Computers & Security 95 (2020) 101827

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Riskio: A Serious Game for Cyber Security Awareness and Education

Stephen Hart[a], Andrea Margheri[a], Federica Paci[b,*], Vladimiro Sassone[a]

[a] Electronics and Computer Science, University of Southampton, Southampton, United Kingdom
[b] Department of Computer Science, University of Verona, Verona, Italy

ARTICLE INFO

Article history:
Received 16 September 2019
Revised 30 March 2020
Accepted 31 March 2020
Available online 29 April 2020

Keywords:
Gamification
Cyber Security
Education
Cyber Attacks
Security Controls

ABSTRACT

Cyber attacks are increasing in number and sophistication, causing organisations to continuously adapt management strategies for cyber security risks. As a key risk mitigation policy, organisations are investing in professional training courses for their employees to raise awareness on cyber attacks and related defences. Serious games have emerged as a new approach that can complement instruction-led or computer-based security training by providing a fun environment where players learn and practice cyber security concepts through the game. In this paper we propose Riskio, a tabletop game to increase cyber security awareness for people with no-technical background working in organisations. Riskio provides an active learning environment where players build knowledge on cyber security attacks and defences by playing both the role of the attacker and the defender of critical assets in a fictitious organisation.

1. Introduction

Cyber-attacks have exponentially increased in the last decade. Threat actors are continuously improving their cyber weapons to timely and effectively exploit vulnerabilities, misconfiguration of IT systems and new technologies such as Internet of Things and Cloud Computing Report. Since the cyber security landscape is rapidly changing, organisations must keep pace with emerging threats in order to be resilient against cyber attacks.

In this context, the management of cyber security risks is a key business objective for every organisation. To help and support management of cyber security risks, several standards and frameworks have been proposed, e.g. the Cyber Essentials scheme from NCSC in UK (National Cyber Security Centre, b), the NIST Cyber Security Framework National Institute of Standards and Technologies, the IEC 62443 International Electrotechnical Commission for industrial control system and the ISO 27001 International Organization for Standardization for information security. These standards guide in the identification, and assessment of the risks posed by cyber attacks to an organisations assets, and also support in the selection of related procedural and technical security controls and countermeasures. One of the key countermeasures that these standards advise an organisation to deploy is education and awareness of organisations' employees. As said by Kevin Mitnick (probably one of the most infamous computer hackers of all time): "*A company can spend hundreds of thousands of dollars on firewalls, intrusion detection systems and encryption and other security technologies, but if an attacker can call one trusted person within the company, and that person complies, and if the attacker gets in, then all that money spent in technology is essentially wasted*". As a matter of fact, employees are a critical component of any organization and they may introduce new vulnerabilities that are often exploited for perpetrating cyber attacks: they click on a link on a email, they visit a malicious website, or accidentally disclose sensitive information. However, unlike computers and software, employees cannot be "patched" when a new vulnerability is discovered. Therefore, it is fundamental for organisations to ensure that all employees are educated on the risks posed by even the simplest cyber attacks, and on how to make more secure decisions to avoid or mitigate these risks (Trickel et al., 2017). The most common method of delivering security education and awareness used by organizations is fact-and-advice training that can be either instructor-led or computer-based. While this type of training provides a good theoretical start, it is not enough and practice is essential for mastering the high complexity of cyber security concepts (Trickel et al., 2017).

In the last few years, serious games have been proposed as a new approach that can complement instruction-led or computer-based cyber security education and training. Serious games provide a fun, enjoyable educational environment where the participants learn theory and concepts in cyber security and put them into practice through the game. In particular, the participants learn how to attack and exploit vulnerabilities in a dynamic setting, and how to react to attacks by developing, on the spot, defences and

* Corresponding author.
E-mail addresses: stephen.hart@soton.ac.uk (S. Hart), a.margheri@soton.ac.uk (A. Margheri), federica.paci@univr.it (F. Paci), vsassone@soton.ac.uk (V. Sassone).

https://doi.org/10.1016/j.cose.2020.101827
0167-4048/

countermeasures. This results in participants' faster learning and mastery of cyber security concepts (Trickel et al., 2017).

A number of serious games have been proposed with the aim of educating on different topics in cyber security: secure software development (Beckers and Pape, 2016), Microsoft, risk estimation (Williams et al., 2010), incident management (Graffer et al., 2015) and threat awareness (Thompson and Irvine, 2011). However, some of these games only educate on a specific category of threats like social engineering (Aladawy et al., 2018) or network attacks (Gondree and Peterson, 2013), or they increase awareness on attacks and defences specific to a given application scenario like industrial control systems (Graffer et al., 2015), cyber physical systems (Frey et al., 2017) or hospitals (Yasin et al., 2019). This prevents them from being easily adapted and modified to be used in different scenarios. Moreover, with few exceptions (Graffer et al., 2015; Haggman, 2019), most of the games either educate players on how to think like an attacker or how to react to an attack but not on both.

Due to the complexity and rapid change of the cyber security landscape, it is therefore fundamental to design a serious game that exposes players to a wide range of cyber security attacks and related countermeasures from industrial and government standards and that allows them to practice attacks and defence strategies through the game. Moreover, the game should be easily modifiable to different training needs (Haggman, 2019).

Contribution. In this paper we propose Riskio, a board game where participants build their knowledge on cyber security attacks and defences by playing both the role of attackers and defenders of critical assets in a fictitious organisation represented on the board. The game is played with attack and defence cards that cover a wide range of attacks and countermeasures from industry and government standards that make the game adaptable to a variety of contexts and scenarios. In order to provide participants an active learning environment, the design of the game is based on the principles of constructivism learning theory where learners build knowledge through experiences (Bada and Olusegun, 2015). The presence of a game master facilitates the construction of such knowledge by making players reflect upon their attack and defend strategies, fostering discussion among the players, and providing immediate feedback on the correctness and effectiveness of their strategies.

We conducted a series of experiments with employees and graduate students to assess the perceived efficacy of Riskio in increasing cyber security awareness. The evaluation shows the effectiveness of the game and points out trade-offs in terms of design and playing experience that can allow the game to better fit different audience.

Outline. Section 2 introduces the literature on serious games for cyber security. Section 3 presents the design principles of Riskio. Section 4 describes Riskio main components and rules to play. Section 5 presents the results of the experiments that we ran to evaluate our game. Section 6 discusses the lessons learned during the design and evaluation of the game. Section 7 concludes the paper.

2. Related work

Gamification techniques applied to the security domain have attracted increasing attention and led to the development of many serious games. We review the most established security-related games from the literature by classifying them according to the main goal for which they have been designed. We conclude by summarising the main limitations of these games.

Secure Software Development. Serious games have been proposed to involve employees with limited security expertise into core activities of secure software development projects, with a particular focus on threat modelling, risk assessment, security requirements elicitation, and secure coding.

Elevation of Privilege (EoP) (Shostack (2014) is a card game proposed by Microsoft to conduct threat modelling as part of the design phase of software projects. EoP is based on the Microsoft STRIDE methodology (Potter, 2009) and aims to facilitate the identification of attacks by exemplifying the different STRIDE threat categories (i.e. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege). Each card represents potential real-world threat scenarios that can target a software artefact. The game mechanics aims to facilitate the discussion on the effect of threats so to elicit additional requirements. Similarly to EoP, Riskio adopts STRIDE threat taxonomy to divide attack cards into different suits, but the threat scenarios on the cards are taken from the latest version reports on attack trends. The game mechanic is also different because Riskio not only support players in the identification of threats, but also foster discussion among the players on which is the best countermeasure an organisation should apply to prevent or deter the threat scenarios. The *OWASP Cornucopia* OWASP is similarly defined but it rests on the well-known OWASP Top 10. Differently from the educational goal of Riskio, both games are meant to be played by developers to help them review and validate the software, thus to identifying attacks scenarios during early stages of software design.

Becker et al. (Beckers and Pape, 2016) propose a serious game to elicit security requirements while capturing the underlying human behaviours exploited by social engineering. The players, organised into teams, learn attack and defence strategies related to human behaviours, and elicit security requirements guided by the game cards. In contrast, Riskio encompasses social engineering attacks and allows players to also experiment with a larger variety of different types of attacks. *Protection Poker* (Williams et al., 2010) builds on the concept of planning poker techniques (Moløkken-Østvold et al., 2008) to support security risk estimations within agile software projects. The game aims at facilitating the interactions among project stakeholders in order to define, for each security risk, the perceived 'ease of attack' and 'asset value'. Differently from Riskio, this poker game does not provide any attack scenarios (e.g. in the forms of cards or game-board), but it relies on security risks already elicited as part of the software project. *Hacker* ThinkFun is a tabletop game focusing on secure coding practices. The game features a number of coding challenges of increasing difficulty that have the aim to educate how code vulnerabilities can be discovered, exploited and protected; this is part of a larger collection of games on coding[5].

