited.

Gamification was first used as a way to promote a business or a product by motivating the players through badges, discounts or other rewards that could apply in the real world. However, by taking advantage of game design elements, gamification provides many potentials on several sectors of the real world such as user engagement, productivity, learning, evaluation, physical exercise and many more. It can also be defined as a set of activities and processes to solve problems by using or applying the characteristics of game elements. In other words, the motivational power of games is used to apply in real-world problems as, for example, the motivational problems in schools, the increase of competition or cooperation based on the organization's needs and targets.

In early gamification strategies, the main "weapon" of the games was the use of rewards in order to make players more engaged. Types of rewards were points, badges, levels, virtual currency and more. But as mentioned in a previous paragraph, as the field becomes more popular, there are six elements that inspire Gamification techniques to feel more like games and that is to allow the participants to have fun, to have a meaningful choice of what they will do in the game, to be equipped with a narrative of the background story, to increase challenge in order to avoid boredom, to increase socializing, competition and cooperation, but most important, each action in the game to have a reflection in the real world, so the participant to be able to parallel the game challenges to real-life problems or challenges.

Sailer et al. (2017: 373 – 374) focus on seven (7) game design elements that can work as motivational mechanisms to enable players to participate in several actions, with those to be:

- Points

It is an element that is rewarded upon successful competition of specific game activities that the designer considered as important to represent that the player has shown an important progress. There might be several types of points, but all serve the same purpose, to provide the necessary feedback to the players and to recognize their effort and progress

- Badges

Badges can have multiple purposes if given as game rewards. First of all, they can have the same goal as the points, to depict player's progress upon completing several activities. Though, points can be used to earn badges. Another aspect is that badges usually are accompanied by a symbol or phrase that indicate the player has achieved something of great importance and thus to have an influence of his attitude and behavior. Last but not least, a badge may be a symbol to one's membership into a group of people having the same badge and this can be important for the social influence, especially if the particular badge is hard to earn

- Leaderboards

This particular element provides a ranking among the players based on several criteria of success. It is of the elements that encourage competition as it depicts the performance of an individual against the performance of others. Though, there are two edges in the use of leaderboards; the first one is that it enables competition and encourages participants to put all their effort and skills to show their value and climb up to the top. On the other side though, the participants that are at the bottom of the list might be discouraged and abandon every effort of doing their best to evolve. The positive effects of this element can only be more visible if all the participants are of the same experience and performance level

- Performance Graphs

These graphs is basically the opposite element of the leaderboards. Performance graphs depict the player's performance but not compared to other players rather with player's own performance over time. By graphically displaying players' performance over time, they can be motivated to make improvements in order to increase their performance

- Meaningful Stories

Meaningful stories may be the most important element that can be used while designing a game, especially nowadays, where gamification is used to make people more engaged in real-world problems through their experience in the in-game activities. This element does not relate to the player's performance and does not follow any rules for rewards after a goal has been reached. Narrative contexts, either real-world related or analogical to real-world ones, can motivate people or make reflections to the real life, especially if the story is something of their own interest

- Avatars

Avatars are the visual representation of the player, either with a simple picture or with a 3D character. Although they serve no purpose for the participant's own improvement through performance metrics, competition with others or real-world parallelism, they help players to become part of community and make them cooperate with others, enhancing teamwork by adopting or creating another identity

- Teammates

It is an element that encourages both competition and cooperation either with other players or even with non-player characters. It is an important aspect, especially for organizations that their main target is competition or, on the other side, working in teams

Although the term "Gamification" was firstly introduced in 2008 it did not gain popularity until 2010, where many companies started using it for marketing purposes. As time has passed, gamification infiltrated in many aspects of life. Examples of gamification in action include the U.S. Army, having introduced a game called "America's Army", that is used to train existing members or recruit new, by providing a first-person shooter interaction where players establish virtual careers and they climb up the ranks by accomplishing missions along with other online players that simulate scenarios that correspond to recent military experiences and modern warfare (Cass: 2011).

Figure 5: America's Army Gameplay (Adopted from Cass: 2011, https://www.technologyreview.com/)

Another example of a game in the service of training, is IBM's CityOne, which simulates virtual cities on a browser-based game engaging the player to work with a team of consultants facing several challenges on energy, water, retail and banking sectors. What is worth mentioning in CityOne is the use of some of the aforementioned motivational elements, as progress (Figure 6) can be measured and depicted to the player through scores that provide metrics on the business climate, citizen happiness and population as the player should manage investments in things such infrastructure and supply chain against several costs and challenges (Cass: 2011).

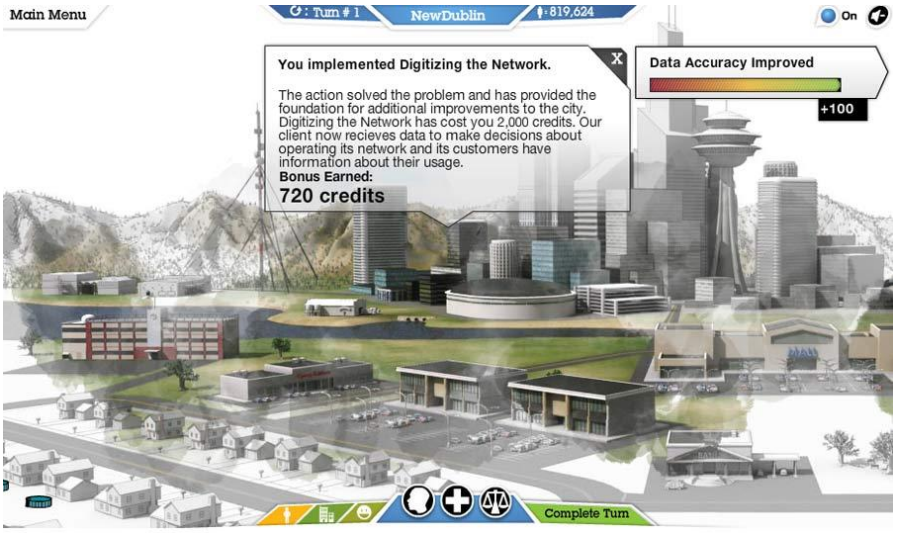

Figure 6: IBM's CityOne Gameplay (Adopted from Cass: 2011, https://www.technologyreview.com/)

NASA Learning Technologies published a game called Moonbase Alpha, with the development to be provided by Army Game Studios - America's Army developers – and Virtual Heroes Inc, which simulates the life of an astronaut in a Moon's outpost which was struck by an asteroid and the mission is to repair the outpost in order to save the 12 years of research. The main goal of the game is the decision making and better solutions provide higher score.