Security awareness and education. Serious games have been used as means for security awareness and education, both in the form of tabletop, video games, or capture-the-flag competitions.

CyberCIEGE (Irvine et al., 2005; Thompson and Irvine, 2011) is an educational video game developed by the US Naval Postgraduate School to offer an environment for the simulation of office scenarios for the cyber education of employees. Players have to invest a limited budget into a range of security activities for a fictional organisation (e.g. network configuration or employee security policies), which are then evaluated with respect to a set of business goals. The game offers high adaptability and control of the played scenarios, but the lack of team-playing hinders peer-learning of technical and decision making skills that tabletop games can offer. Differently from Riskio, the exclusive focus on defence controls prevents players from developing their cyber security awareness on adversarial behaviours. Similarly, the computer game *PERSUADED* (Aladawy et al., 2018) allows players to learn the effective-

[5] https://www.thinkfun.com/learn-coding/.

ness of defence controls against most common social engineering attacks, but it does not raise awareness of the actual attack vectors that attackers can exploit.

Chothia et al. (Chothia et al., 2017) have proposed a capture-the-flag style VM to increase student engagement to an introductory cyber security course. The VM uses gamification in the form of story telling and characters development. The students play the role of a new IT security employee at a fictitious company and are required to solve different exercises for which they receive flags. The students can decide to send the flags to a number of different characters and their choice changes the flow of the story. Riskio supports story telling by means of the game board that allows players to invent an attack scenario that involves the characters and assets depicted on the board.

Haggman (Haggman, 2019) proposes a tabletop wargame for cyber security education that is based on the UK National Cyber Security Strategy. The game board simulates the cyberwar between UK and Russia and represents the main entities that are involved in the implementation of the cyber security strategy in the two antagonist countries: government, national critical infrastructures, people, intelligent agencies, and businesses. Each entity has a set of strategic objectives that they need to achieve using limited resources. Each entity is assigned a set of resources that they can use to buy assets to conduct an attack or defend against it. Similarly to Riskio, this wargame aims to expose players to a variety of cyber attacks and defence dynamics.

Play2Prepare (Graffer et al., 2015) is a tabletop board game whose main goal is to train players on how to handle IT security incidents in Distribution System Operators (DSOs) organizations. The game supports five different attack scenarios inspired to real attacks on industrial control systems where the players have to work together to mitigate the attack. The players play a specific role in the game which is associated with a set of skills that can be used to mitigate an attack. Each attack scenario comes with a set of questions that are designed to create discussions amongst the players and to increase their understating of cyber security concepts. The game also uses "did you know" facts that are short inputs that aim to create dynamics and variation in the game and to provoke player's thinking. Riskio activates players' thinking by having the game master asking questions to help players in the formulation of an attack scenario or defence strategy and by using information cards that force the players to think about a defence strategy for an unexpected attack.

Cyber Security-Requirements Awareness Game (Yasin et al., 2019) is a tabletop card game developed to educate on cyber security risks in hospital related scenarios. The players have to identify vulnerabilities in the scenarios and exploit them to carry out insider or outsider attacks. Discussion among players are used to evaluate and score attack scenarios. The game allows players to learn multiple vulnerabilities and attacks, however it significantly differs from Riskio as it does not follow a standard threat taxonomy, e.g. STRIDE, which prevents the game from being easily adapted and used in different scenarios; most of all it lacks of a defending phase.

Decision & Disruption (Frey et al., 2019) is a tabletop card game designed via a Lego™ game board representing an industrial cyber physical system to protect. The game is organised into rounds during which players must prioritise based on an available budget defence measures to be deployed to protect the system. At the end of each round, the game master rates the effectiveness of the selected defences based on fixed attack profiles which are not known to the players. The players learn the role of defenders and in limited extent about security management strategies. Differently from Riskio, it does not focus on cyber threat awareness and related attacks: players are not challenged to defining attacks nor selecting defences based on a known attack.

[d0x3d!] (Gondree and Peterson, 2013) is a tabletop card game designed to teach network security concepts to K-12 non-CS and non-STEM students. The players impersonate a group of white-hat hackers who break into a network and retrieve valuable digital assets using their capabilities and exploiting network vulnerabilities. At each turn the network is patched to simulate the actions of a network administrator who makes harder for the players to retrieve the digital assets. Riskio, in contrast, allows player to learn a wider range of security threats taken from latest security reports.

Control-Alt-Hack (Denning et al., 2013) is a tabletop card game designed to increase awareness and understanding of computer security concepts. The primary audience of the game is computer and engineering undergraduate students and high school students. Similarly to [d0x3d!], the players play the role of white-hat hackers working for a security company which performs security audits and provides consultation services. The players have to accomplish different missions using their hackers' skills. While Riskio main goal is to educate players on how to think as an attacker and then learn how to deter attacks, Control-Alt-Hack's main focus is on attack and vulnerability exploitation.

The Security Cards (Tamara Denning and Kohno) is a card deck to encourage players to think broadly and creatively about computer security threats. The card deck contains 42 cards organised in 4 categories: 1) Adversary's Motivations, 2) Adversary's Resources, 3) Adversary's Methods, and 4) Human Impact. The cards can be used to support different kind of educational activities in academic and industry settings: for example they can be used to learn about security threats or to elicit threats in software design. Compared to Riskio, the Security Cards deck does not include cards to educate on possible defences to deter security threats.

Summary of Game Limitations. In conclusion, the reported games suffer from one or more of the following limitations: 1) they educate on a specific category of threats rather than allowing player to learn a wide range of attack scenarios (Aladawy et al., 2018; Denning et al., 2013; Frey et al., 2019; Gondree and Peterson, 2013; Graffer et al., 2015; Yasin et al., 2019); 2) they are designed for specific application scenarios and therefore they are not easily modifiable to be used in different contexts (Frey et al., 2019; Graffer et al., 2015; Yasin et al., 2019); 3) they either allow players to learn how to think like attackers or how to defend against attacks and exploits but not both (Aladawy et al., 2018; Chothia et al., 2017; Frey et al., 2019; Irvine et al., 2005, Tamara Denning and Kohno,Thompson and Irvine, 2011).

3. Game Design

This section reports the main goals of our project (Section 3.1), an overview of the principles from constructivism learning theory that have driven our project (Section 3.2), and the selected target audience for the game (Section 3.4).

3.1. Goals

The primary goal of our project is *to create a learning environment that helps to increase players' awareness on cyber security attacks and the possible countermeasures that can be deployed to deter or mitigate them.* This includes:

- Conveying the breadth of vulnerabilities and attack methodologies that can be exploited by attackers.
- Improving the understanding of the diversity of possible countermeasures that can be considered to prevent, detect or mitigate cyber attacks.
- Letting players practice how to attack and exploit vulnerabilities and how to defend against those attacks.

- Reflecting and understanding upon the possible consequences of risk management decisions within a company.
- Being adaptable and modifiable to different training needs.
- Being simple to learn and not requiring any special equipment to be played.

To achieve these goals we will design a serious game based on fundamental principles from game design and constructivism learning theory to create a learning environment that is enjoyable and fun and promotes players' active learning.

3.2. Constructivism Learning Principles

To design our learning environment we followed the principles of constructivism, which has been the predominant learning theory used in education programs for young children, college and university students (Fosnot and Perry, 1996). The constructivist theory is based on the belief that learning occurs as learners are actively involved in a process of meaning and knowledge construction as opposed to passively receiving information (Rolloff, 2010). In a constructivist learning environment, learners work primarily in groups and learning and knowledge are interactive, and facts and knowledge change with experience (Bada and Olusegun, 2015). There is a great focus and emphasis on social and communication skills, as well as collaboration and exchange of ideas. This is contrary to the traditional learning environments where learners work primarily alone, learning is achieved through repetition, and the subjects are strictly adhered to and are guided by a textbook. In particular, the characteristics of a constructivist learning environment are as follows (Maor, 1999):

- *Simulated Authentic Learning (C1).* The environment should be designed to facilitate, simulate and recreate real-life complexities and occurrences.
- *Active Learning (C2).* The environment should give learners opportunities to be active in ways that will promote self-direction, creativity and critical analysis of problems requiring a solution.
- *Collaborative Learning (C3).* The environment should facilitate interaction and possibly collaboration among the learners because through interaction and collaboration they can learn from each other ideas.
- *Interactive Teaching (C4).* The role of the teacher is not to provide knowledge to the learners, but to prompt and facilitate discussion. The teacher can use different strategies such as encourage learners inquiry by asking thoughtful, open-ended questions and encouraging learners to ask questions of each other; seek elaboration of learners' initial responses; encourage learners to engage in dialogue, both with the teacher and with one another; and provide hints and corrective feedback on their responses/solutions to a problem.

The principled application of this theory to serious game, as well as the integration with cyber security methodology for threat and defence modelling, will permit achieving the set goals and overcome limitations of current games.

3.3. Why a card game?

Appropriately designed card games are recognised as one of the appropriate educational games for constructivist learning and they have been adopted as learning activity in different subjects such as Chemistry, Physics and Mathematics (Kordaki, 2015). In particular, games are considered an appropriate means to center the learner, making it possible to learn in a meaningful way, to emphasise problem solving, and to approach learning as an active process of understanding (Prensky, 2004). Games also provide learners with strong motivation to be actively engaged in their learning (Malone and Lepper, 2005). Therefore, we designed Riskio as a tabletop card game that satisfies the following principles from constructivist learning.

- *Simulated Authentic Learning (C1).* One of the key components of the Riskio game is the game board which represents a real-word scenario with different type of assets to be protected from a cyber attack (Stott and Neustaedter, 2013). The board sets the narrative of the game where the players can practice attack scenarios and defense strategies.
- *Active Learning (C2).* The game adopts role-playing to promote active learning of the players: the players impersonate both the role of the attacker and defender on the assets that are part of the scenario. This allows them to find a solution to the problem "how to attack" an asset and "how to prevent, deter or mitigate an attack to the asset".
- *Collaborative Learning (C3).* The card game creates a social environment where players build new knowledge on cyber security concepts through interaction with the other players and the game master (Stott and Neustaedter, 2013).
- *Interactive Teaching (C4).* We deemed that it was essential to have a game master in order to facilitate the construction of players' knowledge. The game master's role is to guide players by asking questions that will lead them to develop their attack and defend strategies. More importantly, the game master will provide immediate feedback on the correctness and effectiveness of the elicited strategies (Stott and Neustaedter, 2013).

3.4. Target Audience

As the primary goal of the game is to educate employees on the nature of the risks coming from cyber attacks and the best strategies to defend against them, we identified employees with no technical background as our *primary audience*. The *secondary audience* is represented by university students who are approaching the field of cyber security and need to practice the cyber security concepts learned in university courses.

4. Riskio: a Serious Cyber Security Game

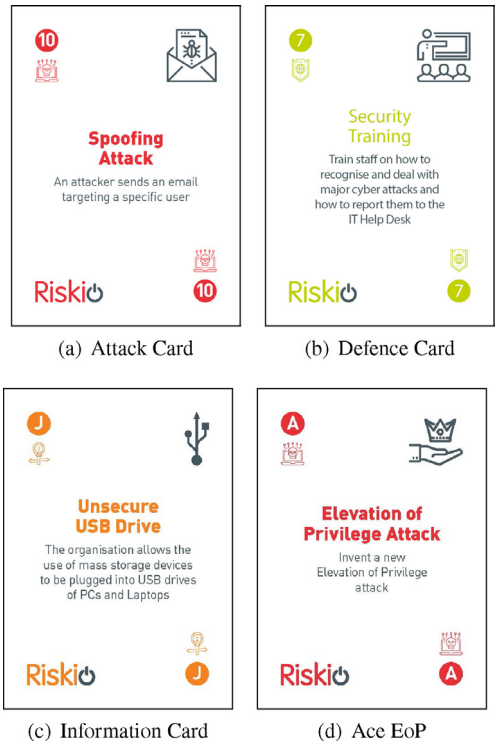
In this section, we first present the Riskio game components, and then the game mechanics and play. Further details about the game are available on the game's website Riskio.

4.1. Game Components

The key components of the game are the *card decks* and the *game boards*.

Card decks. The game has three card decks: *Attack*, *Defence*, and *Information*. The full list of cards is reported in Appendix A (see Figs. A.9–A.12). The card graphics have been chosen to make the game element clearly identifiable via differently coloured logos and texts: red for the attack, green for the defence and amber for the information cards. Fig. 1 reports examples of one card per deck and example of Ace card (see Fig. 1d) which allows players to make their own attack in the relevant STRIDE threat category or make up their own defence.

The attack deck has been designed to expose players to the most common threats and attack vectors identified in cyber security reports (e.g. by SANS and Symantec), security guidance (e.g. by NCSC or NIST), and security practices (e.g. by OWASP). The cards cover a wide range of attacks that allow them to be adapted to a variety of contexts and scenarios. Similarly to EoP, we divided the attack deck in 6 suits where each suit represents one of the Microsoft STRIDE threat categories. Each card contains a textual description of a threat exploiting a vulnerability which can either be



(a) Attack Card (b) Defence Card

(c) Information Card (d) Ace EoP

Fig. 1. Examples of Riskio Cards.

related to software artefacts, physical security policy or social engineering, and that can be used to initiate or carry out an attack. In particular, cards of each category are defined as follows:

- *Spoofing*: threats against authentication procedures that tend to maliciously impersonate users, but can also spoof websites or servers. The cards can be used to create attacks based on (spear-)phishing, credential stealing, password brute-forcing, man-in-the-middle attacks, and abuse of admin configuration.
- *Tampering*: threats against the integrity of data. The cards permit creating attacks that alter data at rest, e.g. by exploiting vulnerability in application front-ends, or in transit, e.g. due lack of message encryption.
- *Non-Repudiation*: threats to claim to have not performed an action. The cards allow the creation of attacks against logging functionality, auditing process and poor user authentication.
- *Information Disclosure*: threats against the confidentiality of information. The cards allow the creation of attacks exploiting poor encryption procedures for data at rest and in transit, flawed system configurations and non adequate user security policies.
- *Denial of Service*: threats against the availability of services to users. The cards allow the creation of attacks based on botnets, physical sabotage, system crash vulnerabilities, and social engineering.
- *Elevation of Privilege*: threats against the authorisation controls. The cards allow the creation of a variety of code execution attacks, as well as abuse of physical security controls and social engineering attacks as baiting.

The defence deck is formed by a suit of 13 cards representing the core security controls that can be directly applied in all enterprise IT settings. These controls were selected from UK Cyber Essentials scheme (National Cyber Security Centre, b) and the NCSC cyber protection programme "10 Steps to Cyber Security" (National Cyber Security Centre, a). The Cyber Essentials scheme consists of five technical security controls that organisations should deploy to defend against common cyber attacks: access control, software updates, firewall, antivirus and malware protection. The "10 Steps to Cyber Security" includes not only technical controls such as anti malware prevention and access control, but also organisational security controls such as risk management, user education and awareness and policies for home working and the use of removable media.

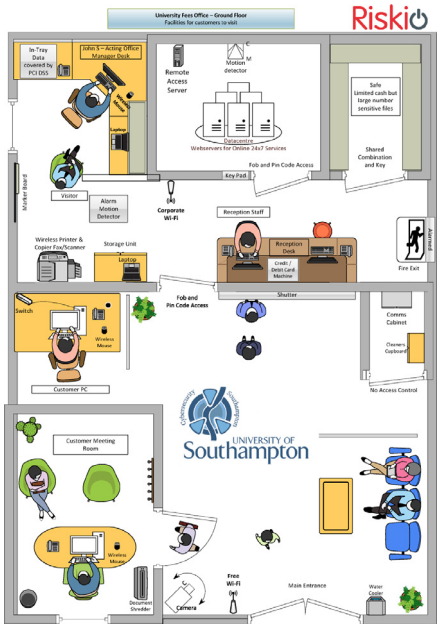


Fig. 2. Game Board: Office Diagram.

The information deck introduces dynamics and variation into the game. It consists of 13 cards representing exceptional or unexpected security-related events that can cause severe consequences to an enterprise and for which the players have to identify on the spot possible countermeasures. These cards were created based on the latest threat reports by SANS and Symantec analysing the technical and organisational practices that made cyber attacks possible.