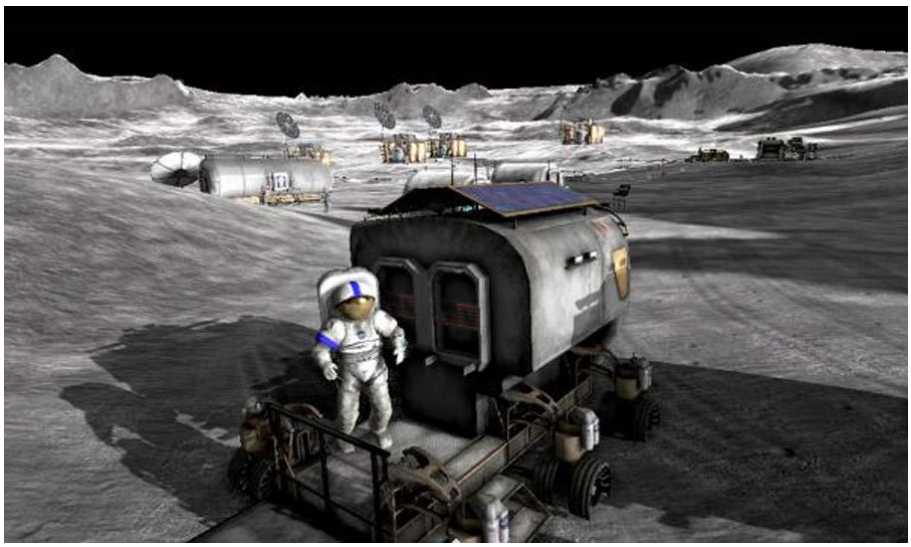

Figure 7: Moonbase Alpha Gameplay (Adopted from Cass: 2011, https://www.technologyreview.com/)

But gamification is not limited to Army or business activities. More examples of gamification in action can be found in American education system where students are ranked in classes based on their grades and in job application as well, where the applicants are subject to questionnaires or mini games to simulate the actual work environment of that company (Reiners and Wood, 2015: 178). More specifically, some of the sectors that gamification is introduced to serve a purpose are:

- Marketing
- Health
- Work Environment
- Education
- Politics
- Technology
- Online Casinos

A case that must be mentioned is the one of Deloitte that introduced gamification in its Deloitte Leadership Academy (DLA). With the integration of gamification in the Academy there has been a 37 percent increase in the number of users returning to the site each week. It has been observed that users are spending increasing amounts of time on the program while the numbers of programs completed have also increased. The most important thing about it though, is that the leaderboard is set in a way that everyone will be willing to participate since the ranking system is reflecting to the users the ten closest competitors rather than the top ten of the global list. Furthermore, the list is refreshing every seven days, giving the chance to participants to restart their performance and climb to higher rankings (Meister, 2013).

But what made Deloitte Leadership Academy so popular to the users? As Palmer, Lunceford and Patton (2012) mention in their article, before designing a gamified application to serve a business purpose the following questions should be considered:

1. What are you trying to accomplish?
2. Who is the audience?
3. How does your design maintain authenticity?
4. Who should help?
5. How do I track the behavioral data?
6. How will you track effectiveness?
7. What is your plan for updating and creating new content?

Having clear and distinct answers on the above core questions can lead to an optimum game design that will be able to serve each organization's needs and in parallel make the participants more engaged on the field of matter.

4. Gamifying Security Awareness

4.1. Move to a more game-centric Security Awareness Training

During recent years it is observed an enormous growth in the use of communication technologies, the Internet and mobile technologies. The same can be told though for the malicious IT threats such as viruses, malicious software, unsolicited e-mail (spam), monitoring software, attempts to make computer resources unavailable (DDoS attacks), human hacking (social engineering) and online identity theft (phishing) (Arachchilage and Love 2013: 1). Therefore, it can be assumed that the importance of security should be reached to users' personal computers or to employees of large organizations. Over the years, there have been developed several techniques for security awareness program but the problem seems to remain. Maybe the human is the 'weakest link'.

Figure 8: The weakest link (Adopted from https://medium.com/@kratikal)

But is this the truth? Or maybe all the techniques for security awareness that were introduced so far lack of motivation for the participants. Holding trainees attention for a long period of time in order to imprint a message is a challenge, especially if the training is mandatory (Cone et al, 2006: 2). Besides, it is proven that if individuals do not interact they, inevitably, lose their attention even if the subject presented is of their interest. Therefore, the awareness programs should be developed in such way that perfectly meets the interests of the people, the changing in their needs as well as the current lifestyles and cultural practices of each country and, by all means, to be engaging (Alotaibi et al, 2016: 661). Cone et al (2007: 64) provide a distinction among the common current training and awareness techniques which can be used as single units or as a combination of them, with those to be:

- Formal Training Sessions

Represents the traditional training approach which is usually instructor-led, seminars or video sessions. It is usually conducted by information security personnel and it success depends on how capable the instructor is to engage the audience

- Passive computer-based and web-based training

Represents a centralized approach to the training and awareness problem. Most of the times, this type of training offers the participants the flexibility of performing the training sessions at their own time, but on the other side, it becomes a monotonous slide show, preventing participants of any thoughts on the matter. The designer of such programs should attempt to make them more engaging and interactive to avoid the above undesired effects

- Strategic placement of awareness messages

The most common awareness messages are e-mail messages, posters, newsletters, screen savers and security labels that have as only purpose to draw the attention of the people and raise the level of consciousness. The pitfall in this technique is the routine. If for example a poster does not change, human brain starts to ignore it after the first times that draw its attention

- Interactive computer-based training

Referred also as video games, which can be distinguished into two categories, the first person games where the player faces an opponent or a problem and must directly confront it or he/she is penalized, while the second category is referring mostly to resource management where the participants should manage a virtual environment with limited resources and their choices will improve or destroy this environment

According to Foreman (in Cone et al, 2007: 64), '*games and simulations have become increasingly accepted as having enormous potential as powerful teaching tools that may result in instructional revolution*'. Although Serious Games, as they are called, are games used for training purposes, they still remain games with the major advantage of fun and interaction. They enable people to develop thoughts and skills through a fun and interactive way and, in addition, they provide the flexibility and adaptability a game requires to keep participants motivated.

Gondree, Peterson and Denning (2013: 64) present five freedoms that games can offer players and should be considered once training games are designed:

- The freedom to test hypotheses against an adversary
- The freedom to observe and learn from adversarial strategy
- The freedom to adopt the identity and explore the motivations of an adversary
- The freedom to experience and interpret a system from multiple perspectives
- The freedom to engage in or disengage from attacks strategically or arbitrarily

Although the combination of gamification with the field of security awareness is still in preliminary and developing phase, several attempts have been made to implement games that will serve the purposes of learning through playing and some of them will be presented in the following subchapter.