Game board. When designing the board we have chosen a scenario that was accessible to a wide audience and could engage players with low computer literacy. The proposed game scenario is based on a fictional University Fees Office (see Fig. 2), which is responsible for processing fees and bursaries. The office is open normal business hours Monday to Friday but also has online services and apps for students, teaching staff and fees office staff to access students' records. Students and teaching staff who visit the office have free movement in the public area and have access to a PC in the corner with internet access. Access to the back-office area is strictly controlled by pin number and University issues ID card which acts as fob access to the door controlled security. However, the office manager John does have visitors from students, university staff and outside visitors at his discretion.

4.2. Game Mechanics and Play

The game mechanic is structured into both attack and defence phases. A typical game play would request players to sit around a table with the game board in the centre (see Fig. 3). The game master shuffles each attack suit and places them face down next to the game board and then gives each player a full Defence deck. The game master keeps the Information deck and can use it during the game. Each turn consists of the following phases:

Attack Phase. The game starts by the first player to the left of the game master acting as the attacker, and all the other players as the Defenders (see Fig. 3). The attacking player selects the top

Fig. 3. Game Preparation and Play: a game master (G) and, per turn, an attacker (A) and the rest defenders (D).

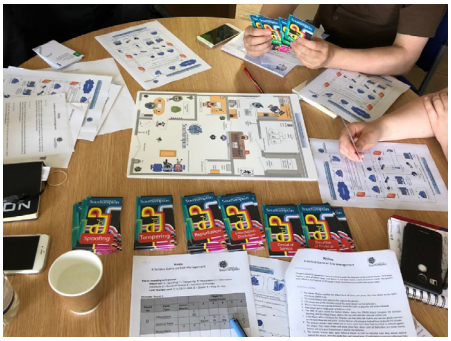


Fig. 4. Testing Riskio, playing with both Office & Network Diagrams with Case Study.

card from a chosen attack suits, then describes a concrete instance of the attack that can be performed against an asset on the game board. If the Ace card is selected, the attacker can create its own attack. The game master can help the attacker in formulating attack scenarios by asking thoughtful questions about the scenario. If the attack scenario formulated is not correct, the game master will provide an example of attack explaining by who and how the attack could be conducted.

Example 4.1. The Attacker (A) selects the top card from the Spoofing Attack Deck. The card is the 10 of Spoofing Attack - An attacker sends an email targeting a specific user. The Attacker proposes the following attack scenario: *"A cyber criminal gathers information from university website and used this to create emails to target John, the Office Manage"*. The Game master (G) then explains "this is a spear-phishing attack and the attacker could have sent an email to John pretending to be IT support service and asking John, to reset his credentials by clicking the link provided in the email. The email exploits urgency to try and get John to click on the malicious link in the email.The impact of the attack could be severe since John has access to sensitive information of students."

Defence Phase. The defence players then select one card from their Defence deck to defend against the formulated attack. They select the card and place it face down until all Defenders have selected a Defence Card (the game master will only give limited time to decide the defence). Each defence player in turn describes how the selected defence would be effective in deterring or preventing the attack. Then, the game master explains which among the played Defence cards was effective and why the others were not. Once the defence phase concludes, the game moves to the next round and the player to the left of the last attacker takes the role of the attacker.

Example 4.2. The Defenders have to select a countermeasure for the spear phishing attack proposed by the Attacker. Defender 1 selects the defence card 6 "Security Training", and motivates his choice as follows: *"Train staff on how to spot spoofed emails and implement a intranet based training solution for staff to test their skills"*. Defender 2 instead selects "Secure Configuration" card and states: *"Configure the Email server to verify the IP Address of the incoming email is from a trusted domain and put in spam folder when is not"*. Defender 3 chooses defence card "Access Control" explaining that "Two factor authentication should be used within the University to stop phishing attacks collecting staff's login and password", while Defender 4 selects the "Ace - Make up your own defence" and proposes the following defence: "Create an environment that encourages users to report phishing attempts". The Game Master, then, explains"spear phishing is a complex attack that requires a multi-layered set of mitigations including technological, process, and people-based security controls. Therefore, training on phishing, multi-factor authentication and having a process to report phishing emails should be used in combination to have an effective defence against spear phishing attacks. The defence proposed by Defender 2 - blocking phishing emails - may not be effective because often attackers spoof legitimate email addresses".

Scoring Phase (Optional). The game master can assign a score to the Attacker and the Defenders. An Attacker can win up to 3 points if the formulated attack contains the threat actor that can initiate the attack, a correct threat scenario and the impact with respect to confidentiality, integrity and availability for the organisation. The Defenders can score up to 3 points if the chosen defence strategy is valid and they can explain why it is the most effective solution. *Information Phase (Optional).* The Game master can introduce an additional layer of difficulty by selecting an information card representing an adversarial situation that all the players should address by selecting a defence card. This phase allows the game master to dynamically change the game scenario and steer the overall education goals. The games master can teach the players different defence strategies for example the use of technical solutions to prevent attacks and detect strategy in training staff to report suspicious activity.

Example 4.3. Games master selects the "Jack of Information - Unsecured USB Drive" and states *"A cyber criminals left a USB stick in the office and a staff member have plugged it into his office computer. Since the USB key was infected by a malware and the AutoRun feature is not disabled on the office computer, when the USBs is plugged in, the malware installs a keylogger to capture user names and passwords"*. All players now play the role of the Defender and select defence card as during the Defence phase stage. For example, Defender 1 selects the defence card "Security Policies" and motivates his choice as follows "When a USB key is plugged in, the USB key should be automatically scanned by antivirus and anti-malware sofware". Defender 2, instead, chooses the defence card "Security Training" and explains "this type of attack could be stopped by training staff members to report to IT Staff Help Desk USB keys found in the office". Then, the Game Master explains that "the use of removable media can expose the university office to risk of loss of information, malware infection and reputational damage. The most effective protection against those risks is to have a security policy that controls and limits the use of removable media within the office".

5. Game Evaluation

In this section we present the design (Section 5.1), realisation (Section 5.2) and result analysis (Section 5.3) of the empirical study carried out to evaluate the Riskio game.

5.1. Study Design

Prior to conduct the study, Riskio has been evaluated through several rounds during the design and the development phase. To conduct the play test and the study we obtained ethical approval from the University of Southamptonâs Ethics and Research Governance Online (ERGO) system (reference number ERGO/FPSE/44919). During the play tests, we tested both the ease of understanding of the attack and defences on the cards, the game board, and the mechanics of the game. We involved security experts, doctoral and postdoctoral students in computer science, and employees in organisations. The participants reported systematically that some of the attacks scenarios described on the cards were not clearly formulated and therefore we revised them to ensure that they were ease to understand for the players. We also played the game with different game boards, the university fees office (see Fig. 2) and the office network diagram (see Fig. 7). All the participants agreed that they preferred the university fees office diagram because it made easier to identify vulnerabilities and formulate attack scenarios. This may be explained by the fact that the university fees office board enables storytelling by allowing the players to invent their own attack scenarios and defence strategies using the characters and assets on the board. Therefore, during the study we played the game using the university fees office board. We also experimented a different game mechanic where the players first play the attack phase and then the next day they play the defence phase. This game mechanic was not appreciated by the players who found difficult and sometime confusing identifying threats without discussing about possible defensive strategies. The game masters also reported that it was very difficult to assign a score to the players' answers and provide feedback on the correctness and effectiveness of their answers. Since providing feedback is a key element of serious games design and constructivism learning theory, we decided to value feedback over scoring. Therefore, we did not perform scoring of players' answers during the study.

The design of the study was based on the Technology Acceptance Model (TAM) (Davis, 1989) which explains how users perceived a technology based on three constructs: 1) *perceived ease of use* (PEOU), the degree to which a person believes that using a particular technology is free of effort; 2) *perceived usefulness* (PU), personâs subjective probability that using a particular system would enhance his or her job performance; 3) *intention to use* (ITU), the extent to which a person intends to use a particular system.

The overall goal of the study was to assess the perception of the Riskio game in increasing cyber security awareness. This hypothesis has been formulated according to the TAM constructs as follows

- *PEOU*: The players find the Riskio game mechanics ease to understand.
- *PU*: The players find Riskio game useful in increasing awareness in cyber security concepts, with particular focus on threat identification and mitigation selection.
- *ITU*: The players intend to use the Riskio game to raise cyber security awareness in their organisation.

Each construct was assessed on both primary and secondary audience (resp., students and employees) in order to identify whether there is a difference of perception among them. To this end, we organised a series of experiments involving students and employees, who have limited or none knowledge in cyber security and have not previously played the game.