4.2. Serious Games in the Service of Security Awareness

As already mentioned in previous sections, a significantly high number of security incidents are caused by human error, resulting to loss of millions or other valuable assets for the organizations. Though, traditional trainings that were first developed to prevent and diminish these problems appeared to be not as effective as they were initially intended. Gamification, which originally was mostly used for marketing purposes, was introduced to security awareness trainings as well, in an attempt of many organizations to assist with securing their valuable assets as well as with the onboarding. To that end, several tools, or with a more official term "Games" were developed with the intention to make employees, students or every other interested party to be more engaged and to cultivate a more security-centric behavior and culture by also being entertained through a training game.

Some games that are developed explicitly for increasing security awareness and security-centric decision making based on the level of the participants are presented in the following subchapters.

4.2.1. Game of Threats™

Inspired by a well-known TV series, PriceWaterhouseCoopers (PwC), developed a digital game, having as audience company leaders and executives, that simulates a real-life security breach scenario targeting their company and demanding participants to make quick, high-impact decisions with minimal information. PwC's security experts through the game environment create a realistic experience with different types of threat actors (attackers) and their preferred methodologies and they explain what players can do to better prevent, detect and respond to an attack. The game's duration is up to three hours and it is limited to up to 15 participants in order maximum interactivity to be guaranteed.

The game is consisted of four parts, as presented below:

1. Welcome Presentation of Game of Threats™ simulation tool that will be used during the course session
2. Introduction to cybersecurity and the responsibilities of business leaders
3. Game of Threats™ role-playing game
    a. The participants will be divided into two teams: the "attackers" and the "company leaders"
        i. Each team member of both teams will have each own iPad controller and they will see the impact of their decisions in real-time on a shared monitor
    b. During the different rounds of the game, the teams will take turns in assuming both roles and must use the cards available to them to attack or defend the company
        i. Players can encounter different options every time they play
4. There will be a short debrief at the end of each round so that the participants to understand what has happened, which actions were decisive and how the attackers and defenders could have adopted a different strategy. At the end, a detailed summary will be provided reviewing both teams' strategy, actions and missed opportunities

The goal of this game-based training is to make the participants:

- be aware of the potential IT threats to their company
- understand where these threats could come from and precisely how they can compromise their company's IT system
- have an insight into the attacker's aims and methods
- understand why it is essential to implement security protocols in their company's IT infrastructure

Figure 9: Game of Threats™ Gameplay (Adopted from https://www.itsecurityguru.org)

PwC's effort with the Game of Threats™ initiative is a bright example of the move towards the gamification of Security Awareness and Security-centric decision making and the idea of putting the participants on both sides seems promising enough on the adoption of a more security-wise behavior having seen the impacts of a breach in a virtual environment that simulates in a high degree the real world. Though, since Game of Threats™ is new to the area of gamification for security purposes, no literature still exists for the effects the game has on the everyday operation of a company or organization.

4.2.2. Kaspersky Security Awareness

As one of the leading companies in IT security and Cybersecurity, Kaspersky could not just remain out of the field of Security Awareness. To that end, they developed a program known as *Kaspersky Security Awareness* which is consisted of three distinct sectors, as depicted in Figure 10, based on the target audience and the what is expected from each member of the audience. However, only the *Kaspersky Interactive Protection Simulation (KIPS)* will be further analyzed in terms of this study since it is the only one that is using a gamified approach of training to increase security awareness and security-centric behavior through the appropriate decision making of Senior Managers.

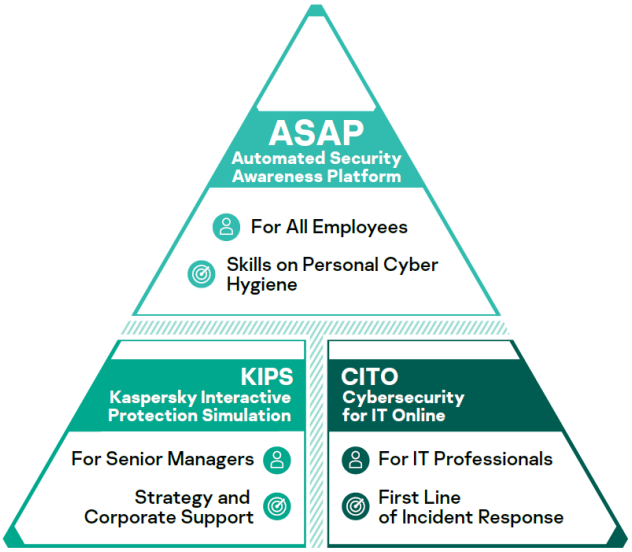

Figure 10: Kaspersky's Training Formats Based on Levels (Adopted from https://media.kaspersky.com)

The problem that KIPS is trying to solve is the so called "People Problem". The problem lies on the fact the senior management of different roles view (cyber)security with different perspectives and thus assign different priorities. From Business perspective, investing in security features contradicts with business' goals of cheaper, faster and better services. From IT security perspective, managers may feel that security as an infrastructure and investment issue moves outside their mission. Last but not least, from cost control management perspective, it may not be clear how security features and measures can relate with revenues and save rather than generate cost.

The idea of KIPS is to bring all the above three individual but in the same time connected parties to a mutual understanding of what security is, how it can improve services and increase profits instead of reducing them. Every decision or reaction made by the teams changes the way the scenario is unfolded and, consequently, how much profit the company makes or fails to make, as the game scenarios are based on real-life events. The game's duration is about 2 hours in order to be as much fun, engaging and fast as possible and requires teams of 4-6 participants who will be responsible of "running" a business but also facing the potential security attacks that target company's performance. Through this game set, Kaspersky's game aims to develop an understanding of cybersecurity measures and in the same time to build cooperation via teamwork and competition that will hopefully lead to initiative and analysis skills. Until this study is conducted, KIPS offers the below scenarios that can be used from the interested parties:

- Corporation

Protecting the enterprise from ransomware, Advanced Persistent Threats (APTs) and automation security flaws

- Bank

Protecting the financial institutions from high-level emerging APTs like Tyupkin and Carbanak, both being malware infecting ATMs to steal money

- Oil & Gas

Exploring influence of variety of threats, from website deface to a highly actual ransomware and a sophisticated APT

- E-Government/Local Public Administrations

Protecting the public web servers from attacks and exploits

- Power Station/Water Plant

Protecting industrial control systems and critical infrastructure from Stuxnet-style cyberattack (worm)

- Transportation

Protecting logistic companies from Heartbleed, APT, B2B Ransomware and Insider

- Petrochemical Industry

Ensuring the normal functioning of the new branch of a large petrochemical holding, focusing on ethylene production

Figure 11: KIPS Gameplay (Adopted from https://www.helpnetsecurity.com)

According to Kaspersky Labs, many large organizations such as CERN, Mitsubishi and also government agencies have used KIPS to their official training courses, providing a positive feedback and characterizing the game as an 'eye-opener' to this field.