During each experiment, we first provided the participants with a short introduction to the Microsoft STRIDE threat taxonomy, to the University fees office scenario and to the rules of the game. Then, we divided them in groups of maximum 5 players, and let each group play the game for about 45 minutes under the guidance of a game master. At the end of the game we administered a demographic questionnaire and a post-task questionnaire to collect participants' perception of the game based on the TAM constructs. This latter questionnaire is reported in Table 1 and consists of 16 questions with answers on a 5-point Likert scale. The questionnaire was adapted from another questionnaire used to evaluate security risk assessment methodologies (Labunets et al., 2013; 2014). The players' answers to the questionnaires were anonymized using a random 4-digit number assigned to the players. The same number was used to link the answer of the participants in the demographic and post-task questionnaire. We have also organised an informal feedback session where participants were asked what they like or dislike about the game at the end of each experiment.

5.2. Study Realisation

The study consisted of four experiments. The first experiment took place in October 2018 at the premises of a company member of the Cyber Security Academy, a partnership between the University of Southampton and industry. This experiment involved 14 graduate students, newly hired by the company. The background of the participants were heterogeneous: they had BSc in Computer Science, Electrical Engineering, Mathematics, Physics and Game

Table 1
Post-task questionnaire.

Q1	I found playing the Riskio Game improved my knowledge of Cyber Security
Q2	I found the Riskio Game easy to learn
Q3	Overall, I think playing the Riskio Game provides an effective solution to the identification of cyber threats
Q4	If the game was adapted based on my organisation, I would use the Riskio Game to identify cyber threats
Q5	Playing the Riskio Game helped me find new threats that I could have not found without playing the game
Q6	Overall, I think playing the Riskio Game provides an effective solution to the identification of cyber defences
Q7	If the game was adapted based on my organisation, I would use the Riskio Game to identify cyber defences
Q8	Playing the Riskio Game helped me find new defences that I could have not found without playing the game
Q9	If I need to increase Cyber Security awareness in a future project at work, I would use the Riskio Game
Q10	Overall, I found playing Riskio Game to be useful
Q11	For the executives and senior managers in my organisation playing the Riskio Game would be a productive method for them to increase cyber awareness
Q12	Playing Riskio Game made me more productive in identification of cyber threats
Q13	Playing Riskio Game made me more productive in identification of cyber defences (counter measures)
Q14	I feel playing a security card game is a effective method to teach cyber security
Q15	I feel playing a security card game is a effective method to identify cyber security threats in my organisation
Q16	I feel playing a security card game is a effective method to identify cyber security defences in my organisation

Development. The participants were divided into three groups and three of the authors of this paper acted as game master. The experiment was a constituent part of the induction training on cyber security for all new employees.

The second experiment, instead, was performed in October 2018 during the Secure Software Development course taught at University of Southampton as part of the MSc in Cyber Security. It involved 15 students enrolled in the MSc in Cyber Security and Software Engineering. The participants were divided into three groups. One of the authors of the paper and two Ph.D. students in Cyber Security played the role of the game master.

The third experiment was organised in January 2019 as part of a professional training course on "Cyber security awareness" delivered to senior managers and executives working for the same company involved in the first experiment. The experiment involved 12 employees with different roles within the organisation: C-level, member of IT Team, Finance Team, Risk/Assurance Team, and practitioner area directors. The participants were divided into three groups. Two of the authors of this paper and one lecturer in Cyber Security played the role of the game master.

The last experiment took place in April 2019 as part of a professional training course for "Chief Data Officers" to allow an audience of 13 legal practitioners and lawyers to develop awareness on cyber security risks and defences. The participants where divided in three groups. Two of the authors of the paper and one Ph.D. student played the role of the game master.

5.3. Analysis of Study Results

We have analysed the post-task questionnaire's responses to assess participants' perception of the Riskio game in increasing awareness in cyber security and if there is a difference in the perception of students and employees. The key outcomes have been motivated based on the feedback provided by the participants to the study.

For the analysis, we have realigned the responses to 5 (which indicates the highest participant's perception). We employ an unpaired t-test to test for statistical significant differences (α set to 0.05) between students and employees' responses. The results are summarised in Table 2. For each question, it is reported the perception variable of the question it refers to (either PEOU, PU or ITU), the mean of the responses by students, by employees and then by all participants, and the resulting p-value; statistically significant responses are outlined in bold. The average responses for each perception variable and for the overall perception are reported at the bottom of the table.

Table 2
t-test of questionnaire'responses (in bold statistically significant questions).

Q	Type	Target Audience			
		Mean			
		Students (n=29)	Employees (n=25)	All (n=54)	p-value
1	**PU**	**3.4**	**4.3**	3.8	**0.001467**
2	PEOU	4.2	4.4	4.3	0.534474
3	**PU**	**3.7**	**4.3**	4.0	**0.012836**
4	ITU	4.0	4.4	4.2	0.57087
5	**PU**	**3.2**	**4.0**	3.6	**0.008803**
6	**PU**	**3.5**	**4.3**	3.9	**0.001561**
7	**ITU**	**3.6**	**4.2**	3.9	**0.013255**
8	**PU**	**3.0**	**4.0**	3.5	**0.00184**
9	ITU	3.8	4.2	4.0	0.235433
10	**PU**	**4.0**	**4.6**	4.2	**0.023232**
11	**PU**	**3.7**	**4.4**	4.0	**0.009693**
12	**PU**	**3.3**	**4.1**	3.7	**0.006241**
13	**PU**	**3.1**	**4.1**	3.6	**0.002555**
14	PU	3.9	4.3	4.1	0.126731
15	ITU	3.6	4.0	3.7	0.223866
16	**ITU**	**3.6**	**4.1**	3.8	**0.030104**
PU		**3.4**	**4.3**	3.8	**2.367073e-18**
ITU		**3.8**	**4.3**	4.0	**0.001728**
PEOU		4.2	4.4	4.3	0.534474
Total		**3.6**	**4.3**	3.9	**3.796929e-18**

In the following, we report the analysis of the results, together with the outcomes of the analysis of the feedback which can explain the difference in perception between employees and students.

Overall Perception. The results show that the overall perceived efficacy of the Riskio game in increasing awareness in cyber security is higher for employees than for students with statistical significance (see Fig. 5a). Specifically, it emerged that for the students the fun element was missing: some complained that they did not feel like they were playing the game but more like: "*We were attending a lecture*". They also mention that "*We were expecting to use the board but we did not really use it during the game play like in other games such as monopoly*". In contrast, employees reported that "*We like the game as it was played*".

Perceived ease of use Both employees and students have high confidence that the Riskio game mechanics and rules are ease to understand (see Fig. 5b). However, this result is not statically significant and we cannot draw any conclusion on the perceived ease of use of the game.

Perceived usefulness. The perceived usefulness of the Riskio game in increasing awareness in cyber security is higher for employees than for students with statistical significance (see Fig. 5c). In particular, employees are more confident that the Riskio game is an effective solution to the identification of cyber threats and more helpful in finding defences than students. Instead, students experienced difficulties in identifying threats to the assets represented on the game board as they suggest "*It may be added to the board the categories of threats that apply to the different assets*.

Intention to Use. The intention to use the Riskio game to identify cyber defences in their organisation is higher for employees than for students (see Fig. 5d). Employees expressed higher intention to use the Riskio game to identify cyber defences in their organisations. This can be due to the fact they reported '*We like the office diagram because we can relate this to our work environment*".

5.4. Threats to Validity

We discuss here the main threats to the validity of our study: construct, internal and external validity (Wohlin et al., 2012). *Internal validity* Internal validity is concerned with issues that may falsely indicate a causal relationship between the treatment and the outcome, although there is none. One of the main threats to internal validity is the use of authors of this paper as game master. The participants who played the game with the authors of this paper might have felt obliged to rate more highly the perception's of the game. We mitigated this threat by making clear at the beginning of the study that the participants' responses would have been anonymous. Another aspect that it might have biased the results is the level of expertise of the game master. For example, the participants who played the game with Ph.D. students as game master might have had a lower perception of the game than the other participants. To mitigate this threat, we trained the Ph.D. students to be a game master by playing the game with them several times.