A research conducted by Yonemura et al. (2018: 3 – 4) to the KOSEN National Institute of Technology students, using the Corporate and Water Plant versions, also reported positive effects of applying KIPS as

a training method. Another result of the same research revealed that, by applying the KIPS multiple times, educational content gaps have appeared, triggering the authors to consider an update or enhancement of the educational contents while at the same time measuring their effect by using the same of a similar gamified training method.

4.2.3. CyberCIEGE

One of the most utilized serious games for security awareness is CyberCIEGE which was developed in 2005 by the Naval Postgraduate School and it was intended to support education on the security of computers and networks. As mentioned in the official page of CyberCIEGE in Naval Postgraduate School, the game uses the same gaming techniques as SimCity™ having users to spend virtual money to purchase and configure workstations, servers, operating systems, applications and network devices while trying to balance the triad of budget, productivity and security while under attack. Though it is not limited to infrastructure schemas; a user is also equipped with configurable firewalls, VPNs, link encryptors, access control mechanisms and identity management components such as biometric scanners and authentication servers. On the other side, attach types include corrupt insiders, trap doors, Trojan horses, viruses, Denial of Service, exploitation of weakly configured systems as well as e-mail attachment awareness and cyber warfare.

CyberCIEGE targets all the levels of an organization and the scenarios are organized in a way that each "campaign" as they are called to address a different security topics. A tool is also provided to the instructors to organize the scenarios into campaigns of their choosing. On top, with the use of the Scenario Development Kit provided by the game makers, instructors can customize existing scenarios and create new ones. Within the game distribution are also included descriptions of security concepts and several animated tutorial videos that cover security topics; this online help facility is called the "encyclopedia". Finally, the scenarios include a student lab manual that describe the concepts and instructions to guide the student through the scenario. If needed, instructor notes can be added as provided by the instructors. What is important is that CyberCIEGE gives the students an environment in which they can learn through experimentation and they can be improved as the scenarios maintain a "flow" based on the students' progress (Thompson and Irvine, 2011: 2 – 3 & Cone et al., 2007: 67).

CyberCIEGE uses a *Scenario Definition Language*, which is a language that expresses security-related risk management tradeoffs for different scenarios using graphics and other interactive elements. The simulation engine interprets the students' choices using this scenario definition language and presents the resulting simulation which is the consequences of players' choices expressed in the aforementioned language (Irvine et al., 2005: 4). As mentioned in Raman's et al (2014: 2) study, the major elements included in the Scenario Definition Language are:

- Asset

Assets are the most valuable components of an organization, usually highly secured Information, business plans, marketing material etc. If an asset is compromised, this means a cost to the organization. Each asset has a different motive value to the attacker and thus different level of motivation for attacks

- Goal

An asset goal is the reason why the specific asset is important, what is the particular goal each asset has to achieve. Each goal usually is attached to a user's need in order to have the desired end effect

- Users

Each scenario within the game includes a set of virtual users. Each one's work serves organizations purposes. Students are responsible of providing the necessary resources in order the users to achieve their goals. Some goals are strictly attached with the user's productivity while other goals with user's happiness. While user's happiness will not cause loss of productivity in the short-term, eventually will end up to an unhappy employee which inevitably will impact organization's security

- Zones

Within each scenario one or more physical zones are included in order to control the physical movement of the users. Not all users have access to every zone and special qualifications will be needed in order to access a restricted zone

- Conditions and Triggers

The scenario designer defines conditions to be assessed by the engine during play and specifies actions to occur as the result of a combination of conditions. Such conditions might be new goal for a user that is requiring access to specific assets, elapsed time, unhappy users etc. Winning and losing are also defined using conditions and triggers

- Objectives and Phases

Scenarios can be divided into several phases with each phase to be consisted of one or more objectives as those are set by the game designer in order to guide the student through the scenario and gives the student a sense of achievement

Each student creates and maintains an environment where all the assets are protected and all the users are compliant with organization's goals and security policies. Failing of protecting the assets leads to loss of profit or reduced user productivity. During the simulation the status of user's productivity and happiness can be monitored by the player. Again, according to Raman et al (2014: 7) the following kinds of student's choices affect the protection of the assets:

- Select components that enforce selected security policies and deploy the components in suitable topologies
- Configure components to aid enforcement of the policies
- Interconnect components using networks
- Instruct users to follow certain procedures and provide users with adequate training
- Impose physical security by limiting which users can enter a physical zone and enforcing these limitations
- Perform selected degree of background checks on different kinds of users

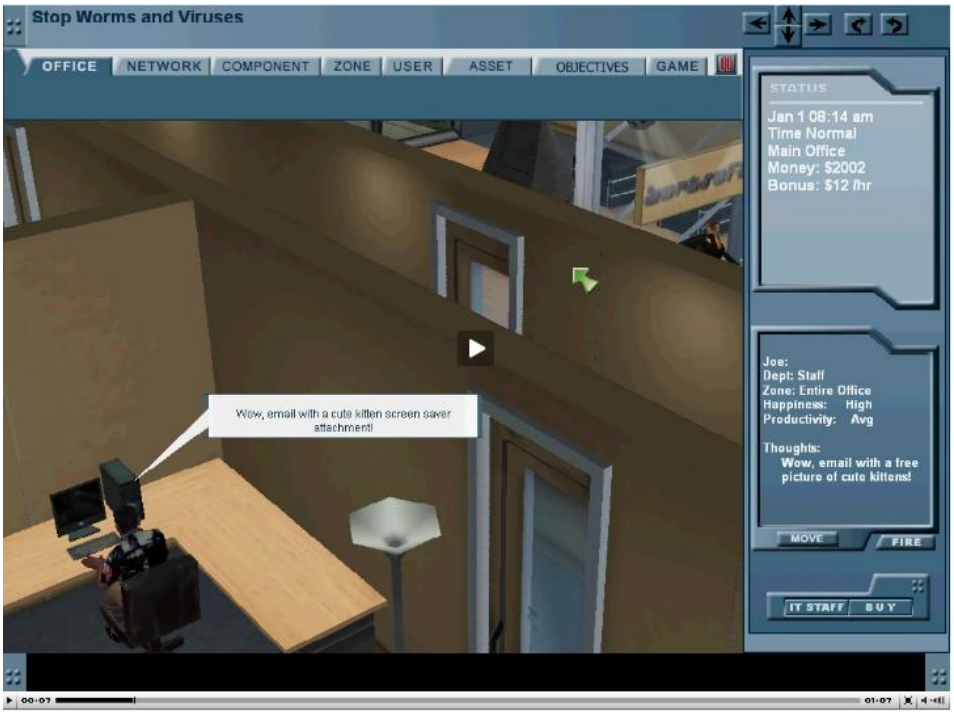

Figure 12: CyberCIEGE "Worms Scenario" Gameplay (Adopted from https://my.nps.edu/)