Construct Validity Construct validity concerns generalising the result of the experiment to the concept and theory behind the experiment. The main threat to construct validity in our study is the design of the post-task questionnaire. The questionnaire

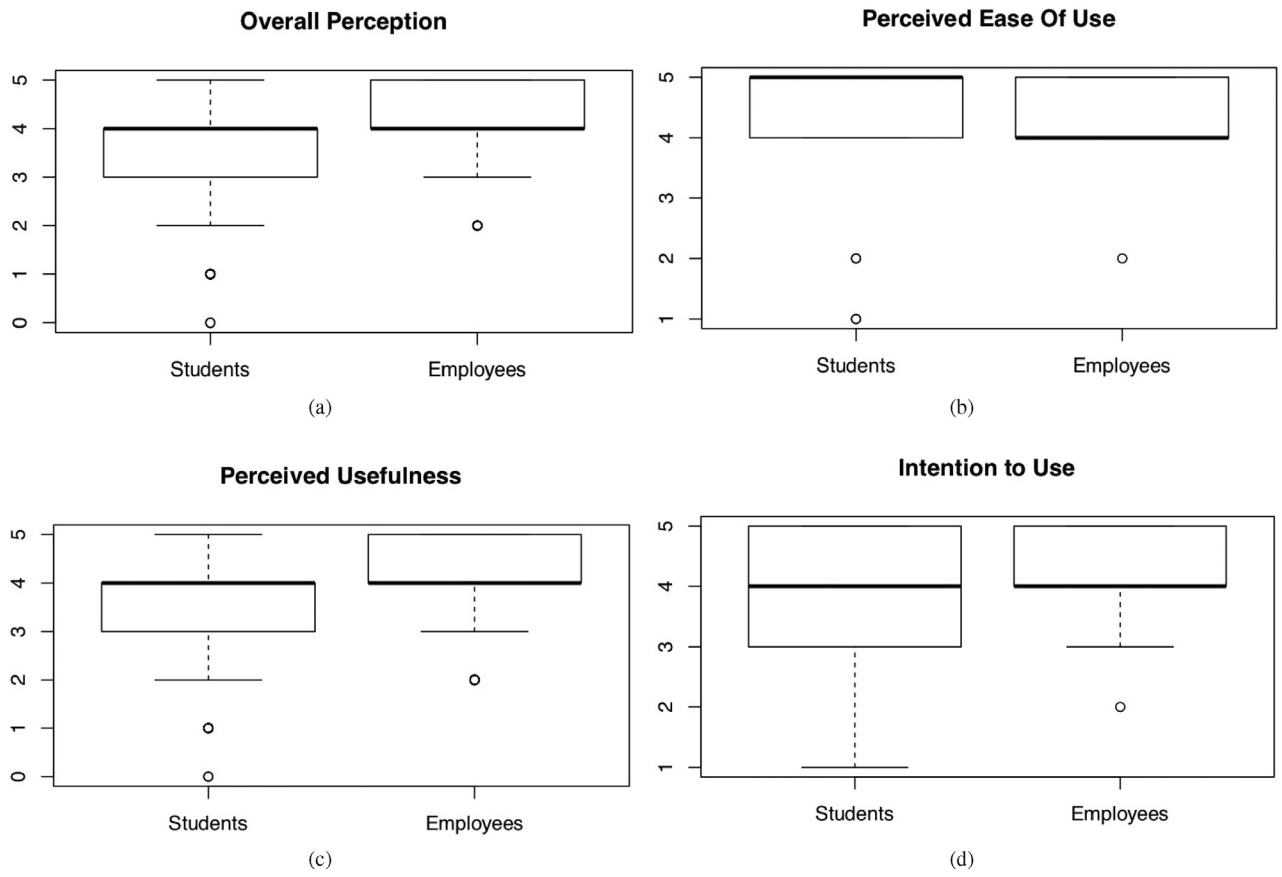


Fig. 5. Study Results for the Students (n=29) and Employees (n=25) groups.

was designed following the Technology Acceptance Model and adapted from a questionnaire used to conduct other experiments (Labunets et al., 2013; 2014). The questionnaire contains multiple questions for perceived usefulness and intention to use but only one question for perceived ease of use. Therefore, we are reasonably confident that the questionnaire measures perceived usefulness and intention to use, while for perceived ease of use conclusions cannot be drawn. *External Validity* External validity concerns the ability to generalise experiment results beyond the experiment settings. External validity is thus affected by the objects and the subjects chosen to conduct our. A possible threat could have been to select the wrong people to participate to our experiments. However, this was not the case because we have selected participants matching our target audience from the game. Another threat could have been playing the game using a toy scenario. We mitigated this threat by using the university fees office board that create opportunities to think about realistic attack scenarios and defensive strategies.

6. Discussion and Reflections

Riskio builds on the learning principles of constructivism to match the goal of raising cyber security awareness via engaging and group-playing activities. The numerous available games (see Section 2) prove the benefits of using (tabletop) games for cyber security education. As the landscape of cyber security threats keep changing over time, the main challenge for the game design was to create game contents i.e., the cards and the board that can be easily adapted to different audience (either operative, administrative or technical) and play scenarios (either real-world business scenario or technical drawings). To this aim, we identified the following trade-offs that can be also pursued for the designing of other serious security game.

Game cards. When we designed the attack card decks we carefully formulated the attack scenarios so they could be easily understood and accessible to non-technical players. To this aim, we have formulated card contents so that they not name an attack but they describe how the attack is conducted: for example, "*An attacker sends email targeting a specific user*" allows players to elicit attacks including, e.g. "Spear Phishing" or "Whaling" techniques, and is widely understood by all types of audience.

Although our card design does not lead to a unique set of correct attacks for each card, our experience with the game has confirmed that players are eager to show their knowledge: if the player currently acting as the attacker does not mention a potential attacking technique based the threat on the card, defenders most likely will mention them. Additionally, as the difficulty of the threats increases according to the card number in the suits, the game can easily support incremental learning strategies and adaptability to different audience.

Game boards. The design of the game board is fundamental to allow players to experiment a variety of attacking and defending scenarios. As the designed cards encompass both software, physical and social engineering techniques, we realised that a board representing a cyber physical game-play was the most fitting choice. The University fees office board (Fig. 2) was positively rated by the players, both for the ease of identifying attack scenarios and for the ability to create multiple plot lines (e.g. exploiting admin personnel, vulnerable online service, or lack of physical security). The board also increased the players engagement by adding a fictional story (Chothia et al., 2017) where players can make their

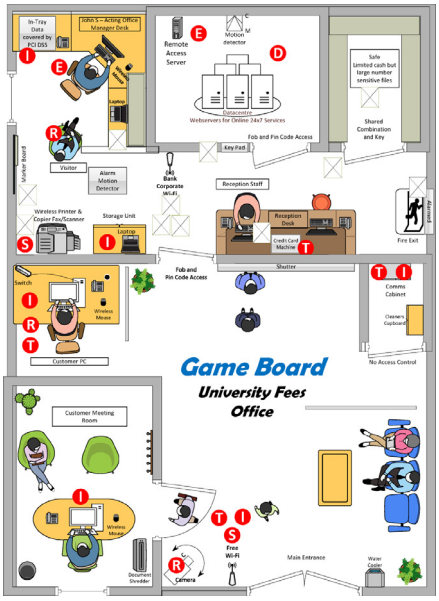


Fig. 6. Office Diagram with Microsoft STRIDE annotations.

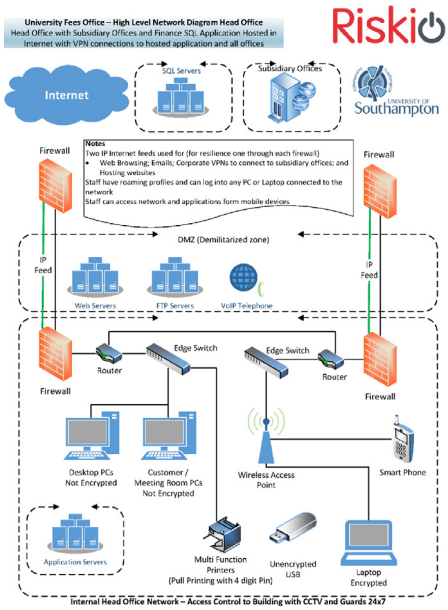


Fig. 7. Office Network Diagram.

own choices of attack and defence, and can simulate real forms of learning as in wargaming (Haggman, 2019).