As already mentioned at the beginning of the subchapter, the effectiveness of CyberCIEGE has been demonstrated in several studies. Cone et al (2006: 7 & 2007: 71) demonstrate the flexibility of CyberCIEGE fulfilling a set of requirements for Navy IA training program with the initial test results to report a positive feedback of the game's usage. Raman et al (2014: 2 – 4) conducted a study having created two groups of graduate students, where the first group was prompted to answer a set of questions concerning cybersecurity while the second group was first encouraged to attempt the CyberCIEGE scenarios that were selected by the researchers and then answer the same set of questions. There were three major observations from this experiment. First of all, practical aspects of cybersecurity were not part of students' studies. Secondly, when introduced to the game and then the assessment, students had many more questions about the various options that they were not aware of before playing the game. And thirdly, exposing students to CyberCIEGE's scenarios had an enormous impact on the extent of their awareness and increase of knowledge, proving serious games with the flexibility of CyberCIEGE are better than traditional training. Jones et al (2010: 177 - 179) compare the effectiveness of CyberCIEGE with the *Department of Defense information Assurance Awareness Video (DoDIAA)* which is designed as a course to fulfill the requirement of the Federal Information Security Management Act and the Office of Management and Budget which require all the users of Federal computer systems to be trained in information security concerns. The experiment was conducted to students of North Carolina A&T State University being separated into two groups and using the two tools without any help on the material but only on how to use them. The results of the pre-test/post-test surveys could not lead to a strong conclusion, though they have shown that the group using the CyberCIEGE had provided more detailed and in-depth answers than the video group. However, what was clearly indicated was that the group using

the CyberCIEGE was more enthusiastic. Similar experiment was conducted by Fung et al (2008: 377 – 379), where the results of a traditional lecture versus the use of CyberCIEGE presented a similar level of understanding on the security questions, though the students participating in the game group demonstrated a deeper level of understanding, enjoyed the game more, found the game more challenging and that the knowledge they acquired can be applied in real-life scenarios with some of them not to want to stop the game even if they did not want to play at the beginning. Though, it is worth mentioning that, there were students that found the game boring and they never completed it. Concluding, Thompson and Irvine (2011: 6) have used CyberCIEGE as part of "Introduction to Computer Science" course, encouraging the students to experiment with several scenarios. Although it is not a part of an official research the results have shown that the students were "winning" in a great scale and some of them even experimenting again with the game, presenting the CyberCIEGE as an effective tool for educational purposes. The best comment concerning CyberCIEGE and gamification in general was made by one of Thompson and Irvine's network security instructors stating that '*If I see that a student has interacted with a reasonable simulation of a network filter for twenty minutes and figured out how to win the scenario, I believe the student has probably learned something*'.

4.2.4. Other Games

4.2.4.1. Anti-Phishing Phil

Phishing is a kind of attack where the attacker uses spoofed e-mails and fake websites to trick people on giving their personal information. Phishing attacks are widely used and many individuals are getting tricked in regular basis, which makes themselves as well as the organizations they are part in, vulnerable to exposure of sensitive information.

Anti-Phishing Phil is a game developed by Sheng et al (2007) with target to teach people to protect themselves from phishing attacks. There are browser embedded tools to prevent users from phishing attack by they cannot effectively protect against these types of attacks as unaware users will be unlikely to install and use an anti-phishing tool or may ignore warnings from them.

The goal of Anti-Phishing Phil is to teach users three things: (1) how to identify phishing URLs, (2) where to look for hints for trustworthy or untrustworthy sites in web browsers and (3) how to use search engines to find legitimate sites. Phil is a small fish, who wants to eat worms in the sea but has to be careful not to eat fake worms which represent phishing attacks. The game is split into four rounds, each one lasting 2 minutes.

Based on a case study performed by the same team, participants that have used the game performed better in identifying phishing websites while they became more knowledgeable about techniques to identify phishing websites.

4.2.4.2. 2025 Ex Machina

Ex Machina is a game targeting the use of social media networks, the connection between private and public life and the responsibility for and impact of one's actions on the internet. The scenario of the game includes people posting personal information making them vulnerable if these information resurface in the future. On the year of 2025, a website called "denicheur.net" has made a powerful database retrieval software accessible to the cybernauts. With it, anyone can search into other's pasts without having to worry about privacy protection laws. If this software fell into the wrong hands, it could result in many victims. By going back in time on the networks, the network Detectives come to aide of those whose pasts have been exposed.

The player is one of these detectives. Their mission: resolve each case that is entrusted to them throughout the four episodes and collect the information that will allow them to put a stop to denicheur.net.

4.2.4.3. Concept Serious Games

Since gamification in security awareness is a continuously growing subject, several researches have targeted the development of concepts concerning the empowerment of security awareness of each organization's members. Arachchilage and Love (2013) have attempted to develop a game design framework which enhances computer users' behavior through motivation to prevent themselves from phishing attacks. Adams and Makramalla (2015) have tried to provide an innovative gamified approach to train employees and organization leaders to develop cybersecurity skills and better defend against and react to data breaches. Amorim et al (2015) presented a possible design of a gamified training system, based on Agile methods, for cyber security that intends to comply with the many relevant requirements while considering new approaches for the development of training. Dabrowski et al (2015) have presented another competitive gaming-based security training approach that they are using at Vienna University of Technology stating that gamification is an effective way of motivating students to put more effort and hard work into their security education.

4.3. Concerns on the use of Gamification as a Training

Gamification as a training approach, as already mentioned, is a relative new subject in a preliminary and developing phase. Researches that have been conducted over the use of gamification for security awareness training have presented a positive feedback over its use, though the results cannot be considered as conclusive for the extended use of gamification for security awareness from the organizations.

The use of gamification appears to be a hot topic the last few years, though despite that it still is in its first steps, several concerns are raised on how gamification is used and what effects it has on human's

behavior, attitude and so called 'ethics'. Marczewski (2017: 58) attempts to explain the ethics concerning the use of gamification by placing 4 simple questions:

1. Does the system offer a choice?
2. What is the intention of the designer?
3. What are the potential positive and negative outcomes of being in the system?
4. Are the beneficial outcomes weighted towards the needs or desires of the user of the designer?

The above questions can be summarized with the statement of Marczewski (2017: 59) that '*gamification becomes unethical when the designer uses the psychology of players to manipulate them to do things that are not in their best interest'*.