However, based on the feedback provided during experiments, we realised that some modifications to the board might be necessary according to the audience. For example, to facilitate audience with no experience in threat identification, students suggested that the assets on the board can be annotated with the applicable STRIDE threat categories (see Fig. 6). Students also suggested to add more game like elements such as the use of dice to select the asset to attack or the threats category. We are currently working on designing a new game board inspired to Monopoly game where players throw a dice and move around the board with random selection of the STRIDE category (see Fig. 8). On the contrary, employees with operational roles suggested that a network diagram of the scenario, e.g. reported on the back of the board, would help them identify low-level threats (see Fig. 7).

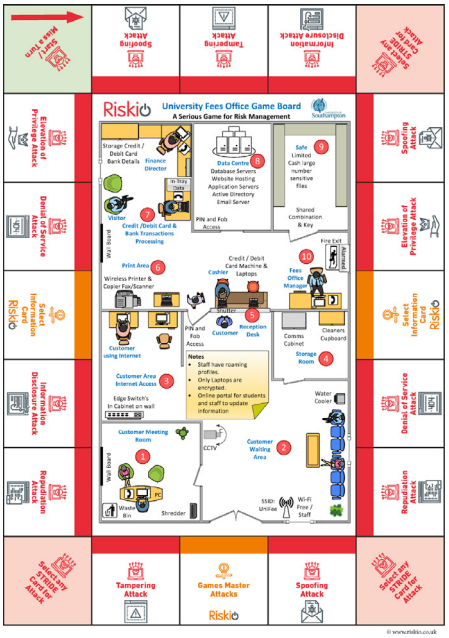


Fig. 8. Alternative Game Board.

Card Graphic Design and Illustration. The graphic design, illustration, and size and quality of paper used to print the cards significantly affect the initial reception of the game by the players. After we hired a professional designer for the cards, players constantly repeated to us that they felt like playing a real card game.

Game Mechanics Trade-offs. To match our goal to allow players to experiment with both attacking and defending phases, we evaluated the following options:

1. to split the play into two stages, first all players in attacking stage then in defending;
2. to split players into two groups, one group attacking the other defending, then switch over;
3. to change attacking player ever turn, leaving all the others acting as single defenders.

The first option led the game play to boil down to two completely secluded sessions, attacking and defending. Defences were barely linked back to the played attacks and players were confused by the overall game fiction. Although the second option facilitated direct links between attacks and defences, many players tended to support players from different attacking or defending groups making the group discussion convoluted. As described in Section 4, our final choice was the third option. This design was proved to be more engaging for the players as they interchangeably play different roles, challenging different players over time. Furthermore, as defenders can play different cards, the feedback process of the game master can cover a wider spectrum of techniques and spawn discussion among players on the effectiveness of different defences.

Game Master. The game master has a focal role in stimulating active learning, as well as fun and entertainment, for the players. The game master should encourage critical thinking and provide feedback on the correctness of the attack and defence strategy, two essential elements of active learning. However, we realised from the experiments that the game master should be “fading in the background” when the players become more knowledgeable, thus avoiding that the players could perceive the game play as a lecture.

Scoring. From the experiments, we realised that players were not interested in the scoring phase of the game. This could be explained by the fact that players can already assess their responses based on the game master feedback and the discussion with the other players. Moreover, scoring can have a negative effect on the player's learning: player can become fixated with scoring points and lose sight of the lessons of the game.

Risk Management Process. The real-life complexity of security decision making encompasses, among others, risk prioritisation and security expenditure. As a matter of fact, budget limitations lead to trade-off in choosing both the highest risks to mitigate and the appropriate defences and countermeasures. These decisions are frequently taken by C-level people who may not fully comprehend security risks: the Riskio game could be used to recreate and educate security decision making processes. It is however advocated to not overload players with complex risk prioritisation methodology which would complicate the game mechanisms and the player experience. To this aim, we will evaluate the introduction of a new game phase during which the game master prioritises the threats identified by the players, and then let the players identify defences within a given budget. Differently from other games (Frey et al., 2019; Williams et al., 2010), we think that players should focus more on understanding the role of threat countermeasures, rather than risk prioritisation for which each organisation may follow different approaches.

7. Conclusions and Future Research

In this paper we proposed Riskio, a card game to increase cyber security awareness for people working in organisations. Riskio addresses three of the main limitations exhibited by existing games for cyber security awareness: 1) they do not convey to the players the breadth of cyber attacks and possible defences to deter them; 2) they do not allow players to practice both offensive and defensive skills, and 3) they are not easily adaptable or modifiable.

Riskio creates an active learning environment where players learn about different attacks and countermeasures by playing both the role of the attacker and the defender of critical assets in a fictitious organisation. A game master prompts and facilitates discussion among the players and asks questions that will lead them to develop their own attack and defence strategies. The game master also provides immediate feedback on the correctness and effectiveness of the chosen attack and defence strategies.

The evaluation of the game has shown that employees have higher confidence than students that Riskio can increase their awareness on cyber security concepts. This difference could be explained by the fact that employees enjoyed the game rules and mechanics and they could relate the game board scenario to their own organisation. In contrast, students missed the fun element in playing the game and perceived the game as a lecture taught by the game master. They also experienced difficulty in identifying threat scenarios and they suggested that the game board should be changed to facilitate the identification.

These results highlighted important aspects to be taken into account when designing a game for cyber security awareness and education. The game board is an essential component to represent the complexity of realistic scenarios, but it may need to contain different information to facilitate the playing according to the audience. The game master is also required to timely provide feedback to help players critically think on their attack and defence strategies. However, the game master must not transform the game play into a lecture, but should only facilitate and drive the discussion among the players.

We are planning to continue our research on serious games for cyber security in several directions.

Framework for Serious Games Design. We would like to develop a framework that could support the design and the evaluation of serious games to educate people on cyber security concepts that reconciles pedagogic and serious games design principles. We will start the design of the framework by looking at the Learning Mechanics and Game Mechanics (LM-GM) framework (Arnab et al., 2015) and by applying it to analyse how gameplay and pedagogy intertwine in the Riskio game.

Longitudinal Study on Riskio Effectiveness. We will investigate the effectiveness of the Riskio game in a longitudinal study. The effectiveness will be assessed in terms of participants' knowledge acquisition and retention. Knowledge acquisition is the ability to process and extract knowledge from education materials and it is usually evaluated by asking people to apply knowledge just after training (Mandl and Levin, 1989). Knowledge retention, instead, is the ability to recall knowledge after some time has passed from the training (Rubin, 1996). The study will be organised as part of one of the cyber security courses at the University of Southampton and it will have the duration of a whole semester. The students will be asked to work in group of five and they will be asked to identify threats and security controls of a realistic case study. Each group will be randomly assigned to two experimental groups: the one who play the Riskio game to elicit threats and security controls for the case study (Riskio group) and the one that simply discuss the case study among themselves without playing the card game (Control Group). The participants in the Control group will receive training material on common threats from NCSC threat reports and security controls from the Cyber Essentials scheme and the NCSC's 10 Steps to Cyber Security. The number of threats and security controls identified by the groups of participants will be used to measure the knowledge acquisition. The correctness of threats and security controls will be evaluated by at least three different security experts. One month after playing the game or discussing the topic, all students will be administered a quiz about the threats and security controls identified for the case study to assess their knowledge retention.

Support for Non-Expert Game Masters. In order to be able to play the game with game masters who are not expert in cyber security, we are preparing a cheat sheet that includes the following information: a) the rules to play the game, b) a description of the assets in the University Fee Office scenario c) for each asset, a list of the attack cards that represent attacks that could target the asset and an instance of the attack, d) for each attack instance a list of possible defense cards that could be played to mitigate the risk associated with the scenario.

Riskio in Cyber Security Education. Riskio can support a variety of educational and training activities in academic and industry settings. For example, Riskio could be played in a Software Security course to help students in identifying threats for a software system and security controls to be deployed or in a Foundations of Cyber Security course to conceptualise threat scenario or perform security risk assessment. In an industrial context, it could also be played as part of the security training of a company to help employees understand the risks that their company is exposed to. To conduct these activities, the educators will need to print the card decks and eventually personalise the game board to fit their training needs. To support educators, we will propose a set of educational activities including learning outcomes, set up of the game, and a description of the activities. The activities will be made available on the Riskio web site.

Declaration of Competing Interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A. Card Decks

Fig. A1. Riskio Defence Cards.

Fig. A2. Riskio Information Cards.

Fig. A3. Riskio Attack Cards Sample 1.

Fig. A4. Riskio Attack Cards Sample 2.