Raftopoulos (by Landsell and Hagglund, 2016: 33 – 34) state that if gamification approach fails in an enterprise setting it may have undesired effects, referred as The Seven Deadly Sins:

- Coercive Participation

Games are fun and sometimes addicting because they rely on the free will of the player to play the game. Though, when gamified training approaches are applied in organizations, they appear to be mandatory and sometimes implant the fear to the people that they should be pressured to complete the game scenarios because their participation will be studied, measured and evaluated

- Leaky Container Problem

It refers to data in one application that might be used or transferred to another application and for other purposes, something that might influence people's behavior if they know they are monitored or their actions might be publicized

- Technological Whip

Gamified training approach is supposed to be a funny way of learning best practices of security and of organization's business principles in general, or it could be interpreted as a 'whip' to behave to the principles of the organization by playing

- Homogenization of the workforce

During gameplay players share several personal or not information. These information are collected from the developers in order to offer a more meaningful upgrade on design. Though, this data collection raises a concern on ethics and on a possible misuse of these data

- Loss of human agency

Players enter a virtual environment. They make decisions, they control virtual users, they win or lose. But there is no human-to-human interaction in this. Concerns are raised if, after all, the traditional techniques of training are a bit less effective though are encouraging human interaction, work experiences and enjoyment

- Illusion of change

A transformation of the workplace process is a complicated task. Although gamification has the power to change how tasks are performed and employees behave, if not applied correctly it can only give the illusion of change and not an actual change

- Shallow and inauthentic

If organization's attempt of making work fun through the use of gamification fails, it may end up with dissatisfied and disillusioned employees that will see the poor work practices

Game design is the primary element on which each concern arises since as suggested by Margalit (2016: 104) training should be implemented in a way that will not teach criminal activities and as stated by Nicholson (2012: 4) games will be meaningful if they do not treat people with the same way but let them set their own goals and strategies. Great issue constitutes game-based training approaches that include some kind of reward and more important real-life reward. But if the real-life motivation is higher for some players, this approach will make them less effective as they will find no interest in competing the training scenarios. It is supported the opinion that games used for training but also providing a reward to the participants do not fulfill their initial purpose as players tend to compete for the reward or for the better position in the leaderboard and they lose the true concept of the training, converting the game into gamble. Based on the research conducted from Hanus and Fox (2015: 160), it is observed that students that attended the gamified class tended to be less intrinsically motivated and resulted to lower final exam scores due to the fact that although the students found the offering of gamified class very interesting, once the rewards were introduced, they felt constrained and forced and thus motivation was lost. Although, one of the advantages of gamification is the sense of competition, at the same time is a disadvantage. Leaderboards, level and badges may serve another negative purpose; they can become the means for work intimidation instead of motivation or lead to lack of group cohesion, if these elements are meant to be visible to all team members and peer-comparison is encouraged (Algashami et al, 2018: 105 - 106).

Apart from the effects that a misleading game design can have, there is one more consideration that can make gamification less effective if used for training purposes; and this is the element of participants do not like (video) games. As observed in the research conducted by Fung et al (2008: 379), there were some participants using the CyberCIEGE game, that was selected for the research, that never completed the whole training as they felt 'bored' as they claimed. Almost aligned to the same element were the results presented by the Landers and Armstrong (2017: 500 – 501 & 504) through their research and literature review, where participants lacking of experience in virtual worlds and video games in general, were led to become more frustrated with this approach of training, commenting that at first a technology training was necessary before moving to gamification approach as a training in order to avoid frustration. If it is also considered that within an organization there will be a wide range of people in different ages, by default the results of a gamified training approach will be spread in a large scale due to the majority of older people not being aware or willing to use technology that at first were not familiar with. The effects of gamification among different ages were observed on the research conducted by Attali and Arieli-Attali (2015: 62) where for the children the correlations between speed and accuracy were significant in contrast to adults where there was no actual difference.

The use of gamification is not limited only by ethical restrictions but it can be of a more tangible element with that to be the limited budget from pure technology perspective. For example, if the organization involved is a large business providing the gamified training approach to several geographical places, it may face technology constraints since the right equipment will be needed to provide feedback for the remote participants. The same applies for the organizations that are looking for a high-tech and high-graphic environments. And if this requirement is of a small, low-funded company, it can be extremely difficult to provide such a technology and in terms it may lose a competitive advantage in the marketplace. But except from the significantly high cost of a high-tech training game, technological issues could arise during the game's lifecycle that will require immediate attention and fix, providing a huge expense to the organization. Last but not least, an important burden to the organization's expense, apart from the game's requirements and maintenance effort, is the significantly large amount of time that will be required to perform the concept design, the initial production, the editing, the trial and the ultimate publishing in order to produce an effective end product, and for the companies time is translated in profits or expenses in that case (Chen, 2015: 477 & 481 - 482). Apart from the above cost-related elements of designing a gamified training approach, another limitation of current gamification techniques is mentioned by Raftopoulos, Walz and Greuter (2015: 11) where all the vendors creating serious games are providing concepts and worlds as the designer intended and thus there is no guarantee on the outcome of game or gamification experience since the business realities may not be reflected, resulting to less value creation or even unnecessary expenses for the organization.

It is obvious that gamification is not panacea. As Marczewski (2017: 59) states '*Like a hammer, gamification is a tool. A hammer can be used to build beautiful houses when used by someone who understands its uses and its limitations. However, a hammer can also be used to break objects and cause great damage when used by those with less creative intentions. This does not make the hammer ethical or unethical, it is just a tool…The same is true of gamification*'.

5. Conclusions

This study has considered an analysis on the field of Information Security and the need of an advanced system of security awareness through trainings and education for the professionals. It has been also presented a review of the existing literature concerning the term "Gamification" and how can be used to make security awareness trainings more effective or, as it is supported by some individuals, to harm the organizations using such an approach.

Over the last years, it has been observed a significant growth in the use of communication technologies and, as a consequence, a similar growth on the several types of attacks to the personal information or valuable assets of the individuals or organizations that utilize these technologies. But not all incidents are performed from external adversaries, as most of the times "the walls fall from inside". Insider threat are a major problem and although it can be reduced, it cannot be eliminated. No matter how many security precautions are taken, the human factor is unpredictable and will always be a gray zone in the field of security, with several surveys to place insider threat in the top ten of the Information Security threat ranking.

However, security awareness programs have been developed to provide employees and individuals in general, with the necessary knowledge or know-how in order to be alerted to possible security risks or to be aware on how to react in case a security incident occurs. Depending on the organizational level and the knowledge depth of each one, either a training or an education can be applied with the latter usually to be accompanied by a diploma. Though, just providing the necessary trainings is not enough; the appropriate evaluation system should be implemented in order to aide security personnel to proceed with the necessary actions based on the reported results.

The traditional trainings approaches followed so far, presentations, lectures, videos, seem not to provide the desired effect with the "insider" incidents to have reduced slightly. The new trend in security awareness training is the use of gamification as it is proven that games make education more fun and motivate participants to engage more. With the use of near real-life scenarios, instructors are trying to provide a hands-on experience and cultivate a decision-making culture that will make employees or individuals more secure aware.

A number of games have been developed and academic studies have been conducted to evaluate the effectiveness of the game as a training approach. All the researches that were evaluated for the needs of this study, reported the same result; gamification seems to have a positive effect on the learning procedure with most of the participants to present a deeper level of understanding on the elements they were trained upon and with more enjoyment. Though, all the experiments were conducted to a small number of participants and thus the results cannot be considered as conclusive for the positive outcome of a game-based training, while some claim that gamification is not the ultimate weapon against the lack of security awareness with several ethical concerns to be raised, technological limitations to be surfaced due to low organization budgets and the current gaming designs not to be able to cover all the range of ages and interests within the organization.

As organizations are trying to adopt the new innovative way of training, the gamified approach, they struggle to provide high-tech technology and graphics resulting in significantly high expenses for it. Even with existing vendor games for security training, not all the organization's needs are covered as currently all the games are created on how the designer intended and not tailored to each organization's needs and fields of work. Apart from the technological or low-budget limitations, today's organizations are consisted of people from a wide range of ages, with some of them not being familiar with electronics and games at all, choosing a traditional way of training with presentations or lectures.

Though, all the limitations that were presented can be justified since gamification as a training approach is relatively new and its potential is presented to organizations and users, introducing innovative thinking, problem solving and competition or teamwork. Young adults, especially of the latest generations and the generations to be, are raised with several electronic sources and are really familiar with the use of games and with an attitude to try more and progress through small "wins". Almost all the researches that were reviewed for the needs of this study were conducted mostly on students and young people with them stating that learning through the game was more fun and interesting and the effect of the game was also presented in the tests the students were submitted to, where they showed a deeper knowledge of the subject they were trained about. Thus, since the new generations are the future of each organization and the games are their way of having fun, learning and evolving as characters, the industry of serious games should invest more and focus on the design and development of such trainings and with a more dynamic approach in order to cover every possible field of interest.

Gamification has infiltrated in several aspects of people's lives such as to support businesses and health sector, to enhance education and as of the latest move to empower security awareness trainings. Based on the positive results of current researches, even with small samples and specific sectors such as students, with more and more people being familiar with technology innovations, with a new type of Serious Games emerging, called First Person Walker and with the Media Convergence (Raftopoulos, 2018), gamification can be used to increase security awareness without reducing employee's productivity and it is expected to present a significant growth in a positive direction.

6. References

Adams M., Makramalla M. (2015), *Cybersecurity Skills Training: An Attacker-Centric Gamified Approach*, Technology Innovation Management Review

Algashami A., Cham S., Vuillier L., Stefanidis A., Phalp K., Ali R. (2018), *Conceptual Gamification Risks to Teamwork within Enterprise*, International Federation for Information Processing (IFIP), Springer Nature Switzerland AG

Ali Yayla (2011), *CONTROLLING INSIDER THREATS WITH INFORMATION SECURITY POLICIES*, European Conference on Information Systems (ECIS)

Alotaibi F., Furnell S., Stengel I., Papadaki M. (2016), *A Review of Using Gaming Technology for Cyber-Security Awareness*, International Journal for Information Security Research (IJISR)

Amankwa Eric, Loock Marianne, Kritzinger Elmarie (2014), *A Conceptual Analysis of Information Security Education, Information Security Training and Information Security Awareness Definitions*, The 9th International Conference for Internet Technology and Secured Transactions (ICITST)

Amorim J. A., Hendrix M., Andler S. F., Gustavsson P. M. (2013), *Gamified Training for Cyber Defence: Methods and Automated Tools for Situation and Threat Assessment*, NATO Modelling and Simulation Group (MSG)

AO Kaspersky Labs (2019), *Kaspersky Interactive Protection Simulation (KIPS) - An effective way of building cybersecurity awareness among top managers and decision makers*, Available: https://media.kaspersky.com/en/business-security/enterprise/KL_SA_KIPS_overview_A4_Eng_web.pdf [18 Jan 2020]

Arachchilage N. A. G., Love S. (2013), *A game design framework for avoiding phishing attacks*, Computers in Human Behavior

Attali Y., Arieli-Attali M. (2015), *Gamification in assessment: Do points affect test performance?*, Computers & Education

Bada M., Sasse A. M., Nurse J. R. C. (2019), *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?*, International Conference on Cyber Security for Sustainable Society, 2015, Cornell University

Blakley Bob, McDermott Elen, Geer Dan (2001) *Information Security is Information Risk Management*, Proceedings New Security Paradigms Workshop

Cass Stephen (Nov. 2011), *Serious Games – Six titles to train employees, educate public or recruit new members*, MIT Technology Review, Available: https://www.technologyreview.com/s/426180/serious-games/ [26 Jan 2020]

Chen E. T. (2015), *The Gamification as a Resourceful Tool to Improve Work Performance*, Gamification in Education and Business, Springer, Cham

Cisco, *What is Information Security?*, Available: https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html [28 Oct 2019]

Cone B. D., Irvine C. E., Thompson M. F., Nguyen T. D. (2007), *A video game for cyber security training and awareness*, Computers & Security

Cone B. D., Thompson M. F., Irvine C., Nguyen T. D. (2006), *Cyber Security Training and Awareness Through Game Play*, International Federation for Information Processing, Springer, Boston, MA

Cooper S., Nickell C., Piotrowski V., Oldfield B., Abdallah A., Bishop M., Caelli B., Dark M., Hawthorne E.K., Hoffman L., Perez L.C., Pfleeger C., Raines R., Schou C., Brynielsson J. (July 2009), *An Exploration of the Current State of Information Assurance Education*, ACM SIGCSE Bulletin

Dabrowski A., Kammerstetter M., Thamm E., Weippl E., Kastner W. (2015), *Leveraging Competitive Gamification for Sustainable Fun and Profit in Security Education*, USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE '15)

Deterding S., Dixon D., Khaled R., Nacke L. (Sep 2011), *From Game Design Elements to Gamefulness: Defining "Gamification"*, Conference: Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments

European Network and Information Security Agency (ENISA) (Jan 2016), *ENISA Threat Landscape 2015*, Available: https://www.enisa.europa.eu/publications/etl2015 [26 Jan 2020]

European Network and Information Security Agency (ENISA) (Jan 2019), *ENISA Threat Landscape Report 2018*, Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 [26 Jan 2020]