CRediT authorship contribution statement

Stephen Hart: Conceptualization, Validation, Writing - original draft. **Andrea Margheri:** Conceptualization, Validation, Writing - original draft. **Federica Paci:** Supervision, Conceptualization, Validation, Writing - review & editing. **Vladimiro Sassone:** Supervision.

References

Aladawy, D., Beckers, K., Pape, S., 2018. PERSUADED: fighting social engineering attacks with a serious game. In: 15th International Conference in Trust, Privacy and Security in Digital Business. Springer, pp. 103–118.

Arnab, S., Lim, T., Carvalho, M.B., Bellotti, F., De Freitas, S., Louchart, S., Suttie, N., Berta, R., De Gloria, A., 2015. Mapping learning and game mechanics for serious games analysis. British Journal of Educational Technology 46 (2), 391–411.

Bada, S.O., Olusegun, S., 2015. Constructivism learning theory: A paradigm for teaching and learning. Journal of Research & Method in Education 5 (6), 66–70.

Beckers, K., Pape, S., 2016. A serious game for eliciting social engineering security requirements. In: 24th International Conference in Requirements Engineering. IEEE, pp. 16–25.

Chothia, T., Holdcroft, S., Radu, A.-I., Thomas, R.J., 2017. Jail, hero or drug lord? turning a cyber security course into an 11 week choose your own adventure story. 2017 {USENIX} Workshop on Advances in Security Education ({ASE} 17).

Davis, F.D., 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly 319–340.

Denning, T., Lerner, A., Shostack, A., Kohno, T., 2013. Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education. In: Conference on Computer & Communications Security. ACM, pp. 915–928.

Fosnot, C.T., Perry, R.S., 1996. Constuctivism: A psychological theory of learning. In: Constructivism: Theory, Perspectives. and Practice. Teachers College Pres, pp. 9–38.

Frey, S., Rashid, A., Anthonysamy, P., Pinto-Albuquerque, M., Naqvi, S.A., 2017. The good, the bad and the ugly: A study of security decisions in a cyber-physical systems game. IEEE Transactions on Software Engineering.

Frey, S., Rashid, A., Anthonysamy, P., Pinto-Albuquerque, M., Naqvi, S.A., 2019. The good, the bad and the ugly: A study of security decisions in a cyber-physical systems game. IEEE Trans. Software Eng. 45 (5), 521–536.

Gondree, M., Peterson, Z.N., 2013. Valuing security by getting [d0x3d!]: Experiences with a network security board game. Presented as part of the 6th Workshop on Cyber Security Experimentation and Test.

Graffer, I., Bartnes, M., Bernsmed, K., 2015. Play2prepare: A board game supporting it security preparedness exercises for industrial control organizations.

Haggman, A., 2019. Cyber wargaming: Finding, designing, and playing wargames for cyber security education.

International Electrotechnical Commission,. IEC 62443 Security for industrial automation and control systems. https://webstore.iec.ch/publication/33615.

International Organization for Standardization,. ISO/IEC 27001 Information Security Management. https://www.iso.org/isoiec-27001-information-security.html.

Irvine, C.E., Thompson, M.F., Allen, K., 2005. Cyberciege: Gaming for information assurance. IEEE Security & Privacy 3 (3), 61–64.

Kordaki, M., 2015. A constructivist, modeling methodology for the design of educational card games. Procedia-Social and Behavioral Sciences 191, 26–30.

Labunets, K., Massacci, F., Paci, F., Tran, L.M.S., 2013. An experimental comparison of two risk-based security methods. In: 2013 ACM / IEEE International Symposium on Empirical Software Engineering and Measurement, Baltimore, Maryland, USA, October 10-11, 2013, pp. 163–172.

Labunets, K., Paci, F., Massacci, F., Ruprai, R.S., 2014. An experiment on comparing textual vs. visual industrial methods for security risk assessment. In: 4th IEEE International Workshop on Empirical Requirements Engineering, EmpiRE 2014, Karlskrona, Sweden, August 25, 2014, pp. 28–35.

Malone, T., Lepper, M., 2005. Making learning fun: A taxonomy of intrinsic motivations for learning. Making Learning Fun: A Taxonomy of Intrinsic Motivations for Learning 3.

Mandl, H., Levin, J., 1989. Knowledge acquisition from text and pictures. SERBIULA (sistema Librum 2.0).

Maor, D., 1999. Teachers-as-learners: The role of a multimedia professional development program in changing classroom practice.. Australian Science Teachers' Journal 45.

Microsoft,. Elevation of Privilege (EoP) Card Game. https://www.microsoft.com/en-us/SDL/adopt/eop.aspx.

Moløkken-Østvold, K., Haugen, N.C., Benestad, H.C., 2008. Using planning poker for combining expert estimates in software projects. Journal of Systems and Software 81 (12), 2106–2117.

National Cyber Security Centre, a. 10 step to cyber security: Guidance on how organisations can protect themselves in cyberspace.

National Cyber Security Centre, b. Cyber essentials - protect your organisation against cyber attack.

National Institute of Standards and Technologies,. Cyber security framework. https://www.nist.gov/cyberframework.

OWASP,. Cornucopia. https://www.owasp.org/index.php/OWASP_Cornucopia.

Potter, B., 2009. Microsoft SDL threat modelling tool. Network Security (1) 15–18.

Prensky, M., 2004. Digital Game-Based Learning. McGraw-Hill Pub. Co..

Report, S. I. S. T.,. Internet security report. https://www.symantec.com/security-center/threat-report.

Riskio,. A serious game for risk management. https://www.riskio.co.uk.

Rolloff, M., 2010. A constructivist model for teaching evidence-based practice. Nursing Education Perspectives 31 (5), 290–293.

Rubin David, C., W.A.E., 1996. One hundred years of forgetting: A quantitative description of retention.. Psychological Review 734–760.

Shostack, A., 2014. Elevation of Privilege: Drawing Developers into Threat Modeling. Summit on Gaming, Games, and Gamification in Security Education. USENIX Association.

Stott, A., Neustaedter, C., 2013. Analysis of gamification in education. Surrey, BC, Canada 8, 36.

Tamara Denning, B. F., Kohno, T.,. The security cards. http://securitycards.cs.washington.edu/.

ThinkFun,. Hacker: Cybersecurity logic game. https://www.thinkfun.com/learn-coding/hacker/.

Thompson, M., Irvine, C., 2011. Active learning with the cyberciege video game. In: Proceedings of the 4th Conference on Cyber Security Experimentation and Test. USENIX Association. 10–10.

Trickel, E., Disperati, F., Gustafson, E., Kalantari, F., Mabey, M., Tiwari, N., Safaei, Y., Doupé, A., Vigna, G., 2017. Shell we play a game? ctf-as-a-service for security education. 2017 USENIX Workshop on Advances in Security Education (ASE 17). USENIX Association, Vancouver, BC.

Williams, L., Meneely, A., Shipley, G., 2010. Protection poker: The new software security "game";. IEEE Security & Privacy 8 (3), 14–20.

Wohlin, C., Runeson, P., Hst, M., Ohlsson, M.C., Regnell, B., Wessln, A., 2012. Experimentation in Software Engineering. Springer Publishing Company, Incorporated.

Yasin, A., Liu, L., Li, T., Fatima, R., Wang, J., 2019. Improving software security awareness using a serious game. IET Software 13 (2), 159–169.

Stephen Hart is s Ph.D. student in the Cyber Security group of the School of Electronics and Computer Science at the University of Southampton. His Ph.D. focuses on the role of gamification in cyber security education and privacy management in organisations.

Andrea Margheri is a Lecturer in the School of Electronics and Computer Science at the University of Southampton. His research interests are in the area of cyber security of distributed computing systems and data management services.

Federica Paci is an Associate professor at the Computer Science Department of the University of Verona in Italy. Before she was a lecturer in Cyber Security in the School of Electronics and Computer Science at the University of Southampton. She published more than 60 papers in top conferences and journals in Cyber Security field. Her recent research interest include privacy for IoT applications, secure personal data sharing and gamification in Cyber Security.

Vladimiro Sassone has worked at the University of Southampton since 2006, where he is a Professor in Cyber Security, the Roke/Royal Academy of Engineering Research Chair in Cyber Security, the Head of the Cyber Security Group, the Director of the GCHQ/EPSRC Academic Centre of Excellence for Cyber Security Research (ACE-CSR), the Director of the Cyber Security Academy (CSA), His recent research include resource access control over untrusted networks, trust management systems, predictive trust-and-reputation models, anonymity and privacy in the presence of trust and attackers belief systems.