European Network and Information Security Agency (ENISA) (Nov 2010), *The new users' guide: How to raise information security awareness*, Available: https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide [11 Jan 2020]

Fung C. C., Khera V., Depickere A., Tantatsanawong P., Boonbrahm P. (2008), *Raising Information Security Awareness in Digital Ecosystem with Games – a Pilot Study in Thailand*, 2008 2nd IEEE International Conference on Digital Ecosystems and Technologies, Published by IEEE

Gondree M., Peterson Z. N. J., Denning T. (2013), *Security through play*, IEEE Security & Privacy, Published by IEEE

Hanus M. D., Fox J. (2015), *Assessing the effects of gamification in the classroom: A longitudinal study on intrinsic motivation, social comparison, satisfaction, effort, and academic performance*, Computers & Education

Herold Rebecca (2005), *Managing an information security and privacy awareness and training program*, Taylor & Francis Group, LLC

ISO/IEC 27000 (2018) *Information technology - Security techniques - Information security management systems - Overview and vocabulary*

Irvine C. E., Thompson M. F., Allen K. (2005), *CyberCIEGE™: An Information Assurance Teaching Tool for Training and Awareness*, Defense Technical Information Center

Jones J., Yuan X., Carr E., Yu H. (2010), *A comparative study of CyberCIEGE game and Department of Defense Information Assurance Awareness video*, Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon), Published by IEEE

Kruger H.A., Kearney W.D. (2006), *A prototype for assessing information security awareness*, Computers & Security

Landers R. N., Armstrong M. B. (2017), *Enhancing instructional outcomes with gamification: An empirical test of the Technology-Enhanced Training Effectiveness* Model, Computers in Human behavior

Landsell J., Hagglund E. (2016), *Towards a Gamification Framework: Limitations and opportunities when gamifying business processes*, Department of Informatics, Umea University

Lee J., Hammer J. (Jan 2011), *Gamification in Education: What, How, Why Bother?*, Academic Exchange Quarterly

Marczewski Andrzej (2017), *The Ethics of Gamification*, The ACM Magazine for Students Volume 24, Number 1, Pages 56-59

Margalit O. (2016), *Using Computer Programming Competition for Cyber Education*, 2016 IEEE International Conference on Software Science, Technology and Engineering (SWSTE), Published by IEEE

Meister J. C. (2013), *How Deloitte Made Learning a Game*, Harvard Business Review, Available: https://hbr.org/2013/01/how-deloitte-made-learning-a-g [12 Jan 2020]

Moore Michelle (Apr 2019), *Bringing Gamification to Cyber Security Training*, Available: https://www.globalsign.com/en/blog/bringing-gamification-to-cybersecurity-training/ [13 Jan 2020]

NASA (July 2010), *Moonbase Alpha*, Available: https://www.nasa.gov/offices/education/programs/national/ltp/games/moonbasealpha/index.html [26 Jan 2020]

Naval Postgraduate School – Center for Cybersecurity and Cyber Operations, *CyberCIEGE*, Available: https://my.nps.edu/web/c3o/cyberciege [18 Jan 2020]

Nicholson Scott (2012), *A User-Centered Theoretical Framework for Meaningful Gamification*, Paper Presented at Games+Learning+Society 8.0, Madison, WI

Organization for Economic Co-operation and Development (25 July 2002), *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, 1037th of OECD Council

Organization for Economic Co-operation and Development (October 1st, 2015), *Digital Security Risk Management for Economic and Social Prosperity – OECD Recommendation and Companion Document*, OECD Council

Palmer D., Lunceford S., Patton A. J. (2012), *The engagement economy: How gamification is reshaping businesses*, Deloitte Insights, Available: https://www2.deloitte.com/us/en/insights/deloitte-review/issue-11/the-engagement-economy-how-gamification-is-reshaping-businesses.html [12 Jan 2020]

Peltier Thomas R. (2013), *Information Security Fundamentals, Second Edition*, Auerbach Publications

PwC, *Game of Threats™ - Cyber Threat Simulation*, Available: https://www.pwc.com/lk/en/services/consulting/technology/information_security/game-of-threats.html [18 Jan 2020]

Raftopoulos M. (2018), *Has Gamification Failed?*, GamificationEurope, Available: https://www.youtube.com/watch?v=esnEAuazR6I&t=270s [17 Feb 2020]

Raftopoulos M., Walz S., Greuter S. (2015), *How enterprises play: Towards a taxonomy for enterprise gamification*, 2015 Authors & Digital Games Research Association DiGRA

Raman R., Lal A., Achuthan K. (2014), *Serious games based approach to cyber security concept learning: Indian context*, 2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE), Published by IEEE

Rantos Konstantinos, Fysarakis Konstantinos, Manifavas Charalampos (Dec 2012), *How Effective Is Your Security Awareness Program? An Evaluation Methodology*, Information Security Journal: A Global Perspective

Reiners Torsten, Wood Lincoln C. (2015), *Gamification in Education and Business*, Springer International Publishing

Roer Kai, Petric Gregor (2017), *Deep insights into the human factor - the security culture report 2017*, CLTRe North America, Inc

Sailer M., Hense J. U., Mayr S. K., Mandl H. (2017), *How gamification motivates: An experimental study of the effects of specific game design elements on psychological need satisfaction*, Computers in Human Behavior

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*, SOUPS '07: Proceedings of the 3rd symposium on Usable privacy and security, Association for Computing Machinery, New York, NY, United States

Thompson M., Irvine C. (2011), *Active Learning with the CyberCIEGE Video Game*, 4th Workshop on Cyber Security Experimentation and Test, San Francisco, Naval Postgraduate School

Tralalere, *2025 Ex Machina*, Available: http://www.2025exmachina.net/en/project [18 Jan 2020]

U.S. Army (2002, 2009), *America's Army*, Available: https://www.americasarmy.com/ [26 Jan 2020]

Whitman Michael E. (2004), *In defense of the realm: understanding the threats to information security*, International Journal of Information Management

Wikipedia, *Information Security*, [Online], Available: https://en.wikipedia.org/wiki/Information_security [27 Jan 2020]

Wikipedia, *Information Security Awareness*, [Online], Available: https://en.wikipedia.org/wiki/Information_security_awareness [27 Jan 2020]

Wikipedia, *Gamification*, [Online], Available: https://en.wikipedia.org/wiki/Gamification [12 Jan 2020]

Wilson Mark, Hash Joan (2003), *Building an Information Technology Security Awareness and Training Program*, National Institute of Standards and Technology (NIST)

Yonemura K., Komura R., Sato J., Takeichi Y., Yajima K. (2018), *Security Education Using Gamification Theory*, 2018 International Conference on Engineering, Applied Sciences, and Technology (ICEAST), Published by IEEE